United States Government Accountability Office

Report to the Ranking Member, Committee on Homeland Security, House of Representatives

June 2023

COUNTERTERRORISM

Action Needed to Further Develop the Information Sharing Environment

Accessible Version

GAO-23-105310

GAO Highlights

Highlights of GAO-23-105310, a report to the Ranking Member, Committee on Homeland Security, House of Representatives.

June 2023

COUNTERTERRORISM

Action Needed to Further Develop the Information Sharing Environment

Why GAO Did This Study

Evolving terrorist threats, such as those posed by lone offenders and those who are radicalized online, highlight the continued need for effective information sharing between the federal government and its non-federal partners. In 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act, which required the President to establish and develop the ISE. The ISE Implementation Plan has guided federal efforts in this area.

GAO was asked to review federal efforts related to the ISE Implementation Plan. This report examines, among other things, the extent to which agencies took action to complete the plan's objectives. GAO reviewed agency documents and interviewed ODNI, DHS, DOJ and White House officials about their implementation efforts. GAO assessed these efforts against statutory provisions.

What GAO Recommends

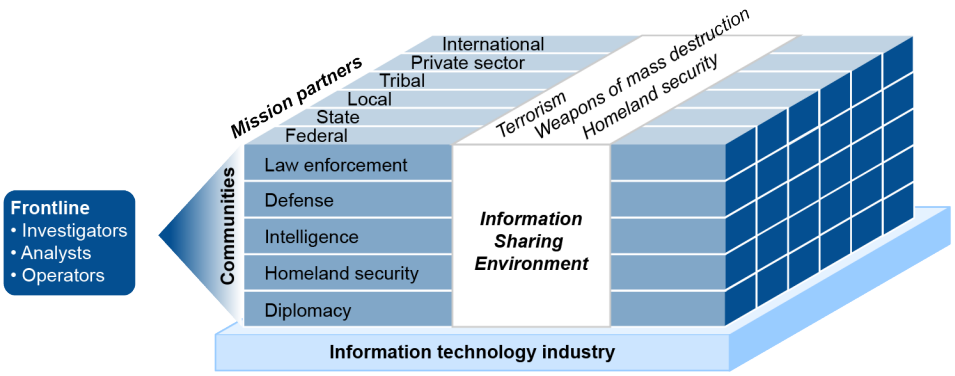
Congress should consider amending the ISE's enabling statute to clarify authorities for filling the Program Manager position. In addition, GAO is recommending that the Assistant to the President for Homeland Security and Counterterrorism take steps to ensure that (1) a Program Manager is in place and (2) implementation efforts are assessed. The Executive Office of the President

View GAO-23-105310. For more information, contact Triana McNeil at (202) 512-8777 or McNeilT@gao.gov.

What GAO Found

The Information Sharing Environment (ISE) is a framework to improve terrorism-related information sharing among federal and non-federal partners (i.e., Tribal, state, local, territorial, and private sector partners) through policy guidelines, common standards, and technologies. In 2013, federal officials developed an implementation plan that identified 16 priority objectives (e.g., develop baseline sharing capabilities) needed to implement the framework. As of 2017, federal agencies—including the Office of the Director of the National Intelligence (ODNI), Department of Homeland Security (DHS), and Department of Justice (DOJ)—had completed all but three of the 16 priority objectives.

The Information Sharing Environment



Source: Office of the Program Manager for the Information Sharing Environment. | GAO-23-105310

Text of The Information Sharing Environment

Information technology industry:

- **Frontline**:
  - Investigators
  - Analysts
  - Operators
- **Communities**: (information sharing environment)
  - Law enforcement
  - Defense
  - Intelligence
  - Homeland Security
  - Diplomacy

- **Mission Partners**:
  - Federal
  - State
  - Local
  - Tribal
  - Private sector
  - International

Source: Office of the Program Manager for the Information Sharing Environment. | GAO-23-105310

GAO found that agencies have implemented ISE-related projects to complete the three remaining priority objectives since 2017. However, since that time, there has not been a Program Manager to guide and assess those efforts. Assessing agencies' progress with the ISE is a statutory responsibility of the Program Manager. Without someone in this position to assess agency efforts, how much work is needed to complete the ISE Implementation Plan's' remaining objectives remains undetermined.

GAO also identified recent amendments to the statute establishing the ISE that, according to White House and ODNI officials, have complicated efforts to name a new ISE Program Manager. Clarifying that the President has full statutory authority to fill the Program Manager position would help ensure that a new Program Manager is named to continue work on the ISE Implementation Plan and broader federal terrorism information sharing goals.

Contents

Tables

Figures

Abbreviations

DOJ	Department of Justice
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
ISE	Information Sharing Environment
ODNI	Office of the Director of National Intelligence

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

June 26, 2023

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

Dear Mr. Thompson:

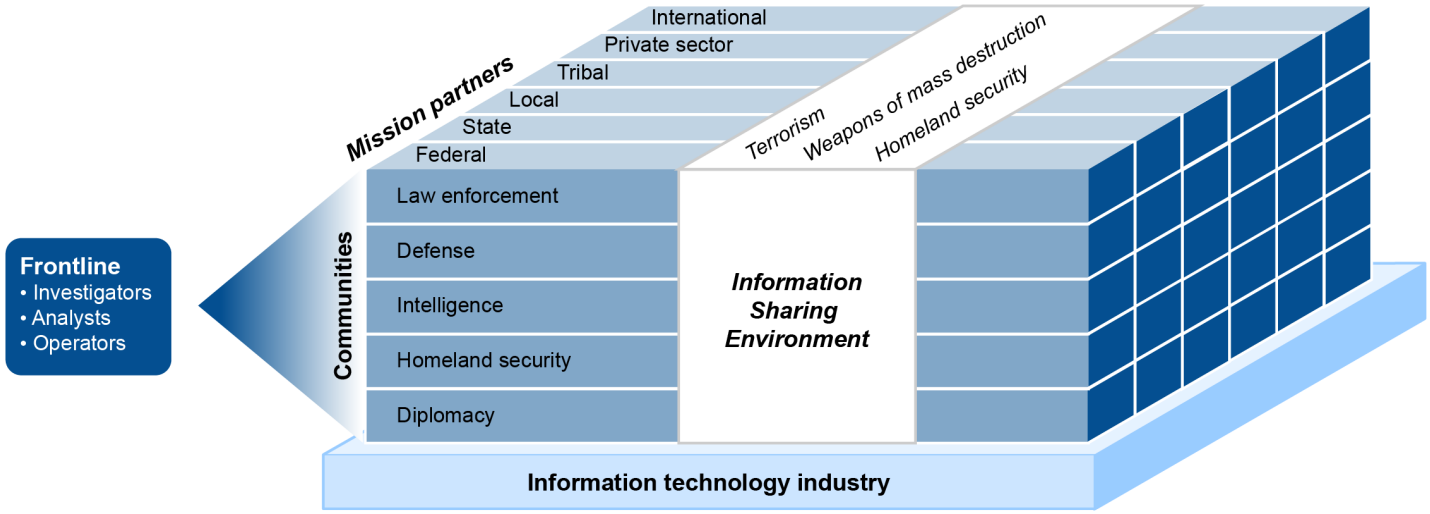
In the 20 years since the terrorist attacks of September 11, 2001, the threats related to international and domestic terrorism have significantly evolved. According to a 2021 federal government assessment, the greatest terrorist threat comes from lone offenders, often radicalized online, who are motivated and inspired by political goals and personal grievances against their targets.[1] These threats highlight the continued need for collaboration and coordination between federal agencies and their non-federal partners, including tribal, state, local, and territorial governments, and the private sector, to ensure the timely sharing of intelligence.

One effort to promote such collaboration and coordination is the Information Sharing Environment (ISE), a framework which provides and facilitates the sharing of terrorism-related information among federal and non-federal partners (see fig. 1). The ISE framework relies on the use of policy guidelines, common standards, and various technologies.[2]

[1]Federal Bureau of Investigation and Department of Homeland Security, *Strategic Intelligence Assessment and Data on Domestic Terrorism* (Washington, D.C.: May 2021).

[2]Specifically, the ISE is an approach that facilitates the sharing of information on terrorism, weapons of mass destruction, and homeland security, each of which has its own statutory definition. See 6 U.S.C. § 482(f)(1), 485(a)(1), (3), (5)-(6). To capture these three types of information, and other information that may be relevant to terrorism, we use the term "terrorism-related information" (or, as applicable, "domestic terrorism-related information") for the purposes of this report. In addition, terrorism-related information shared can be either classified, sensitive, or public information.

Figure 1: The Information Sharing Environment



Source: Office of the Program Manager for the Information Sharing Environment. | GAO-23-105310SU

Text of Figure 1: The Information Sharing Environment

Information technology industry:

- **Frontline**:
  - Investigators
  - Analysts
  - Operators
- **Communities**: (information sharing environment)
  - Law enforcement
  - Defense
  - Intelligence
  - Homeland Security
  - Diplomacy
- **Mission Partners**:
  - Federal
  - State
  - Local

- Tribal
- Private sector
- International

Source: Office of the Program Manager for the Information Sharing Environment. | GAO-23-105310

In 2004, Congress passed a law requiring the President to establish the ISE.[3] The law was one of several measures taken by Congress and the executive branch to strengthen the nation's ability to identify, detect, and deter terrorism-related activities. In 2013, federal officials developed a plan to guide federal efforts to establish the ISE (ISE Implementation Plan) that identifies 16 priority objectives, or activities, needed to achieve the ISE.[4] Officials aligned the ISE Implementation Plan and its associated objectives with five strategic goals identified within the 2012 *National Strategy for Information Sharing and Safeguarding*, an executive initiative intended to promote secure and responsible national security information sharing.[5] Therefore, agencies' progress with the ISE Implementation Plan also advances goals within the 2012 Strategy.

In 2005, we designated terrorism-related information sharing as high risk because the government faced significant challenges analyzing and disseminating this information effectively among government and private sector partners. Based on the significant progress key departments and agencies made to strengthen information sharing, including efforts to complete the ISE Implementation Plan, we removed terrorism-related

[3]Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, tit. I, subtit. A, § 1016, 118 Stat. 3638, 3664-70 (codified, as amended, at 6 U.S.C. § 485).

[4]*Strategic Implementation Plan for the National Strategy for Information Sharing and Safeguarding* (Washington, D.C.: 2013). Examples of the priority objectives described in the ISE implementation plan include governance (aligning information sharing and safeguarding governance to foster better decision-making, performance, and accountability); safeguarding (implementing safeguarding capabilities to support information sharing); and interoperability (defining and adopting baseline capabilities and common requirements to enable data, service, and network interoperability).

[5]The strategic goals of the 2012 strategy included improving information discovery and access through common standards; optimizing mission effectiveness through shared services and interoperability; and strengthening information safeguarding through structural reform, policy, and technical solutions.

information sharing from our High-Risk List in February 2017.[6] While these cumulative efforts met the criteria for removal from the High-Risk List, there were three key ISE priority objectives for which efforts were in progress when we last reported on this issue.[7]

You asked us to review the status of the ISE Implementation Plan and agency activities to share terrorism information. This report examines: (1) the extent to which actions have been taken since 2017 to complete the ISE Implementation Plan, including any assessments of progress that have been conducted; and (2) the mechanisms that the Department of Homeland Security (DHS), the Department of Justice (DOJ), and the Office of Director of National Intelligence (ODNI) use to share terrorism-related information with non-federal partners, including information on domestic terrorism and other threats.

To address our first objective, we focused our analysis on the efforts of DHS, DOJ—particularly the Federal Bureau of Investigation (FBI) within DOJ—and ODNI to complete the three priority objectives from the ISE Implementation Plan that were not yet fully implemented by the end of fiscal year 2016, when we last reviewed the program.[8] We reviewed documentation to describe these incomplete, or open, priority objectives, their role and function within the ISE, and how their implementation may improve the sharing of information with non-federal partners.[9] We analyzed documents provided by DHS, DOJ, and ODNI on the status of the open priority objectives. This documentation included ISE

[6]Specifically, we removed "establishing effective mechanisms for sharing and managing terrorism-related information to protect the homeland" from the High-Risk List; we use the phrase "terrorism-related information sharing" to refer to the aforementioned high-risk area. See GAO, *Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

[7]See GAO-17-317. We describe these three priority objectives (Data Tagging; Federal Identity, Credential, and Access Management; and Discovery and Access) later in the report.

[8]The key departments and agencies that are critical to implementing and sustaining the ISE—in addition to DHS, DOJ, and ODNI—include the Departments of State and Defense. This report focuses on DHS, DOJ, and ODNI efforts because these are the agencies that have a role in sharing terrorism-related information with non-federal partners. In addition, DHS and FBI maintain numerous offices and advisory groups that seek to establish working relationships with non-federal partners. For the purposes of this report, we focused on those that explicitly share information or intelligence related to potential or active terrorism investigations.

[9]For this report, we describe priority objectives for which work had been completed as being "closed," and priority objectives for which work was in process or incomplete as being "open."

performance management annual reports submitted to Congress by ODNI for calendar years 2017 (the year following our last review of the ISE), 2018, and 2019, which describe progress with the ISE Implementation Plan.[10] We did not review reports for calendar years 2020 and 2021 because they were not completed.[11]

We also reviewed documents demonstrating DHS, DOJ, or ODNI actions related to the open priority objectives, particularly those referenced in ODNI's annual reports to Congress. We interviewed DHS, DOJ, and ODNI officials about their respective efforts to complete the open priority objectives. Finally, because the President is required to establish the ISE, we spoke with officials in the White House Counsel's Office representing the National Security Council to obtain information on the President's current role overseeing the ISE.

To address our second objective, we focused our efforts on DHS, DOJ, and ODNI mechanisms for sharing terrorism-related information. For this report, we considered a mechanism for sharing with non-federal partners to be (1) any office or agency organization with an information-sharing mission; (2) any council, committee, task force, or program with a mission that includes facilitating the sharing of information; and (3) any information technology system (including databases and information sharing platforms) where terrorism-related information is made available to partners. To identify and catalogue these mechanisms, we reviewed the three available ISE annual reports submitted by ODNI since 2017, as well as DHS and DOJ documentation, such as annual performance reports, inspector general assessments, and memorandums of agreement.

For each office, council, committee, and information technology system we identified, we reviewed relevant public documents and other information found on web sites and open source statements from DHS, DOJ, and ODNI that described its organization and mission. In addition, we reviewed DHS, DOJ, and ODNI policy documentation on these mechanisms that discussed their purpose, scope, and membership, as

[10]See Office of Director of National Intelligence, *Information Sharing Environment 2017 Annual Report to Congress* (Washington, D.C.: 2017); Office of Director of National Intelligence, *Information Sharing Environment 2018* (Washington, D.C.: Oct. 2018); and Office of Director of National Intelligence, *Information Sharing Environment Report to the Congress* (Washington, D.C.: Nov. 2019).

[11]Prior to 2017, the Program Manager for the ISE issued annual reports on the ISE to Congress in accordance with statutory requirements. Following the Program Manager's departure, ODNI continued to issue these annual reports to Congress until 2020.

available. Finally, we reviewed department-level federal policies that describe terrorism information sharing to identify any broad policy changes that would affect how our identified mechanisms are used to share information on domestic terrorism.[12]

In addition, we interviewed selected non-federal partners to obtain their perspectives on federal information sharing mechanisms. Specifically, we interviewed directors of six "fusion centers," which are state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering, and sharing of threat-related information among the states and federal and non-federal partners. We interviewed directors of fusion centers in New York, Texas, California (two fusion centers), Oregon, and Alabama. We identified these fusion centers based on various factors, including the number of domestic terrorism incidents reported over the past ten years, geographic dispersion, and recommendations from the president of the National Fusion Center Association.[13] We also spoke with state and local representatives associated with two Joint Terrorism Task Force Executive Boards, one in Texas and another in Oregon, to obtain their perspectives on information sharing mechanisms.[14] We selected these two locations to represent the geographic areas of our selected fusion centers.

Finally, we interviewed selected representative organizations for non-federal users of terrorism information, including the chair of the Criminal

[12]For example, we reviewed the *National Strategy for Counterterrorism* and the 2021 *National Strategy for Countering Domestic Terrorism*, to identify any changes with respect to the sharing of domestic terrorism-related information. See Executive Office of the President, *National Strategy for Counterterrorism* (Washington, D.C.: Oct. 2018); and Executive Office of the President, *National Strategy for Countering Domestic Terrorism* (Washington, D.C.: June 2021).

[13]The National Fusion Center Association represents the interests of state and major urban area fusion centers, as well as associated interests of tribal nations, states, and units of local government, in order to promote the development and sustainment of fusion centers; encourage effective, ethical, and lawful intelligence and information sharing; and prevent and reduce the harmful effects of crime and terrorism on victims, individuals, and communities.

[14]Joint Terrorism Task Forces are the FBI's counterterrorism task forces in the field for leading and coordinating the operational law enforcement counterterrorism response and other related activities within the authority of the Attorney General. FBI personnel and co-located deputized partners from federal and non-federal law enforcement agencies within a specific area of responsibility constitute the membership of a task force. FBI Joint Terrorism Task Force Executive Boards consist of federal, state, and local representatives within the Joint Terrorism Task Force's area of responsibility. FBI officials, as well as personnel from state and local law enforcement agencies, provide executive board members with threat briefings.

Intelligence Coordinating Council, the President of the National Fusion Center Association, and members of the International Association of Chiefs of Police. Based on our previous ISE work, we found that these organizations have longstanding experience with federal initiatives to improve federal and non-federal partners' ability to share terrorism and other threat information.[15] The results of our interviews with non-federal partners represent the perspectives and views of those interviewed and cannot be generalized across all non-federal partners.

We conducted this performance audit from July 2021 to June 2023 in accordance with generally accepted government auditing standards.[16] 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

Statutory Responsibilities for Implementing the ISE and 2020 Changes

Under the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, the President, the Program Manager for the ISE, and federal departments and agencies have key statutory responsibilities for satisfying ISE-related requirements.[17]

[15]The International Association of Chiefs of Police is an association for police leaders that has more than 32,000 members in over 170 countries. The Criminal Intelligence Coordinating Council is a group under the U.S. Department of Justice's Global Justice Information Sharing Initiative, an advisory body to the U.S. Attorney General. Since 2001, the council has played a role in numerous efforts and initiatives to develop and improve federal and non-federal law enforcement and homeland security agencies' ability to share criminal and terrorism intelligence. These efforts include the establishment of fusion centers and the continued implementation of intelligence-led policing.

[16]GAO completed audit work for this engagement in November 2022. However, finalization and issuance of the report were suspended from November 2022 through May 2023 while ODNI conducted a sensitivity review.

[17]See Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, tit. I, subtit. A, § 1016, 118 Stat. 3638, 3664-70. References to "Program Manager" include the Program Manager and any staff supporting the Program Manager.

The President. The President is responsible for creating an ISE consistent with privacy and civil liberty legal standards; designating the ISE's organizational and management structures; and determining and enforcing the policies, directives, and rules that govern the ISE.[18] Through these efforts, the President must ensure that the ISE provides and facilitates the means for information sharing among federal, tribal, state, and local entities, and the private sector.[19]

The President must also, to the greatest extent possible, ensure that the ISE has, or otherwise supports, fifteen key criteria for information sharing.[20] These criteria include, for example, ensuring direct and continuous online electronic access to information, and facilitating the sharing of information at and across all levels of security.[21]

Since the ISE's establishment, the President has had responsibility for designating a Program Manager to help accomplish ISE-related requirements, which involved choosing an individual to serve in that role. For most of the ISE's existence, the President has also had the ability to delegate authority for the ISE without restriction.

The President delegated responsibility for the ISE to the Director of National Intelligence in April 2007.[22] The Director of National Intelligence remained responsible for the ISE until December 2020, when Congress passed the Intelligence Authorization Act for Fiscal Year 2021, which restricted the President from delegating responsibility for the ISE to that official.[23] The President has not since delegated responsibility for the ISE to another official or agency. Currently, the President and the Assistant to the President for Homeland Security and Counterterrorism remain

[18]6 U.S.C. § 485(b)(1).

[19]*Id.* § 485(b)(2).

[20]*Id.*

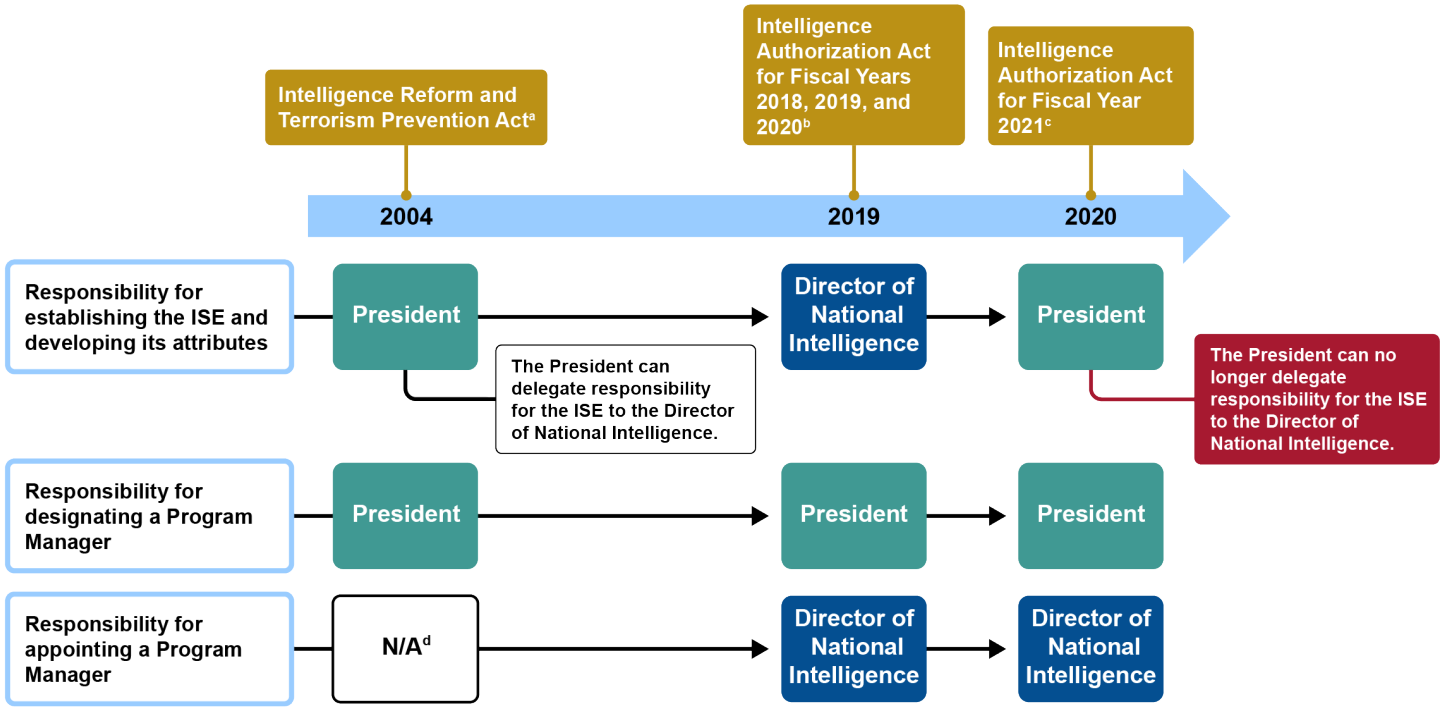
[21]*Id.*

[22]Assignment of Functions Relating to the Information Sharing Environment, 72 Fed. Reg. 18,561 (Apr. 10, 2007).

[23]For a brief period, the Director of National Intelligence was statutorily responsible for establishing the ISE and its attributes and for appointing a Program Manager, although the President remained responsible for designating someone for that position.

responsible for the ISE.[24] In addition, despite the 2020 Act's delegation restriction, it left the Director of National Intelligence statutorily responsible for appointing a Program Manager for the ISE (see figure 2).[25]

Figure 2: Key Statutory Changes in Responsibilities for Establishing the Information Sharing Environment (ISE) and Naming a Program Manager



Source: GAO legal analysis. | GAO-23-105310

[24]The Assistant to the President for Homeland Security and Counterterrorism serves as the President's homeland security and counterterrorism advisor and, thus, assists with policy related to the Information Sharing Environment.

[25]We discuss challenges related to this amended statutory framework later in the report.

Text of Figure 2: Key Statutory Changes in Responsibilities for Establishing the Information Sharing Environment (ISE) and Naming a Program Manager

	2019[26]	2019[27]	2020[28]
Responsibility for establishing the ISE and developing its attributes	President (The President can delegate responsibility for the ISE to the Director of National Intelligence).	Director of National Intelligence	President (The President can no longer delegate responsibility for the ISE to the Director of National Intelligence).
Responsibility for designating a Program Manager	President	President	President
Responsibility for appointing a Program Manager	N/Ad	Director of National Intelligence	Director of National Intelligence

Source: GAO legal analysis. | GAO-23-105310

[a]Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, tit. I, subtit. A, § 1016(b), (f)(1), 118 Stat. 3638, 3665, 3667. The ISE was established in 2005.

[b]Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020, Pub. L. No. 116-92, div. E, subdiv. 2, tit. LXIV, subtit. A, § 6402(a)-(b), 133 Stat. 2111, 2196 (2019).

[c]Intelligence Authorization Act for Fiscal Year 2021, Pub. L. No. 116-260, div. W, tit. III, subtit. A, § 307, 134 Stat. 2361, 2368 (2020).

[d]The 2004 statute only required a designation by the President.

The Program Manager for the ISE. The Program Manager has broad, government-wide authority for ISE-related information sharing efforts.[29] The Program Manager's responsibilities include managing the ISE; assisting with policy development; issuing procedures, guidelines, instructions, and functional standards for the ISE; identifying and resolving information sharing disputes; and assessing and reporting to Congress on federal efforts to implement the ISE.[30] The last Program Manager for the ISE resigned in 2017.

Federal departments and agency heads. Department and agency heads involved in the ISE are responsible for complying with information sharing policies and procedures; for supporting implementation of the

[26] Intelligence reform and terrorism preventaion act

[27] Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020b

[28] Intelligence Authorization Act for Fiscal Year 2021c

[29]6 U.S.C. § 485(f)(1).

[30]*Id.* § 485(f)(2)(A).

ISE; and for reporting on their implementation activities.[31] Historically, agencies have reported these activities to the Program Manager.

Status of the ISE Implementation Plan in 2017

We reported in 2017 that the Program Manager and his staff had worked with key departments and agencies to complete work on 13 of the ISE Implementation Plan's 16 objectives (see app. I for a list of the completed priority objectives).[32] We also reported that the Program Manager and relevant agencies were making progress implementing the three open priority objectives and had planned to work on these objectives through fiscal year 2019 (see table 1).

Table 1: Information Sharing Environment (ISE) Implementation Plan – Open Priority Objectives and Remaining Work, as of fiscal year 2016[a]

Priority objectives	Description	Importance of Completing Priority Objective
Data tagging[b]	The adoption of data standards to facilitate federated discovery, access, correlation, and monitoring across federal networks and security domains.	Intended to address the lack of common identification standards for database content across all security domains, which inhibits effective data search, correlation, and the simultaneous safeguarding of data and user identities.
Federal Identity, Credential, and Access Management	A framework intended to, among other things, establish standards for the technologies and services used to create trusted digital credentials that can verify and provide individuals authorized access to an agency's information.	Intended to address the lack of a government-wide capability to control access to sensitive information on computer networks[c] Also intended to assure compliance with legal, regulatory, and mission-area policies, while simultaneously allowing access to that same sensitive information by authorized persons.
Discovery and Access[d]	The definition and implementation of common processes and standards to support automated, policy-based discovery and access decisions.	Intended to address the lack of an automated, policy-based decision process to approve users for the discovery, access, and delivery of information.

Source: GAO analysis of Office of the Program Manager for the Information Sharing Environment information. | GAO-23-105310.

[a]The ISE Implementation Plan had a total of 16 priority objectives. We reported in 2017 that agencies had completed work on all but three of these objectives. See GAO, Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

[b]Data tags are descriptors applied to resources, and are critical to the ability to both locate information and enable automated access control decisions.

[c]Information that should not be released to the public, but is not classified.

[d]Discovery and access is a term that describes the ability to find and retrieve information across federal systems.

[31]*Id.* § 485(h).

[32]GAO-17-317.

Roles and Responsibilities for Terrorism Information Sharing

Within their respective missions, DHS, DOJ, ODNI, and non-federal partners each have roles and responsibilities related to sharing terrorism-related information with non-federal partners in addition to the ISE responsibilities discussed above. The following entities serve as the primary organizations within each agency that are responsible for sharing such information:

DHS. The DHS Office of Intelligence and Analysis is charged with analyzing intelligence information and sharing that information with federal, tribal, state, local, territorial, and private sector partners, and obtaining information from those partners for DHS and the U.S. Intelligence Community.[33]

DOJ. The Attorney General, acting through the FBI, has the lead responsibility for the criminal investigation of terrorist threats or incidents within the United States. This responsibility includes the collection, coordination, analysis, management, and dissemination of related intelligence and criminal information, as appropriate. In the course of their investigative and intelligence efforts, the FBI's Field Offices actively and regularly share terrorism information with their federal, tribal, state, local, territorial, and law enforcement partners.

ODNI. The ODNI Office of Domestic Engagement, Information Sharing, and Data is responsible for building, enabling, and maintaining domestic partnerships with federal stakeholders, as well as tribal, state, local, and private sector organizations, to include industry, non-government organizations, and academia. In addition to this office, the ODNI National Counterterrorism Center shares updated, unclassified threat assessments with federal, tribal, state, local, and territorial partners.

Tribal, State, Local, Territorial, and Private Sector Entities. In concert with federal agencies, tribal, state, local, territorial, and select private sector organizations coordinate the gathering,

[33]The U.S. Intelligence Community consists of 18 organizations, such as the intelligence components of the five military services within the Department of Defense as well as the Central Intelligence Agency, which is an independent agency. These organizations gather, analyze, and produce the intelligence necessary to conduct foreign relations and national security activities.

analysis, and dissemination of law enforcement, homeland security, public safety, and terrorism information to partners within their jurisdictions. They do so through participation in key initiatives such as fusion centers. They also document and submit potential threat information to federal agencies through Suspicious Activity Reports, which are official documentation of observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity, and other intelligence products.[34]

Agencies Implemented Some ISE Projects, but There Has Not Been a Program Manager to Assess Progress

Agencies Implemented Some ISE-Related Projects, but Did Not Assess Progress toward Completing Open Priority Objectives

According to ODNI officials, since 2017 the agency has collaborated with DHS and DOJ on ISE-related projects. However, we found that progress toward fully completing the ISE Implementation Plan has not been determined because agencies did not assess the impact of their efforts to complete priority objective milestones.[35] ODNI officials conducted multiple pilot projects and other efforts that ODNI jointly conducted with DHS and DOJ that related to the ISE Implementation Plan's three open priority objectives (see table 2).

[34]According to DHS officials, the development of Suspicious Activity Reports is a two-part process. First, analysts or law enforcement officers at either a state or major urban area fusion center, or a federal agency, review newly reported information for suspicious behavior based on his or her training and expertise and against specific behavior criteria. Second, based on the context, facts, and circumstances, the analyst or investigator determines whether the information meeting the criteria has a potential nexus to terrorism (i.e., to be reasonably indicative of pre-operational planning associated with terrorism) or criminal activities associated with terrorism.

[35]GAO completed audit work for this engagement in November 2022. However, finalization and issuance of the report were suspended from November 2022 through May 2023 while ODNI conducted a sensitivity review. During that time, agencies did not provide any additional updates on assessment activities.

Table 2: Efforts to Address Open Priority Objectives from the Information Sharing Environment (ISE) Implementation Plan for calendar years 2017 through 2022[a]

Priority Objective Title	Milestones Remaining (as of 2017)	Agency Efforts to Address ISE Priority Objective from 2017 through 2022	Remaining Work to Address ISE Priority Objective as of 2022
Data Tagging[b]	Implement pilot projects; begin tagging new data and retroactively tag legacy data.	According to Office of the Director of National Intelligence (ODNI) officials, in 2019, ODNI partnered with the Department of Justice (DOJ) on a pilot program to add additional information from their internal systems to records held by the Terrorist Screening Center, an interagency component of the United States government administered by the Federal Bureau of Investigation that manages the consolidated Terrorist Watchlist[c] The program uses information from state and local databases connected through DOJ's Regional Information Sharing Systems to augment records[d]	Unknown because agencies did not assess the impact of their efforts to complete priority objective milestones. In 2017, remaining work included retroactively tagging all existing or legacy data, and tagging all newly created data across federal networks.
Federal Identity, Credential, and Access Management	Implement credentialing and access framework for Top Secret, Secret, and Unclassified information systems.	In 2019, ODNI partnered with the Department of Homeland Security (DHS) to jointly publish acquisition guidance for state and local partners to assist them in procuring identity and credential access management systems, including multifactor authentication capabilities, for their respective jurisdiction[e]	Unknown because agencies did not assess the impact of their efforts to complete priority objective milestones. In 2017, remaining work included developing a framework to support interoperable user authentication, credentialing, and access across federal networks.
Discovery and Access[f]	Develop and issue government-wide policy on discovery and access, and pilot implementation.	According to ODNI officials, in 2017, ODNI and DOJ established a program to connect key state and local data sets with the Regional Information Sharing Systems' Secure Cloud Criminal Intelligence Database in order to broaden search capability and expand access to criminal intelligence information pertaining to terrorism.	Unknown because agencies did not assess the impact of their efforts to complete priority objective milestones. In 2017, remaining work included identification of automated requirements for discovery and access decisions, and development and issuance of a government-wide policy regarding discovery.

Source: GAO analysis of DHS, DOJ, and ODNI documentation. | GAO-23-105310.

Note: GAO completed audit work for this engagement in November 2022. However, finalization and issuance of the report were suspended from November 2022 through May 2023 while ODNI conducted a sensitivity review. During that time, agencies did not provide any additional updates on activities.

[a]The ISE Implementation Plan had a total of 16 priority objectives. We reported in 2017 that agencies had completed work on all but three of these objectives. See GAO, Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others, GAO-17-317 (Washington, D.C.: Feb. 15, 2017). After December 2020, when Congress passed the Intelligence Authorization Act for Fiscal Year 2021, which restricted the President from delegating responsibility for the ISE to the Director of National Intelligence, ODNI officials told us they conducted this work as part of ODNI's mission to share information with non-federal entities.

[b]Data tags are descriptors applied to resources, and are critical to the ability to both locate information and enable automated access control decisions.

[c]The Terrorist Watchlist is the U.S. government's consolidated list of unclassified biographic and biometric information of known or suspected terrorists. The Terrorist Screening Center shares the

Terrorist Watchlist with agencies and officials authorized or required to conduct terrorist screening, to include diplomatic, military, intelligence, law enforcement, immigration, transportation security, visa, and protective screening processes.

[d]The Regional Information Sharing Systems is a nationwide program, congressionally funded and administered through the U.S. Department of Justice, Office of Justice Programs. Its mission is to assist federal, tribal, state, and local criminal justice partners by providing adaptive solutions and services that facilitate information sharing, support criminal investigations, and promote officer safety. The program provides investigative case support such as analytical services, publications, and training as well as secure information and intelligence sharing solutions and access to law enforcement databases and systems.

[e]Multifactor authentication uses a combination of credentials to provide a higher assurance that the individual attempting to access a protected resource is that individual. The factors include something you have (a banking debit card), something you are (a fingerprint or other biometric), or something you know (a password or personal identification number).

[f]Discovery and access is a term that describes the ability to find and retrieve information across federal systems.

We compared agencies' ISE-related projects since 2017 with plans for remaining work established for each priority objective. We found it was unclear how agencies' projects addressed milestones established for the remaining work. For example, according to a 2016 briefing to ISE stakeholders, there were four outstanding milestones for the data tagging priority objective. As described in table 2, ODNI and DOJ developed a pilot program to enhance the Terrorist Watchlist in 2019.[36] However, there were no assessments to show how this pilot program helped address any of the four milestones for data tagging. Similarly, for two other open priority objectives (the Federal Identity, Credential, and Access Management objective and the Discovery and Access objective) there were five and six outstanding milestones, respectively. We also found that there was no evidence, such as an ODNI assessment, to verify how the projects agencies completed since 2017 addressed the relevant milestones.

Without assessments from a Program Manager or other designated entity, the impact of agencies' ISE-related efforts on completing the open priority objectives is unknown. Consequently, it remains unclear how much work remains for the ISE Implementation Plan overall. Prior to 2017, the Program Manager for the ISE would assess agencies' efforts

[36]The Terrorist Watchlist is the U.S. government's consolidated list of unclassified biographic and biometric information of known or suspected terrorists. The Terrorist Screening Center shares the Terrorist Watchlist with agencies and officials authorized or required to conduct terrorist screening, to include diplomatic, military, intelligence, law enforcement, immigration, transportation security, visa, and protective screening processes.

against plans that included milestones for each priority objective.[37] Each milestone represented a discrete task needed to achieve a given priority objective. By reviewing agencies' efforts with each milestone, the Program Manager was able to assess incremental progress on a given priority objective. When the Program Manager resigned in 2017, the President did not name a replacement who would carry out these assessments.

ODNI officials said that after the Program Manager resigned in 2017, the agency distributed the functions of the Program Manager's Office to other offices within ODNI (including, for example, the Office of Domestic Engagement, Information Sharing, and Data). However, an ODNI official from one office that worked on ISE projects related to open priority objectives said the office did not complete any assessments against planned work on objectives after 2017. In addition, officials with the DHS Office of Intelligence and Analysis and the FBI—two agencies that worked on projects related to the open objectives—said they had not assessed progress on the completion of the open priority objectives. Further, DOJ officials stated that assessing progress remained ODNI's responsibility.

We have previously reported on how the Program Manager assessed and reported on agency efforts to implement the ISE. Specifically, in our *High-Risk* work we reported that the Program Manager's office worked with agencies to confirm that milestones related to ISE priority objectives were completed and the goals of the strategy were attained.[38] Officials from both federal and non-federal organizations, such as the National Fusion Center Association, told us that while some efforts to implement open priority objectives continued to move forward after 2017, the departure of the Program Manager removed an effective oversight function. Officials told us the Program Manager was best positioned to bring government partners together to further the goals of the ISE and assess progress on its various initiatives. Officials also said that the Program Manager was an effective steward with the requisite authority to broker issues related to information access, coordination, and sharing between DHS, FBI, and non-federal partners.

[37]Milestones for the Data Tagging and Federal Identity, Credential, and Access Management priority objectives began in fiscal year 2014 and were to be completed by fiscal year 2018. Milestones for the Discovery and Access priority objective began in fiscal year 2014 and were to be completed by fiscal year 2019.

[38]See GAO-17-317.

As discussed, the act establishing the ISE requires there to be a Program Manager who is to assess federal implementation efforts. From 2013 (when the ISE Implementation Plan was created) through 2017, there was a designated Program Manager to assess agency progress toward meeting the Plan's priority objectives. However, when the Program Manager resigned in 2017 it appears that no other official or agency assumed this activity, and the position remained unfilled as of July 2022. Without a Program Manager it will be difficult to ensure the ISE receives continued leadership commitment and a means to monitor actions and assess progress in completing work on the open priority objectives.

Efforts to Name a New Program Manager Have Been Complicated by Conflicting Statutory Provisions

According to White House and ODNI officials, conflicting provisions within the Intelligence Reform and Terrorism Prevention Act of 2004, resulting from 2020 amendments, have made it challenging to name a new Program Manager. As discussed, since the ISE's establishment, designating a Program Manager has been the responsibility of the President. Amendments enacted in 2019 to the Intelligence Reform and Terrorism Prevention Act of 2004 made the Director of National Intelligence responsible for appointing a Program Manager, while still leaving the President responsible for designating someone for that position. However, 2020 amendments to the act restricted the President from delegating responsibility for the ISE to the Director of National Intelligence, but left in place the requirement that the Director of National Intelligence appoint the individual whom the President designates as Program Manager.[39] The law, therefore, restricts the Director of National Intelligence from being delegated responsibilities to the ISE, but still requires that the Director perform the task of appointing a Program Manager. According to an ODNI official, the delegation restriction on the President makes it challenging for ODNI to implement responsibilities within the Act as Congress intended. Moreover, according to White House officials, efforts to name an ISE Program Manager have been complicated by these conflicting statutory responsibilities and authorities.

Despite these complications, the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, assigns the President with

[39]*Compare* 6 U.S.C. § 485(b)(3)(B) (restricting the President from delegating responsibility for the ISE to the Director of National Intelligence), *with id.* § 485(f)(1) (requiring the Director of National Intelligence to appoint the Program Manager).

overarching responsibility for establishing the ISE and its implementation.[40] In particular, the President must designate the Program Manager and the ISE's organizational and management structures and determine and enforce the policies, directives, and rules that govern the ISE.[41] The President must also, to the greatest extent possible, ensure that the ISE supports 15 key information sharing criteria.[42] Given that the President has broad-ranging, enumerated responsibilities for the ISE that cannot be delegated to the Director of National Intelligence, and that the Program Manager has related ISE responsibilities, it would be unusual for the President not to have full statutory authority to fill the Program Manager position.

Conflicting provisions within the Intelligence Reform and Terrorism Prevention Act of 2004, resulting from 2020 amendments, have made it challenging to name a new Program Manager for the ISE. Congressional action to further amend the Intelligence Reform and Terrorism Prevention Act of 2004 by clarifying that the President has statutory responsibility both to designate and to appoint the Program Manager for the ISE would facilitate this process. Without this amendment, the Assistant for Homeland Security and Counterterrorism, acting on behalf of the President, will continue to experience challenges in filling the Program Manager position. Further, a new Program Manager would help ensure that work on the ISE Implementation Plan continues moving forward and that the vision of secure and responsible national security information sharing set forth in the 2012 *National Strategy for Information Sharing and Safeguarding* is achieved.

Agencies Use a Variety of Mechanisms to

[40]Intelligence Authorization Act for Fiscal Year 2021, Pub. L. No. 116-260, div. W, tit. III, subtit. A, § 307, 134 Stat. 2361, 2368 (2020) (amending the Intelligence Reform and Terrorism Prevention Act of 2004 to reassign responsibility for the ISE from the Director of National Intelligence to the President).

[41]6 U.S.C. § 485(b)(1), (f)(1).

[42]*Id.* § 485(b)(2).

Share Information on Terrorism and Other Threats

DHS, DOJ, and ODNI each share terrorism-related information with non-federal and private sector partners using a variety of mechanisms, and generally these mechanisms treat information on domestic terrorism the same as information on international terrorism and other emerging threats. Based on our review of key agency documents as well as interviews with federal officials, we identified approximately 26 different mechanisms used to share or promote the sharing of terrorism-related information among federal, non-federal, and private sector entities.[43] This included eight agency offices or organizations with terrorism information sharing as part of their respective missions; eleven working groups or committees intended to build relationships and facilitate coordination on terrorism information sharing; and seven technological systems, platforms, and databases used to document, store, and make terrorism-related and other threat information available (see app. II for descriptive information on these mechanisms). We also identified four mechanisms with joint involvement by DHS, DOJ, and ODNI.

We also found that DHS and DOJ use their respective mechanisms and procedures to share information on all threats—including those related to domestic and international terrorism. According to officials from DHS and DOJ, many of the information sharing mechanisms created after the attacks of September 11, 2001, continue to assist the U.S. government's counterterrorism efforts. DHS and DOJ officials stated that generally these mechanisms do not treat domestic and international terrorism information differently with respect to generating and sharing intelligence products with non-federal partners. Specifically, FBI officials stated they use the same mechanisms to help increase the sharing of terrorism-related information with non-federal stakeholders for both international and domestic terrorism. For example, according to FBI officials, as the lead agency for investigating and coordinating all federal crimes of terrorism, the FBI's Joint Terrorism Task Forces routinely share

[43]For this report, we defined a "mechanism" as 1) any office or organization with an information sharing mission; 2) any council, committee, or task force with a mission that includes facilitating the sharing of information; and 3) any information technology system (including databases and information sharing platform) where terrorism-related information is made available to partners. These are mechanisms we identified as of November 2022 when GAO completed audit work for this engagement. However, finalization and issuance of the report were suspended from November 2022 through May 2023 while ODNI conducted a sensitivity review.

information on international and domestic terrorism with federal and non-federal partners.

According to the FBI, these task forces serve as information sharing mechanisms in several ways. First, non-FBI task force members are fully integrated into FBI operations as investigators, which provides them access to information related to ongoing investigations, including access to classified terrorism information. Second, Task Force Officers, who have access to international and domestic terrorism information, fulfill investigative responsibilities on the task forces and serve as liaisons between the FBI and their home agency.[44] Additionally, Joint Terrorism Task Forces provide information through periodic meetings in which domestic terrorism information may be presented, and disseminate unclassified information via email to a broad distribution of law enforcement partners. These task forces also engage in liaison efforts with law enforcement partners, who may not have permanent task force representation, to share appropriate information.

The FBI confirmed that other DOJ and FBI technology systems used by non-FBI users do not differentiate between those individuals accessing services for information related to terrorism and other criminal justice information. For example, the FBI, federal partners, and non-federal partners use the FBI's eGuardian system to share Suspicious Activity Reports.[45] The FBI reviews all Suspicious Activity Reports, identifies those related to terrorism (both international and domestic), and subsequently assigns those cases to the appropriate Joint Terrorism Task Force(s) for further investigative action.

DHS officials stated that mechanisms they use to share unclassified terrorism-related information with non-federal stakeholders do not distinguish between international and domestic terrorism. For example, the DHS Office of Intelligence and Analysis, through its Counterterrorism Mission Center, authors finished intelligence products on both domestic

[44]In addition to Task Force Officers, individuals that are not law enforcement officers but are employees of federal, tribal, state, or local agencies can also serve on Joint Terrorism Task Forces as Task Force Members or Task Force Participants.

[45]The FBI eGuardian system is a Sensitive But Unclassified information-sharing platform used since 2007 to share sensitive but unclassified terrorism-related information, among other things. The FBI hosts the service on its Law Enforcement Enterprise Portal, an on-line portal that centralizes access to FBI criminal justice services along with those of other agencies.

and international terrorism and disseminates them across DHS systems.[46] Terrorism-related information is primarily shared by posting documentation to the Homeland Security Information Network and its Intelligence Community of Interest in addition to briefings and other engagements.[47]

In addition, DHS officials said that their general strategy for sharing terrorism information with non-federal partners is to distribute that information to the broadest possible audience irrespective of whether it is domestic or international in nature. Therefore, DHS also posts its products on systems outside of DHS, such as the FBI's Law Enforcement Enterprise Portal. DHS officials confirmed that federal and non-federal stakeholders routinely upload and share unclassified terrorism-related information on the Homeland Security Information Network, but there is no categorization of information as pertaining to international or domestic terrorism. However, users can assign a specialized "counterterrorism" data tag to the document or product they upload to the system so that others can search by that specific criteria.

Although FBI and DHS officials stated that technology platforms and products accessible by non-federal users do not distinguish between international and domestic terrorism, both agencies track this information for products they develop internally and share on the systems previously described. For example, according to FBI officials, of the 10,718 Situational Information Reports the FBI disseminated through its Law Enforcement Enterprise Portal from fiscal years 2017 through 2021, 761

[46]The DHS Office of Intelligence and Analysis' Counterterrorism Mission Center is responsible for synthesizing and integrating counterterrorism intelligence from all federal, state, and local partners for distribution within DHS and to its partners. It therefore develops all-source finished intelligence products on both international and domestic terrorism that are disseminated across platforms run by other organizations. These products are, depending on classification level, posted to internal DHS networks for downloading by appropriately cleared partners. The mission center utilizes open source information, Intelligence Community-disseminated information, and DHS-collected information.

[47]The Homeland Security Information Network maintains numerous communities of interest, or customized portals within the larger site that are dedicated to specific topics. In particular, DHS uses the Intelligence Community of Interest to share Sensitive But Unclassified intelligence products with federal and non-federal partners, to include those related to terrorism. As a minimum for eligibility to access this specific site, users must, among other things, be a current, full-time employee of a law enforcement, criminal justice, intelligence, or homeland security government agency, and directly support information and intelligence analysis, sharing, or collection activities.

were related to domestic terrorism.[48] In addition, 27 of the 130 Joint Intelligence Bulletins distributed through the system from fiscal years 2017 through 2021 concerned domestic terrorism.[49] Similarly, officials from the DHS Office of Intelligence and Analysis said that for fiscal years 2017 through 2021, they issued 1,097 raw intelligence reports and approximately 140 finished intelligence products related to domestic terrorism.[50]

Feedback from selected non-federal stakeholders on FBI and DHS information sharing mechanisms was generally positive, and most officials we spoke with from these groups stated that terrorism-related information sharing had improved since 2017. Specifically, this was stated by five of six officials representing selected fusion centers and both of the Joint Terrorism Task Force Executive Boards we interviewed. In general, all of these officials confirmed the importance of information sharing relationships with their federal partners, the utility of information shared, and the usefulness of the mechanisms that provide them with access to terrorism-related information.

With respect to DHS and DOJ information sharing mechanisms, we found agreement among fusion center officials we interviewed that information sharing had improved since 2017. For example, senior officials from all six fusion centers we spoke with highlighted increases in fusion center connectivity and integration with federal systems and platforms, as well

[48]Situational Information Reports are FBI reports that FBI field offices use to share actionable criminal or terrorism information with non-federal partners.

[49]Joint Intelligence Bulletins are intelligence products specifically prepared for dissemination and created as part of FBI intelligence activities, and typically jointly authored with DHS, the National Counterterrorism Center, or other Intelligence Community partners.

[50]According to the DHS Office of Intelligence and Analysis, raw intelligence reports are intelligence products that record, but do not analyze, identified information. These include open source intelligence reports (which contain unevaluated open source information), Field Intelligence Reports (developed by DHS officials from field offices), or Intelligence Information Reports. Field Intelligence Reports are published via the Homeland Security Information Network, while Intelligence Information Reports may be published on the Homeland Security Information Network or a classified system depending on their classification. In contrast, finished intelligence reports contain analytic assessments, judgment, or other analytic input based on internal analysis performed by the DHS Office of Intelligence and Analysis. Finished intelligence reports may contain information on an immediate threat to homeland security or other exigent crisis. These reports may also be published on the Homeland Security Information Network or a classified system depending on their classification, and may be issued directly to fusion centers and FBI Field Offices.

as greater access to security clearances for fusion center analysts. These senior officials also noted that participation in initiatives like Joint Terrorism Task Forces was critical for remaining informed on potential threats. Officials from five of the six fusion centers stated that their centers generally maintain positive and active working relationships with DHS and the FBI, and all of them said they believed the capabilities of different technology platforms like the Homeland Security Information Network were effective tools their analysts use.[51]

While there was general agreement that information sharing had improved, a representative from the National Fusion Center Association, as well as two fusion centers, noted that centers often receive the same information and products from multiple federal information sharing mechanisms, including notifications on the release and distribution of those products. These officials attributed this to federal agencies using their own distribution lists for intelligence products, resulting in situations where the same products are issued through multiple mechanisms. Officials added that although this information could, at times, be duplicative, they nevertheless preferred that information be shared and not withheld.[52]

Officials from all six fusion centers also emphasized the importance of having field-based staff from federal agencies, either co-located at the fusion center or in nearby regional offices, as critical to the development of interpersonal relationships between fusion center staff and federal staff. Fusion center officials noted this relationship-building also often occurs through participation in interagency forums like Joint Terrorism Task Forces, as well as regularly scheduled meetings where direct interactions can take place. Similarly, state and local law enforcement officials associated with two Joint Terrorism Task Force Executive Boards we spoke with confirmed that one significant benefit of Task Force membership has been the ability to develop relationships with locally-based federal and non-federal colleagues while remaining informed about current threats. For example, state and local law enforcement officials from Oregon and Texas said that information they have received about domestic terrorism issues through Joint Terrorism Task Force meetings

[51]One senior official said that, historically, his fusion center did not have a relationship with the FBI, which affected the center's ability to receive terrorism-related information. However, the official said that, as of early 2022, the FBI has been increasing communications and the situation is improving.

[52]We did not assess the extent to which there is duplication, fragmentation, and overlap in how federal agencies share terrorism-related information with non-federal partners because it was outside the scope of our review.

has been instrumental in helping them plan for domestic terrorism-related activities in their jurisdictions.

Officials from non-federal stakeholder organizations and fusion centers that we interviewed also identified areas for improvement. In particular, officials from five of the six fusion centers we spoke with said that compared to the FBI, the DHS Office of Intelligence and Analysis deploys fewer analysts to the fusion centers. These officials stated that this situation is different for each center. For example, they said California, Oregon, and New York state fusion centers all maintain full-time intelligence officers from DHS, but other centers do not. Officials from two of the six fusion centers expressed concern that the lack of experienced analyst support staff from the Office of Intelligence and Analysis limits the ability for fusion center staff to develop interpersonal relationships with them. They noted that such relationships were a key element of productive information sharing partnerships.

In response, DHS officials told us that in fiscal year 2022, the Office of Intelligence and Analysis added Regional Intelligence Officers to select fusion centers which previously did not have assigned full-time officers.[53] As a result, DHS officials said that all 80 fusion centers nationwide now have representation from the Office of Intelligence and Analysis, thereby providing a conduit to coordinate intelligence sharing with stakeholders from those geographic areas.[54]

Officials also cited issues affecting access to FBI and other federal information systems. For example, officials from two fusion centers cited challenges with their analysts gaining access to discrete elements of an FBI system, due to different requirements for granting user access (such as username and password). These officials noted that access to classified information, particularly from FBI systems, continues to be an important factor in the efficiency and effectiveness of their analysts' work.

[53]DHS deploys Intelligence Officers to support non-federal and private sector partners in advancing the homeland security mission. Intelligence officers are embedded in recognized state and major urban area fusion centers to advance the sharing of threat-related information among federal, non-federal, and private sector partners in their respective regions or areas of responsibility. Among other things, Intelligence Officers assist fusion centers and non-federal partners in sharing and analyzing intelligence and information to develop a comprehensive threat picture, as well as provide guidance in the production and dissemination of intelligence and information products to non-federal entities.

[54]DHS officials noted that this support may include Regional Intelligence Officers, Regional Intelligence Analysts, Reports Officers, and Human Intelligence Collection Operations Managers from the Office of Intelligence and Analysis.

Additionally, a senior official representing both the National Fusion Center Association and the Criminal Intelligence Coordinating Council cited feedback received from fusion centers indicating challenges connecting DHS and FBI systems. Specifically, this feedback included issues related to single sign-on access, such as between systems like the Homeland Security Information Network and the Law Enforcement Enterprise Portal, due to different security measures and standards for users.[55] This official noted that prior to 2017, the former Program Manager for the ISE effectively helped address these types of issues between federal agencies. In addition, as discussed earlier in this report, one of the three outstanding ISE priority objectives relates to identity management and access to technical systems. Fully implementing this priority objective would help address these challenges.

Conclusions

Completing the ISE Implementation Plan has been a core goal to improve the effectiveness of terrorism-related information sharing. At the start of 2017, 13 of the Plan's 16 priority objectives were complete, but since then progress has stalled due in part to the absence of a Program Manager to guide and assess the effort. In past work, GAO found that the Program Manager's leadership was pivotal in bringing about progress towards implementation of the ISE. When the ISE Program Manager resigned in 2017 and was not replaced, the program lost an oversight function that served to effectively review and assess if progress was made on various ISE initiatives.

Without a Program Manager to assess agency efforts to complete the remaining priority objectives, it will be difficult to determine agencies' overall progress with the ISE Implementation Plan. Although the designation of a Program Manager has always been the responsibility of the President, 2020 amendments made to the Intelligence Reform and Terrorism Prevention Act of 2004 resulted in conflicting provisions that have complicated this process. Amending the Intelligence Reform and Terrorism Prevention Act of 2004 to clarify that the President has statutory responsibility both to designate and to appoint a Program Manager, and then taking action to get a Program Manager in place, would ensure the ISE receives continued leadership commitment and a means to assess actions and demonstrate progress in completing work

[55]Single sign-on permits a user to use one set of login credentials to access multiple applications.

on the open priority objectives. Fully implementing the open ISE priority objectives should bolster the ability of both federal and non-federal agencies to gain the benefits of the ISE as conceptualized in the ISE Implementation Plan and the *National Strategy for Information Sharing and Safeguarding*.

Matter for Congressional Consideration

Congress should consider further amending the Intelligence Reform and Terrorism Prevention Act of 2004 to clarify that the President has responsibility both to designate and to appoint a Program Manager for the ISE. (Matter for Consideration 1)

Recommendations for Executive Action

We are making the following two recommendations to the Executive Office of the President:

The Assistant to the President for Homeland Security and Counterterrorism should take steps to ensure the presidential responsibilities related to the Information Sharing Environment (ISE) within the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, including the designation of a Program Manager for the ISE, are fulfilled. (Recommendation 1)

The Assistant to the President for Homeland Security and Counterterrorism should take steps to ensure that the Program Manager, once appointed, reviews and assesses agencies' progress implementing the Information Sharing Environment, consistent with responsibilities in the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, and in coordination with other appropriate agencies. (Recommendation 2)

Agency Comments and Our Evaluation

We provided a draft of this report to the Executive Office of the President, DHS, DOJ, and ODNI for review and comment. DHS, DOJ and ODNI provided technical comments, which we incorporated, as appropriate. The Executive Office of the President did not provide comments on our recommendations.

We provided copies of this report to the appropriate congressional committees, the Assistant to the President for Homeland Security and Counterterrorism, the Attorney General, the Secretary of Homeland Security, the Director of National Intelligence, and other interested parties. In addition, the report will be available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact Triana McNeil at (202) 512-8777 or McNeilT@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 III.

Sincerely yours,

Triana McNeil
Director, Homeland Security and Justice

Appendix I: Completed Priority Objectives from the Strategic Implementation Plan for the Information Sharing Environment

The following table describes the 13 priority objectives from the Strategic Implementation Plan for the Information Sharing Environment that the Program Manager determined to be complete as of fiscal year 2016. The table also contains examples of demonstrated progress. For example, work on several priority objectives—such as reference architecture and standards-based acquisitions—resulted in concrete guidance based on best practices that was then made available to stakeholders to use in their own organizations.

Table 3: Description of Completed Priority Objectives from the Strategic Implementation Plan for the Information Sharing Environment and Examples of Demonstrated Progress, as of Fiscal Year 2016[a]

Priority objectives	Description	Examples of demonstrated progress
Governance	Align information sharing and safeguarding governance to foster better decision making, performance, accountability, and implementation of strategic goals.	• Identified best practices and common governance requirements
Agreements	Develop guidelines for information sharing and safeguarding agreements to address common requirements while allowing flexibility to meet mission needs.	• Created a framework of recommendations for streamlining information sharing and access agreements.
Safeguarding	Implement safeguarding capabilities to support information sharing.	• Convened a working group to determine safeguarding priorities, and developed metrics to measure implementation.
Interoperability	Define and adopt baseline capabilities and common requirements to enable data, service, and network interoperability.	• Developed and implemented the capability of systems to communicate with one another and to exchange and use information.
Training	Provide information sharing, safeguarding, and handling training to appropriate stakeholders using a common curriculum tailored to promote consistent yet flexible and trusted processes.	• Developed and posted core awareness training to Program Manager's website.
Private sector	Establish information sharing processes and sector-specific protocols with private sector partners to improve information quality and timeliness and secure the nation's infrastructure.	• Made appropriate fusion center products accessible to critical infrastructure owners and operators.
Reference architecture	Develop a reference architecture to support a consistent approach to data discovery and correlation across disparate datasets.	• Published reference architecture document and other tools and guidance.

Priority objectives	Description	Examples of demonstrated progress
Shared services	Implement activities to facilitate adoption of shared services.	• Implemented program for shared service offerings across the federal government.
Standards-based acquisition	Refine processes enabling standards-based acquisitions among departments and agencies, standards bodies, and vendors to promote interoperable products and services.	• Developed and published "Acquisitions Playbook" to provide guidance to departments, agencies, and other entities.
Foreign partner sharing	Promote adherence to existing interagency processes to coordinate information sharing initiatives with foreign partners, as well as adopt and apply necessary guidelines to ensure consistency when sharing and safeguarding information.	• Catalogued existing agreement templates and models to guide foreign partner sharing.
Requests for information, and Alerts-Warnings-Notifications	Create a common process across all levels of government for Requests for Information to enable timely receipt and dissemination of information and appropriate response. Create a common process across all levels of government for Alerts, Warnings, and Notifications to enable timely receipt and dissemination of information and appropriate response.	• Analyzed Request for Information terminology and derived best practices and recommendations for improvements. • Working group issued Alerts, Warnings, and Notifications Report of Findings.
Nationwide suspicious activity reporting initiative	Complete the implementation of the Nationwide Suspicious Activity Reporting Initiative program while expanding training and outreach beyond law enforcement to the rest of the public safety community[b]	• Refined and enhanced Suspicious Activity Report analysis tools, and secured funding for related training materials.
Fusion centers	Achieve the four Critical Operational Capabilities, four Enabling Capabilities, and other prioritized objectives across the National Network of Fusion Centers to help them effectively and lawfully execute their role as a focal point within the state and local environment for receiving, analyzing, gathering, and sharing threat-related information[c]	• Ensured appropriate federal analytic products are posted, shared, and cataloged within DHS's secure information network.

Source: GAO analysis of Office of the Program Manager for the Information Sharing Environment information. | GAO-23-105310.

[a]Fiscal year 2016 was the latest time period that information was available when we last reported on this issue in February 2017.

[b]The FBI and DHS-led Nationwide Suspicious Activity Reporting Initiative is a collaborative effort for federal, state, and local law enforcement entities to share information on suspicious activities. The initiative serves as the unified focal point for sharing Suspicious Activity Report information and provides standards, policies, processes, and trainings that allow fusion centers and law enforcement agencies to easily share information to help identify, report, and share tips and leads linked to terrorism.

[c]The National Network of Fusion Centers consists of 80 state and major urban area fusion centers. Fusion Centers are state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering, and sharing of threat-related information between federal, tribal, state, local, territorial, and private sector partners.

Appendix II: Federal Mechanisms Used to Share Terrorism-Related Information with Non-Federal Partners

This appendix provides an overview of the various mechanisms the Office of the Director of National Intelligence (ODNI); the Department of Homeland Security (DHS); and the Department of Justice (DOJ), to include the Federal Bureau of Investigation (FBI), use to share terrorism-related information with tribal, state, local, territorial, and private sector (non-federal) partners. It also provides descriptions of various joint mechanisms used by one or more of these agencies to share such information with non-federal partners.

We grouped the identified terrorism-related information sharing mechanisms into the following broad categories.

- **Agency offices and organizations used to execute agency missions—**includes key offices, organizations, and programs within DHS, DOJ, and ODNI that share terrorism-related information as part of their defined mission or purpose;
- **Working groups, committees, councils, and programs used to facilitate coordination—**includes interagency working groups, committees, councils, and programs that help build relationships and partnerships, share information on threats (including those that are terrorism-related), and facilitate coordination across criminal justice and homeland security entities at all levels of government; and
- **Technological platforms, systems, and databases used to document, store, and make information available—**includes technological platforms or information systems that contain information used to execute criminal justice and homeland security-related missions, to include counterterrorism.

The following tables provide a descriptive overview of these mechanisms, by department, as well as their purpose, intended audience or customers, select statistics on the number of users and products produced or contained within them (as available), and means by which those

customers provide feedback to DHS, DOJ, and ODNI on the information that is shared.[1]

Table 4: Department of Homeland Security Information Sharing Mechanisms

Agency Offices and Organizations

Name	Description and Purpose
National Threat Evaluation and Reporting Office	The DHS Office of Intelligence and Analysis' National Threat Evaluation and Reporting Office, established in 2019, provides law enforcement and homeland security partners with resources and training to assist in identifying and preventing targeted violence and mass casualty incidents, including terrorism. National Threat Evaluation and Reporting is the program and training lead for the Nationwide Suspicious Activity Reporting Initiative to assist partners in identifying, reporting, and sharing suspicious activity. Moreover, the National Threat Evaluation and Reporting Office's Master Trainer Program, established in 2020, certifies federal, tribal, state, local, and territorial partners in behavioral threat assessment and management to assist local communities in preventing targeted violence.
Office of Intelligence and Analysis— Counterterrorism Mission Center	Within DHS, the Office of Intelligence and Analysis is responsible for collecting, analyzing, integrating, and disseminating intelligence and other information related to terrorism. In 2018, the office realigned its structure to create five mission centers tasked with a mission goal focused on mitigating threats to the homeland. Mission centers collect information to address DHS and national priorities and provide available reporting from federal, tribal, state, local, and territorial partners to the U.S. Intelligence Community and other partners.[a] Of the five mission centers developed, the Counterterrorism Mission Center is responsible for synthesizing and integrating counterterrorism intelligence from all federal, tribal, state, local, and territorial partners for distribution within DHS and to its partners. It therefore develops all-source finished intelligence products on both international and domestic terrorism that are shared with federal, tribal, state, local, territorial, and private sector partners through dissemination across platforms run by DHS and other organizations.
Office of Partnership and Engagement	The Office of Partnership and Engagement coordinates the Department of Homeland Security's outreach efforts with critical stakeholders nationwide, including tribal, state, local, and territorial governments, elected officials, and law enforcement; the private sector; and colleges and universities, to ensure a unified approach to external engagement. The Office of Partnership and Engagement advocates and represents interests of these stakeholders through the Department's policy making process and is also a conduit for the Secretary to engage with stakeholders or share information.

[a]The U.S. Intelligence Community consists of 18 organizations, such as the intelligence components of the five military services within the Department of Defense as well as the Central Intelligence Agency, which is an independent agency. These organizations independently and collaboratively gather, analyze, and produce the intelligence necessary to conduct foreign relations and national security activities.

[1]We did not assess the extent to which there is duplication, fragmentation, and overlap in how federal agencies share terrorism-related information with non-federal partners because it was outside the scope of our review.

Working Groups, Committees, Councils, and Programs

Name	Description and Purpose
Corporate Security Symposia	The Corporate Security Symposia, sponsored and hosted by the DHS Office of Intelligence and Analysis, provides a forum for public and private sector partners to discuss current and emerging security threats relevant to their regions, with a strong focus on the businesses, infrastructure, and cyber security systems within them. Events feature speakers from both the public sector and the private sector on issues such as cyber security, infrastructure protection, global intelligence, communications, border security, and insider threats. According to DHS, from 2017 through 2021, the Office of Intelligence and Analysis has hosted over 40 of these events with around 8,600 combined participants.
Public-Private Analytic Exchange Program	The Public-Private Analytic Exchange Program, sponsored by the DHS Office of Intelligence and Analysis on behalf of ODNI, facilitates collaborative partnerships between members of the private sector and teams of experienced U.S. government analysts. Program participants work to create joint analytic deliverables (e.g., reports or presentations) of interest to both the private sector and U.S. government; some of these deliverables address terrorism issues.
State and Local Fellows Program	The DHS Office of Intelligence and Analysis' State and Local Fellows Program is designed to integrate state and local partners into the intelligence and information sharing processes across the federal government and the Intelligence Community. The program enables state and local partners to collaborate with DHS and the Intelligence Community in order to ensure that threat information is most effectively shared between all levels of government.
State and Local Intelligence Council	The DHS Office of Intelligence and Analysis established the State and Local Intelligence Council to create a trusted community of state and local professionals from the homeland security, intelligence, law enforcement, and emergency responder communities who utilize and share homeland security information to address threats to the U.S. The council is a practitioner-level forum that reviews and provides feedback to facilitate and enhance the operational sharing of information between the Office of Intelligence and Analysis and state and local partners.

Technological Platforms, Systems, and Databases

Name	Description and Purpose
Homeland Security Information Network	The Homeland Security Information Network is DHS' official system for trusted sharing of Sensitive But Unclassified information among federal, tribal, state, local, territorial, international, and private sector partners. Mission operators use the network to access homeland security data, send requests securely between agencies, manage operations, coordinate planned event safety and security, respond to incidents, and share the information they need to fulfill their missions. The Homeland Security Information Network maintains numerous communities of interest—customized portals within the larger site dedicated to specific topics. In particular, DHS uses the Intelligence Community of Interest to share Sensitive But Unclassified intelligence products with federal and non-federal partners, to include those related to terrorism. To be eligible to access this specific site, users must, at a minimum, be a current, full-time employee of a law enforcement, criminal justice, intelligence, or homeland security government agency, and directly support information and intelligence analysis, sharing, or collection activities.

Source: GAO. I GAO-23-105310

Table 5: Department of Justice and Federal Bureau of Investigation Information Sharing Mechanisms

Agency Offices and Organizations

Name	Description and Purpose
FBI Field Offices	The FBI's 56 field offices regularly engage in terrorism information exchange with federal and non-federal law enforcement partners via the Joint Terrorism Task Forces and the National Network of Fusion Centers. Currently, there are 98 FBI personnel—Special Agents, Intelligence Analysts, and Professional Staff—assigned to 69 of the 80 fusion centers in operation across the country. Eight fusion centers are co-located with the FBI, operating from an FBI office or in a shared space where the FBI is paying the lease. In addition to directly coordinating with non-federal law enforcement personnel through fusion centers or direct communications, FBI field offices also disseminate Situational Information Reports to those entities, which contain actionable criminal or terrorism information, as well as other intelligence information pertinent to all threat programs within the FBI field office's area of responsibility. Field offices use their intelligence collection and analysis capabilities to facilitate this information sharing function.
Joint Terrorism Task Forces and Executive Boards	Joint Terrorism Task Forces are the FBI's counterterrorism task forces in the field for leading and coordinating the operational law enforcement counterterrorism response and other related activities within the authority of the Attorney General. These task forces are composed of FBI personnel and co-located deputized partners from federal and non-federal law enforcement agencies within a specific area of responsibility. All individuals working on the task force are under FBI supervision, have a security clearance, have a signed non-disclosure agreement, and must follow FBI policies (to include the FBI's rules on sharing information). All Joint Terrorism Task Forces investigate and share information for international and domestic terrorism. Joint Terrorism Task Forces serve as information sharing mechanisms in several ways. First, non-FBI task force members are fully integrated into FBI operations as investigators, which provides them access to (operational) investigative information as well as access to classified terrorism information. According to the FBI, Task Force Officers fulfill investigative responsibilities on the task force and act as a liaison between the FBI and their home agency. These Task Force Officers have access to international and domestic terrorism information. As a part of the Joint Terrorism Task Forces, each FBI field office hosts a Joint Terrorism Task Force Executive Board, which consists of command personnel representing the agencies from which the Task Force Officers are assigned within their respective area of responsibility. According to the FBI, over 500 non-federal and 50 federal agencies have Task Force Officers assigned to Joint Terrorism Task Forces across the country. The number of task forces and participants has remained relatively constant over the last five years, with full-time Task Force Officer representation in over 200 locations, including each of the FBI's 56 field offices.
Office of Partner Engagement	The FBI Office of Partner Engagement, based in FBI headquarters, liaises with federal and non-federal law enforcement partners and aids in sharing information on domestic terrorism and other topics with those partners. Part of the Intelligence Branch, the office serves as the FBI's primary liaison for the law enforcement community on a national level, representing the perspectives of chiefs, sheriffs, and law enforcement associations within the FBI. The Office of Partner Engagement cultivates active relationships and meets regularly with executive boards of law enforcement associations, key members of federal agencies, and operational divisions within the FBI. The office shares unclassified products on both terrorism and non-terrorism in a number of different ways, to include posting them on unclassified FBI systems; attending national and regional law enforcement conferences; and hosting or participating in national, regional, or small group teleconferences with law enforcement partners, when appropriate, to provide situational awareness of upcoming events, threats, or issues. In addition, the Office of Partner Engagement provides training and support to fusion center personnel as well as FBI personnel assigned to liaise with the fusion centers.

Name	Description and Purpose
Office of Private Sector	The FBI Office of Private Sector, based in FBI headquarters, works to enhance the FBI's understanding of the private sector's risks and needs and increase collaboration and information sharing between the FBI and the private sector.

Working Groups, Committees, Councils, and Programs[a]

Mechanism Name	Description and Purpose
Criminal Intelligence Coordinating Council	The Criminal Intelligence Coordinating Council is a group under the U.S. Department of Justice's Global Justice Information Sharing Initiative, an advisory body to the U.S. Attorney General. Since 2001, the council has played a role in numerous efforts and initiatives to develop and improve federal and non-federal law enforcement and homeland security agencies' ability to share criminal and terrorism intelligence. These efforts include the establishment of fusion centers, the Nationwide Suspicious Activity Reporting Initiative, and the continued implementation of intelligence-led policing. The council also collaborates with federal partners, including DOJ, DHS, and ODNI. The FBI Office of Partner Engagement's Assistant Director is a member of the council.
Domestic Terrorism Executive Committee	The Domestic Terrorism Executive Committee helps to ensure national-level coordination on domestic terrorism issues. It consists of senior officials from DOJ's National Security Division, Civil Rights Division, Tax Division, as well as the FBI, U.S. Attorney community, and other federal law enforcement agencies who work on domestic terrorism issues. According to DOJ, the committee is a forum in which information on domestic terrorism is shared among partner agencies. While this forum engages in information sharing, it is generally at a broader policymaking level, and the group does not create discrete information products.
U.S. Attorneys' Anti-Terrorism Advisory Council	Established after 9/11, Anti-Terrorism Advisory Councils are specialized coordinating bodies overseen by U.S. Attorneys within their districts that work to ensure information is shared on terrorism investigations. The councils work in partnership with Joint Terrorism Task Forces and coordinate among FBI field offices and their respective counterparts in federal, state, and local law enforcement and intelligence agencies in conducting international and domestic terrorism investigations. According to DOJ, there are currently 93 councils across the country.

[a]According to the FBI, the below list should not be considered a comprehensive list of all working groups or task forces that exist between the FBI and its non-federal partners, as FBI field offices may have established working groups or task forces with its local partners, as well as task forces that are created based on need.

Technological Platforms, Systems, and Databases

Name	Description and Purpose
eGuardian	eGuardian is an information system owned, managed, and used by the FBI. It was developed in 2007 to meet the challenges of collecting and sharing information about terrorism-related activities amongst law enforcement agencies across jurisdictions. The system is a Sensitive but Unclassified information sharing platform hosted by the FBI, and it is accessed through the Law Enforcement Enterprise Portal. The FBI, Department of Defense, and non-federal partners use eGuardian to share Suspicious Activity Reports, which are official documentation of observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activities associated with terrorism. The FBI migrates the information captured in eGuardian to its internal Guardian system, a classified system housing records. After reviewing the Suspicious Activity Report, the FBI assigns the incident to the appropriate Joint Terrorism Task Force or squad to investigate.

Name	Description and Purpose
InfraGard Portal	InfraGard is an information sharing and analysis partnership between the FBI and individual U.S. citizens. According to the FBI, the InfraGard program provides a vehicle for public-private collaboration with government that expedites the exchange of information and promotes mutual learning opportunities relevant to the protection of critical infrastructure. The InfraGard Portal is a network platform where information on possible threats against critical infrastructure is shared with individual members who have been vetted by respective FBI Field Offices to receive information from the FBI. The portal contains information at the unclassified level, with the highest classification of For Official Use Only. No Law Enforcement Sensitive information is shared.
Law Enforcement Enterprise Portal	The Law Enforcement Enterprise Portal is a secure platform for law enforcement agencies, intelligence groups, and criminal justice entities. The portal provides web-based investigative tools and analytical resources, and enables user collaboration in a secure environment while offering customized tools to assist in case analysis and share departmental documents. For example, the portal contains a link to the Regional Information Sharing Systems Network, another key mechanism for sharing terrorism-related information. According to the FBI, the portal is designed to protect and manage access to systems by federal, tribal, state, local, and territorial criminal justice, national security, and public safety communities. Select international entities and private sector individuals also access the portal to share information with federal, tribal, state, local, and territorial agencies. The portal provides access to national security, public safety, and terrorism information contained within dozens of federal information systems. It also connects users to other federations serving the United States Intelligence Community, the criminal intelligence community, and the homeland security community.
National Data Exchange	The National Data Exchange system is an unclassified national information sharing system that enables criminal justice agencies to search, link, analyze, and share federal, tribal, state, and local records. The system also functions as a strategic investigative information sharing system that fills informational gaps and provides situational awareness on suspects, and is accessible via the FBI's Law Enforcement Enterprise Portal. According to the FBI, the system complements other well-known FBI systems, such as the National Crime Information Center, that provide critical information to the criminal justice community, by allowing the user to search these multiple data systems. All of the information contained within or disseminated by the system is already collected by criminal justice agencies when fulfilling their official criminal justice functions. The system aggregates already existing criminal justice information and makes linkages between that information that were previously not apparent.
Regional Information Sharing Systems	The Regional Information Sharing Systems is a nationwide program which assists federal, tribal, state, and local criminal justice partners by providing services that facilitate information sharing, support criminal investigations, and promote officer safety. According to the FBI, it enables the sharing of information from different platforms, databases, or systems using a federated distributed model that allows the owner of key data to maintain information and system users to search for it through a federated search engine.

Name	Description and Purpose
Threat Screening System	The Terrorist Screening Center maintains the Threat Screening System (formerly known as the Terrorist Screening Database) to serve as the U.S. Government's consolidated watchlist for terrorism screening information. The current terrorist watchlisting process supports the U.S. Government's efforts to combat terrorism by (1) consolidating the watchlist within the Threat Screening System; (2) helping screeners and intelligence agencies accurately identify watchlisted persons; (3) providing screeners with information to help them respond appropriately during encounters with watchlisted persons; and (4) subsequently ensuring information about the watchlisted persons gathered during the encounter is available for use in assessing threats and supporting investigations. The collected information may be used to enhance subject record within the Terrorist Identities Datamart Environment, the U.S. Government's classified, central repository of information on international terrorist identities, which is owned by the National Counterterrorism Center, within the Office of the Director of National Intelligence. In this way, the watchlisting process functions as a continuous cycle whereby information is added to or deleted from the watchlist after appropriate analysis.

Source: GAO. I GAO-23-105310

Table 6: Office of the Director of National Intelligence Information Sharing Mechanisms

Agency Offices and Organizations

Name	Description and Purpose
Office of Domestic Engagement, Information Sharing, and Data	The ODNI Office of Domestic Engagement, Information Sharing, and Data is responsible for building, enabling, and maintaining domestic partnerships with federal stakeholders, as well as tribal, state, local, and private sector organizations, to include industry, non-government organizations, and academia.
National Counterterrorism Center	The ODNI National Counterterrorism Center serves as the primary organization in the U.S. government for integrating and analyzing all intelligence pertaining to terrorism possessed or acquired by the U.S. government (except exclusively domestic terrorism). The Center serves as the central and shared knowledge bank on terrorism information and provides all-source intelligence support to government-wide counterterrorism activities. The Center also serves as the principal advisor to the Director of National Intelligence on intelligence operations and analysis relating to counterterrorism. Among other things, the Center produces Joint Intelligence Bulletins that communicate updated threat information and assessments to federal, tribal, state, and local partners at the Unclassified/Law Enforcement Sensitive level. As a joint product, Joint Intelligence Bulletins are distributed by the National Counterterrorism Center, FBI, and DHS co-authors through their respective channels, such as Joint Terrorism Task Forces and fusion centers. The bulletins may include information to alert partners to significant arrests—including those accomplished through collaboration among different law enforcement entities—and trends observed in both domestic and international terrorism.

Groups, Committees, and Councils

Name	Description and Purpose
Federal, State, Local, and Tribal Partnerships Group	Located within the ODNI Domestic Engagement, Information Sharing and Data office, the Federal, State, Local, and Tribal Partnerships Group establishes and strengthens trusted partnerships and programs that foster effective information sharing and oversaw the execution of the statutory duties and responsibilities of the Program Manager for the Information Sharing Environment. Specifically the partnership group • Facilitates coordination and collaboration between the Intelligence Community and federal and non-federal partners by planning and executing advisory boards and working groups, and participating in conferences and national meetings to establish, maintain, and enhance partnerships. • Promotes and facilitates intelligence and information sharing between agencies, by establishing relationships with federal and non-federal leaders and intelligence professionals, and bringing together mission partners to identify and address common mission requirements and goals. • Identifies information sharing barriers and opportunities to enhance the domestic intelligence and information sharing enterprise. As part of its mission, the partnership group oversees and manages the ODNI's Homeland Security and Law Enforcement Program, which provides the ODNI and the Intelligence Community opportunities to gain perspectives on homeland security and law enforcement partners' intelligence needs and capabilities.
Homeland Security and Law Enforcement Partners Advisory Board	The DNI's Homeland Security and Law Enforcement Partners Advisory Board is an external advisory group to the DNI and other senior intelligence officials and is comprised of 12 state and local executives who serve as leaders in national level professional law enforcement associations. The board provides an opportunity for the Intelligence Community and state and local partners to discuss national security threats, and for the Intelligence Community to hear the state and local perspectives on national security threats and homeland security and law enforcement priorities.
Federal, State, Local, and Tribal Working Group	According to ODNI, the Federal, State, Local, and Tribal Working Group serves as a forum for discussion and shared understanding of federal and non-federal partner engagement efforts. The working group includes membership from ODNI and FBI Office of Partner Engagement, DHS Office of Intelligence and Analysis, Office of National Drug Control Policy, and the Drug Enforcement Agency. The working group: • Coordinates ODNI engagement with Federal, State, Local, and Tribal partners to ensure shared situational awareness of the activities of all parties in the Group; • Synchronizes ODNI partnership efforts to de-conflict law enforcement activities of Group members; and • Shares information on engagement best practices and lessons learned.

Source: GAO. I GAO-23-105310

Table 7: Joint Information Sharing Mechanisms

Name	Description and Purpose
Domestic Director of National Intelligence Representative Program	The Domestic DNI Representative Program is one of three DNI Representative Programs described in Intelligence Community Directive 402 and is a joint initiative between ODNI and the FBI that facilitates intelligence integration and coordination among Intelligence Community, federal, and non-federal partners on national security issues in the homeland.

Name	Description and Purpose
Domestic Security Alliance Council	The Domestic Security Alliance Council program is a strategic partnership between the FBI, DHS, and U.S. private sector intended to enhance timely communications and effective exchange of security and intelligence information between the federal government and the private sector. The council also maintains a portal that its members can use to access critical, unclassified information from the FBI and DHS that has relevance for the private sector, and upload that information for sharing amongst fellow council members.
Joint Counterterrorism Assessment Team	The Joint Counterterrorism Assessment Team is a joint DHS, FBI, and National Counterterrorism Center organization that produces primarily unclassified counterterrorism-focused products for tribal, state, local, and territorial partners. The mission of the Joint Counterterrorism Assessment Team is to improve information sharing and enhance public safety. ODNI's National Counterterrorism Center, the FBI, and DHS collaborate with tribal, state, local, and territorial fellows, and other members of the Intelligence Community to research, produce, and disseminate counterterrorism intelligence products for federal, non-federal, and private sector entities.
National Network of Fusion Centers	Fusion Centers are state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between tribal, state, local, territorial, federal, and private sector partners. The National Network of Fusion Centers consists of 80 state and major urban area fusion centers. Fusion centers are owned and operated by state and local entities with support from federal personnel, training, technical assistance, exercise support, security clearances, grants technology, and connectivity to federal information. Both FBI and the DHS Office of Intelligence and Analysis have field personnel assigned to almost every fusion center to assist with bi-directional information sharing efforts. For the FBI, engagement with fusion centers is not limited to field personnel assigned to liaise with the centers. Rather, information can be exchanged between fusion centers and management of FBI field offices, to include Special Agents in Charge.

Source: GAO. I GAO-23-105310

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Triana McNeil, (202) 512-6691, McNeilT@gao.gov

Staff Acknowledgments

In addition to the contact named above, the following individuals made important contributions to this report: Jan Montgomery, Assistant General Counsel; Mona Nichols Blake, Assistant Director; Anthony DeFrank, Analyst-in-Charge; Jason Blake; Ben Crossley; Amanda Miller; Janet Temko-Blinder; and Christopher Zubowicz.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

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

Strategic Planning and External Liaison

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