



November 2016

DEFENSE INTELLIGENCE

Additional Steps Could Better Integrate Intelligence Input into DOD's Acquisition of Major Weapon Systems

Accessible Version

GAO Highlights

Highlights of [GAO-17-10](#), a report to congressional committees

Why GAO Did This Study

DOD has reported that it expects to invest \$1.6 trillion on acquiring 80 major defense acquisition programs, many of which depend on intelligence input both during the acquisition process and to effectively perform missions once deployed. The complexity of advanced weapon systems, such as the F-35, is creating increasing demand for intelligence mission data—such as radar signatures—for sensors and processes supporting warfighters.

The National Defense Authorization Act for Fiscal Year 2016 includes a provision that GAO review intelligence integration into DOD acquisitions. This report evaluates, for major defense acquisition programs, the extent to which DOD has (1) processes and procedures for certifying and training personnel providing intelligence input into acquisition programs; (2) efforts to improve processes and procedures for integrating intelligence into its acquisitions; and (3) efforts to develop tools to integrate intelligence into its acquisitions. GAO compared certification and training to relevant guidance; reviewed relevant documents to identify intelligence inputs and the provision of intelligence input into acquisition programs; and interviewed cognizant officials.

What GAO Recommends

GAO recommends DOD create certifications and training for intelligence support personnel, require that intelligence mission data be prioritized, develop a communication plan for a threat information tool, and determine the need to develop another tool. DOD concurred with GAO's recommendations.

View [GAO-17-10](#). For more information, contact Joseph W. Kirschbaum at (202) 512-9971, kirschbaumj@gao.gov.

November 2016

DEFENSE INTELLIGENCE

Additional Steps Could Better Integrate Intelligence Input into DOD's Acquisition of Major Weapon Systems

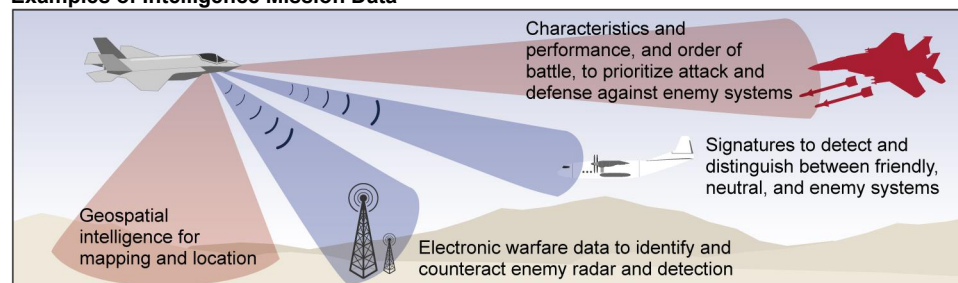
What GAO Found

The Department of Defense (DOD) has developed certifications and training for acquisition and intelligence personnel, but it does not have certifications for certain personnel who provide intelligence support to acquisition programs. These personnel help integrate threat information on foreign capabilities and intelligence mission data—technical intelligence such as radar signatures and geospatial mapping data—into acquisition programs. DOD uses certifications to determine that an employee has necessary education, training, and experience. The lack of certifications for personnel providing intelligence support to acquisition programs has led to the services developing varying levels of training: the Air Force certifies and requires training specific to providing intelligence support, the Army offers training that is not required, and the Navy has no formal training. Without certifications for personnel providing intelligence support to acquisition programs, DOD does not have assurance that these personnel are prepared to carry out their duties.

DOD has multiple efforts underway to improve processes and procedures for integrating intelligence into its acquisitions but does not require prioritization of intelligence mission data, which would identify those data most needed for a weapon system to perform its mission. A task force DOD created in 2015 to better integrate intelligence into acquisition programs identified the need for prioritization and proposed processes and procedures for doing so. Without department-wide requirements to prioritize intelligence mission data, new processes and procedures such as those developed by the task force may not be fully implemented and weapon systems could be deployed without the intelligence mission data they need to perform their missions.

DOD is developing two tools for integrating intelligence into major defense acquisition programs. One tool to share threat information lacks a communication plan to obtain feedback from users to better ensure its effectiveness. Without user feedback, DOD may not receive useful information to develop the tool. The other tool is for acquisition programs to communicate their intelligence needs to the intelligence community, though the services did not identify a need for the tool and there is no mechanism to fund its implementation and operation. Without assessing the need for such a tool or plans or funding for implementation and operation, DOD may be using funds unnecessarily to develop an unneeded tool.

Examples of Intelligence Mission Data



Source: GAO analysis of Department of Defense information. | GAO-17-10

United States Government Accountability Office

Contents

Letter	1	
	Background	5
	DOD Has Processes and Procedures for Certifying Both Intelligence and Acquisition Personnel but Not for Personnel Providing Intelligence Support to Acquisition Programs, and Services' Training Varies	11
	DOD Has Multiple Efforts Underway to Improve Processes and Procedures for Integrating Intelligence into Major Defense Acquisition Programs but Faces Challenges Prioritizing Intelligence Mission Data Needs	17
	DOD Is Developing New Tools for Integrating Intelligence into Acquisition Programs but Faces Challenges in Development and Implementation	25
	Conclusions	31
	Recommendations for Executive Action	32
	Agency Comments and Our Evaluation	33
Appendix I: Information on DOD's Efforts to Assess the Intelligence-Gathering Capability of Weapon Systems beyond the Scope of Their Mission		36
Appendix II: Objectives, Scope, and Methodology		37
Appendix III: Intelligence Inputs in the Defense Acquisition Process		43
Appendix IV: Comments from the Department of Defense		51
Appendix V: GAO Contact and Staff Acknowledgments		54
	GAO Contact	54
	Staff Acknowledgments	54
Appendix VI: Accessible Data	55	
	Agency Comment Letter	55
Tables		
	Table 1: Personnel Who Provide Intelligence Support to Acquisition Programs	9
	Table 2: Intelligence-related Tasks Identified by the Under Secretary of Defense for Acquisition, Technology, and Logistics in the Better Buying Power 3.0 Initiative	18

Table 3: Intelligence Inputs in the Defense Acquisition Process	44
---	----

Figures

Figure 1: Intelligence Input in the Defense Acquisition System	6
Figure 2: Examples of Intelligence Mission Data	8

Abbreviations

DIA	Defense Intelligence Agency
DOD	Department of Defense
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



November 1, 2016

Congressional Committees

Congress and the Department of Defense (DOD) have long sought to improve the acquisition of major weapon systems, an area that we first placed on our High Risk List in 1990.¹ DOD reported in March 2016 that it expects to invest \$1.6 trillion on the development or procurement of its portfolio of 80 major defense acquisition programs, many of which depend on intelligence input both during the acquisition process and subsequently, to effectively perform their missions once deployed.² The intelligence community provides this information not only when systems are deployed in support of the warfighter, but also as the platforms are developed and procured as a defense acquisition program.³ This latter role of the intelligence community, known as intelligence support to acquisition, has become increasingly important as weapon systems have become more advanced and dependent on processing data from on-board sensors to perform their mission.

¹GAO, *High-Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: Feb. 11, 2015).

²Department of Defense (DOD), *Department of Defense Selected Acquisition Reports*, NR-106-16 (Washington, D.C.: March 31, 2016).

³The U.S. Intelligence Community comprises 17 components. The Office of the Director of National Intelligence oversees the intelligence community, and is counted as one of the 17 components. The other 16 components are as follows: the National Security Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, Defense Intelligence Agency, Army Intelligence, Navy Intelligence, Marine Corps Intelligence, Air Force Intelligence (Air Force Intelligence, Surveillance, and Reconnaissance), Central Intelligence Agency, Department of Homeland Security (Office of Intelligence and Analysis), Department of State (Bureau of Intelligence and Research), Department of Treasury (Office of Intelligence and Analysis), Federal Bureau of Investigation (National Security Branch), Drug Enforcement Administration (Office of National Security Intelligence), U.S. Coast Guard (Intelligence and Criminal Investigations), and Department of Energy (Office of Intelligence and Counterintelligence). For the purposes of this report we use "intelligence community" to refer to the organizational elements of the Defense Intelligence Enterprise, which include the National Security Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, Defense Intelligence Agency, Army Intelligence, Navy Intelligence, Marine Corps Intelligence, and Air Force Intelligence (Air Force Intelligence, Surveillance, and Reconnaissance), among others.

The intelligence community provides support to acquisition programs in two broad categories: threat intelligence on foreign capabilities, and intelligence mission data. Threat intelligence identifies the capability and strategy of an adversary's system that could defeat or reduce the effectiveness of a friendly military mission. Intelligence mission data refer to technical intelligence information such as radar signatures or geospatial mapping data that weapon systems use to carry out a mission once deployed.⁴

Further, according to DOD, adversaries are developing new threats more rapidly than the department can develop new systems to counter them. There is a growing concern that the technological superiority of the United States over foreign adversaries has been decreasing, thereby representing a threat to national security and military capabilities. The confluence of these trends has created recognition within DOD of the need for more effective collaboration across the defense acquisition and intelligence communities. To address this issue, among others, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) has implemented a series of reform efforts known as Better Buying Power to improve various aspects of the defense acquisition enterprise, such as improving collaboration between the acquisition and intelligence communities. In the third phase of this effort, known as Better Buying Power 3.0, USD(AT&L) identified a need for stronger partnerships among the acquisition and intelligence communities in order to maintain knowledge of current and potential threats.

The National Defense Authorization Act for Fiscal Year 2016 includes a provision that we review the processes and procedures for the integration of intelligence into the defense acquisition process.⁵ This report evaluates, for major defense acquisition programs, the extent to which DOD has (1) processes and procedures for certifying⁶ and training

⁴Intelligence mission data are data essential for building system models; developing algorithms; optimizing sensor design, system testing and evaluation; and validating sensor functionality. Functional areas and categories of intelligence mission data include but are not limited to Characteristics and Performance, Electronic Warfare Integrated Reprogramming, Geospatial Intelligence, Order of Battle, and Signatures.

⁵Pub. L. No. 114-92, § 1638 (2015).

⁶Certification is the procedure through which DOD components determine that an employee meets education, training, and experience elements for each career field.

personnel assigned to provide intelligence support to acquisition programs; (2) efforts to improve processes and procedures for integrating intelligence into its acquisition programs; and (3) efforts to develop new tools for integrating intelligence into its acquisition programs. We also collected information related to DOD's efforts to identify opportunities for weapon systems to collect intelligence even when unrelated to their primary mission, which is presented in appendix I.

To address each of our three objectives, we reviewed written directives, instructions, publications, guides, and briefs related to the role of intelligence in acquisitions. We also interviewed officials from the acquisition, intelligence, and requirements components of DOD, including the offices of the USD(AT&L) and the Under Secretary of Defense for Intelligence (USD(I)); the Joint Staff; the Army, Navy, Air Force, and Marine Corps; and the Defense Intelligence Agency (DIA). We interviewed members of the Acquisition Intelligence Requirements Executive Steering Group and Task Force to assess their efforts to better integrate intelligence into DOD acquisitions. We also interviewed officials from the offices of the Director of National Intelligence; Cost Assessment and Program Evaluation; Director of Operational Test and Evaluation; and USD(AT&L) Office of Performance Assessments and Root Cause Analyses.

To address the first objective we reviewed DOD guidance governing the management of intelligence and acquisition personnel. We interviewed officials from USD(AT&L), USD(I), the Joint Staff, and the Army, Navy, Air Force, and Marine Corps intelligence and acquisition communities who participate in the development of policy and management of personnel regarding staffing, qualifications, certification, and training of personnel providing intelligence support to acquisition programs. We also interviewed and received written responses from Defense Acquisition University officials regarding changes to the acquisition curriculum that included additional intelligence material. We analyzed the certifications and qualifications established by DOD for implementing the Defense Acquisition Workforce Improvement Act; DOD guidance for acquisition personnel; and certifications and qualifications for intelligence personnel under USD(I) guidance, to determine whether any certifications apply to personnel who provide intelligence support to acquisition programs.

To address the second objective we interviewed or requested information from acquisition program offices, as well as from staff who provide intelligence support to those programs. We selected a non-generalizable sample of six Acquisition Category I programs from the four services—

including two each from the Navy and Air Force, and one each from the Army and Marine Corps—to obtain an understanding of how intelligence is integrated into acquisition programs.⁷ We discussed the questions orally or received written responses from each program. While the responses we obtained are not generalizable to all major defense acquisition programs, the information learned from program officials provided context and important insights for our understanding of the interaction between acquisition and intelligence personnel. To determine current intelligence inputs and processes for major defense acquisition programs, we reviewed both department-wide and service-level guidance, including Department of Defense Instruction 5000.02, *Operation of the Defense Acquisition System*, and analyzed the guidance to determine where DOD guidance indicated that intelligence inputs into acquisition programs are to occur.⁸ Due to the evolving nature of the role of intelligence in acquisitions, we also sent a set of structured questions to officials from the Office of USD(I), Joint Staff, DIA, and the intelligence organizations of the services to confirm the key intelligence inputs into major defense acquisitions as of June 1, 2016.

To address the third objective, we identified two tools that DOD is currently developing through discussions with Acquisition Intelligence Requirements Task Force officials. We verified that these tools were in development through interviews with officials responsible for oversight of acquisitions and intelligence, including officials at USD(AT&L), USD(I), and DIA. We interviewed DOD officials and viewed demonstrations of the developmental versions of these tools. We compared the developmental plans and information provided to us by DIA and Performance

⁷DOD categorizes acquisition programs into Acquisition Categories I, IA, II, and III. Acquisition Category I programs are major defense acquisition programs, estimated by USD(AT&L) as requiring an eventual total expenditure for research, development, and test and evaluation of more than \$480 million in fiscal year 2014 constant dollars; or, for procurement, of more than \$2.79 billion in FY2014 constant dollars; or those acquisitions that are designated as major defense acquisition programs or designated as Special Interest by USD(AT&L), the head of the DOD component, or the component acquisition executive. The Special Interest designation is typically based on one or more of the following factors: technological complexity; congressional interest; a large commitment of resources; or criticality of a program to the achievement of a capability or set of capabilities, part of a system of systems, or a joint program. See DOD Instruction 5000.02, *Operation of the Defense Acquisition System* (Jan. 7, 2015).

⁸DOD Instruction 5000.02, *Operation of the Defense Acquisition System* (Jan. 7, 2015).

Assessments and Root Cause Analyses officials against standards developed by professional organizations, such as the Project Management Institute's *A Guide to the Project Management Body of Knowledge*,⁹ federal standards for internal controls,¹⁰ and key practices for collaboration among federal agencies.¹¹ Further details of our objectives, scope, and methodology are presented in appendix II.

We conducted this performance audit from December 2015 to November 2016 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.

Background

DOD manages the acquisition of weapon systems through the Defense Acquisition System, which is an event-based process. Acquisition programs proceed through a series of milestone reviews and other decision points that may authorize entry into the next program phase (see figure 1).¹² Based upon DOD's acquisition-related guidance, for major defense acquisition programs that begin during the materiel solution analysis phase, intelligence inputs into the acquisition process are expected to be provided prior to the Milestone A review,¹³ the point at

⁹Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, Fifth Edition, 2013. *PMBOK* is a trademark of Project Management Institute, Inc.

¹⁰GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 2014).

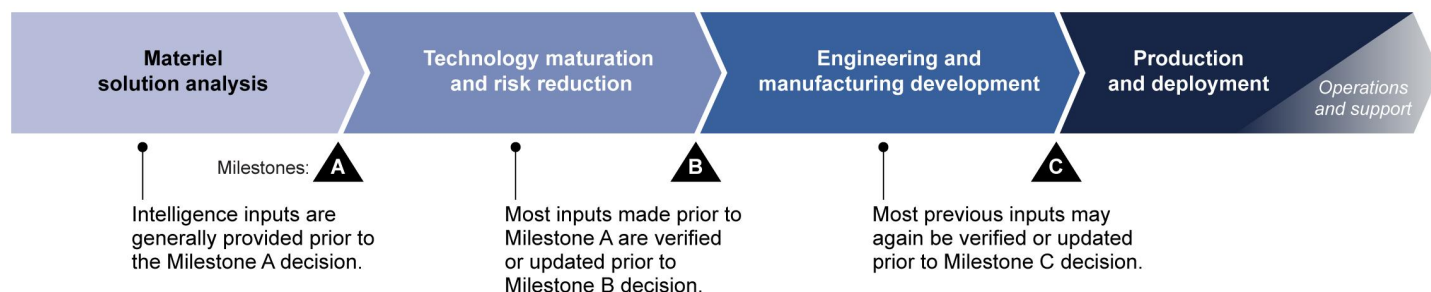
¹¹*Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, [GAO-06-15](#) (Washington, D.C.: Oct. 21, 2005).

¹²Programs may enter the Defense Acquisition System prior to Milestone A, or they may enter directly at Milestones B or C in some circumstances. For our purposes, we are describing programs that entered prior to Milestone A.

¹³The purpose of the materiel solution analysis phase is to conduct the analysis and other activities needed to choose the concept for the product that will be acquired, to begin translating validated capability gaps into system-specific requirements, and to conduct planning to support a decision on the acquisition strategy for the product.

which approval is sought to proceed to the next phase in the process.¹⁴ Further, most of the intelligence inputs are to be verified or updated at points prior to the Milestone B decision and again prior to the Milestone C decision, the point at which approval is sought in order to progress to the production and deployment phase.¹⁵ We describe the intelligence inputs and key DOD guidance for providing intelligence support to acquisition programs in appendix III.

Figure 1: Intelligence Input in the Defense Acquisition System



Source: GAO analysis of Department of Defense information. | GAO-17-10

The USD(AT&L) is responsible for acquisition policy and oversight, and as the Defense Acquisition Executive has responsibility for supervising the Defense Acquisition System. The milestone decision authority is the designated individual with overall responsibility for a program and has the authority to approve its progression to the next phase of the acquisition process.¹⁶ The milestone decision authority is accountable for cost, schedule, and performance reporting. The service acquisition

¹⁴We defined intelligence inputs as actions (such as formation of a working group or certification), products (such as reports or data), or processes (such as a formal review).

¹⁵The production and deployment phase consists of three efforts—low-rate initial production, operational testing and evaluation, and full-rate production and deployment.

¹⁶The milestone decision authority for major defense acquisition programs can be the Defense Acquisition Executive, the head of the DOD component, or the Component or Service Acquisition Executive. The Defense Acquisition Executive is the milestone decision authority for Acquisition Category ID programs. The head of the DOD component or, if delegated, the Component or Service Acquisition Executive is the milestone decision authority for Acquisition Category IC programs. For the purposes of this report we are referring to Acquisition Category ID when we describe major defense acquisition programs.

communities are led by Service Acquisition Executives who are assistant secretaries within their respective military departments. For example, the Assistant Secretary of the Army (Acquisition, Logistics, and Technology) serves as the Army acquisition executive, while the Assistant Secretary of the Navy (Research, Development, & Acquisition) serves as the Navy acquisition executive. The program manager is the designated individual with responsibility for individual acquisition programs who has the authority to accomplish that program's development, production, and sustainment objectives to meet the user's operational needs, and is accountable for cost, schedule, and performance reporting to the milestone decision authority.

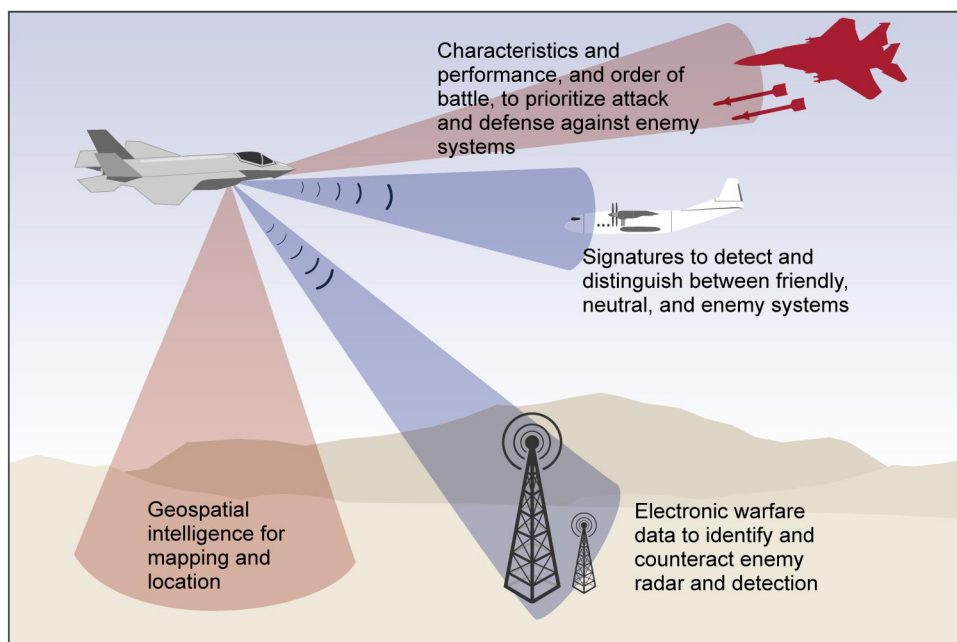
At the Chairman of the Joint Chiefs of Staff level, the J-8 Directorate provides support to the Joint Staff for evaluating and developing force structure requirements, and its director serves as Secretary of the Joint Requirements Oversight Council and as Chairman of the Joint Capabilities Board. In these capacities, the director orchestrates Joint Staff support of the capabilities development process through the Joint Capabilities Integration and Development System. One of the J-8 Directorate's objectives is to provide early capability development guidance to the services. The services have different organizational structures that define their respective requirements communities. For example, according to the Air Force, via its Major Commands, the Air Force has personnel responsible for 12 capability portfolios such as Air Superiority and Global Precision Attack that manage Air Force capability requirements.

According to DOD, the speed of technical innovation and the complexity of advanced weapon systems, such as the F-35, are creating an increasing demand for specialized intelligence mission data to provide information for sensors and automated processes supporting the warfighter.¹⁷ There are several types of intelligence mission data, each used by weapon systems in different ways, including signatures, electronic warfare integrated reprogramming data, characteristics and performance, order of battle, and geospatial intelligence (see figure 2). Signatures are distinct, repeating characteristics, such as radio frequencies or acoustic characteristics, which are associated with a

¹⁷DOD, *IMD Cost Methodology Guidebook* (Washington, D.C.: Feb. 2013).

particular type of equipment, materiel, activity, individual, or event. For example, a weapon system may associate a specific signature with an enemy system, and identify it as such. Electronic warfare integrated reprogramming data also describe radio frequencies, and are typically used to attack or control other electronic systems—for example, jamming enemy radar capabilities. Characteristics and performance data describe the abilities of a particular foreign military system, while order of battle describes the strength and structure of armed forces. These can assist a weapon system and its operator to prioritize and determine appropriate actions against the enemy.

Figure 2: Examples of Intelligence Mission Data



Source: GAO analysis of Department of Defense information. | GAO-17-10

The title, specific duties, and organizational structure for the personnel providing intelligence support to acquisition programs vary by service (see table 1). Personnel who provide intelligence support to acquisition programs may also coordinate, and in some cases create, the completion of key intelligence products that accompany the acquisition process through documented processes such as Threat Steering Groups, which assemble intelligence and acquisition representatives with knowledge of systems that are specific to the acquisition program.

Table 1: Personnel Who Provide Intelligence Support to Acquisition Programs

Service	Position Title	Number of Positions ^a /Job Classification	Parent Organization
Army	Threat analyst (civilian) or threat integration staff officer (military)	73/Intelligence Specialist	Army Intelligence
	Threat manager		Training and Doctrine Command
	Foreign intelligence officer		Army Materiel Command
Navy	Scientific and Technical Intelligence Liaison Officer, Acquisition Intelligence Professional	47/Intelligence Specialist, Intelligence Aid and Clerk, Program Analyst, Engineers, Security Administrator, Information Technology Management, Computer Science, Operational Research Analyst, and Physicist	Acquisition system commands such as Naval Air Systems Command and Naval Sea Systems Command
	Acquisition Intelligence Professional	12/Intelligence specialist, engineers	Office of Naval Intelligence and Executive Support Office, OPNAV N2N6I
Marine Corps	Intelligence analysts, Scientific and Technical Intelligence Liaison Officer	11/Intelligence Specialist	Marine Corps Intelligence Activity
Air Force	Acquisition intelligence specialist (Officers, enlisted, and civilian)	243/Intelligence Specialist, Engineer, Program Manager, and Scientist	Air Force Headquarters, Major Commands, ^b National Air and Space Intelligence Center

Source: GAO analysis of Service Information. | GAO-17-10

Notes:

^aNumber of positions as of July 2016.

^bAir Force Major Commands include Air Force Space Command, Air Combat Command, Air Force Global Strike Command, Air Mobility Command, and Air Force Materiel Command.

In the Army, during the acquisition lifecycle, the threat integration staff officers assigned to Army Intelligence coordinate intelligence support to acquisition programs through the Threat Steering Group, in which Training and Doctrine Command threat managers and Army Materiel Command foreign intelligence officers participate.¹⁸ Threat assessments before Milestone B are generally managed by Training and Doctrine Command threat managers. Threat assessments from Milestone B and beyond are typically managed by Army Materiel Command foreign intelligence officers.

¹⁸ See generally Army Regulation 381-11, *Intelligence Support to Capability Development* (Jan. 26, 2007).

In the Navy, intelligence support to acquisition programs is provided by intelligence personnel in the Office of Naval Intelligence, which is responsible for the production and validation of intelligence inputs to Navy acquisition programs.¹⁹ The acquisition programs are supported by scientific and technical intelligence liaison officers who are hired and funded by the Navy entities responsible for management of assigned acquisition programs, called system commands, and are responsible for coordinating between the system command and the intelligence community.²⁰ For example, the scientific and technical intelligence liaison officer is responsible for requesting the production and validation of intelligence inputs such as threat assessments, which are used to obtain the threat intelligence required to inform acquisition cost, schedule, and performance decision making by program managers.

For programs that are managed by the Marine Corps acquisition agencies (Marine Corps System Command and Program Executive Officer Land Systems), intelligence support is provided by military and civilian intelligence analysts at Marine Corps Intelligence Activity, the service intelligence center. Marine Corps System Command's intelligence support is coordinated by a scientific and technical intelligence liaison officer. Marine Corps-funded programs at other Navy system commands follow the intelligence support processes for the hosting organization. For example, the Marine Corps version of the F-35 or helicopter acquisitions would both follow processes for intelligence support to acquisition programs used by Naval Air Systems Command.

The Air Force materiel commands (Air Force Space Command and Air Force Materiel Command) use acquisition intelligence specialists to support acquisition programs identified as intelligence sensitive. These specialists, along with intelligence analysts at the National Air and Space Intelligence Center, provide intelligence products and input based on their individual levels of experience and training.

¹⁹See generally Office of the Chief of Naval Operations Instruction 3811.1F, *Threat Support to the Defense Acquisition System* (May 16, 2016).

²⁰See generally Office of the Chief of Naval Operations Instruction 3880.6A, *Scientific and Technical Intelligence Liaison Officer (STILO) Program and Intelligence Support for the Naval Research, Development, Test & Evaluation, and Acquisition Communities* (Nov. 5, 2007).

DOD Has Processes and Procedures for Certifying Both Intelligence and Acquisition Personnel but Not for Personnel Providing Intelligence Support to Acquisition Programs, and Services' Training Varies

DOD has processes and procedures for the certification of both intelligence and acquisition personnel, but it has not established certifications for personnel providing intelligence support to acquisition programs. Though DOD has not developed certifications specific to personnel who provide intelligence support to acquisition programs, the Air Force and the Army have each developed certifications for these personnel. In the absence of department-wide certifications, the services have developed varying levels of training for personnel providing intelligence support to acquisition programs, and this training may not be specific to providing intelligence support to acquisition programs.

DOD Has Certifications for Intelligence and Acquisition Personnel and the Air Force and Army Have Developed Certifications for Personnel Who Provide Intelligence Support to Acquisition Programs

Neither USD(I) certifications for the defense intelligence workforce nor USD(AT&L) certifications for the defense acquisition workforce include a certification specific to those personnel providing intelligence support to acquisition programs. The Defense Acquisition Workforce Improvement Act generally requires DOD to establish policies and procedures for the management of DOD's acquisition workforce, including education, training, and career development.²¹ USD(AT&L) subsequently organized certain acquisition-related positions into 14 career fields and established a certification process by which DOD components determine that employees have met standard requirements for education, training, and experience for each field. However, personnel who provide intelligence support to acquisition programs are not included in the 14 career fields with established certifications. According to service officials, acquisition certifications for personnel who provide intelligence support to acquisition programs have not been developed because there is no career field for intelligence support to acquisition. As a result, personnel providing

²¹ See generally Pub. L. No. 101-510, §1202 (1990) (codified as amended at chapter 87 of Title 10, U.S. Code); 10 U.S.C. § 1701(a). The Defense Acquisition Workforce Improvement Act also required DOD to establish the Defense Acquisition University, which is responsible for designing, maintaining, and delivering certification training courses at each level, among other course offerings.

intelligence support to acquisition programs are not required to obtain certification for any of the acquisition-related career fields. Officials from the Air Force stated that the lack of certification has resulted in critical skill gaps for personnel providing intelligence support to acquisition programs.

Similarly, USD(I) is responsible for establishing a department-level certification program for the defense intelligence workforce.²² As a result, certifications for 15 different intelligence disciplines have been developed, such as geospatial intelligence and collection management, and several other certifications are currently being developed for disciplines such as all-source analysis—an intelligence activity that involves the integration, evaluation, and interpretation of information from all available data sources and types.²³ Intelligence officials stated that personnel providing intelligence support to acquisition programs may become eligible for fundamental intelligence certifications, such as all-source analysis certification. However, these officials stated that the certification is designed to certify fundamental competencies for all intelligence analysts, and is not specific to providing intelligence support to acquisition programs.

Though DOD has not developed certifications specific to personnel who provide intelligence support to acquisition programs, the Air Force and the Army have each developed certifications for these personnel.²⁴ The Air Force has established a certification for personnel who provide intelligence support to acquisition programs via both service-wide guidance and guidance from organizations involved in acquisition, such as Air Force Materiel Command. The Air Force requires that, for initial certification, personnel assigned to positions providing intelligence support to acquisition programs must complete certain training, including Air Force and Defense Acquisition University classes, and have 1 year of

²²DOD Instruction 3115.11, *DOD Intelligence Human Capital Management Operations*, encl. 2, para. 1.c (Jan. 22, 2009) (incorporating change Dec. 9, 2011).

²³See DOD Directive 5240.01, *DOD Intelligence Activities*, para. E2.1 (Aug. 27, 2007) (incorporating change and certified current through Aug. 27, 2014) (defining all-source analysis).

²⁴As of July 2016, the Navy and Marine Corps had not developed certifications for personnel providing intelligence support to acquisition programs.

experience in a designated “acquisition intelligence” position.²⁵

Additionally, individual acquisition organizations, such as the Air Force Life Cycle Management Center, require additional training and also require that intelligence managers certify that personnel providing intelligence support to acquisition programs have completed the required training, met the experience requirements, and can complete a list of unique tasks specific to the performance of their individual job.

The Army developed an optional certification for civilian personnel in intelligence positions, including intelligence support to acquisition programs. A 2001 training plan describes a process for individuals to document competency in different specialty areas based on the job duties and seniority of the position. The plan shows that the intelligence support to acquisition specialty requires competency in areas such as threat intelligence and technical knowledge of acquisition organizations. Personnel may achieve these competencies through any combination of previous experience, classroom, and on-the-job training. Subsequently, they may request an optional certification from their command organization if a supervisor certifies the individual’s qualifications.

The Services and USD(AT&L) Have Developed Some Training for Personnel Providing Intelligence Support to Acquisition Programs, but Cannot Ensure Personnel Are Trained to Carry Out Duties

The services have developed varying levels of training for the personnel who provide intelligence support to acquisition programs in the absence of certifications required by DOD for these personnel. Air Force officials stated that training for personnel providing intelligence support to acquisition programs is accomplished through their certification process, which requires these personnel to complete a series of classroom and on-the-job training units, including Defense Acquisition University classes in acquisition management fundamentals, among others, and an Air Force 4-day training course called the Acquisition Intelligence Formal Training Unit. Individual acquisition organizations such as the Air Force Life Cycle Management Center require additional training, including courses on intelligence acquisition life-cycle management and the Joint Capabilities Integration and Development System; a review of key acquisition documents; and on-the-job training based on unit-specific missions. Air

²⁵Air Force Instruction 14-111, *Intelligence Support to the Acquisition Life-Cycle*, paras. 2.6.3, 2.9.1.3 (May 18, 2012) (incorporating change June 16, 2014). The Air Force refers to personnel who provide intelligence support to acquisition programs as acquisition intelligence specialists.

Force officials also stated that experience as an active-duty intelligence officer and an acquisition program manager all also provided training for the position.

Army officials stated that threat managers and foreign intelligence officers, two of the three groups that provide intelligence support to acquisition programs, are required to take several courses through the Defense Acquisition University and Defense Security Service. In addition, the threat intelligence branch of Army Intelligence has an annual training course that includes training in subjects specific to providing intelligence support to acquisition programs, such as critical threats and technology protection. However, according to Army officials, Army personnel providing intelligence support to acquisitions are not required to take this course. An Army intelligence official stated that the course is optional because of a lack of travel and training funds.

The Navy and Marine Corps have identified and required different levels of training relevant for their personnel. Navy officials stated that, as of June 2016, there was no formal training across the department for personnel providing intelligence support to acquisition programs, although some Navy organizations have developed training policies specific to their organizations. For example, according to Navy officials, Naval Air Systems Command, the Navy acquisition organization generally responsible for naval aircraft, weapons, and systems, has a training program for its scientific and technical intelligence liaison officers. This training includes intelligence community and Defense Acquisition University courses, computer-based training, and a certification exam, which requires its liaison officers to attend the Air Force's Acquisition Intelligence Formal Training Unit. According to Navy officials, personnel providing intelligence support to acquisition programs at other naval system commands, such as those responsible for sea and space systems, receive primarily ad hoc and on-the-job training.

Marine Corps officials stated that, as of June 2016, personnel who provide intelligence support to acquisition programs were required to take an online Defense Acquisition University course on acquisition management fundamentals that is not specific to providing intelligence support to acquisition programs, in addition to on-the-job training in order to perform their job duties. These officials also stated that in 2016 personnel were required to attend a version of the Air Force Acquisition Intelligence Formal Training Unit, and that although the Marine Corps is exploring the use of the Army Intelligence training course, it is not required for personnel to attend the training.

USD(AT&L), working with the Defense Acquisition University, established training related to the integration of intelligence and acquisition. In May and June 2015, Defense Acquisition University increased the integration of intelligence and acquisition in its curriculum.²⁶ For example, the university added a case study regarding critical intelligence parameters to the program manager's course, and it also added discussion topics about the need for intelligence in acquisition programs to several courses intended for acquisition executives and senior officials.²⁷ Both entry-level and advanced courses were modified to include content on the relationship between intelligence and acquisition organizations. For example, officials stated that they invited a speaker from the Joint Staff to an advanced course to speak about the relationship between intelligence and acquisition.

While this training is intended to address the identified need for greater intelligence training for acquisition personnel, the training may not be accessible to personnel providing intelligence support to acquisition programs. Service intelligence officials stated that because positions for providing intelligence support to acquisition programs are not designated as acquisition-related for the purposes of Defense Acquisition Workforce Improvement Act certification, some courses are available to these personnel only on a space-available basis. Some other courses, such as those for program managers, require Defense Acquisition Workforce Improvement Act certification in designated career fields as a pre-requisite. As described above, DOD has not required certification for personnel providing intelligence support to acquisition programs. As a result, these personnel may be unable to access these courses.

Without requiring certifications for personnel who provide intelligence support to acquisition programs, DOD has no assurance that these personnel are qualified and prepared to carry out their duties. The department has established certifications for both acquisition and intelligence positions in order to ensure that those respective workforces

²⁶According to Defense Acquisition University officials, these changes were in response to the Better Buying Power 3.0 Initiative. See table 2, task 8, below.

²⁷Critical intelligence parameters identify thresholds that, if breached, indicate an adversary's potential to substantially reduce the performance or even defeat the capability of the weapon system undergoing development.

are qualified to carry out their duties. Key principles for the management of federal employees state that agencies should develop training strategies and tools that, among other things, can be aligned to improve the critical skills needed in their workforce.²⁸ We previously found that when intelligence training is not fully implemented or required, programs and organizations may be unable to fully succeed in their goals.²⁹ The DOD Inspector General has also found that the lack of common training standards has resulted in difficulties for personnel in performing common tasks and in a critical skills gap across military intelligence services and agencies.³⁰ While all four services have established or identified training for personnel providing intelligence support to acquisition programs, without department-wide required certifications that include training standards, there may be inconsistent levels of expertise and skill among these personnel. Without a certification process that includes required training for personnel who provide intelligence support to acquisition programs, DOD may not be able to ensure that all personnel who provide intelligence support to acquisition programs are familiar with and able to provide intelligence inputs to their assigned acquisition programs.

²⁸GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, [GAO-04-39](#) (Washington, D.C.: Dec. 11, 2003).

²⁹GAO, *Intelligence Community Personnel: Strategic Approach and Training Requirements Needed to Guide Joint Duty Program*, [GAO-12-679](#) (Washington, D.C.: June 20, 2012).

³⁰U.S. Department of Defense Inspector General. *Evaluation of DOD Intelligence Training and Education Programs for the Fundamental Competencies of the DOD Intelligence Workforce*, DODIG-2015-015 (Oct. 31, 2014).

DOD Has Multiple Efforts Underway to Improve Processes and Procedures for Integrating Intelligence into Major Defense Acquisition Programs but Faces Challenges Prioritizing Intelligence Mission Data Needs

As of July 2016, DOD had multiple efforts underway to improve processes and procedures for integrating intelligence into major defense acquisition programs. For example, USD(AT&L) had identified several intelligence-related tasks in its Better Buying Power 3.0 initiative. Further, USD(AT&L), USD(I), and the Joint Staff had created an executive steering group and a task force—the Acquisition Intelligence Requirements Task Force—to improve the integration of intelligence into major defense acquisition programs. This task force has identified the need for intelligence mission data to be prioritized, but DOD has not required such prioritization.

USD(AT&L) Has Identified Several Intelligence-Related Tasks to Address Challenges Integrating Intelligence into Acquisitions

In order to increase the productivity, efficiency, and effectiveness of DOD's acquisition, technology, and logistics efforts, USD(AT&L) issued the Better Buying Power 3.0 initiative in January 2015. This initiative contains nine tasks related to integrating intelligence into acquisitions, which are described in table 2.

Table 2: Intelligence-related Tasks Identified by the Under Secretary of Defense for Acquisition, Technology, and Logistics in the Better Buying Power 3.0 Initiative

Task	Description	Status Reported By USD(AT&L) as of June 2016
1. Review/Revise Defense Intelligence Agency's (DIA) Critical Intelligence Parameter Instruction	Review and, as necessary, recommend changes to DIA Instruction on the identification, monitoring, and reporting of Critical Intelligence Parameters.	Stakeholder input has been adjudicated and final guidance is under legal review prior to release.
2. Program Manager/Service Acquisition Executive Critical Intelligence Parameter Process	As appropriate, acquisition officials, with requirements sponsors, will establish initial critical intelligence parameters for their programs and create processes to address changes in foreign threats that may affect the performance of the weapon system under development.	The services have reached agreement on a phased approach to critical intelligence parameter development and monitoring and are developing guidance for signature.
3. Ensure That Defense Acquisition Boards Evaluate Program Based upon Threat Projections, Intelligence Mission Data Requirements, and Critical Intelligence Parameters.	Acquisition officials will ensure that all Defense Acquisition Board reviews include an evaluation of program plans based on threats, operational intelligence mission data requirements, critical intelligence parameters, and the validity of program requirements.	Proposals have been reviewed and approved by leadership but not yet implemented.
4. Intelligence Mission Data Financial Policy	Review and recommend changes to the financial management policies for funding intelligence mission data to ensure that they are consistent with DOD Instruction 5000.02, <i>Operation of the Defense Acquisition System</i> , and with initiatives associated with intelligence support to acquisitions.	Proposals have been prepared for leadership review.
5. Revise Department of Defense (DOD) <i>Directive 5250.01: Management of Intelligence Mission Data (IMD) in DOD Acquisition</i>	Review and prepare update to DOD Directive 5250.01 to ensure that processes are in place to enhance prioritizing of intelligence mission data supply and demand for acquisition programs.	Stakeholder comments on the revised directive are under review.
6. Develop Dynamic Threat Library/ Validated Online Lifecycle Threat Report	Develop a plan for reducing latency in providing intelligence data to acquisitions by implementing the Validated Online Lifecycle Threat and Threat Library. DIA will complete on-going pilots and present findings and a plan for transition to the new system to an executive decision making group.	The threat library and the Validated Online Lifecycle Threat have been piloted with the Joint Surveillance Target Attack Radar System Recapitalization program and the Air and Missile Defense Radar, among others, and development of the Validated Online Lifecycle Threat is underway.
7. Modeling & Simulation	Evaluate options for using modeling and simulation capabilities to manage acquisition requirements and risks associated with foreign threats.	Meetings regarding friendly and enemy data have been completed. Program-specific plans are under development.

Task	Description	Status Reported By USD(AT&L) as of June 2016
8. Increasing Professionalization to Integrate Intelligence Into Acquisition	Defense Acquisition University will increase acquisition-intelligence-requirements focus in revised curriculum specifically in the program management and requirements areas. DIA will work with the National Intelligence University and Professional Analyst Career Education to revise intelligence professional training that supports the Acquisition Community.	Defense Acquisition University has modified several courses with additional acquisition-intelligence content. DIA has completed analysis for class content and the results have been briefed to leadership.
9. Develop Key Leader Positions for Intelligence Support	Evaluate options for establishing key leadership positions for intelligence support at the program executive office level or elsewhere in the acquisition chain. Recommendations will be provided to the Under Secretary of Defense for Acquisition, Technology, and Logistics.	Data have been analyzed and leadership has been briefed.

Source: GAO analysis of USD(AT&L) information. | GAO-17-10

Among the nine tasks, USD(AT&L) describes the use of critical intelligence parameters as a key aspect of the linkage among the acquisition, intelligence, and requirements communities.³¹ Critical intelligence parameter thresholds, if breached, indicate an adversary's potential ability to substantially reduce the performance or even defeat the capability of the weapon system undergoing acquisition. The intelligence community monitors foreign threat capabilities and informs the acquisition community of a breach, which triggers a review process to resolve or mitigate the breach.

Other intelligence-related tasks under Better Buying Power 3.0 include direction to the Assistant Secretary of Defense for Acquisitions to work with the Office of the USD(I) to review DOD Directive 5250.01, *Management of Intelligence Mission Data (IMD) in DOD Acquisition*. As of July 2016, this review is being facilitated by the Acquisition Intelligence Requirements Task Force, described below, which is coordinating a revised draft among stakeholder entities.

³¹Critical intelligence parameters are established and examined through the joint and collaborative efforts of the intelligence, acquisition, and requirements communities to aid in developing intelligence production requirements to support an acquisition program.

USD(AT&L), USD(I), and Joint Staff Created an Executive Steering Group and Task Force to Improve the Integration of Intelligence into Acquisition Programs

DOD created an executive steering group and task force to better integrate intelligence into acquisition programs. On December 4, 2015, the offices of USD(AT&L) and USD(I), along with the Joint Staff, created the Acquisition Intelligence Requirements Executive Steering Group and the Acquisition Intelligence Requirements Task Force through a joint memorandum to better integrate, coordinate, and prioritize intelligence processes and procedures for providing intelligence support to acquisition programs.³² The steering group is co-chaired by senior level members of the offices of USD(AT&L) and USD(I), and the Joint Staff, and it is composed of representatives from the Office of the Director of National Intelligence, Director of Operational Test and Evaluation, Office of Cost Assessment and Program Evaluation, service acquisition executives, military service intelligence staffs, and DIA, among other stakeholders.

The memorandum states that the steering group replaces the Intelligence Mission Data Oversight Board and the Intelligence Mission Data Senior Steering Group that were previously established in DOD Directive 5250.01, issued in January 2013.³³ A DIA official explained that the Intelligence Mission Data Senior Steering Group never met and that the Acquisition Intelligence Requirements Task Force was created to address intelligence support to acquisition, including intelligence mission data issues.

Both the executive steering group and the task force began to meet prior to their formal creation in December 2015. The task force initially met in October 2015 and subsequent to January 2016 has generally held weekly meetings, while the executive steering group initially met in August 2015 and met quarterly subsequent to December 2015. Since February 2016, a senior executive service-level director has led the task force composed of O-6 level representatives from the organizations that form the steering group. According to task force officials, early efforts of the task force included engaging major defense acquisition programs that the task force identified as intelligence mission data-dependent in order to identify and

³²Joint Staff J8, Assistant Secretary of Defense (Acquisition), Undersecretary of Defense (Intelligence) Memorandum, *Acquisition Intelligence Requirements Executive Steering Group*, December 04, 2015.

³³DOD Directive 5250.01, *Management of Intelligence Mission Data (IMD) in DOD Acquisition*, encl. 2 (Jan. 22, 2013).

summarize intelligence supportability issues and raise them to decision makers prior to milestone reviews for the acquisition programs.³⁴

DOD's Acquisition Intelligence Requirements Task Force Identified the Need for, but DOD Has Not Required Prioritization of, Intelligence Mission Data

Officials from USD(AT&L), USD(I), and Joint Staff stated that while there have previously been other weapon systems with intelligence mission data shortfalls, such as the F-22 and F-18G, the F-35's greater reliance on intelligence mission data and concerns regarding the service intelligence centers' ability to produce the needed data brought the problem to the forefront. For example, DOD reported in 2013 that the initial release of intelligence mission data requirements for the F-35 in 2008 presented a unique challenge with regard to the amount and breadth of intelligence requirements for the intelligence community, and for the service intelligence centers specifically.³⁵ These officials stated that the main impetus for creating the Acquisition Intelligence Requirements Executive Steering Group and the Acquisition Intelligence Requirements Task Force concerned the shortfall in providing intelligence mission data to the F-35 program—data needed for the F-35 to perform its mission once it became an operational weapon system. Task force officials stated that prioritizing intelligence mission data will ensure that the data provided are sufficient to meet the requirements of advanced weapon systems, such as the F-35.

DOD has processes and procedures related to intelligence mission data, such as those in DOD Instruction 5000.02 and DOD Directive 5250.01, but they do not require prioritization of the data.³⁶ For example, DOD

³⁴Officials from the Acquisition Intelligence Requirements Task Force stated that its overall agenda is to open lines of communication and enhance coordination; improve prioritization of requirements; codify processes to conduct risk assessment and mitigation; review existing databases for redundancy and duplication; establish a baseline for Intelligence Mission Data production; and enhance data standardization.

³⁵DOD, *IMD Cost Methodology Guidebook* (Washington, D.C.: Feb. 2013).

³⁶See, e.g., DOD Instruction 5000.02, *Operation of the Defense Acquisition System*, at 54 (Jan. 7, 2015); see generally DOD Directive 5250.01, *Management of Intelligence Mission Data (IMD) in DOD Acquisition* (Jan. 22, 2013). According to DOD officials, both the directive and the instruction were under revision as of July 2016. Officials from DIA and the Acquisition Intelligence Requirements Task Force stated that as of July 2016 comments to the draft revision of DOD Directive 5250.01 were being coordinated among stakeholders. We reviewed the version of the draft directive dated April 28, 2016, and it did not include specific requirements to prioritize intelligence mission data.

guidance requires DOD's intelligence mission data-dependent acquisition programs to develop a Lifecycle Mission Data Plan to identify anticipated intelligence mission data needs over the life of a weapon system, from program start through the life-cycle of the program to disposal. However, the plan categorizes the intelligence mission data needs by means of a spectrum arranged by data availability—that is, showing data ranging from those that are most available to those that are least available. That presentation of information does not convey a prioritization of what the weapon system most needs to perform its mission.

DOD Directive 5250.01 directs DIA to establish the Intelligence Mission Data Center, which is to serve as the focal point for intelligence mission data development, production, and sharing, but it does not assign the agency the role of prioritizing intelligence mission data needs. Task force officials stated that a DIA working group for intelligence mission data was created to oversee and coordinate intelligence mission data production across the defense intelligence enterprise, and that the Intelligence Mission Data Center will support the working group by facilitating the discovery and sharing of existing intelligence mission data. However, although it may be helpful in preventing the duplication of efforts in the collection of intelligence mission data, the Intelligence Mission Data Center's work does not constitute a means for prioritizing mission data by need for individual acquisition programs.

Officials from USD(AT&L), USD(I), Joint Staff, and the task force described a lack of prioritization at multiple levels, to include within the individual acquisition programs, as well as at the service and department levels. Officials from USD(AT&L), USD(I), and Joint Staff, as well as service-level officials on the task force, stated that there were currently no required processes or procedures for prioritizing intelligence mission data needs at any of these levels. For example, at the acquisition program level, an F-22 will have different intelligence mission data needs and priorities from those of a Navy submarine. At the service level, each service will have intelligence mission data needs based on the types of weapon systems it is developing and has already deployed. At the department level, the Air Force and the Navy may have similar intelligence mission data needs for their respective fighter aircraft, but the Army's intelligence mission data needs will likely differ greatly from those of its sister services based on the respective threats each faces.

As of July 2016, no requirements existed within DOD guidance to prioritize intelligence mission data, though there were efforts underway in 2016 by the task force and within the Air Force to develop processes and

procedures for intelligence mission data prioritization. According to task force and Air Force officials, the Acquisition Intelligence Requirements Task Force worked in parallel with an Air Force effort to identify potential processes to prioritize intelligence mission data at the acquisition program and service levels, respectively. These officials presented proposals in June and July 2016 for potential processes and procedures to prioritize intelligence mission data at the acquisition program level. They also described how prioritization at the service and department levels may be accomplished, as shown below:

- Acquisition program prioritization: The task force proposal would involve prioritization of intelligence mission data into the following four levels of impact on the acquisition program's capabilities were the data not acquired or unavailable:³⁷
 1. Level I denotes unacceptable degradation: intelligence mission data requirements that, if not satisfied, would result in unacceptable mission task degradation with no work-around possible;
 2. Level II denotes significant degradation: intelligence mission requirements that, if not satisfied, would result in a significant mission task degradation that is unacceptable to the operator but for which a work-around is available, acceptable to the operator, and must be applied;
 3. Level III denotes partial degradation: intelligence mission data requirements that, if not satisfied, would result in a partial or minimal degradation that is acceptable to the operator and for which a work-around is optional; and,
 4. Level IV denotes little to no impact: intelligence mission data requirements that, if not satisfied, would result in little to no degradation to the mission.
- Service prioritization: Air Force officials described an effort undertaken in May 2016 to apply the individual program approach using levels 1

³⁷ According to task force officials, they developed the proposed prioritization process for individual acquisition programs using a systems engineering approach. Task force officials stated that this type of approach would be familiar to acquisition professionals. Task force officials stated their belief that such a system would rely on computerized modeling and simulation tools to help inform the amount of intelligence needed for a weapon system to perform its mission.

to 4 described above to categorize 150 intelligence mission data needs at the service level. Task force officials stated that the Air Force effort undertaken in fiscal year 2016 would use a cost-capability approach to better inform the fiscal year 2017 service-wide prioritization effort.³⁸

- Department prioritization: Task force officials indicated that implementing prioritization at the individual program and service levels would be required prior to developing an enterprise-wide capability to prioritize intelligence mission data. Officials from USD(AT&L) stated that the enterprise-wide prioritization of intelligence mission data could also be informed by efforts related to developing Integrated DOD Intelligence Priorities.³⁹ Furthermore, officials from the DIA stated that there is a lack of coordination regarding how the service intelligence centers conduct their business, and that the centers currently were not prioritizing, verifying, or balancing the work related to producing intelligence mission data. Task force officials stated that DIA was developing an intelligence mission data production prioritization process that would respond to enterprise-wide intelligence mission data priorities.

Though DOD has taken efforts to identify and develop processes and procedures to prioritize intelligence mission data, previous efforts have not succeeded in implementing intelligence mission data prioritization. Federal internal control standards state that management should establish an organizational structure, assign responsibility, and delegate authority to achieve objectives.⁴⁰ Per the joint memorandum that established the Acquisition Intelligence Requirements Executive Steering Group, the steering group and associated task force were created to integrate, coordinate, and prioritize intelligence support functions and

³⁸Cost capability analysis is the process of gathering data from a range of sources to identify instances where small changes in capability have a large impact on cost so that weapon systems can be developed more affordably.

³⁹DOD issued Directive-type Memorandum 15-004, *Integrated DOD Intelligence Priorities*, on September 3, 2015. The guidance establishes policy, assigns responsibilities, and provides procedures for internal coordination and prioritization of intelligence priorities of the Office of the Secretary of Defense, the Joint Staff, the Combatant Commands, and the military departments to improve identification of the intelligence needs of DOD.

⁴⁰GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 2014).

processes. However, previous efforts have not succeeded in implementing a system to prioritize these data at any level. For example, the Intelligence Mission Data Senior Steering Group never met, and the DIA's standing working group efforts may lead to a prevention of duplication of intelligence mission data production efforts, but would not lead to prioritization of the data. The Acquisition Intelligence Requirements Task Force was created to address intelligence support to acquisition, including intelligence mission data issues, and it has developed some proposed processes and procedures for prioritization of intelligence mission data. Without specific DOD guidance requiring intelligence mission data prioritization, new processes and procedures such as those developed by the task force and the services may not be fully implemented. With no required process to prioritize intelligence mission data, the intelligence community may continue to process requests for intelligence mission data as they are received, and thus weapon systems may not have the intelligence mission data they need to successfully perform their missions once operational.

DOD Is Developing New Tools for Integrating Intelligence into Acquisition Programs but Faces Challenges in Development and Implementation

As of July 2016, DOD was developing new tools to better integrate intelligence into acquisition programs. DIA was developing the Validated Online Lifecycle Threat, an online tool to provide threat information to acquisition programs in a more timely and effective manner than the current manually generated process in use. However, DIA had not effectively communicated with stakeholders about the tool or sought feedback from its intended users. Separately, officials from Performance Assessments and Root Cause Analyses, an office within USD(AT&L), were developing a tool for the acquisition community to communicate intelligence needs from individual acquisition programs to the intelligence community. However, intelligence community users had not expressed a need or defined requirements for this tool. If the tool does not meet the user's needs, or will not be used, moving forward with its development could use funds unnecessarily.

DOD Is Developing the Validated Online Lifecycle Threat Tool but Has Not Effectively Communicated with Stakeholders and Intended Users of the Tool.

DOD began developing a new tool in fiscal year 2015 to better report threat information from the intelligence community to acquisition programs, but it has not effectively communicated with stakeholders about the tool or sought feedback from its intended users. As reported by DIA and described in USD(AT&L)'s Better Buying Power 3.0 initiative, the Validated Online Lifecycle Threat is a new tool that DIA began developing in fiscal year 2015 to develop and report threat information to acquisition programs. DOD guidance describes the System Threat Assessment Report as the primary threat document for supporting the Defense Acquisition Board's milestone reviews.⁴¹ DOD officials described the System Threat Assessment Report as a primary intelligence input into major DOD acquisitions.

DOD officials described challenges regarding the timeliness and usefulness of the System Threat Assessment Report. Specifically, officials from USD(AT&L), Joint Staff, and DIA, as well as service intelligence officials, stated that the System Threat Assessment Reports historically arrived at acquisition program offices late, not until after the requirements for a new weapon system had been identified and approved as part of the Joint Capabilities Integration Development System process well after the designing of the weapon system had begun. Furthermore, officials from DIA, USD(AT&L), and the service intelligence and acquisition communities stated that these reports are often several hundred pages in length, take as long as 9 months to produce, and are not substantively used by acquisition program managers. According to these officials, as well as officials from the Acquisition Intelligence Requirements Task Force, program managers simply used System Threat Assessment Reports to check off a box on a list of required documents for the next acquisition milestone decision meeting. Specifically, Air Force officials from the Joint Surveillance Target Attack

⁴¹ See Defense Intelligence Agency Instruction 5000.002, *Intelligence Threat Support for Major Defense Acquisition Programs*, para. 4.2.4 (Feb. 1, 2013). The Defense Acquisition Board advises the Defense Acquisition Executive on critical acquisition decisions when the Defense Acquisition Executive is the milestone decision authority. DOD Instruction 5000.02, *Operation of the Defense Acquisition System*, para. 5.a(4)(b) (Jan. 7, 2015). The milestone decision authority has the authority to approve entry of an acquisition program into the next phase of the acquisition process, and is accountable for cost, schedule, and performance reporting to higher authority, including congressional reporting. DOD Directive 5000.01, *The Defense Acquisition System*, para. 3.4 (May 12, 2003) (certified current Nov. 20, 2007).

Radar System Recapitalization acquisition program stated that the system threat assessment reports were not usable because they did not contain the level of relevance and specificity needed by the acquisition program, and because they were too long, fragmented, and difficult to navigate. Lastly, DIA officials stated they had determined that as much as 80 percent of all System Threat Assessment Reports are repetitive with each other and are not program specific.

According to DIA, the Validated Online Lifecycle Threat is a planned system-specific threat tool created by selecting relevant modules from a library of threat information. DIA and officials from USD(AT&L) described the planned threat library as consisting of dynamic modules based upon threat category, such as fighter aircraft, that would be updated by the analyst at the services' intelligence centers with new threat information as it is produced within the intelligence community. DIA officials reported that as part of a broader piloting effort the agency completed in 2015, they were able to develop a Validated Online Lifecycle Threat in 3 months for the Joint Surveillance Target Attack Radar System recapitalization program. According to DIA officials, the agency will have spent nearly \$2.5 million from fiscal year 2015 through the end of fiscal year 2016 to begin developing the Validated Online Lifecycle Threat and the associated threat library, and it plans to have the tool completed by the end of fiscal year 2017.

DIA officials reported that they had not effectively "marketed" the Validated Online Lifecycle Threat tool to its intended stakeholders and users. While Marine Corps officials stated that the threat modules can be updated in a shorter timeframe than a System Threat Assessment Report, officials from the Navy and the Army did not know that DIA intended the Validated Online Lifecycle Threat to be a dynamic system, and they stated that they believed the planned tool to be a static, online version of the System Threat Assessment Report. For example, Army officials stated that the tool may be less useful than its predecessor because it is composed of static modules that may not provide the same level of individualized detail. Though some Navy officials who provide intelligence support to acquisition programs indicated that they had received briefs and other information about the new tool, other Navy officials expressed concerns that the Validated Online Lifecycle Threat would not be customizable to programs and could, similar to the System Threat Assessment Report, include extensive information that was not program-specific and could therefore be as inefficient as the System Threat Assessment Reports. Air Force officials from the Joint Surveillance Target Attack Radar System Recapitalization acquisition program stated

that the Validated Online Threat Assessment tool was intended to alleviate resource constraints in the intelligence community, but that the tool was being implemented without input from the acquisition community and individual program management offices.

The Project Management Institute's *A Guide to the Project Management Body of Knowledge* states that managing stakeholders' engagement helps to increase the probability of project success by ensuring that stakeholders clearly understand the project goals, objectives, benefits, and risks.⁴² This enables stakeholders to be active supporters of the project and to help guide activities and project decisions. Federal internal control standards state that management should communicate quality information externally so that external parties can help the entity achieve its objectives and address related risks.⁴³ We found that some potential users of the Validated Online Lifecycle Threat report have not received information regarding the intended capabilities of the new system because DIA has not effectively communicated information about the tool with stakeholders and intended users. A communication plan would include processes for communicating the intended capabilities of the Validated Online Lifecycle Threat tool to stakeholders such as USD(AT&L) and USD(I) and users such as personnel who provide intelligence support to acquisition programs. Without effectively communicating such information to potential users, DIA may not receive useful feedback as it develops the tool, and concerns regarding timeliness, usability, and redundancy may not be effectively addressed.

⁴²Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, Fifth Edition (Newton Square, Pa: 2013).

⁴³[GAO-14-704G](#).

Users Have Not Expressed a Need or Defined Requirements for a Tool for Acquisition Programs to Communicate Their Intelligence Needs to the Intelligence Community

Officials from Performance Assessments and Root Cause Analyses, an office within USD(AT&L), are developing a tool for communication of intelligence needs from acquisition programs to the intelligence community, but intended users have not expressed a need or defined requirements for the tool. The office is responsible for conducting root-cause analyses of acquisition programs that encounter Nunn-McCurdy breaches, among other things.⁴⁴ According to these officials, the Assistant Secretary for Defense (Acquisitions) requested that the office perform an analysis of the root causes of challenges faced by the integration of intelligence into acquisitions. This analysis identified issues with threat intelligence and intelligence mission data and resulted in pilot projects of new tools such as the Validated Online Lifecycle Threat.

According to Performance Assessments and Root Cause Analyses officials, acquisition programs request intelligence both through informal means, such as conversations and emails, and through formal means via information systems, such as the Community On-Line Intelligence System for End Users and Managers.⁴⁵ These officials reported that the formal requests for intelligence often contain vague or inaccurate information and do not allow the intelligence community to prioritize or fulfill requests efficiently. Officials told us that to resolve this issue they are developing an online tool called the Acquisition Intelligence Support Assessment that would allow acquisition personnel to communicate intelligence needs to the intelligence community over an online system.

According to Performance Assessments and Root Cause Analyses officials, personnel providing intelligence support to acquisition programs will be able to access the online tool and determine whether particular threat intelligence is currently available. If it is not, requests can be made via the tool to the intelligence community, which would then use the

⁴⁴A Nunn-McCurdy breach occurs when a major defense acquisition program's unit cost exceeds certain thresholds. See 10 U.S.C. § 2433.

⁴⁵Community On-Line Intelligence System for End Users and Managers is an information management system managed by DIA for defense and intelligence community users from the United States, Australia, Canada, New Zealand, and the United Kingdom. Users can search for past or current intelligence, determine outstanding intelligence requests or requirements, and submit intelligence needs to a central system, which routes the request to the appropriate intelligence community production center. Requests are referred to as requests for information or production requests.

tracking capabilities planned for the tool to monitor requests from multiple programs, and assign staff and resources as necessary. Performance Assessments and Root Cause Analyses officials stated that this tool could also be useful for personnel with limited knowledge or familiarity with acquisition programs due to time and resource constraints. They also stated that it would be useful for the intelligence community to manage and prioritize intelligence requests from the acquisition community.

Officials from the office of Performance Assessments and Root Cause Analyses stated that they were independently developing the tool for the acquisition and intelligence communities before integrating it into existing processes. These officials stated that they chose this approach after conducting their root cause analysis and identifying challenges related to integrating intelligence into acquisition programs. DOD awarded contracts in August and December 2015 for the initial analysis and for commencing development of the communication tool for a cost of approximately \$1.1 million. Officials stated that they expected to spend in total about \$1.2 million, sourced from available operational funding within the Office of Performance Assessments and Root Cause Analyses.

While Performance Assessments and Root Cause Analyses has funded the development of the Acquisition Intelligence Support Assessment tool, these officials stated that there is currently no mechanism to fund future implementation and operation of the tool once fully developed, and they estimated that the system will cost \$3 million to \$5 million per year to operate. These officials reported that another office must be tasked to oversee the implementation of the tool, and suggested that the Acquisition Intelligence Requirements Task Force or a Joint Staff office might assume responsibility for the system. Officials from the task force have recommended that the task force evaluate whether the Acquisition Intelligence Support Assessment tool should be used or merged with existing tools, but no decision regarding the planned implementation or operation of the tool had been made as of July 2016.

Performance Assessments and Root Cause Analyses officials described several steps they had taken to introduce the tool to potential stakeholders, including holding demonstration events, working groups, and briefings. Specifically, these officials stated that they had introduced the Acquisition Intelligence Support Assessment tool to acquisition and intelligence stakeholders in October 2015 and June 2016, but service officials who are potential users of the tool told us that they had not identified a need for the tool. Air Force officials stated that they already track intelligence requests through existing information systems, and that

the new tool would likely duplicate existing processes. Officials from the Navy stated that the developmental nature of the tool prevents a full assessment of its strengths and weaknesses. Officials from the Army stated that they would wait until the tool is fully developed before deciding whether to use it, and officials from the Marine Corps stated that their input had not been solicited.

We have previously identified leading practices for increased collaboration among agencies, including defining and articulating a common outcome; agreeing on roles and responsibilities, and establishing compatible policies, procedures, and other means to operate across agency boundaries.⁴⁶ Given that acquisition and intelligence personnel have not identified requirements for the Acquisition Intelligence Support Assessment tool, it may not fulfill the needs of acquisition programs and the intelligence community or work as intended, and the services may prefer to use existing systems. As a result, DOD may use funds unnecessarily to develop a tool that is not needed. Further, without plans or funding for implementation and operation, the Acquisition Intelligence Support Assessment tool may not be fully implemented or sustained once operational.

Conclusions

DOD has long recognized the need to improve its process for the acquisition of major weapon systems, and it has recently undertaken efforts to improve intelligence input both during the acquisition process and, subsequently, to help enable weapon systems to more effectively perform their missions once deployed. For example, the department has worked to integrate intelligence into its acquisition program manager courses and has developed potential processes for prioritizing intelligence mission data needs. Addressing gaps we identified in several key areas will enable DOD to better leverage its efforts. First, without a department-wide certification process that includes training standards, DOD may not be able to ensure that all personnel who provide intelligence support to acquisition programs are familiar with and able to provide intelligence inputs to their portfolios of acquisition programs. Second, without specific requirements for intelligence mission data prioritization in DOD guidance, DOD may not be able to ensure that weapon systems have the data they

⁴⁶[GAO-06-15](#).

need to successfully perform their missions once operational. Third, potential users of DOD's planned Validated Online Lifecycle Threat report have not received information or provided feedback regarding the intended capabilities of the new tool because the DIA has not effectively communicated the intended capabilities to stakeholders and potential users. Without a communication plan, DIA may not receive useful feedback as it develops the system, and ongoing concerns regarding timeliness, usability, and redundancy of threat information may not be effectively addressed. Fourth, without conducting an assessment of the need for and defining requirements for development of its proposed Acquisition Intelligence Support Assessment tool, DOD may be using funds to unnecessarily develop a tool that is not needed or, if needed, may not be fully implemented or sustained once operational.

Recommendations for Executive Action

To enhance DOD's efforts to better integrate and improve intelligence support to major defense acquisition programs, we recommend that the Secretary of Defense direct—as appropriate—the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense for Intelligence; and/or the Secretaries of the military departments, to take the following four actions in coordination with one another:

- To better enable personnel to provide intelligence inputs to their portfolios of acquisition programs, establish certifications that include having these personnel complete required training.
- To facilitate implementation of improved processes and procedures developed by the Acquisition Intelligence Requirements Task Force and by the Air Force for the integration of intelligence into major defense acquisition programs, revise relevant guidance and procedures—including DOD Instruction 5000.02 and DOD Directive 5250.01—to require that intelligence mission data at the acquisition program, service, and department levels be prioritized.
- To better ensure that DOD obtains useful feedback from stakeholders and the intended users of the Validated Online Lifecycle Threat tool, instruct the Director of the Defense Intelligence Agency to develop a communication plan for the tool that includes plans for communicating with and obtaining feedback from stakeholders and intended users such as acquisition program offices and personnel providing intelligence support to acquisition programs.
- To ensure that it fulfills the needs of acquisition programs and the intelligence community and works as intended, assess the need for

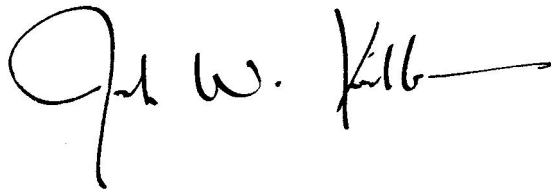
the Acquisition Intelligence Support Assessment tool and, if validated by this assessment, define this tool's requirements for development and identify the entity responsible for providing oversight and funding for its continued development, implementation, and operation.

Agency Comments and Our Evaluation

We provided a draft of this report to DOD for review and comment. DOD provided technical comments, which we incorporated as appropriate. DOD concurred with all four of our recommendations and the responses are reprinted in their entirety in appendix IV. Based on discussions with the department, we also revised our recommendations to more accurately characterize the relevant DOD organizations and offices.

We are sending copies of this report to the appropriate congressional committees; the Secretary of Defense; the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense for Intelligence; the Secretaries of the Air Force, Army, and Navy; and other interested parties. In addition, this report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-9971 or kirschbaumj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.



Joseph W. Kirschbaum
Director, Defense Capabilities and Management

List of Committees

The Honorable John McCain
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Richard Burr
Chairman
The Honorable Dianne Feinstein
Vice Chairman
Select Committee on Intelligence
United States Senate

The Honorable Thad Cochran
Chairman
The Honorable Richard J. Durbin
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Mac Thornberry
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

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

The Honorable Rodney Frelinghuysen
Chairman
The Honorable Pete Visclosky
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Information on DOD's Efforts to Assess the Intelligence-Gathering Capability of Weapon Systems beyond the Scope of Their Mission

We reviewed relevant acquisition-related processes and procedures and found that the Department of Defense (DOD) has no requirement to assess a weapon system's ability to gather intelligence beyond or outside the scope of its mission.

DOD officials we spoke with from Joint Staff, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), and the services indicated that there are no requirements for them to consider the ability of a system to gather intelligence beyond or outside the scope of its mission during the acquisition process, or otherwise, and that currently there were no plans to consider performing such assessments. Officials from the Army and Marine Corps indicated that this had not been considered because their services were generally focused on non-advanced weapons such as tanks that were ill-suited for this purpose. Air Force officials told us that current advanced weapon systems such as the B-2 and F-22, and future systems such as the F-35 have or will have the capability to gather intelligence outside and beyond the scope needed to perform their missions, but that there were not currently any plans to assess this capability during the acquisition process. These officials told us that these assessments may occur, such as for the non-traditional use of intelligence, surveillance, and reconnaissance systems, in the post-deployment period as opportunities and capabilities arise.

Officials from some of the service intelligence communities as well as from USD(AT&L) indicated that one of the challenges faced by current and future advanced weapon systems is the ability to store and then offload intelligence data in such a way as to be immediately useful to analysts in the intelligence community. Air Force officials we spoke with indicated that there have been efforts to make use of non-traditional intelligence, surveillance, and reconnaissance systems in the field as a way of gathering signals intelligence information, but that assessing this capability was not considered during the acquisition process.

Appendix II: Objectives, Scope, and Methodology

The National Defense Authorization Act for Fiscal Year 2016 includes a provision that we review the processes and procedures for the integration of intelligence into the defense acquisition process.¹ This report evaluates, for major defense acquisition programs, the extent to which DOD has (1) processes and procedures for certifying² and training personnel assigned to provide intelligence support to acquisition programs; (2) efforts to improve processes and procedures for integrating intelligence into its acquisition programs; and (3) efforts to develop new tools for integrating intelligence into its acquisition programs. We also collected information related to DOD's efforts to identify opportunities for weapon systems to collect intelligence even when unrelated to their primary mission, which is presented in appendix I.

To determine the extent to which DOD has processes and procedures for certifying and training of personnel assigned to provide intelligence support to acquisition programs, we reviewed DOD guidance governing the management of intelligence and acquisition personnel. We interviewed officials from the offices identified in this appendix who participate in the development of guidance and management of personnel providing intelligence support to acquisition. We submitted written requests for guidance regarding staffing, qualifications, certification, and training of personnel to these officials, and we reviewed their responses. We also interviewed and received written responses from officials from the Defense Acquisition University regarding changes to the acquisition curriculum that included additional intelligence material. We reviewed the certifications and qualifications DOD has established in implementing the Defense Acquisition Workforce Improvement Act, and other DOD guidance for the training and management of acquisition personnel, and Under Secretary for Intelligence (USD(I)) guidance related to certifications and qualifications for intelligence personnel.³ We reviewed training and

¹Pub. L. No. 114-92, § 1638 (2015).

²Certification is the procedure through which DOD components determine that an employee meets education, training, and experience elements for each career field.

³Department of Defense (DOD) Directive 5000.52, *Defense Acquisition, Technology, and Logistics Workforce Education, Training, and Career Development Program* (Jan. 12, 2005); DOD Instruction 5000.66, *Operation of the Defense Acquisition, Technology, and Logistics Workforce Education, Training, and Career Development Program* (Dec. 21, 2005); and DOD Instruction 3115.11, *DOD Intelligence Human Capital Management Operations* (Jan. 22, 2009) (incorporating change Dec. 9, 2011).

certification guidance for both acquisition personnel, as administered by USD(AT&L), and intelligence personnel, as administered USD(I), because interviews with DOD officials indicated that personnel who provide intelligence support to acquisition programs are managed by acquisition and intelligence components, depending on the service.

To determine the extent to which DOD has processes and procedures for the integration of intelligence into the acquisition of weapon systems, we reviewed department-level directives, instructions, and other guidance that governs intelligence input into the acquisition process. To identify additional processes specific to the military services, we interviewed officials from the offices identified in this appendix, and we submitted written requests for information in order to obtain the documents identified by these officials. To determine the validity of the document sources used to identify the intelligence inputs, we reviewed written responses from service acquisition and intelligence officials at the Army, Navy, Air Force, and Marine Corps to verify that the documents were current and in use by the respective services. To determine the extent to which ongoing DOD initiatives will address identified issues with acquisition and intelligence integration, we interviewed officials from offices identified in this appendix and requested documentation on the progress of intelligence-related tasks identified in USD(AT&L)'s Better Buying Power 3.0 initiatives. We also observed meetings of the Acquisition Intelligence Requirements Task Force, and we observed briefings from the task force to the Acquisition Intelligence Requirements Executive Steering Group. We also compared the proposed intelligence mission data prioritization processes with *Standards for Internal Control in the Federal Government*, which states that management should establish an organizational structure, assign responsibility, and delegate authority to achieve objectives.⁴

After receiving the documents, an analyst reviewed each document and identified actions (such as formation of a working group or certification), products (such as reports or data), or processes (such as an intelligence parameter breach or formal review) that could be considered as intelligence inputs required for an acquisition program classified by DOD

⁴GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept., 2014).

as Acquisition Category I.⁵ We defined an intelligence input as any action, process, or product that involved or included the participation of an intelligence professional and was provided for a specific acquisition program. The analyst categorized those inputs with similar names or document sources and then entered each category and input onto a spreadsheet. The intelligence inputs are provided in appendix III.

To verify our identification of intelligence inputs, we created a standard data collection instrument based on the spreadsheet of identified intelligence inputs. The data collection instrument asked respondents to identify, for Acquisition Category I programs initiated as of June 1, 2016, (1) when, if at all, each of the identified intelligence inputs would be used throughout an acquisition lifecycle; (2) whether their office would provide input into the item; (3) whether these inputs were required to be provided; and (4) to provide any comments or additional inputs, if necessary. We sent this data collection instrument to officials of the intelligence components of the Army, Navy, Air Force, and Marine Corps; the DIA; the Office of the Under Secretary of Defense for Intelligence; and the Joint Staff Directorate for Intelligence, J-2, for a total of seven responses. We selected these officials and organizations because document sources identified these organizations as providers of intelligence inputs, and thus the most likely to identify intelligence inputs. Data were reviewed by two analysts to ensure that all data were fully extracted and correctly tabulated.

To provide illustrative examples and determine how processes and procedures are implemented for individual acquisition programs, we selected a nongeneralizable sample of six major defense acquisition programs. We used a stratified purposeful sampling procedure in which

⁵DOD categorizes acquisition programs into Acquisition Categories I, IA, II, and III. Acquisition Category I programs are major defense acquisition programs, estimated by USD(AT&L) as requiring an eventual total expenditure for research, development, and test and evaluation of more than \$480 million in fiscal year 2014 constant dollars or, for procurement, of more than \$2.79 billion in fiscal year 2014 constant dollars, or those acquisitions that are designated as major defense acquisition programs or designated as Special Interest by USD(AT&L), the head of the DOD component, or the component acquisition executive. The Special Interest designation is typically based on one or more of the following factors: technological complexity; congressional interest; a large commitment of resources; or criticality of a program to the achievement of a capability or set of capabilities, part of a system of systems, or a joint program. See DOD Instruction 5000.02, *Operation of the Defense Acquisition System* (Jan. 7, 2015).

we intentionally chose acquisition programs with particular characteristics to capture both important similarities and variations. We selected from a population of acquisition programs identified by the Acquisition Intelligence Requirements Task Force as having significant intelligence needs. Two analysts then classified each program with characteristics using information from a GAO assessment of major defense acquisition programs, including whether the program was focused on warfare domains of land, air, or sea; and what service was primarily responsible for the program.⁶ We excluded space and satellite programs from selection due to the unique differences and higher security classifications of these programs, as compared with other major defense acquisition programs. Based on these characteristics, we then selected two Air Force programs, two Navy programs, one Army program, and one Marine Corps program. The programs included the following:

- Army, Armored Multi-Purpose Vehicle
- Navy, Ohio-Class Replacement
- Navy, Air and Missile Defense Radar
- Air Force, F-22 Increment 3.2B Modernization
- Air Force, Joint Surveillance Target Attack Radar System Recapitalization
- Marine Corps, CH-53K Heavy Lift Replacement Helicopter

We selected this number and distribution of acquisition programs because officials from the Air Force and Navy stated that they had many programs that used intelligence mission data, and officials from the Army and Marine Corps stated that they did not have many intelligence mission data-dependent programs. We submitted identical questions and requests for information to officials from each program management office, as well as individuals identified by the program as being personnel who provide intelligence input into the acquisition program. We discussed the questions orally or received written responses from officials and intelligence personnel from each program. While the responses we obtained are not generalizable to all major defense acquisition programs, the information obtained from program officials provided context and

⁶*Defense Acquisitions: Assessments of Selected Weapon Programs*, [GAO-16-329SP](#) (Washington, D.C.: Mar. 31, 2016).

important insights for our understanding of the interaction of acquisition and intelligence personnel.

To examine the extent to which DOD has efforts to develop new tools for integrating intelligence into acquisitions we identified two tools that were currently in development through discussions with Acquisition Intelligence Requirements Task Force officials. We verified that these tools were in development through interviews with officials involved in oversight of acquisitions and intelligence, including officials at USD(AT&L), USD(I), and DIA. We conducted a site visit to DIA's Technology and Long-Range Assessment offices in Charlottesville, Virginia, where we interviewed officials and observed a demonstration of a developmental version of the Validated Online Lifecycle Threat tool. We also interviewed officials from Performance Assessments and Root Cause Analyses, and we viewed a presentation and demonstration of a developmental version of the Acquisition Intelligence Support Assessment tool. We collected developmental plans and briefings for both of these tools, and we compared our observations and statements made by DIA and Performance Assessments and Root Cause Analyses officials against the documents, and against statements from acquisition, intelligence, and program management office officials. We compared the developmental plans and information provided to us by DIA and Performance Assessments and Root Cause Analyses officials against standards in the Project Management Institute's *A Guide to the Project Management Body of Knowledge*,⁷ federal standards for internal controls,⁸ and key practices for collaboration among federal agencies.⁹

To examine DOD's processes and procedures for assessing during the acquisition process a weapon system's ability to gather intelligence when unrelated to its primary mission, we reviewed DOD reports and guidance for acquisition management identified for the previous objectives. We systematically reviewed the content of these documents for any information relevant to assessing during the acquisition process a

⁷Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*, Fifth Edition, 2013.

⁸[GAO-14-704G](#).

⁹*Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, [GAO-06-15](#) (Washington, D.C.: Oct. 21, 2005).

system's ability to gather intelligence. We were unable to identify any process or procedure relevant to this objective. To confirm this finding, we interviewed acquisitions, intelligence, and requirements professionals from offices identified in this appendix. Further details are provided in appendix I.

We obtained relevant documentation and interviewed officials from the following organizations:

- Office of Under Secretary of Defense for Intelligence;
- Office of Under Secretary of Defense for Acquisition, Technology, and Logistics
- Office of Performance Assessments and Root Cause Analyses;
- Director of Operational Test and Evaluation;
- Cost Assessment and Program Evaluation;
- Acquisition Intelligence Requirements Task Force and Executive Steering Group;
- Defense Intelligence Agency;
- Defense Acquisition University;
- U.S. Army;
- U.S. Navy;
- U.S. Marine Corps;
- U.S. Air Force;
- Joint Staff; and
- Office of the Director of National Intelligence

We conducted this performance audit from December 2015 to November 2016 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.

Appendix III: Intelligence Inputs in the Defense Acquisition Process

We defined intelligence input in this report as any action, process, or product that involved or included the participation of an intelligence professional and was provided for a specific acquisition program, and we then grouped the intelligence inputs we identified by inputs with similar names, document sources, or categories. To confirm our appropriate identification of intelligence inputs, we created a data collection instrument based on the spreadsheet of identified intelligence inputs. The instrument asked respondents to identify, for an Acquisition Category I program initiated as of June 1, 2016, (1) when, if at all, each of the identified intelligence inputs would be used throughout its acquisition lifecycle; (2) whether their office would provide input for each entry we identified; (3) whether these inputs are required to be provided; and (4) to provide any comments or additional inputs, if necessary.

For programs begun prior to Milestone A, the intelligence inputs that we identified from a review of DOD's acquisition-related guidance are to be provided prior to Milestone A review, with several updated at points prior to subsequent milestone reviews. The responses to our data collection instrument from the Joint Staff, USD(I), DIA, and the service intelligence community indicated that each intelligence input we identified had one or more respondent reporting that the respondent's office would make that input, which verified the individual inputs we identified (see table 3). DIA, and Army also remarked that the Validated Online Lifecycle Threat report will replace the Capstone Threat Assessment, and DIA, the Air Force, and the Army remarked that the Validated Online Lifecycle Threat report will replace the System Threat Assessment Report. We have noted that these inputs are to be phased out once the Validated Online Lifecycle Threat is operational.

The responses regarding when the identified intelligence inputs would be used throughout the lifecycle varied among the respondents, but every input had one or more respondent reporting that the input would be made prior to Milestone A. We attribute this variance to different interpretations of inputs that do not align with every milestone, such as threat-related inputs that occur prior to Milestone A and then are continuously monitored for changes; or to inputs that are made through groups that meet on a schedule independent of acquisition milestones. The responses to the data collection instrument regarding whether each input is required to be provided for every Acquisition Category I also varied.

The threat assessment and validation category of inputs represent direct inputs from the intelligence community into acquisition programs. Others, such as Critical Intelligence Parameter and Critical Program Information,

are foreign threat factors monitored by the intelligence community for changes that may impact an acquisition program. For the other categories of input, the intelligence community provides varying degrees of direct and indirect inputs into the acquisition process. On some of the responses to our data collection instrument, the respondents provided comments that indicated they were not familiar with the input, and on the others, we attribute the variance to different understandings of guidance among the respondents.

Table 3: Intelligence Inputs in the Defense Acquisition Process

Input	Description of Input	DOD Intelligence Organization(s) Providing Input, as of July 2016
Threat Intelligence Support	Threat intelligence support to the acquisition process provides an understanding of foreign threat capabilities that is integral to the development of future U.S. military systems and platforms. Identifying projected adversarial threat capabilities, to include scientific and technical developments that may affect a program's or a capability's design or implementation is crucial to a successful development process.	
System Threat Assessment Report ^a	An authoritative, system-specific threat assessment report must be validated by the Defense Intelligence Agency (DIA) for Acquisition Category ID programs. A validated System Threat Assessment Report is required at program initiation for shipbuilding programs and Milestone A for other programs, and updated at the development request for proposals release decision point, Milestone C, and the full-rate production decision or full deployment decision point.	DIA, Service Intelligence Centers
Validated Online Lifecycle Threat ^b	This is a planned system-specific threat summary that a threat analyst creates by selecting relevant modules from a library of threat information.	DIA, Service Intelligence Organizations
Capstone Threat Assessment ^a	This input provides the analytic foundation for intelligence support to the defense acquisition process. It projects foreign capabilities in particular warfare areas out 20 years in the future. These assessments constitute the primary source of threat intelligence for the preparation of System Threat Assessment Reports and for the threat portions of documents supporting the requirements development process. These assessments are maintained by the responsible production center and must be updated every 2 years, independent of acquisition decision events.	DIA, Service Intelligence Centers
Threat Steering Group	This is co-chaired by the Service Intelligence Centers and DIA. Intelligence production centers, commands, and offices supporting system acquisition programs requiring DIA-validated threats are required to convene Threat Steering Groups during the System Threat Assessment Report or Capstone Threat Assessment production process.	DIA, Service Intelligence Centers

Appendix III: Intelligence Inputs in the Defense Acquisition Process

Input	Description of Input	DOD Intelligence Organization(s) Providing Input, as of July 2016
Threat Review and Intelligence Certification	Intelligence certification is required for capability requirement documents for certain programs to ensure that the system and protection threats remain valid, and that changes within the intelligence community will still support program development. Performed by the Joint Staff J283/Intelligence Requirements Certification Office and valid until the next acquisition milestone or for 2-years, depending on the circumstances. The intelligence certification granted for a requirements document in support of Milestone C sets the baseline for intelligence mission data production requirements for operation of the system once deployed.	DIA/Joint Staff (Intelligence Requirements Certification Office) ^c
Intelligence Mission Data Support	Intelligence mission data are essential data for building system models, developing algorithms, optimizing sensor design, system testing, and evaluation, and validating sensor functionality. Functional areas and categories of intelligence mission data include but are not limited to Characteristics and Performance, Electronic Warfare Integrated Reprogramming, Geospatial Intelligence, Order of Battle, and Signatures (Radar, Thermal, and Acoustic).	
Life-cycle Mission Data Plan	This plan is a statement of program needs that is applied throughout the life of an intelligence mission data-dependent acquisition program and potentially influences programmatic decisions based on the availability of the data over the life of the program.	DIA/Intelligence Mission Data Center, Service Intelligence Centers
Intelligence Certification Working Group	The group convenes monthly, or as required, to address intelligence mission data, intelligence supportability, and threat assessment issues in support of intelligence certification. DIA/Joint Staff (Intelligence Requirements Certification Office) convenes Intelligence Certification Working Group, composed of the defense intelligence components and other agencies, as required, to facilitate review, coordination, and recommendations for intelligence supportability.	Defense Intelligence Components
Capability Requirement Documents Review	Capability Requirement Documents are used to articulate capability requirements, which are capabilities required to meet an organization's roles, functions, and missions in current or future operations. If a capability requirement is not satisfied by a capability solution, there is also an associated capability gap.	DIA/Joint Staff (Intelligence Requirements Certification Office)
Intelligence Certification of Intelligence Mission Data Requirements	Review and intelligence certification will be conducted as part of validation of each capability requirement document, in support of each acquisition decision point.	DIA/Joint Staff (Intelligence Requirements Certification Office)
Critical Intelligence Parameter Support	This is a threat capability or threshold established by the program manager, changes to which could critically affect the effectiveness and survivability of the proposed system. Critical Intelligence Parameters may be included in capability requirement documents and System Threat Assessment Reports.	

**Appendix III: Intelligence Inputs in the Defense
Acquisition Process**

Input	Description of Input	DOD Intelligence Organization(s) Providing Input, as of July 2016
Critical Intelligence Parameter Breach Notification	These are made to appropriate departmental offices and entities when the supporting military Service Intelligence Center determines that an approved Critical Intelligence Parameter has been breached and the acquisition program office(s) will be impacted by the breach.	Service Intelligence Centers
Critical Intelligence Parameter Breach Review	This review is a collaborative assessment of the relationship between changes to an approved Critical Intelligence Parameter and associated threat-dependent capability requirements that have been validated.	Service Intelligence Centers
Acquisition Oversight		
Defense Acquisition Board	This is DOD's senior-level forum for advising the Under Secretary of Defense for Acquisition, Technology, and Logistics on critical decisions concerning Acquisition Category ID programs, and selected Acquisition Category IA programs.	National Geospatial Intelligence Agency (advisory) and others by invitation from USD(AT&L)
Counterintelligence and Program Protection		
Supply Chain Risk Management	This is a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout DOD's "supply chain" and developing mitigation strategies to combat those threats. It includes managing and producing Supply Chain Threat Assessments that provide an analytical foundation for counterintelligence support to supply chain risk management.	DIA
Affordability Analysis		
Affordability Analysis	This analysis is part of the long-range planning and decision making that determines the resources a component can allocate for each new capability by ensuring that the total of all such allocations— together with all other fiscal demands that compete for resources in the component—are not above the component's future total budget projection for each year.	Service Intelligence Organizations
Joint Capability Requirements Development, Review, and Certification		
Initial Capability Document, Capability Development Document, and Capability Production Document reviews	J283/ Intelligence Requirements Certification Office review and intelligence certification will be conducted as part of validation of each capability requirement document, in support of each acquisition decision point – i.e., the Initial Capability Document for Milestone A, the Capabilities Development Document for the developmental Request for Proposal release decision point before Milestone B, and the Capability Production Document for Milestone C.	DIA/Joint Staff (Intelligence Requirements Certification Office)

Appendix III: Intelligence Inputs in the Defense Acquisition Process

Input	Description of Input	DOD Intelligence Organization(s) Providing Input, as of July 2016
Intelligence Supportability	Supportability refers to the availability, suitability, and sufficiency of intelligence support required by a capability. Categories of support include Intelligence Manpower, Intelligence Resources, Intelligence Planning and Operations, Targeting, Intelligence Mission Data, Warning, Space Intelligence, Counterintelligence, and Intelligence Training.	
Intelligence Supportability Review Prior to Granting Intelligence Certification	This is performed to ensure that intelligence requirements have been identified at the earliest possible point, and that all likely intelligence support requirements and shortfalls (if applicable) have been documented.	DIA/Joint Staff (Intelligence Requirements Certification Office)
Intelligence Support Requirements	Intelligence support requirements will be reviewed by subject matter experts from DOD and service intelligence organizations for supportability prior to granting intelligence certification. Sponsors are to engage their supporting intelligence entities at the earliest stages of development to ensure understanding of the requirements to be levied against the intelligence community.	DOD and Service Intelligence Organizations
Testing and Evaluation	This is the process by which a system or components are exercised and results are analyzed to provide performance-related information. The information has many uses, including risk identification, risk mitigation, and the creation of empirical data to validate models and simulations. Testing and Evaluation enables an assessment of the attainment of technical performance, specifications, and system maturity to determine whether systems are operationally effective, suitable and survivable for intended use, and/or lethal.	
Testing and Evaluation Master Plan	This plan documents the overall structure and objectives of the Test and Evaluation program and articulates the necessary resources to accomplish each phase of test. It provides a framework within which to generate detailed Testing and Evaluation plans and documents schedule and resource implications associated with the program.	DIA (determination of operational threat environment)
Testing and Evaluation Working Level Integrated Product Team	The team develops and tracks the Testing and Evaluation program in all phases. The integrated product team will include empowered representatives of test data stakeholders such as Systems Engineering; Developmental, Operational, and Live Fire Testing and Evaluation; Product Support; the user; intelligence community; and certification authorities.	Intelligence Community (unspecified)

Source: GAO analysis of DOD information. | GAO-17-10

^aTo be phased out when the Validated Online Lifecycle Threat is operational.

^bThe Validated Online Lifecycle Threat is under development by DIA as of July 2016.

^cIntelligence Requirements Certification Office supports J-2, the intelligence component of the Joint Staff, and is composed of personnel from Joint Staff and DIA.

During our review of DOD guidance to identify intelligence inputs into acquisition programs throughout the acquisition lifecycle we identified the

following key guidance documents for providing intelligence support to acquisition programs:

- DOD Directive 5000.01: *The Defense Acquisition System*, issued May 12, 2003, provides management principles and mandatory policies and procedures for managing all acquisition programs, along with DOD Instruction 5000.02. This directive notes that intelligence and the understanding of threat capabilities are integral to system development and acquisitions decisions, and that program managers are to keep threat capabilities current and validated in program documents throughout the acquisition process.
- DOD Instruction 5000.02: *Operation of the Defense Acquisition System*, issued January 7, 2015, provides the detailed procedures that guide the operation of the Defense Acquisition System. Regarding intelligence inputs into the acquisition process, among others, the guidance identifies the requirement for a Lifecycle Mission Data Plan for acquisition programs dependent upon intelligence mission data.¹ Additionally, the guidance describes the need to consider threat projections in the context of Analyses of Alternatives. It further notes that affordability analysis should involve a DOD component's intelligence and acquisition communities. Finally, DOD Instruction 5000.02 lists requirements for a number of intelligence inputs, such as Capstone Threat Assessments, Initial Threat Environment Assessments, System Threat Assessment Reports, and Technology Targeting Risk Assessments. According to DOD officials, several of these inputs are being phased out.
- DOD Directive 5250.01: *Management of Intelligence Mission Data (IMD) in DOD Acquisition*, issued January 22, 2013, establishes policies and assigns responsibilities to provide linkages between the management, production, and application of DOD intelligence mission data and accommodation of intelligence mission data in the acquisition process. It helps to synchronize the acquisition,

¹DOD guidance describes an intelligence mission data-dependent program as any acquisition program that will require intelligence mission data, such as programs that carry out combat identification, intelligence, surveillance, and reconnaissance, and targeting using information including, but not limited to, signatures, electronic warfare integrated reprogramming, order of battle, characteristics and performance, and geospatial intelligence. DOD Directive 5250.01, *Management of Intelligence Mission Data (IMD) in DOD Acquisition*, at 13 (Jan. 22, 2013).

intelligence, and requirement communities regarding intelligence integration into the requirements process and acquisition life cycle. According to Acquisition Intelligence requirements Task Force officials, this directive is currently under revision.

- Chairman of the Joint Chiefs of Staff Instruction 5123.01G: *Charter of the Joint Requirements Oversight Council (JROC)*, issued February 12, 2015, implements the Joint Requirements Oversight Council, established by statute, which supports the Chairman of the Joint Chiefs of Staff in carrying out the duties of the principal military advisor to the President, National Security Staff, and Secretary of Defense, among other functions.² This instruction notes that the Secretary of Defense has designated the Under Secretary of Defense for Intelligence as one of the advisors to the Council, and identifies the Director of the Joint Staff Directorate for Intelligence as an advisor on intelligence supportability and intelligence interoperability issues, among other things.
- *Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS)*, issued February 12, 2015 (including changes through December 18, 2015): The manual provides detailed guidelines and procedures for the Joint Capabilities Integration and Development System, and describes interactions of that process with several other departmental processes. Among other things, the manual contains a content guide for intelligence supportability, providing general descriptions of categories of intelligence support, to assist with the identification of intelligence support requirements and sufficiency or risk of shortfalls in intelligence infrastructure required to support a proposed potential acquisition program throughout its lifecycle. The manual indicates that in cases where the intelligence support requirements exceed the intelligence community's ability to provide support, resources required to augment the intelligence support must be accounted for in program affordability documentation. Categories of intelligence support listed in the manual include intelligence manpower support, intelligence resource support, intelligence planning and operations support, targeting support, and intelligence mission data support, among others. Intelligence manpower support is to be addressed where the proposed acquisition

²Section 181 of Title 10, U.S. Code, establishes the Joint Requirements Oversight Council and describes its mission and composition.

will require intelligence personnel for development, testing, training, or operation. In some circumstances, the category may address necessary manpower changes or specific required skills. Intelligence resource support is to be addressed if the proposed acquisition or supporting efforts will require or depend upon intelligence funding.

- *Defense Acquisition Guidebook*: The Defense Acquisition University maintains this DOD best practice guide, which complements DOD Directive 5000.01 and DOD Instruction 5000.02. Chapter 8 – Intelligence Analysis Support to Acquisition—describes various aspects of providing intelligence support to acquisition programs such as threat intelligence support and signature and other intelligence mission data support. The Defense Acquisition Guidebook is currently under revision, according to Acquisition Intelligence Requirements Task Force officials.
- Defense Intelligence Agency Instruction 5000.002, *Intelligence Threat Support for Major Defense Acquisition Programs*, issued February 1, 2013: Referenced in guidance such as DOD Instruction 5000.02, the DIA instruction assigns responsibilities and establishes procedures for DIA and DOD components to provide intelligence threat support for major defense acquisition programs.

Appendix IV: Comments from the Department of Defense



INTELLIGENCE

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

OCT 06 2016

Mr. Joseph Kirschbaum
Director, Defense Capabilities Management
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Mr. Kirschbaum,

Attached please find the Department of Defense (DoD) response to the GAO Draft Report GAO-17-10, "DEFENSE INTELLIGENCE: Additional Steps Could Better Integrate Intelligence Input into DoD's Acquisition of Major Weapon Systems," dated August 19, 2016 (GAO Code 100507). We concur with the GAO findings and their four recommendations.

My point of contact is Ms. Joyce Grant at 703-695-4320 or via email at joyce.j.grant.civ@mail.mil.

Sincerely,

Todd R. Lowery
Performing Duties of Principal Deputy Under
Secretary of Defense for Intelligence

Attachments:
As stated



GAO Draft Report Dated August 19, 2016

GAO-17-10 (GAO CODE 100507)

**“DEFENSE INTELLIGENCE: ADDITIONAL STEPS COULD BETTER INTEGRATE
INTELLIGENCE INPUT INTO DOD’S ACQUISITION OF MAJOR WEAPON
SYSTEMS”**

**DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION**

Recommendations for Executive Action

To enhance DoD’s efforts to better integrate and improve intelligence support to major defense acquisition programs, GAO recommends that the Secretary of Defense direct—as appropriate—the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense for Intelligence; and/or the Secretaries of the military departments, to take the following four actions in coordination with one another:

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense, to better enable personnel to provide intelligence inputs to their portfolios of acquisition programs, establish certification(s) that includes these personnel completing required training.

DoD RESPONSE: The Department concurs.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense, to facilitate implementation of improved processes and procedures developed by the Acquisition Intelligence Requirements Task Force and by the Air Force for the integration of intelligence into major defense acquisition programs, revise relevant guidance and procedures—including DoD Instruction 5000.02 and DOD Directive 5250.01—to require that intelligence mission data at the acquisition program, service, and department levels be prioritized.

DoD RESPONSE: The Departments concurs.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense, to better ensure that DOD obtains useful feedback from stakeholders and the intended users of the Validated Online Lifecycle Threat tool, instruct the Director of the Defense Intelligence Agency to develop a communication plan for the tool that includes plans for communicating with and obtaining feedback from stakeholders and intended users such as acquisition program offices and personnel providing intelligence support to acquisition programs.

DoD RESPONSE: The Department concurs.

RECOMMENDATION 4: The GAO recommends that the Secretary of Defense, to ensure that it fulfills the needs of acquisition programs and the intelligence community and works as intended, assess the need for the Acquisition Intelligence Support Assessment tool and, if validated by this assessment, define this tool’s requirements for development and identify the

entity responsible for providing oversight and funding for its continued development, implementation, and operation.

DoD RESPONSE: The Department concurs.

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Joseph W. Kirschbaum (202) 512-9971 or kirschbaumj@gao.gov

Staff Acknowledgments

In addition to the contact named above, GAO staff who made contributions to this report include Brian Mazanec, Assistant Director; Scott Behen, Pat Donahue, Ben Emmel, Amie Lesser, Jason Lyuke, C. James Madar, Ronald Schwenn, Michael Shaughnessy, and Cheryl Weissman.

Appendix VI: Accessible Data

Agency Comment Letter

Department of Defense,
Office of the Under
Secretary of Defense

Mr. Joseph Kirschbaum

Director, Defense Capabilities Management

U.S. Government Accountability Office 441 G Street, NW

Washington DC 20548 Dear Mr. Kirschbaum,

Attached please find the Department of Defense (DoD) response to the GAO Draft Report GA0-17-10, "DEFENSE INTELLIGENCE: Additional Steps Could Better Integrate Intelligence Input into DoD's Acquisition of Major Weapon Systems," dated August 19, 2016 (GAO Code 100507). We concur with the GAO findings and their four recommendations.

My point of contact is Ms. Joyce Grant at 703-695 -4320 or via email at joyce.j.grant.civ@mail.mil.

Performing Duties of Principal Deputy Under Secretary of Defense for Intelligence

Attachments: As stated

GA0-17-10 (GAO CODE 100507)

"DEFENSE INTELLIGENCE: ADDITIONAL STEPS COULD BETTER INTEGRATE INTELLIGENCE INPUT INTO DOD'S ACQUISITION OF MAJOR WEAPON SYSTEMS"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO
RECOMMENDATION

Recommendations for Executive Action

To enhance DoD's efforts to better integrate and improve intelligence support to major defense acquisition programs, GAO recommends that the Secretary of Defense direct-as appropriate- the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary

Page 1

Page 2

of Defense for Intelligence; and/or the Secretaries of the military departments, to take the following four actions in coordination with one another:

RECOMMENDATION 1:

The GAO recommends that the Secretary of Defense, to better enable personnel to provide intelligence inputs to their portfolios of acquisition programs, establish certification(s) that includes these personnel completing required training.

DoD RESPONSE: The Department concurs.

RECOMMENDATION 2:

The GAO recommends that the Secretary of Defense, to facilitate implementation of improved processes and procedures developed by the Acquisition Intelligence Requirements Task Force and by the Air Force for the integration of intelligence into major defense acquisition programs, revise relevant guidance and procedures-including DoD Instruction 5000.02 and DOD Directive 5250.01-to require that intelligence mission data at the acquisition program, service, and department levels be prioritized.

DoD RESPONSE: The Departments concurs.

RECOMMENDATION 3:

The GAO recommends that the Secretary of Defense, to better ensure that DOD obtains useful feedback from stakeholders and the intended users of the Validated Online Lifecycle Threat tool, instruct the Director of the Defense Intelligence Agency to develop a communication plan for the tool that includes plans for communicating with and obtaining feedback from stakeholders and intended users such as acquisition program offices and personnel providing intelligence support to acquisition programs.

DoD RESPONSE: The Department concurs.

RECOMMENDATION 4:

The GAO recommends that the Secretary of Defense, to ensure that it fulfills the needs of acquisition programs and the intelligence community and works as intended, assess the need for the Acquisition Intelligence

Page 3

Support Assessment tool and, if validated by this assessment, define this tool's requirements for development and identify the

entity responsible for providing oversight and funding for its continued development, implementation, and operation.

DoD RESPONSE: The Department concurs.

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 GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

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, <http://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 [E-mail Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@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

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