



Report to Congressional Requesters

January 2026

FBI INVESTIGATIVE ACTIVITIES

(U//FOUO) Oversight
Efforts of Opening and
Conducting
Assessments Should
be Strengthened



FBI INVESTIGATIVE ACTIVITIES

Oversight Efforts of Opening and Conducting Assessments Should Be Strengthened

GAO-26-106994SU

January 2026




A report to congressional requesters.
For more information, contact: Triana McNeil at McNeilT@gao.gov.

What GAO Found

The Federal Bureau of Investigation (FBI) can open assessments with an authorized purpose and clearly defined objective and without a particular factual predication. An assessment may be conducted to collect information or facts to determine if there is a criminal or national security threat and requires the FBI to use the least intrusive method to obtain information. (U//FOUO) Our analysis of FBI data found that from 2018 through 2024, the FBI opened and subsequently closed about 127,000 assessments. Of these assessments, about 14 percent of Type I/II assessments were converted into an investigation, which has different requirements to open.

Comparing Assessments and Investigations

FOR OFFICIAL USE ONLY

Assessments...	Investigations...
 gather information to determine if a potential threat or criminal activity warrants an investigation,	gather evidence and further build a case for potential prosecution or other law enforcement actions
 require an authorized purpose but not any particular factual predication.	require allegations, reports, facts, or circumstances indicative of possible criminal activity or a threat to national security
 use investigative methods of relatively low intrusiveness, such as searching public records.	can use all lawful investigative methods such as polygraphs and undercover operations.

(U) Source: GAO analysis of the Attorney General’s Guidelines for Domestic FBI Operations; Icon-Studio/adobestock.com. | GAO-26-106994SU

FOR OFFICIAL USE ONLY

(U//FOUO) The FBI relies on staff to self-report noncompliance with assessment policy requirements. The FBI noted that self-reporting likely undercounts actual noncompliance, but has not assessed if other tools could identify it. Assessing whether other tools exist would help the FBI determine when assessments should receive compliance reviews.

(U//FOUO) About every 4 years, each FBI field office receives a National Security Review, in which the Department of Justice (DOJ) audits, among other things, a sample of national security assessments and recommends corrective actions as necessary. In June 2025, the FBI began a new process to address recommendations from National Security Reviews but has not identified who permanently will be responsible for the process to ensure recommendations are addressed. Identifying staff to lead the process would help the FBI ensure these recommendations are addressed.

(U//FOUO) The FBI does not share potentially useful information from National Security Reviews conducted at one field office with other field offices. Our analysis of selected National Security Review recommendations found commonalities among instances of noncompliance. Shared information from National Security Reviews across field offices may help the FBI proactively take steps to improve noncompliance across the agency.

Why GAO Did This Study

The FBI states it takes a leadership role to identify and address emerging threats and continually reviews and evaluates intelligence and information from multiple sources to ensure it appropriately identifies and categorizes national security threats. The FBI opens assessments for multiple reasons, including to protect against federal crimes or threats to the national security or to collect foreign intelligence.

GAO was asked to review data on the number of assessments the FBI opened and FBI requirements for opening and conducting assessments. This report (1) describes FBI procedures for opening and conducting assessments and information on how many Type I/II and Type III assessments the FBI opened and subsequently closed from 2018 through 2024, and (2) evaluates the extent DOJ and FBI oversee the implementation of FBI requirements for opening and conducting assessments.

GAO reviewed policies the FBI is to follow for opening and conducting assessments and analyzed assessment data from 2018 through 2024. GAO also reviewed FBI assessment data and found it sufficiently reliable for these purposes. Further, GAO reviewed DOJ and FBI reports on assessments and conducted site visits to three FBI field offices interviewing staff and supervisors. These field offices were among those that opened the most assessments from 2018 through 2023.

What GAO Recommends

GAO is making three recommendations related to improving how the FBI identifies noncompliance in assessments. The FBI concurred with all recommendations.

Contents

Letter		1
	Background	6
	(U//FOUO) The FBI Has a Process to Open and Conduct Assessments Concerning Federal Crimes or National Security and Opened Approximately 127,000 From 2018 to 2024	10
	(U//FOUO) The FBI Undercounts Noncompliance with Assessment Policy by Relying on Self-Reporting and Infrequent Audits	35
	Conclusions	44
	Recommendations for Executive Action	45
	Agency Comments	46
Appendix I	Review and Approval Process for Assessments Involving a Sensitive Investigative Matter	48
Appendix II	GAO Contacts and Staff Acknowledgments	52
Tables		
	(U//FOUO) Table 1: Characteristics of Federal Bureau of Investigation (FBI) Assessment Types as Described in the Domestic Investigations and Operations Guide	7
	Table 2: Federal Bureau of Investigation Categories of Investigations That May Result From Assessments	9
Figures		
	(U//FOUO) Figure 1: Federal Bureau of Investigation's Process for Staff to Open and Conduct a Type I/II Assessment	12
	(U//FOUO) Figure 2: Federal Bureau of Investigation's Process for Staff to Open and Conduct a Type III Assessment	14
	(U//FOUO) Figure 3: Authorized Investigative Methods for Federal Bureau of Investigation Assessments	16
	(U//FOUO) Figure 4: Description and Characteristics of a Sensitive Investigative Matter	19
	(U//FOUO) Figure 5: Total Number of Federal Bureau of Investigation Type I/II and Type III Assessments Opened and Subsequently Closed, by Type, 2018-2024	22

(U//FOUO) Figure 6: Percent of Type I/II and Type III Assessments Not Converted to Investigations Closed Within Time Period of Supervisory Reviews, by Type, 2018-2024	24
(U//FOUO) Figure 7: Number of Federal Bureau of Investigation Type I/II and Type III Assessments Opened and Subsequently Closed Designated as a Sensitive Investigative Matter (SIM), by Type, 2018-2024	26
(U//FOUO) Figure 8: Number of Type I/II and Type III Assessments Opened and Subsequently Closed Designated as a Sensitive Investigative Matter (SIM), by Type and Category of SIM, 2018 to 2024	27
(U//FOUO) Figure 9: Percent of All Type I/II and Type III Assessments and Those Designated a Sensitive Investigative Matter (SIM) Closed Within Time Period of Supervisory Reviews, by Type, 2018-2024	30
(U//FOUO) Figure 10: Number of Threat to Life Incidents Opened and Subsequently Closed as Type I/II and Type III Assessments, by Type, 2018-2024	32
(U//FOUO) Figure 11: Percent of All Type I/II and Type III Assessments and Threat to Life Incidents Opened as Type I/II and Type III Assessments Closed Within Time Period of Supervisory Reviews, by Type, 2018-2024	34
(U//FOUO) Figure 12: Characteristics of Type I/II and Type III Assessment Compliance Reviews	38

Abbreviations

DIOG	Domestic Investigations and Operations Guide
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
NSCLB	National Security and Cyber Law Branch
SIM	Sensitive Investigative Matter



January 8, 2026

Congressional Requesters

Within the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI) is responsible for investigating federal crimes and threats to national security. An initial investigative action the FBI can take is to open and conduct an assessment, which generally involves seeking information about activities or threats related to violations of federal crimes or national security.¹ (U//FOUO) The FBI is authorized by policy to collect information through, among other sources, public information records; information already collected within the FBI, DOJ, and other government agencies; online services; confidential human sources; and physical surveillance that does not require a court order.² (U//FOUO) According to FBI policy, assessments must include an authorized purpose and clearly defined objective and can be opened without a particular factual predication.³ Members of Congress and external interest groups have raised concerns that a low threshold to open assessments and broad authorities could lead to abuses by the FBI.

According to the FBI, it takes a leadership role in identifying and addressing emerging threats and continually reviews and evaluates intelligence and information from multiple sources to ensure it

¹FBI policy gives the word 'assessment' multiple meanings. For purposes of this report, an assessment is an investigative activity as defined in the FBI's Domestic Investigations and Operations Guide, Section 5. Specifically, we refer to Type I/II and Type III assessments, which generally involve seeking information related to activities or threats related to violations of federal crimes or national security.

²A Confidential Human Source is any individual who is believed to be providing useful and credible information to the FBI for any authorized information collection activity, and from whom the FBI expects or intends to obtain additional useful and credible information in the future, and whose identity, information, or relationship with the FBI warrants confidential handling, *The Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources* (Washington, D.C. 2020). In addition to those listed above, additional investigative methods may be authorized depending on the assessment type. FBI, *Domestic Investigations and Operations Guide* (Washington, D.C.; Jan. 3, 2024).

³(U//FOUO) FBI policy further notes that an authorized purpose must be for an authorized national security, criminal, or foreign intelligence collection purpose. FBI, *Domestic Investigations and Operations Guide* (Washington, D.C.; Jan. 3, 2024); Department of Justice, *Attorney General's Guidelines for Domestic FBI Operations*, (Washington, D.C. Sept. 29, 2008).

appropriately identifies and categorizes national security threats.⁴ The Attorney General's Guidelines for Domestic FBI Operations, which govern the FBI's investigative activities, state the FBI cannot be content to wait for leads to intervene and prevent criminal or national security events before they occur.

You asked us to review data on FBI assessments and the agency's policies for overseeing and implementing requirements for opening and conducting assessments. This report (1) describes FBI procedures for opening and conducting assessments and provides information on how many Type I/II and Type III assessments the FBI opened and closed from 2018 through 2024 and (2) evaluates the extent to which the DOJ and FBI oversee the implementation of FBI requirements for opening and conducting assessments.

To understand the procedures the FBI has for opening and conducting Type I/II and Type III assessments, we reviewed key documents that explain how the FBI is to oversee the implementation of FBI requirements for opening and conducting assessments. For example, we reviewed sections of the FBI's Domestic Investigations and Operations Guide (DIOG), which contains internal policy guidance and procedures that govern aspects of FBI operational and intelligence activities and administrative functions, and the *Department of Justice Attorney General's Guidelines for Domestic FBI Operations*.⁵

Further, we analyzed from the FBI Sentinel system Type I/II and Type III data of assessments that were opened and subsequently closed from calendar year 2018 through 2024, including assessments that FBI closed

⁴Federal Bureau of Investigation, Department of Homeland Security, *Strategic Intelligence Assessment and Data on Domestic Terrorism* (Washington, D.C.; Oct. 2022).

⁵The FBI occasionally updates the DIOG based on revisions to policy. To complete our analysis, we reviewed the DIOG released March 31, 2020, updated September 17, 2021, along with provisions in the *Attorney General's Guidelines for Domestic FBI Operations*. Collectively, we refer to these policies in our review as FBI policy. In June 2025, the FBI provided us with excerpts from the DIOG released January 3, 2024. We used the January 3, 2024 version to complete our analysis when there were relevant changes to policy.

and converted to an investigation.⁶ (U//FOUO) The data included the dates the assessment was opened and closed, its type, which field office opened it, and whether it was designated a Sensitive Investigative Matter (SIM). Assessments can pertain to certain types of organizations or individuals, and can also be designated as a Threat to Life, which is used to identify any incident that contains information of a threat to human life, serious bodily injury, or significant violent action.⁷ The data also included the outcome of the assessment, such as whether the FBI converted the assessment to an investigation or closed with no further action. We analyzed the data by these variables and identified trends across the years.

We also conducted site visits to FBI field offices in Sacramento, California; Boston, Massachusetts; and New York City, New York. (U//FOUO) We selected these field offices because they were among the top five field offices that opened the most assessments between 2018 through 2023.⁸ At each field office, we interviewed agents who conduct assessments, and separately interviewed supervisors who review and approve opening them, and the field office's Chief Division Counsel and

⁶Sentinel is an FBI information and case management system used to enter, review, approve, and research investigative activities including assessments. Unless noted otherwise, all numbers and figures reported from FBI's assessment data includes all assessments that were opened and subsequently closed (including those assessments that were closed and converted to investigations) from 2018 to 2024. *The Department of Justice Attorney General's Guidelines for Domestic FBI Operations* distinguishes assessments from "predicated" investigations that are opened based on allegations, reports, facts or circumstances indicative of possible criminal or national security-threatening activity and include preliminary or full investigations and enterprise investigations, which are a type of full investigations. For purposes of this report, we refer to all types of predicated investigations as "investigations" and activities conducted under assessments as "assessments."

⁷(U//FOUO) The FBI uses the terms "complaint," and "incident" to refer to information obtained by the FBI that could prompt an investigative activity. Additionally, the term "incident" is used to refer to opened assessments. For the purposes of this report, we use the term "incident" to describe both information obtained prior to opening an assessment or an opened Type I/II or Type III assessment.

⁸We used data between 2018 and 2023 to select which FBI field offices to visit because we did not yet have 2024 assessment data.

Division Compliance Officer.⁹ Finally, we asked each group questions pertaining to how they identify and report noncompliance with Type I/II and Type III assessments and what training or guidance they receive about these assessments. We asked each group questions about the procedures they follow for opening and conducting assessments and the extent to which they can follow them. The information from our site visits is not generalizable to the experiences of all FBI staff across the country, but provides perspectives about how the FBI opens and conducts Type I/II and Type III assessments.

To assess the reliability of the data, we conducted various tests, reviewed documentation on the FBI data systems that produced the data and interviewed knowledgeable FBI officials about the data system. We determined that the data were sufficiently reliable to report descriptive statistics on Type I/II and Type III assessments for the years we reviewed.

To evaluate the extent the DOJ and FBI oversee the implementation of requirements for opening and conducting assessments, we reviewed each of the five FBI DIOG audit reports the agency completed on Type I/II and Type III assessments since 2013 through fiscal year 2024.¹⁰ We analyzed these reports to identify, for each audit, its scope; the number of assessments audited; and if the audit identified observations, instructions, or recommendations, and if so, what they were.¹¹ We analyzed DOJ audits of Type I/II assessments in the most recent National Security Reviews, conducted at each of the 56 FBI field offices, through December 31, 2024.¹² (U//FOUO) Each FBI field office receives a National Security

⁹The Chief Division Counsel (CDC) is the principal legal advisor within each FBI field office. The Division Compliance Officer reports potential noncompliance to the proper FBI officials and to the FBI Legal Compliance and Enterprise Risk Unit, Inspection Division. (U//FOUO) The FBI states it has an organizational request pending approval by the Office of Management and Budget. The request integrates the Legal Compliance and Enterprise Risk Unit into the Inspection Division. Part of the Office of Integrity and Compliance has been reporting through the Inspection Division since May 30, 2025. The Division Compliance Officer at the FBI Boston field office was unavailable at the time of our visit and later provided written responses to our questions.

¹⁰(U//FOUO) The assessments included in the earliest DIOG report we reviewed were opened between May 1, 2013 and April 30, 2014.

¹¹FBI policy states observations are findings of noncompliance and must be addressed by recommendations or instructions.

¹²During the years of our review, the FBI had 56 field offices and in fiscal year 2025, the FBI consolidated two field offices into one.

Review approximately every 4 years and these reviews identify whether a sample of assessments had a sufficient authorized purpose and if authorized investigative methods were used to conduct the work. For each review, we recorded the number of assessments reviewed; the number of assessments DOJ identified that had an insufficient or an undocumented authorized purpose; the number of assessments that used unauthorized investigative methods; and recommendations to address such instances. We assessed what actions the FBI takes in response to DIOG compliance reports and National Security Reviews against criteria from the Project Management Institute and GAO's Standards for Internal Controls in the Federal Government.¹³

We conducted this performance audit from August 2023 to January 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This product has been designated FOR OFFICIAL USE ONLY because of the sensitive nature of the information it contains. Because the unauthorized disclosure of the sensitive information contained in the product could reasonably be expected to cause a foreseeable harm to U.S. government or other interest protected by law, recipients may not discuss or release this product to anyone whose official duties do not require access to the information it contains. This product should be safeguarded when not being used and destroyed when no longer needed.

¹³Project Management Institute, Inc. *Process Groups: A Practice Guide* (2023). The Project Management Institute is a not-for-profit association that, among other things, provides standards for managing various aspects of projects, programs, and portfolios; GAO, *Standards for Internal Control in the Federal Government*, GAO-25-107721, (Washington, D.C., May 2025).

Background

The FBI is responsible for investigating allegations of federal law violations and threats to national security.¹⁴ Published in December 2008, the Attorney General's Guidelines for Domestic FBI Operations state that it was recognized that the FBI's functions needed to be expanded and better integrated to meet contemporary needs. These guidelines further state that in line with these objectives, the FBI reorganized and reoriented its programs and missions. The guidelines were extensively revised to effect a more complete integration and harmonization of standards to provide DOJ components with more clear, consistent, and accessible guidance for their activities. The guidelines also establish a set of basic principles that are to serve as the foundation for all FBI mission-related activities. The FBI states that these principles demonstrate respect for civil liberties and privacy as well as adherence to the Constitution and laws of the United States.

One of the investigative actions the FBI can take to address a potential threat to national security or potential violation of federal criminal law is through opening and conducting an assessment.¹⁵ (U//FOUO)

Assessments may be carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to national security or to collect foreign intelligence. The subject of an assessment can be an individual or organization that is potentially violating federal laws, posing a threat to national security, or is the target of those actions. The DIOG includes the standards and processes the FBI must follow when opening or conducting an assessment.

(U//FOUO) The FBI has authorized five types of assessments. Table 1 shows details about differences in the five types.

¹⁴See, e.g., 28 U.S.C. § 533 (authorizing the Attorney General to appoint officials to detect and prosecute crimes against the United States); 28 C.F.R. § 0.85(a) (providing that the FBI investigates violations of the laws of the United States, except in cases in which such responsibility is by statute or otherwise exclusively assigned to another investigative agency); Exec. Order No. 12333, 46 Fed. Reg. 59941 (Dec. 8, 1981) *amended by* Exec. Order No. 13284, 68 Fed. Reg. 4075 (Jan. 3, 2003), Exec. Order No. 13355, 69 Fed. Reg. 53593 (Aug. 27, 2004), Exec. Order No. 13470, 73 Fed. Reg. 45325 (July 30, 2008) (authorizing, among other things, the intelligence elements of the FBI to collect, analyze, produce, and disseminate foreign intelligence and counterintelligence in support of national and departmental missions).

¹⁵FBI employees can initiate some investigative activities prior to opening an assessment. Such investigative activities may be used when an FBI employee initially processes complaints, observations, or information prior to opening an assessment if they have a reason that is tied to an authorized FBI criminal or national security purpose.

(U//FOUO) Table 1: Characteristics of Federal Bureau of Investigation (FBI) Assessment Types as Described in the Domestic Investigations and Operations Guide

Type	Description	Assessment Target	Duration
I/II	Seek information, proactively or in response to investigative leads, relating to activities—or the involvement or role of individuals, groups, or organizations relating to those activities—constituting violations of federal criminal law or threats to the national security.	Individuals, groups, or organizations.	No time limit, but expected to be “relatively short.”
III	Identify, obtain and utilize information about actual or potential national security threats or federal criminal activities, or the vulnerability to such threats or activities.	Actual or potential threats within a field office’s area of responsibility.	As long as necessary to achieve its authorized purpose and clearly defined objective(s).
IV	Obtain and retain information to inform or facilitate intelligence analysis and planning.	Internal FBI information gaps.	As long as necessary to achieve its authorized purpose and clearly defined objective(s).
V	Seek information to identify potential human sources, assess their suitability, credibility, or value of individuals as human sources.	Individuals.	As long as necessary to achieve its authorized purpose and clearly defined objective(s) or when it is determined that the individual named subject cannot or should not be recruited as a confidential human source.
VI	Seek information, proactively or in response to investigative leads, relating to matters of foreign intelligence interest responsive to foreign intelligence requirements.	Information on foreign intelligence.	As long as necessary to achieve its authorized purpose and clearly defined objective(s).

Source: GAO analysis of FBI’s Domestic Investigations and Operations Guide. | GAO-26-106994SU

(U//FOUO) Note: In the original DIOG (Dec. 16, 2008), Types I/II assessments were separate. Because they, however, have many commonalities, the 2021 DIOG update states they were merged and named Type I/II assessments.

(U//FOUO) Multiple entities at the FBI are responsible for opening and conducting assessments. Tips from the public reported to the FBI’s National Threat Operation Center on threats and potential criminal activity are vetted and shared through one of the FBI’s internal data systems, Guardian.¹⁶ The FBI determines when tips warrant entering them into the Guardian system as an assessment or as “information only.” (U//FOUO) Multiple divisions within the FBI open and conduct assessments, such as the Counterterrorism Division and Criminal Investigative Division. Most assessments are opened and conducted by FBI field offices.

(U//FOUO) When FBI staff complete an assessment, supervisors must decide whether to close it with no further action or convert it into an

¹⁶The National Threat Operation Center is the central intake for all telephone and electronic tips from the public to the FBI.

investigation. The DIOG describes different requirements for opening and conducting assessments and investigations. For example, FBI policy states that assessments do not require particular factual predication, and the authorized investigative methods used in assessments are generally those of relatively low intrusiveness, such as checking government records and obtaining publicly available information.

According to FBI policy, initiating an investigation requires predication, such as allegations, reports, facts, or circumstances indicative of possible criminal or national security threatening activity. Converting assessments to investigations allows the FBI to gather additional evidence and further build a case for potential prosecution or other law enforcement actions. Investigations may include particular lawful methods that are not allowed in certain types of assessments. For example, DOJ policy states that investigations may employ polygraph examinations or undercover operations which are methods not allowed when conducting a Type I/II and Type III assessment. Investigations that stem from assessments—including Type I/II and Type III assessments—are divided into categories based on the amount of factual predication that exists. Table 2 provides details on the investigative categories the FBI can open.

Table 2: Federal Bureau of Investigation Categories of Investigations That May Result From Assessments

Investigative Category	Definition
Preliminary investigation	May generally be initiated based on any allegation or information indicative of federal criminal activity or threats to national security that have or may have occurred, is or may be occurring, or will or may occur in the future and the investigation may obtain information relating to the activity or the involvement of an individual, group, or organization in such activity. Additionally, a preliminary investigation may be initiated based on any allegation or information indicating an individual, group, organization, entity, information, property, or activity is or may, for example, be a target of attack in connection with criminal activity or threats to national security and the investigation may obtain information that would help protect against such activity or threat.
Full investigation	May be initiated if there is an articulable, factual basis that reasonably indicates the existence of federal criminal activity or a threat to national security and the investigation may obtain information relating to the activity or the involvement of an individual, group, or organization in such activity. Additionally, a full investigation may be initiated if there is an articulable, factual basis that reasonably indicates an individual, group, organization, entity, information, property, or activity is or may, for example, be a target of attack in connection with criminal activity or threats to national security and the investigation may obtain information that would help protect against such activity or threat. A full investigation may also be initiated if the investigation may obtain foreign intelligence that is responsive to a foreign intelligence requirement.
Enterprise investigation	May be initiated if there is an articulable, factual basis for the investigation that reasonably indicates that a group or organization may have engaged in, may be engaged in, or may have or may be engaged in planning, preparing, or providing support for: a pattern of racketeering activity as defined in 18 U.S.C. § 1961(5); international terrorism or other threat to national security, domestic terrorism as defined by 18 U.S.C. § 2331(5) involving the violation of federal criminal law, furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law; or a different offense described in 18 U.S.C. § 2332b(g)(5)(B) or 18 U.S.C. § 43.

Source: GAO analysis of The Attorney General's Guidelines for Domestic FBI Operations. | GAO-26-106994SU

Note: Not all assessments become investigations and may be closed without the FBI taking any further action.

DOJ and FBI Oversee Assessments

The DOJ and FBI each take steps to ensure the FBI follows requirements for conducting assessments. For example, the DOJ National Security Division conducts National Security Reviews that audit a sample of Type I/II assessments at FBI field offices. The FBI Office of the General Counsel National Security and Cyber Law Branch (NSCLB) consults with the DOJ to address any instances of noncompliance National Security Reviews identify. In addition, the FBI Inspection Division occasionally selects Type I/II and Type III assessments to audit to ensure FBI staff are following policies and procedures described in the DIOG. FBI officials also stated the FBI conducts field office inspections about every 4 years at each field office, in which it audits all the Type I/II and Type III assessments a field office opens within a specified year.

In 2020, the DOJ Inspector General examined assessments opened by the FBI Counterterrorism Division and reported various weaknesses

related to its assessment process that may have impacted its ability to fully investigate certain subjects who later committed terrorist attacks in the United States.¹⁷ The Inspector General recommended that in conjunction with another recommendation, the FBI should examine current field office initiatives that provide an ongoing mechanism to revisit subjects of closed assessments and investigations. The report states this examination should identify any legal, policy, and civil liberties implications so that a decision can be made as to whether all FBI field offices should undertake similar initiatives. The FBI concurred with this recommendation and in June 2025, officials from the Inspector General's office told us the FBI is working to implement it.

(U//FOUO) The FBI
Has a Process to
Open and Conduct
Assessments
Concerning Federal
Crimes or National
Security and Opened
Approximately
127,000 From 2018
to 2024

The FBI Established a
Formal Process for
Opening and Conducting
Assessments

(U//FOUO) FBI and DOJ policy guidelines provide FBI staff a structured process for opening and conducting assessments. In 2008, the FBI first published the DIOG, which establishes the standards and controls for conducting investigative activities, including assessments.¹⁸ The DIOG states that no particular factual predication is required to open an assessment, but it does require an authorized purpose and clearly

¹⁷Department of Justice, Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Efforts to Identify Homegrown Violent Extremist through Counterterrorism Assessments*, Audit Division 20-030 (Washington, D.C., March 2020).

¹⁸The FBI occasionally updates the DIOG based on revisions to policy. As of the time of this audit, the most recent DIOG version was released January 3, 2024. Additionally, the Attorney General's Guidelines for Domestic FBI Operations is incorporated into many sections in the DIOG.

defined objectives.¹⁹ The DIOG states that, although difficult to define, “no particular factual predication” is less than “information or allegation.” An assessment may be conducted when there is reason to collect information or facts to determine if there is a criminal or national security threat and there is a rational and articulable relationship between the stated authorized purpose, the information sought, and the proposed means to obtain that information.²⁰

(U//FOUO) To illustrate when an assessment can and cannot be conducted, the DIOG includes scenarios and the appropriate response. For example, the DIOG states that if a marina owner contacts a local FBI office stating that five Middle Eastern males have just rented a boat for 3 days and asked for marine charts, conducting an assessment would not be appropriate without additional information because there is no indication of criminal conduct, a threat to the national security, or information that might be foreign intelligence information. However, the DIOG distinguishes that if the owner also stated that five men, who appear to be Middle Eastern, asked the owner to circle the military installations and nuclear power plants on the marine charts, the DIOG states that conducting an assessment may be appropriate because of the potential for either criminal activity or a threat to the national security exists and provides an authorized purpose for conducting an assessment.

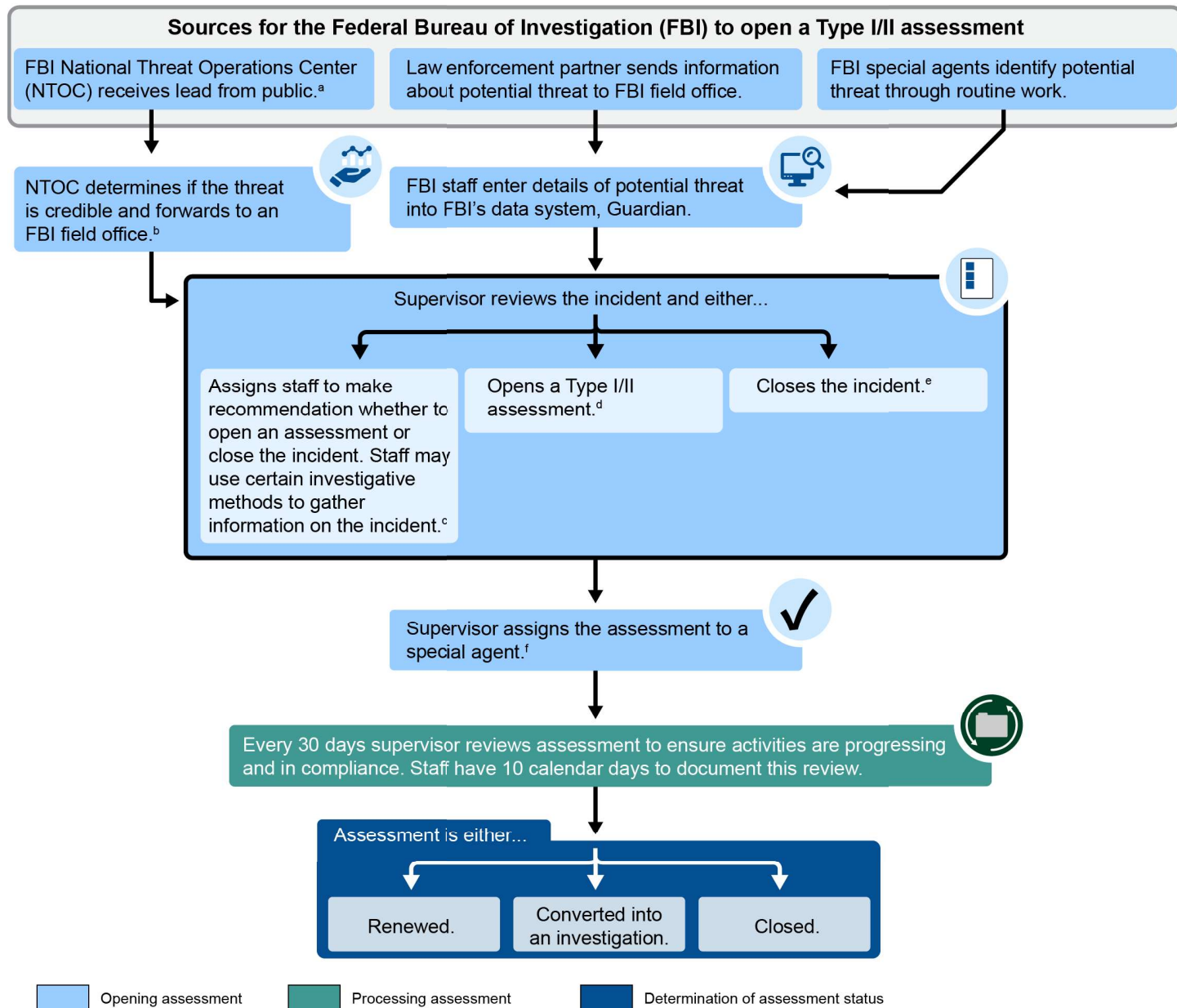
(U//FOUO) The FBI has a process for conducting Type I/II assessments in response to tips from multiple sources, as illustrated in figure 1. Type I/II assessments generally relate to information on activities—or the involvement or role of individuals, groups, or organizations relating to those activities—constituting violations of federal criminal law or threats to the national security.

¹⁹The DIOG further explains that although no particular factual predication is required, an assessment cannot be based on arbitrary or groundless speculation, nor solely on the exercise of First Amendment protected activities or based on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject.

²⁰See FBI, Domestic Investigations and Operations Guide Section 5.1 (Washington, D.C.; Jan. 3, 2024).

(U//FOUO) Figure 1: Federal Bureau of Investigation's Process for Staff to Open and Conduct a Type I/II Assessment

FOR OFFICIAL USE ONLY



(U) Source: GAO analysis of FBI documents and interviews with FBI officials; Icon-Studio/adobestock.com. | GAO-26-106994SU

FOR OFFICIAL USE ONLY

Note: Type I/II assessments generally relate to information on activities—or the involvement or role of individuals, groups, or organizations relating to those activities—constituting violations of federal criminal law or threats to the national security.

^aThe National Threat Operations Center is the central intake for all telephone and electronic tips from the public to the FBI.

^bSome FBI field offices have dedicated teams that review tips from NTOC before they are further evaluated.

(U//FOUO) ^cFBI staff may use certain investigative methods when gathering information about an incident prior to opening an assessment. These include obtaining publicly available information; accessing records or information from the FBI, Department of Justice, or other federal, state, local, tribal, or foreign government agency; using online services and resources that are publicly available or that the FBI has obtained by subscription or purchase for official use; conducting a clarifying interview of the complainant or person who initially furnished the information; and accepting information voluntarily provided by government or private entities. An authorized purpose must exist whenever using these methods prior to opening an assessment. The FBI uses the terms “complaint,” and “incident” to refer to information obtained by the FBI that could prompt an investigative activity. Additionally, the term “incident” is used to refer to opened assessments.

(U//FOUO) ^dBefore opening or approving an assessment, the supervisor must determine whether an authorized purpose and clearly defined objective exists for the conduct of the assessment; that the assessment is not based solely on the exercise of First Amendment rights or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject, or a combination of only such factors; and that the assessment is an appropriate use of personnel and financial resources.

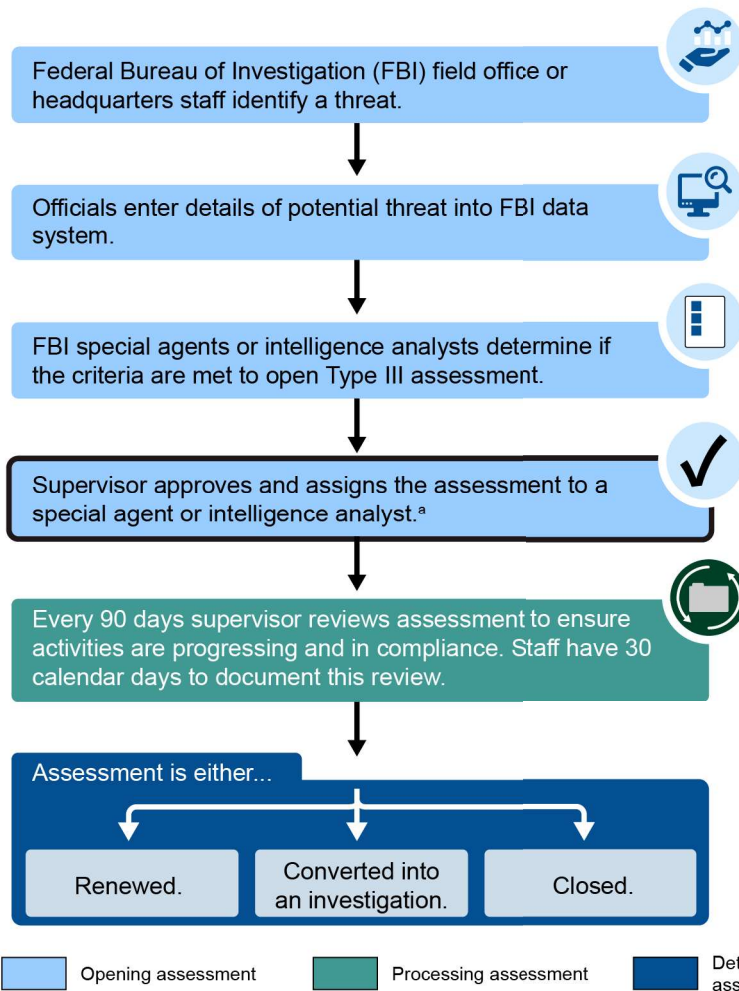
(U//FOUO) ^eSupervisors may choose to close the incident if they determine investigative activity is not warranted or if the information received is solely based on activities that are protected by the First Amendment or on race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject, or a combination of only such factors. If it is determined that the information received is credible concerning serious criminal activity not within the FBI’s investigative jurisdiction, the supervisor must promptly transmit the information or refer the incident to a law enforcement agency having jurisdiction, unless an exemption exists for sharing the information.

(U//FOUO) ^fAssessments concerning categories of individuals or organizations specified in the Domestic Investigations and Operations Guide (e.g., domestic political candidate or religious organization) are designated as sensitive investigative matters (SIM). Assessments designated as a SIM must receive a legal review and an executive approval to be opened or—in the event it is determined the assessment involves a SIM after it has been opened—continued.

(U//FOUO) While the information that prompts a Type I/II assessment can originate from various sources, the information that prompts a Type III assessment is identified internally by the FBI. Type III assessments generally aim to identify, obtain, and utilize information about actual or potential national security threats or federal criminal activities, or the vulnerability to such threats or activities. Figure 2 shows the process for opening and conducting a Type III assessment.

(U//FOUO) Figure 2: Federal Bureau of Investigation’s Process for Staff to Open and Conduct a Type III Assessment

FOR OFFICIAL USE ONLY



(U) Source: GAO analysis of FBI documents and interviews with FBI officials; Icon-Studio/adobestock.com. | GAO-26-106994SU

FOR OFFICIAL USE ONLY

Note: Type III assessments generally aim to identify, obtain, and utilize information about actual or potential national security threats or federal criminal activities, or the vulnerability to such threats or activities.










(U//FOUO) ^aAssessments concerning categories of individuals or organizations specified in the DIOG (e.g., domestic political candidate or religious organization) are designated as sensitive investigative matters (SIM). Assessments designated as a SIM must receive a legal review and an executive approval to be opened or—in the event it is determined the assessment involves a SIM after it has been opened—continued.

(U//FOUO) The DIOG further requires the FBI to consider and—if reasonable based on the circumstances—use the least intrusive method to obtain information, intelligence, and evidence.²¹ The DIOG also specifies which investigative methods are permitted for assessments, which include requesting records from U.S. government agencies, and physical surveillance not requiring a court order. Figure 3 provides the authorized investigative methods for conducting assessments.

²¹(U//FOUO) In situations where multiple investigative methods may be used that are each operationally sound and effective, the Attorney General's Guidelines for Domestic FBI Operations requires using the least intrusive method or methods to conduct investigative activities. DOJ, *Attorney General Guidelines for Domestic FBI Operations* (Washington, D.C. Sept. 29, 2008). The FBI policy requires FBI agents to consider a number of factors to judge the relative intrusiveness, including the nature, scope, and source of the information sought; the scope of the use of the investigative method; and the risk of public exposure of the information sought or use of the investigative method. FBI, *Domestic Investigations and Operations Guide* (Washington, D.C.; Sept. 17, 2021).

(U//FOUO) Figure 3: Authorized Investigative Methods for Federal Bureau of Investigation Assessments

FOR OFFICIAL USE ONLY

Method	Description
 Public information	Access information that is publicly available. ^a
 Records or information from Federal Bureau of Investigation (FBI) and Department of Justice (DOJ)	Access and examine FBI and DOJ records and obtain information from FBI or DOJ personnel. ^b
 Records or information from other federal, state, local, tribal, or foreign government	Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities.
 Online services and resources	Use any online service or resource that is publicly available or that the FBI has obtained by subscription or purchase for official use.
 Confidential human source use and recruitment ^c	Recruit, task, and obtain information from confidential human sources.
 Interview or request information from public or private entities	Question an individual (including a subject or target) in order to gather information that is pertinent to and within the scope of an authorized assessment or predicated investigation, or otherwise within the scope of FBI authority.
 Information voluntarily provided by governmental or private entities	Accept information voluntarily provided by federal, state, local, tribal, or foreign governmental or private entities and individuals.
 Physical surveillance (not requiring a court order)	The deliberate observation of persons, places, or events, on either a limited or continuous basis, in areas where there is no reasonable expectation of privacy.
 Grand jury subpoenas to providers of electronic communication services or remote computing services for subscriber or customer information (Only for Type I/II assessments)	Request a Federal Grand Jury subpoena from an appropriate US Attorney's Office for the limited purpose of obtaining subscriber or customer information from providers of electronic communication services or remote computing services (such as telephone companies, electronic mail providers, social media providers, etc.).

(U) Source: GAO analysis of FBI Domestic Investigations and Operations Guide; Icon-Studio/adobestock.com. | GAO-26-106994SU

FOR OFFICIAL USE ONLY

Note: The investigative methods in this figure may be used for all assessment types unless it is specified otherwise. Type I/II assessments generally relate to information on activities—or the involvement or role of individuals, groups, or organizations relating to those activities—constituting violations of federal criminal law or threats to the national security. Type III assessments generally aim to identify, obtain, and utilize information about actual or potential national security threats or federal criminal activities, or the vulnerability to such threats or activities. Supervisors conduct reviews

of Type I/II and Type III assessments every 30 and 90 days, respectively, according to FBI policy. During these reviews, FBI policy requires supervisors to evaluate if investigative methods employed throughout the assessment were compliant with FBI policy. Additionally, FBI policy describes methods the FBI may employ for other investigative activities (e.g., preliminary or full investigations), that are not permitted for Type I/II and Type III assessments, including undercover operations and polygraph examinations.

(U//FOUO) ^aPer FBI policy, examples of publicly available information include, but are not limited to, material that is published or broadcast for public consumption or available on request to the public.

(U//FOUO) ^bAccess and examination of certain data sets and records are subject to additional rules and restrictions according to FBI policy.

(U//FOUO) ^cA confidential human source is any individual believed to be providing useful and credible information to the FBI for any authorized information collection activity, and from whom the FBI expects or intends to obtain additional useful and credible information in the future, and whose identity, information, or relationship with the FBI warrants confidential handling. *The Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources* (Washington, D.C. Dec. 23, 2020).

(U//FOUO) In addition, FBI policy designates certain assessments for additional action which may include extra review.

- (U//FOUO) Sensitive Investigative Matter (SIM). SIMs are investigative matters involving the activities of various individuals or organizations defined by FBI policy. The DIOG states that the phrase “investigative matter involving the activities of” is intended to focus on the behaviors or activities of the subject, target, or subject matter of the assessment. As described in the DIOG, the individuals and organizations encompassed in the SIM definition are:
 - domestic public officials or domestic political candidates (involving corruption or a threat to national security),
 - religious or domestic political organizations or an individual prominent in such organizations,
 - the news media,
 - an investigative matter with an academic nexus,

-
- or any other matter which, in the judgment of the official authorizing the assessment, should be brought to the attention of FBI headquarters and other DOJ officials.²²

(U//FOUO) The FBI can designate an assessment as a SIM at any point. Figure 4 describes what a SIM is and certain characteristics.

²²(U//FOUO) An assessment may be designated as a sensitive investigative matter if it focuses on the behaviors or activities of categories of individuals or organizations specified in the DIOG (e.g., domestic public official or domestic political organization) as a subject, target, or subject matter. An assessment that has an academic nexus is considered a sensitive investigative matter if it involves 1) a faculty member or administrator employed by any college or university located in the United States, provided the matter under assessment is related to the individual's position at the institution, or 2) a student association recognized and approved by the college or university at which the student association at issue is located, and the college or university is located in the United States. FBI, *Domestic Investigations and Operations Guide* (Washington, D.C.; Jan. 3, 2024).

(U//FOUO) Figure 4: Description and Characteristics of a Sensitive Investigative Matter

FOR OFFICIAL USE ONLY**What is a Sensitive Investigative Matter (SIM)?**

A SIM involves the activities of certain individuals or organizations which, in the judgment of the official authorizing the investigation, should be brought to the attention of Federal Bureau of Investigation headquarters and other Department of Justice officials.

**Domestic public official**

An elected or appointed official serving in a judicial, legislative, management, or executive level position in a federal, state, local, or tribal government entity or political subdivision. A matter involving a domestic public official is a SIM if the assessment involves corruption or a threat to the national security.

**Domestic political candidate**

An individual seeking election to, or nomination for election to, or who has authorized others to explore on his or her behalf the possibility of election to an office in a federal, state, local, or tribal governmental entity or political subdivision. A matter involving a domestic political candidate is a SIM if the assessment involves corruption or a threat to the national security.

**Domestic political organization or individual prominent in such an organization**

Includes political parties at any level, political action groups or committees, or committees or groups formed for the purpose of electing an individual to public office or to advocate or educate the public concerning a political or social issue. If the assessment concerns a person prominent in such an organization, but not the organization itself, it must still be treated as a SIM.^a

**Other matters**

Any matter that in the judgment of the official authorizing an investigation should be brought to the attention of Federal Bureau of Investigation headquarters and other Department of Justice officials.^d

**Religious organization or individual prominent in such an organization**

Includes any association of persons whose primary purpose is worship or other entity whose principal purpose is the study or advancement of religion.^b If the assessment concerns a person prominent in such an organization, but not the organization itself, it must still be treated as a SIM.

**Member of the news media or news organization**

Includes persons and organizations that gather, report, or publish news, whether through traditional means (e.g., newspapers, radio, magazines, news service) or the online or wireless equivalent.^c A member of the news media is a person who gathers, reports, or publishes news through the news media.

**Academic Nexus**

Issues related to the responsibilities of an administrator or faculty member employed by any college or university located inside the United States, provided the issue under assessment is related to the individual's position at the institution. In addition, issues that involve any student association recognized and approved by the college or university where the student association, college or university is located inside the United States.

(U) Source: GAO analysis of FBI Domestic Investigations and Operations Guide; Icon-Studio/adobestock.com. | GAO-26-106994SU

FOR OFFICIAL USE ONLY

(U//FOUO) Note: Sensitive Investigative Matters (SIM) are investigative matters involving the activities of various individuals or organizations defined by Federal Bureau of Investigation (FBI) policy, as described in the figure above. The FBI's Domestic Investigations and Operations Guide (DIOG) states that the phrase "investigative matter involving the activities of" is intended to focus on the behaviors or activities of the subject, target, or subject matter of the assessment.

(U//FOUO) ^aAccording to the DIOG, to be "prominent" in such an organization means to serve in a formal or informal leadership capacity with influence over the organization's operations, management, or functions. The DIOG further states that if there is doubt about whether a particular person should be considered "prominent" in a domestic political organization, the doubt should be resolved in favor of considering the person to be "prominent."

(U//FOUO) ^bReligious organizations may be organized in a variety of ways, such as an unincorporated association, non-profit corporation, charitable trust, or an association in fact, according to the DIOG.

(U//FOUO) ^cAs defined in the DIOG, the term “news media” also includes an entity organized and operated for the purpose of gathering, reporting, or publishing news. The DIOG further states that the definition does not include a person or entity who posts information or opinion on the Internet in blogs, chat rooms, or social networking sites unless that person or entity falls within the definition of a member of the media or news organizations under the other provisions within this definition. According to the DIOG, if there is doubt about whether a particular person or entity should be considered part of the news media, the doubt should be resolved in favor of considering the person or entity to be the news media.

(U//FOUO) ^dAs a matter of FBI policy, “judgment” means that the decision of the authorizing official is discretionary, according to the DIOG.

(U//FOUO) Assessments involving a SIM have additional review and approval requirements before they can be opened or continued. Appendix I describes the review and approval requirements for assessments that involve a SIM.

(U//FOUO) Incidents that contain information about a threat to human life, serious bodily injury, or a significant violent action are designated as “threat to life incidents,” and the FBI may open an assessment based on such an incident. The DIOG states that when the intended victim is known or can be identified through reasonable means, the FBI must attempt expeditiously to warn the intended victim of the nature and extent of the threat and to notify other law enforcement agencies that have investigative jurisdiction concerning the threat.²³

(U//FOUO) FBI staff log information about assessments into the agency’s data systems. FBI staff input information about Type I/II assessments into its Guardian data system and information about Type III assessments into

²³(U//FOUO) According to the DIOG, the FBI is not required to inform individuals or law enforcement of a potential threat to life or bodily harm if providing the notification is likely to cause equal or greater physical harm to one or more persons or if the party already knows the nature and extent of the specific threat to the intended victim. Per the DIOG, when time and circumstance permit, the decision to not notify the individual or law enforcement must be approved by an Assistant Special Agent in Charge or higher. In all cases, FBI staff must document the reason for not providing notification, according to the DIOG. Additionally, the DIOG provides that information indicating a threat to life acquired via a Foreign Intelligence Surveillance Act of 1978 authorized investigative technique requires further coordination along with a collective determination by the relevant individuals of the appropriate way to proceed. If the decision is made not to disseminate the threat information, that decision must be approved by an Assistant Special Agent in Charge or higher and the reasons must be documented in the applicable investigative file, according to the DIOG.

its Sentinel data system.²⁴ These systems include checks for agents and supervisors to ensure assessments are opened and reviewed according to policies in the DIOG. For example, the DIOG requires staff to document in the systems the assessment's authorized purpose, indicate which investigative method(s) they used, and if it should be designated a SIM.

(U//FOUO) Finally, the DIOG requires FBI supervisory staff to review assessments at regular intervals. Supervisors provide justification reviews for Type I/II assessments every 30 days, and provide file reviews for Type III assessments every 90 days, per the DIOG.²⁵ During these reviews, the DIOG requires supervisors to evaluate if staff have made progress toward achieving the assessment's authorized purpose and clearly defined objective or toward specified investigative or intelligence collection objectives.

The DIOG further requires supervisors to evaluate whether the investigative activities are compliant with the DIOG, determine whether to continue or close the assessment, and consider if adequate predication has been developed to open a predicated investigation. For file reviews of Type III assessments, the DIOG requires supervisors to consider, whenever applicable, additional factors compared to justification reviews of Type I/II assessments. For example, supervisors should consider whether evidence was stored and disposed of properly and if documentation was completed according to evidence protocol policies. Following a review, the DIOG provides that supervisors may choose to close, continue, or convert the Type I/II or Type III assessment to an investigation.

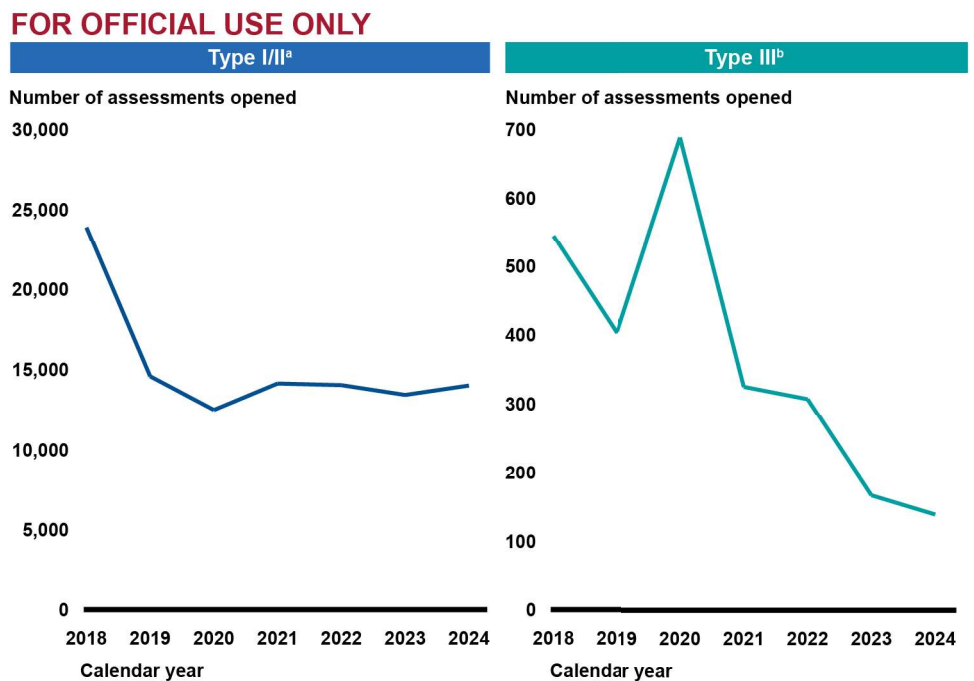
²⁴(U//FOUO) Sentinel is FBI's enterprise-wide case management system and documents all assessments and investigations across the agency's data systems. When staff input information about Type I/II assessments into the Guardian data system, it is copied to Sentinel. As a result, while Type I/II assessments are opened in Guardian, Sentinel maintains information about both Type I/II and Type III assessments. Additionally, Guardian also includes "information only" incidents.

²⁵(U//FOUO) The DIOG states that supervisors must conduct file reviews every 60 days for Type III assessments opened by probationary staff.

(U//FOUO) The FBI Opened and Subsequently Closed Approximately 127,000 Assessments From 2018 to 2024

(U//FOUO) The FBI opened approximately 127,000 Type I/II and Type III assessments, comprising about 124,000 Type I/II and 2,800 Type III assessments from calendar year 2018 to 2024. As shown in figure 5, the number of assessments the FBI opened each year varied, though the FBI opened no fewer than 12,472 Type I/II or 139 Type III assessments in any year.

(U//FOUO) Figure 5: Total Number of Federal Bureau of Investigation Type I/II and Type III Assessments Opened and Subsequently Closed, by Type, 2018-2024



(U) Source: GAO analysis of Federal Bureau of Investigation data. | GAO-26-106994SU

FOR OFFICIAL USE ONLY

(U//FOUO) Note: This figure includes Type I/II and Type III assessments opened and subsequently closed from 2018 to 2024, but does not include Type I/II and Type III assessments the Federal Bureau of Investigation (FBI) converted to an investigation or that remained open after 2024. As such, the combined number of Type I/II and Type III assessments for each year does not equal the total number of assessments opened.

^aType I/II assessments generally relate to information on activities—or the involvement or role of individuals, groups, or organizations relating to those activities—constituting violations of federal criminal law or threats to the national security, according to FBI policy.

^bType III assessments generally aim to identify, obtain and utilize information about actual or potential national security threats or federal criminal activities, or the vulnerability to such threats or activities, according to FBI policy.

(U//FOUO) FBI officials stated that a number of factors impact how many assessments they open each year. They specifically noted most tips that

result in Type I/II assessments come from the public, confidential human sources, and other government agencies and there are a number of factors that impact what these entities report. They noted Type III assessments are primarily opened based on threats and vulnerabilities the FBI identifies as it conducts analysis. According to FBI officials, increases or decreases between assessments opened in a given year cannot be attributed to a specific event.

(U//FOUO) As shown in figure 6, the FBI tended to close Type I/II assessments more quickly than Type III assessments. Among the approximate 107,000 Type I/II and 2,600 Type III assessments that were closed but not converted to an investigation, the FBI closed 63 percent of Type I/II assessments within 60 days and 53 percent of Type III assessments within 180 days. Consistent with the DIOG, these represent two supervisory review periods for both assessment types.

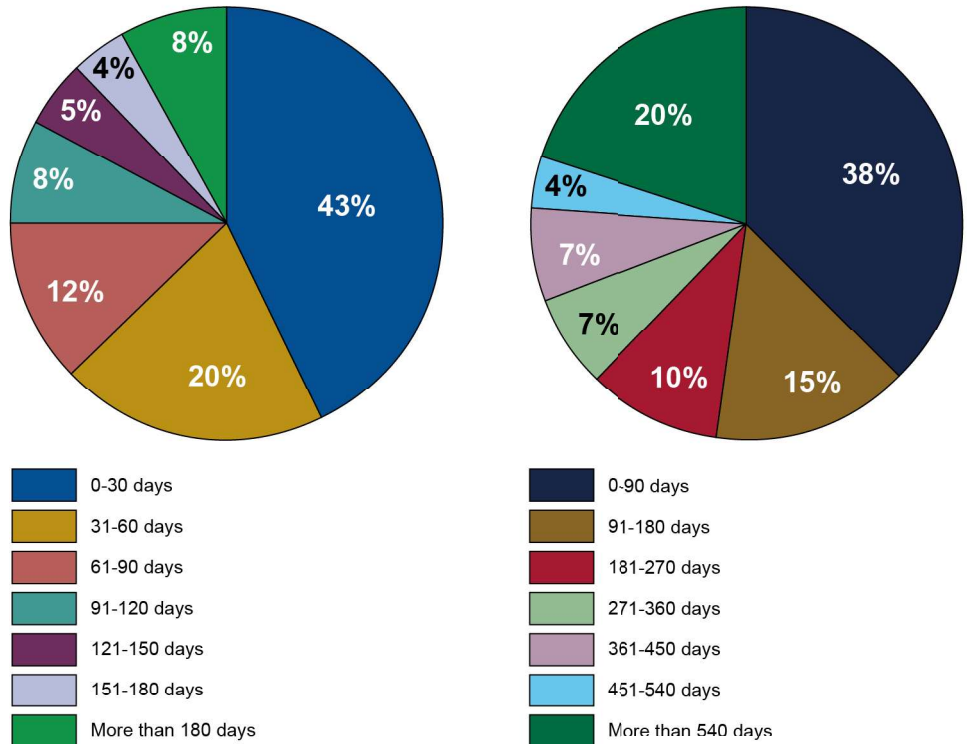
FBI officials and agency policy indicate staff tend to close Type I/II assessments in a shorter time period than Type III assessments. FBI officials stated that, compared to Type I/II assessments, Type III assessments generally have a broader scope and may focus on persisting threats (e.g., terrorist organizations). They also said staff will not close such assessments until the threat is resolved. While the DIOG states neither type of assessment has a time limit in which it must be closed, it also states that it is anticipated a Type I/II assessment will be open for a relatively short period of time.

(U//FOUO) Figure 6: Percent of Type I/II and Type III Assessments Not Converted to Investigations Closed Within Time Period of Supervisory Reviews, by Type, 2018-2024

FOR OFFICIAL USE ONLY

Type I/II^a (106,504 assessments)

Type III^b (2,576 assessments)



(U) Source: GAO analysis of Federal Bureau of Investigation data. | GAO-26-106994SU

FOR OFFICIAL USE ONLY

(U//FOUO) Note: This figure includes Type I/II and Type III assessments opened and subsequently closed from 2018 to 2024, but does not include Type I/II and Type III assessments the Federal Bureau of Investigation (FBI) converted to an investigation. As such, the number of Type I/II and Type III assessments is less than the total number of Type I/II and Type III assessments the FBI opened in the time frame. Additionally, due to rounding, the total percentage for Type III assessments is greater than 100 percent in this figure.

(U//FOUO) ^aType I/II assessments generally relate to information on activities—or the involvement or role of individuals, groups, or organizations relating to those activities—constituting violations of federal criminal law or threats to the national security, according to FBI policy. According to the FBI's Domestic Investigations and Operations Guide (DIOG), supervisors must review Type I/II assessments every 30 days. During these reviews, supervisors are to assess progress toward the achieving the authorized purpose and clearly defined objective of the assessment; if investigative activities conducted throughout the assessment are compliant with FBI policy; and if the assessment should be closed, continued, or converted to an investigation.

(U//FOUO) ^bType III assessments generally aim to identify, obtain and utilize information about actual or potential national security threats or federal criminal activities, or the vulnerability to such threats or activities, according to FBI policy. According to the DIOG, supervisors must review Type III assessments every 90 days. These reviews provide supervisors an opportunity to assess numerous

factors of an assessment, including, but not limited to, progress toward achieving the assessment's intelligence collection objectives and if the assessment should be closed, continued, or converted to an investigation.

(U//FOUO) We also analyzed the approximate 82,000 Type I/II assessments opened and subsequently closed from 2020 to 2024 and found that approximately 97 percent of these assessments received all supervisory reviews within the 30-day time frame required by the DIOG.²⁶

(U//FOUO) Further, our analysis found that most Type I/II and Type III assessments did not lead to a subsequent FBI investigation. Of the approximate 124,000 Type I/II and 3,000 Type III assessments the FBI opened and subsequently closed, the FBI closed approximately 86 percent of Type I/II and 94 percent of Type III assessments without referring them for further investigations. According to FBI officials, many investigative leads that prompt assessments are determined to not be credible, resulting in staff often closing assessments without opening a subsequent investigation.

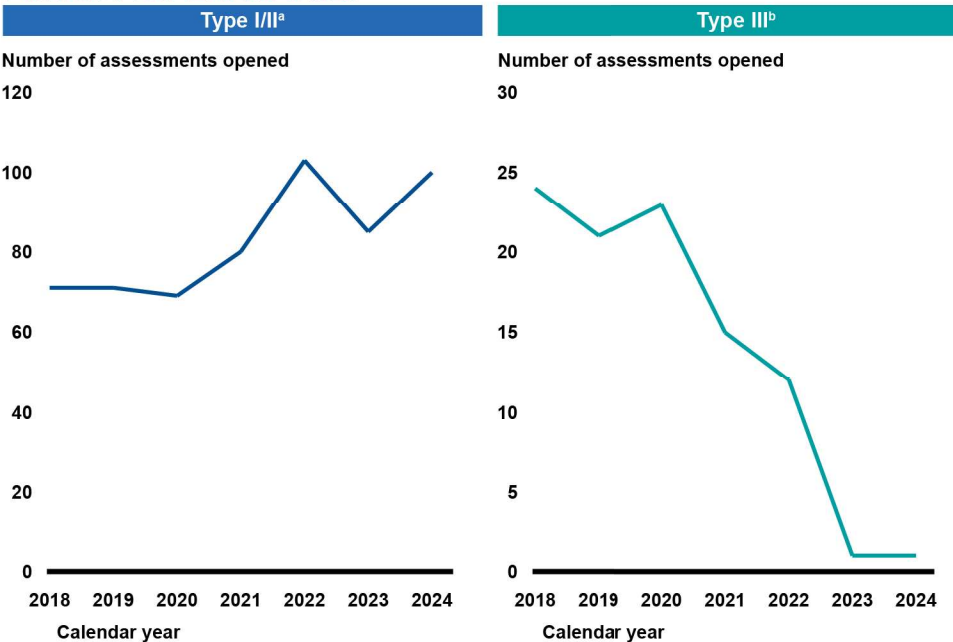
(U//FOUO) Assessments
Designated as Sensitive
Investigative Matters

(U//FOUO) Assessments designated as SIMs represent a relatively small number of the assessments the FBI opened from 2018 to 2024, though they had distinct characteristics relative to all assessments (i.e., assessments with or without SIM designation). This includes the FBI converting Type I/II assessments with SIM designation to investigations at a higher rate and taking a longer time to close assessments with SIM designation. During these years, the FBI designated approximately 1,100 Type I/II and 100 Type III assessments as SIMs. Figure 7 shows that while the number of assessments opened and designated as a SIM each year varied, the FBI opened no fewer than 69 Type I/II assessments as SIMs and no more than 24 Type III assessments as SIMs in any year.

²⁶(U//FOUO) Due to limitations with the data about supervisory reviews for Type III assessments and assessments opened in 2018 and 2019, we could only calculate the number of Type I/II assessments from 2020 to 2024 that received supervisory reviews in the time frame required by the DIOG.

(U//FOUO) Figure 7: Number of Federal Bureau of Investigation Type I/II and Type III Assessments Opened and Subsequently Closed Designated as a Sensitive Investigative Matter (SIM), by Type, 2018-2024

FOR OFFICIAL USE ONLY



(U) Source: GAO analysis of Federal Bureau of Investigation data. | GAO-26-106994SU

FOR OFFICIAL USE ONLY

(U//FOUO) Note: According to Federal Bureau of Investigation (FBI) policy, Sensitive Investigative Matters (SIM) are investigative matters involving the activities of a domestic public official, domestic political candidate, religious or domestic political organizations or an individual prominent in such organizations, the news media, an investigative matter with an academic nexus, or any other matter which, in the judgment of the official authorizing the investigation, should be brought to the attention of Federal Bureau of Investigation headquarters and other Department of Justice officials. The FBI's Domestic Investigations and Operations Guide (DIOG) states that the phrase "investigative matter involving the activities of" is intended to focus on the behaviors or activities of the subject, target, or subject matter of the assessment, per FBI policy. This figure includes Type I/II and Type III assessments designated as a sensitive investigative matter opened and subsequently closed from 2018 to 2024, but does not include assessments that were closed and converted to an investigation. As such, the number of Type I/II and Type III assessments for each year is less than the total number of Type I/II and Type III assessments opened.

^aType I/II assessments generally relate to information on activities—or the involvement or role of individuals, groups, or organizations relating to those activities—constituting violations of federal criminal law or threats to the national security, according to FBI policy.

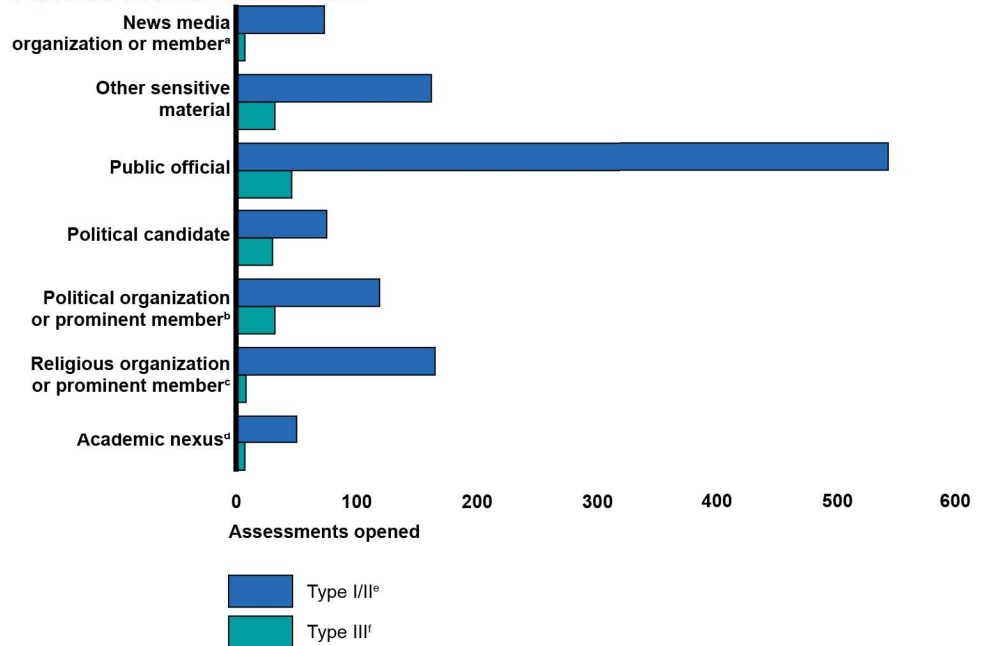
^bType III assessments generally aim to identify, obtain and utilize information about actual or potential national security threats or federal criminal activities, or the vulnerability to such threats or activities, according to FBI policy.

(U//FOUO) The FBI can designate an assessment a SIM either when the individual or organization is the subject, or the target of, a potential federal crime or threat to national security. Further, an assessment may

belong to multiple SIM categories. (U//FOUO) As shown in Figure 8, out of all SIM categories, our analysis found assessments most commonly involved domestic public officials for both Type I/II and Type III assessments. Academic nexus was the least common category for Type I/II assessments and tied with news and media as the least common category for Type III assessments.

(U//FOUO) Figure 8: Number of Type I/II and Type III Assessments Opened and Subsequently Closed Designated as a Sensitive Investigative Matter (SIM), by Type and Category of SIM, 2018 to 2024

FOR OFFICIAL USE ONLY



(U) Source: GAO analysis of Federal Bureau of Investigation data. | GAO-26-106994SU

FOR OFFICIAL USE ONLY

(U//FOUO) Note: According to Federal Bureau of Investigation (FBI) policy, Sensitive Investigative Matters (SIM) are investigative matters involving the activities of a domestic public official, domestic political candidate, religious or domestic political organizations or an individual prominent in such organizations, the news media, an investigative matter with an academic nexus, or any other matter which, in the judgment of the official authorizing the investigation, should be brought to the attention of Federal Bureau of Investigation headquarters and other Department of Justice officials. The FBI's Domestic Investigations and Operations Guide (DIOG) states that the phrase "investigative matter involving the activities of" is intended to focus on the behaviors or activities of the subject, target, or subject matter of the assessment. Further, an assessment may belong to multiple SIM categories.

(U//FOUO) ^aAccording to the DIOG, the term "news media" includes persons and organizations that gather, report, or publish news whether through traditional means or the online or wireless equivalent. A "member of the news media" is a person who gathers, reports, or publishes news through the news media. The DIOG further states that "news media" also includes an entity organized and operated for the purpose of gathering, reporting, or publishing news. The definition does not include a person or entity who posts information or opinion on the Internet in blogs, chat rooms, or social networking sites

unless that person or entity falls within the definition of a member of the media or news organizations under the other provisions within this definition. According to the DIOG, if there is doubt about whether a particular person or entity should be considered part of the news media, the doubt should be resolved in favor of considering the person or entity to be the news media.

(U//FOUO) ^bAccording to the DIOG, to be “prominent” in such an organization means to serve in a formal or informal leadership capacity with influence over the organization’s operations, management, or functions. The DIOG further states that if there is doubt about whether a particular person should be considered “prominent” in a domestic political organization, the doubt should be resolved in favor of considering the person to be “prominent.”

(U//FOUO) ^cReligious organizations may be organized in a variety of ways, such as an unincorporated association, non-profit corporation, charitable trust, or an association in fact, according to the DIOG.

(U//FOUO) ^dAn assessment that has an academic nexus is considered a sensitive investigative matter if it involves issues related to the responsibilities of an administrator or faculty member employed by any college or university located inside the United States, provided the issue under assessment is related to the individual’s position at the institution. In addition, it is considered an academic nexus if it relates to issues that involve any student association recognized and approved by the college or university where the student association, college or university is located in the United States.

^eType I/II assessments generally relate to information on activities—or the involvement or role of individuals, groups, or organizations relating to those activities—constituting violations of federal criminal law or threats to the national security, according to FBI policy.

^fType III assessments generally aim to identify, obtain and utilize information about actual or potential national security threats or federal criminal activities, or the vulnerability to such threats or activities, according to FBI policy.

(U//FOUO) Our analysis of assessments that were opened and subsequently closed from 2018 to 2024 found that the FBI converted Type I/II assessments designated a SIM into an investigation at a higher rate than all Type I/II assessments (i.e., those with or without SIM designation). Among the approximate 1,100 Type I/II assessments with SIM designation, the FBI converted 48 percent into investigations in contrast to 14 percent of all the approximate 124,000 Type I/II assessments into investigations. In addition, the FBI converted 4 percent of the approximate 100 Type III assessments with SIM designation into investigations, and 6 percent of all the approximate 3,000 Type III assessments.

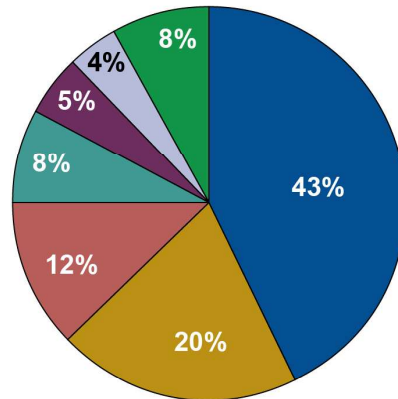
(U//FOUO) Additionally, for assessments the FBI closed but did not convert to an investigation, it took longer to close Type I/II and Type III SIM assessments than all assessments opened and subsequently closed from 2018 to 2024 of the same type. As previously stated, among all assessments, the FBI closed 63 percent of all the approximate 107,000 Type I/II assessments within 60 days and 53 percent of all the approximate 2,600 Type III assessments within 180 days, which, consistent with the DIOG, represents two supervisory review periods. In contrast, as shown in figure 9, for assessments designated as SIMs, the FBI closed 35 percent of the approximate 600 Type I/II assessments

within 60 days and 32 percent of the approximate 100 Type III assessments within 180 days. In other words, in the span of time in which the FBI closed the majority of all assessments, it closed approximately one-third of SIM assessments.

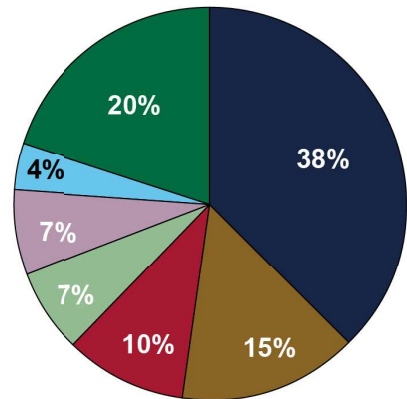
(U//FOUO) Figure 9: Percent of All Type I/II and Type III Assessments and Those Designated a Sensitive Investigative Matter (SIM) Closed Within Time Period of Supervisory Reviews, by Type, 2018-2024

FOR OFFICIAL USE ONLY

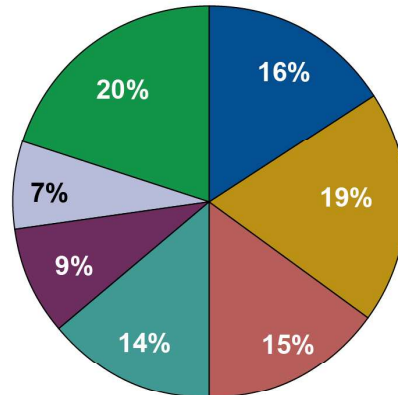
Type I/II^a (106,504 assessments)



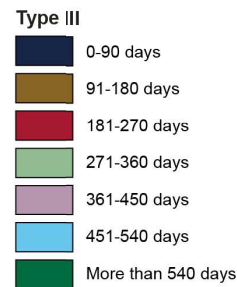
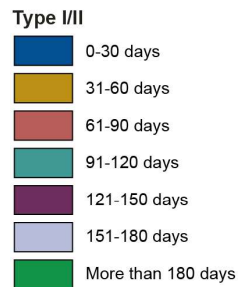
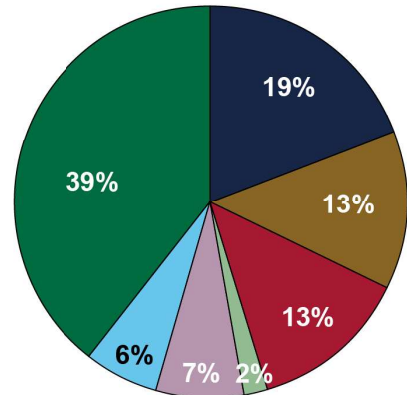
Type III^b (2,576 assessments)



Type I/II designated as SIM^c (579 assessments)



Type III designated as SIM (97 assessments)



(U) Source: GAO analysis of Federal Bureau of Investigation data. | GAO-26-106994SU

FOR OFFICIAL USE ONLY

(U//FOUO) Note: This figure includes Type I/II and Type III assessments opened and subsequently closed from 2018 to 2024, but does not include Type I/II and Type III assessments closed and converted to an investigation. As such, the number of Type I/II and Type III assessments reported is less than the total number of Type I/II and Type III assessments the Federal Bureau of Investigation (FBI) opened in the time frame. Additionally, due to rounding, the total percentage for all Type III assessments is greater than 100 percent and the total percentage for Type III assessments designated as a Sensitive Investigative Matter is less than 100 percent in this figure.

(U//FOUO) ^aType I/II assessments generally relate to information on activities—or the involvement or role of individuals, groups, or organizations relating to those activities—constituting violations of federal criminal law or threats to the national security, according to FBI policy. According to the FBI's Domestic Investigations and Operations Guide (DIOG), supervisors must review Type I/II assessments every 30 days. During these reviews, supervisors are to assess progress toward the achieving the authorized purpose and clearly defined objective of the assessment; if investigative activities conducted throughout the assessment are compliant with FBI policy; and if the assessment should be closed, continued, or converted to an investigation.

(U//FOUO) ^bAccording to FBI policy, Sensitive Investigative Matters (SIM) are investigative matters involving the activities of a domestic public official, domestic political candidate, religious or domestic political organizations or an individual prominent in such organizations, the news media, an investigative matter with an academic nexus, or any other matter which, in the judgment of the official authorizing the investigation, should be brought to the attention of Federal Bureau of Investigation headquarters and other Department of Justice officials. The DIOG states that the phrase "investigative matter involving the activities of" is intended to focus on the behaviors or activities of the subject, target, or subject matter of the assessment, per FBI policy.

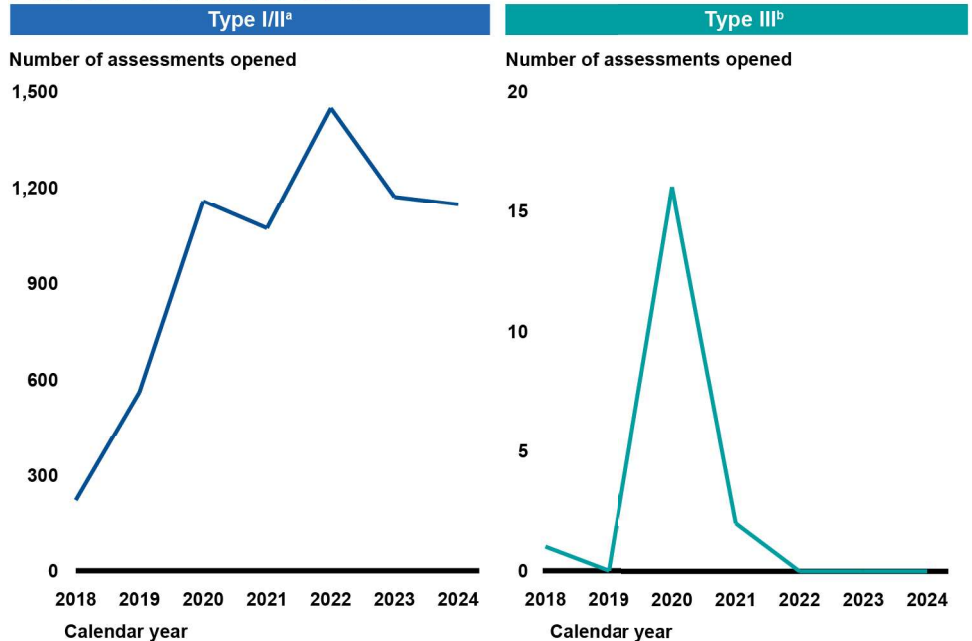
(U//FOUO) ^cType III assessments generally aim to identify, obtain and utilize information about actual or potential national security threats or federal criminal activities, or the vulnerability to such threats or activities, according to FBI policy. According to the DIOG, supervisors must review Type III assessments every 90 days. These reviews provide supervisors an opportunity to assess numerous factors of an assessment, including, but not limited to, progress toward achieving the assessment's intelligence collection objectives and if the assessment should be closed, continued, or converted to an investigation.

(U//FOUO) Threat to Life Incidents Opened as Assessments

(U//FOUO) As shown in figure 10, threat to life incidents opened as assessments also represented a relatively small number of all assessments opened from 2018 to 2024, totaling approximately 6,800 Type I/II and 20 Type III assessments. FBI officials noted that the number of threat to life incidents opened as Type I/II has increased since 2018 because, since that year, additional FBI divisions have been included in the Guardian data system that may open assessments in response to threat to life incidents. Officials also noted that threat to life incidents are generally not opened as a Type III assessment, and that if a threat to life incident is to arise during a Type III assessment, a Type I/II assessment will typically be opened to investigate the incident. Officials acknowledged that the increase in threat to life incidents opened as Type III assessments in 2020 was a significant increase, but could not identify a specific reason.

(U//FOUO) Figure 10: Number of Threat to Life Incidents Opened and Subsequently Closed as Type I/II and Type III Assessments, by Type, 2018-2024

FOR OFFICIAL USE ONLY



(U) Source: GAO analysis of Federal Bureau of Investigation data. | GAO-26-106994SU

FOR OFFICIAL USE ONLY

(U//FOUO) Note: Incidents that contain information about a threat to human life, serious bodily injury, or a significant violent action are designated as “threat to life incidents,” and the Federal Bureau of Investigation (FBI) may open an assessment based on such an incident. This figure includes threat to life incidents opened as Type I/II and Type III assessments that were opened and subsequently closed from 2018 to 2024, but does not include Type I/II and Type III assessments closed and converted to an investigation. As such, the number of Type I/II and Type III assessments for each year is less than the total number of Type I/II and Type III assessments opened.

^aType I/II assessments generally relate to information on activities—or the involvement or role of individuals, groups, or organizations relating to those activities—constituting violations of federal criminal law or threats to the national security, according to FBI policy.

^bType III assessments generally aim to identify, obtain and utilize information about actual or potential national security threats or federal criminal activities, or the vulnerability to such threats or activities, according to FBI policy.

(U//FOUO) Our analysis found that the FBI converted threat to life incidents opened as Type I/II and Type III assessments to an investigation at a similar rate as any given Type I/II and Type III assessment regardless of designation. Among threat to life incidents opened as assessments, the FBI converted about 12 percent of the approximate 6,800 Type I/II assessments and 5 percent of approximate 20 Type III assessments to investigations. As previously stated, among all

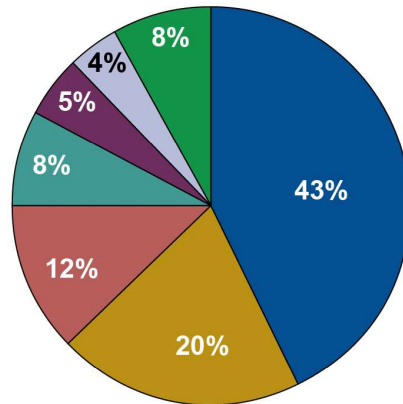
Type I/II and Type III assessments we reviewed, the FBI converted 14 percent of Type I/II and 6 percent of Type III assessments to investigations.

(U//FOUO) We also found that, for assessments the FBI closed but did not convert to an investigation, staff tended to close threat to life incidents opened as Type I/II and Type III assessments more quickly than all Type I/II and Type III assessments. As previously stated, the FBI closed 63 percent of Type I/II and 53 percent Type III assessments we reviewed within 60 and 180 days, respectively, which represents two supervisory review periods. In contrast, for threat to life incidents opened as assessments, the FBI closed 83 percent of the approximate 6,000 Type I/II assessments within 60 days and 95 percent of approximate 20 Type III assessments within 180 days (see figure 11).

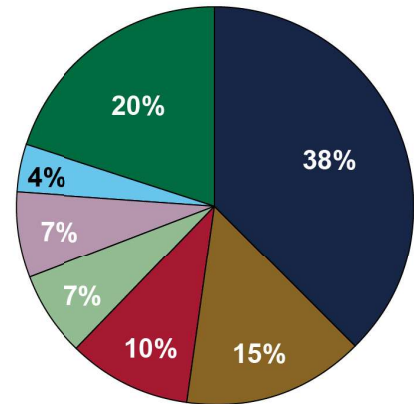
(U//FOUO) Figure 11: Percent of All Type I/II and Type III Assessments and Threat to Life Incidents Opened as Type I/II and Type III Assessments Closed Within Time Period of Supervisory Reviews, by Type, 2018-2024

FOR OFFICIAL USE ONLY

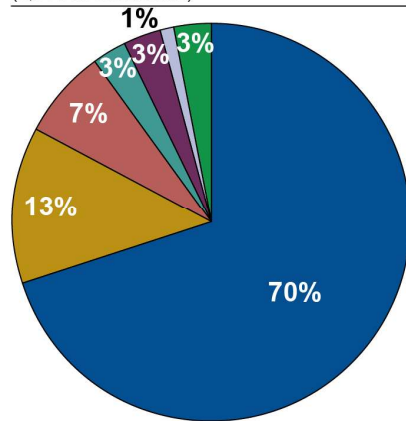
Type I/II^a (106,504 assessments)



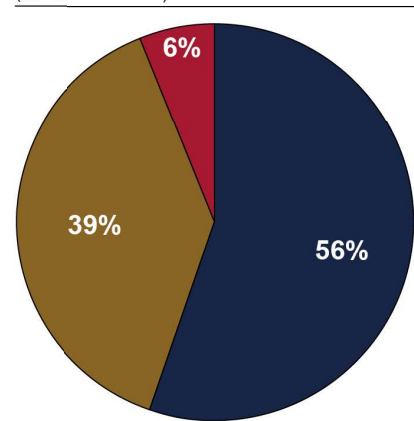
Type III^b (2,576 assessments)



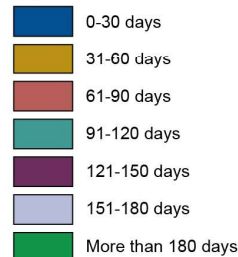
Threat to life incidents opened as Type I/II^c (5,936 assessments)



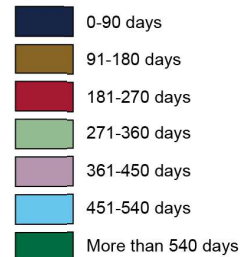
Threat to life incidents opened as Type III (18 assessments)



Type I/II



Type III



(U) Source: GAO analysis of Federal Bureau of Investigation data. | GAO-26-106994SU

FOR OFFICIAL USE ONLY

(U//FOUO) Note: This figure includes Type I/II and Type III assessments opened and subsequently closed from 2018 to 2024, but does not include Type I/II and Type III assessments closed and converted to an investigation. As such, the number of Type I/II and Type III assessments reported in this figure is less than the total number of Type I/II and Type III assessments the Federal Bureau of Investigation (FBI) opened in the time frame. Additionally, due to rounding, the total percentage for all Type III assessments is greater than 100 percent in this figure.

(U//FOUO) ^aType I/II assessments generally relate to information on activities—or the involvement or role of individuals, groups, or organizations relating to those activities—constituting violations of federal criminal law or threats to the national security, according to FBI policy. According to the FBI's Domestic Investigations and Operations Guide (DIOG), supervisors must review Type I/II assessments every 30 days. During these reviews, supervisors are to assess progress toward the achieving the authorized purpose and clearly defined objective of the assessment; if investigative activities conducted throughout the assessment are compliant with FBI policy; and if the assessment should be closed, continued, or converted to an investigation.

(U//FOUO) ^bIncidents that contain information about a threat to human life, serious bodily injury, or a significant violent action are designated as “threat to life Incidents,” and the FBI may open an assessment based on such an incident.

(U//FOUO) ^cType III assessments generally aim to identify, obtain and utilize information about actual or potential national security threats or federal criminal activities, or the vulnerability to such threats or activities, according to FBI policy. According to the DIOG, supervisors must review Type III assessments every 90 days. These reviews provide supervisors an opportunity to assess numerous factors of an assessment, including, but not limited to, progress toward achieving the assessment's intelligence collection objectives and if the assessment should be closed, continued, or converted to an investigation.

(U//FOUO) The FBI Undercounts Noncompliance with Assessment Policy by Relying on Self-Reporting and Infrequent Audits

(U//FOUO) DOJ and the FBI Audit Compliance with Assessment Requirements

(U//FOUO) Both DOJ and FBI audit assessments to ensure FBI staff are compliant with requirements in the DIOG and the Attorney General's Guidelines for Domestic FBI Operations. The FBI conducts DIOG compliance audits, which review a sample of assessments if FBI's risk assessment process determines them a high-risk area for noncompliance with policies and procedures.²⁷ FBI officials said they also conduct field office inspections, which are reviews of assessments a field office opens

²⁷(U//FOUO) FBI officials said these audits do not always include assessments as FBI takes a risk-based approach in selecting what topics to examine and includes other potential noncompliance areas such as investigations.

in the span of about 1 year. DOJ conducts audits through its National Security Review program.

- **(U//FOUO) DIOG audit reports.** FBI officials conduct DIOG compliance audits, which primarily focus on specific investigative activities such as Type I/II and Type III assessments and investigations. These audits identify instances of noncompliance based on DIOG requirements.²⁸
- **(U//FOUO) Field office inspections.** FBI officials said that approximately every 4 to 5 years, FBI staff independently review all Type I/II and Type III assessments that were opened in a field office during a year. The FBI Inspection Division evaluates specific factors related to these assessments.²⁹ When these inspections identify noncompliance, FBI Inspection Division officials said they brief field office management, produce a report of their findings, and require the field office to develop a written response to resolve the noncompliance. They also share with field office management summary information from all previously completed field office inspections so the field office management can assess their findings relative to other field offices.
- **(U//FOUO) National Security Reviews.** DOJ's National Security Division conducts reviews of FBI field offices to examine, in part, whether a sufficient authorized purpose existed and authorized investigative methods were used in a sample of Type I/II national security assessments.³⁰ These reviews also examine "information only" incidents, which are incidents when the FBI receives and evaluates information to determine whether to open an assessment

²⁸(U//FOUO) In its DIOG audit reports, the FBI refers to noncompliance as all compliance-related errors.

²⁹(U//FOUO) For Type I/II assessments, FBI officials said these factors include the assessment's scope, which includes the authored purpose and methods. Type III assessments include identifying the authorized purpose.

³⁰(U//FOUO) These reviews also examine, for example, if FBI investigative activities prior to opening an assessment were permitted and if predicated investigations were compliant. The DOJ National Security Division and the FBI Office of General Counsel National Security and Cyber Law Branch used to conduct National Security Reviews but, beginning May 15, 2024, only DOJ conducts these reviews with participation from the National Security and Cyber Law Branch.





and decides not to do so.³¹ Each year DOJ's National Security Division completes approximately 15 National Security Reviews, which results in all FBI field offices receiving a review about every 4 years.

(U//FOUO) Figure 12 illustrates certain characteristics of these reviews for Type I/II and Type III assessments.

³¹(U//FOUO) The FBI categorizes some incidents as "information only" for many reasons, including when the information contained within the incident does not warrant further investigative action (e.g., sufficient detail is missing or there is a lack of federal jurisdiction), when the incident correlates to an existing investigation (e.g., a full investigation is ongoing into the same subject or there are multiple reports with similar content), and when there is a lack of authorized purpose to conduct an assessment (e.g., someone calls in a complaint based solely on an individual exercising their First Amendment rights such as attending a protest).

(U//FOUO) Figure 12: Characteristics of Type I/II and Type III Assessment Compliance Reviews

FOR OFFICIAL USE ONLY

	National Security Reviews	Domestic Investigations and Operations Guide audit reports
What is reviewed? 	Reviews Type I/II national security assessments conducted by the Federal Bureau of Investigation (FBI) to identify whether the authorized purpose and investigative methods are compliant with the Domestic Investigations and Operations Guide.	Reviews a range of FBI investigative activities, including at times Type I/II and Type III assessments.
How often have reviews been conducted? 	Each field office is reviewed approximately every four years and each review consists of fewer than 50 Type I/II assessments.	Type I/II assessments have been reviewed three times since 2013, with a range of 65 to 766 assessments in each. Type III assessments have been reviewed four times since 2013, with a range of 297 to 509 assessments in each.
How are review findings documented? 	Reports include recommendations to correct specific instances of noncompliance in individual assessments.	Reports include observations from a sample of assessments which may result in instructions and/or recommendations.
How are results of review circulated? 	Final report sent to the field office that was reviewed, FBI's Legal Compliance and Enterprise Risk Unit (Inspection Division) ^a , and FBI's Office of Internal Auditing.	Final report sent to all relevant stakeholders, such as the FBI Legal Compliance and Enterprise Risk Unit, Inspection Division and Office of General Counsel. Report includes instructions to correct any noncompliance, review the policy that resulted in noncompliance, and support changes to reduce the likelihood of a negative future impact from repeated noncompliance.

(U) Source: GAO analysis of National Security Reviews and FBI Domestic Investigations and Operations Guide audit reports; Icon-Studio/adobestock.com. | GAO-26-106994SU

FOR OFFICIAL USE ONLY

Note: National Security Reviews are conducted by the Department of Justice National Security Division and include reviewing a sample of Type I/II national security assessments at FBI field offices examining whether a sufficient authorized purpose existed and if authorized investigative methods were used. Domestic Investigations and Operations Guide audit reports are conducted by FBI staff and focus on specific investigative activities, such as assessments.

^a(U//FOUO) According to FBI officials, as of October 2025, it has an organizational request pending approval by the Office of Management and Budget. The request integrates the Legal Compliance and Enterprise Risk Unit into the Inspection Division. Part of the Office of Integrity and Compliance has been reporting through the Inspection Division since May 30, 2025.

(U//FOUO) The FBI Relies on Staff Self-Reporting to Identify Noncompliance with Assessment Requirements

(U//FOUO) The FBI uses several methods to provide oversight of Type I/II and Type III assessments to ensure staff are compliant with requirements. For example, every 4 to 5 years, FBI headquarters staff audit each field office through its field office inspection program. Additionally, assessments are occasionally selected for audit of compliance with DIOG requirements if there is a determination that they are at a high-risk for noncompliance. This means that assessments at a particular field office may not be reviewed for several years. The FBI relies on staff to self-report noncompliance when it occurs as an ongoing method to identify noncompliance with DIOG requirements.

(U//FOUO) Additionally, the FBI uses instances of self-reporting of DIOG noncompliance to identify when assessments should be included in broader DIOG compliance audits. Specifically, when selecting which DIOG topics to audit for potential noncompliance for the FBI's DIOG audit reports, we found that the FBI relies on staff and supervisors' self-reported instances of noncompliance with the DIOG to identify high-risk areas of noncompliance, which can include Type I/II and Type III assessments.³² This means if self-reporting of noncompliance is low, assessments may not be included as a topic of the DIOG compliance audit.

(U//FOUO) The FBI knows relying on staff to self-report noncompliance with the DIOG likely underreports the total amount of noncompliance. For example, our analysis of FBI data identified that the agency received about 160 instances of self-reported substantial noncompliance related to assessments from fiscal year 2018 to 2023, which is noncompliance that is significant to the matter and is more than a minor deviation from a DIOG requirement.³³ Of these, 85 instances pertained to Type I/II

³²In addition to reviewing self-reported noncompliance, FBI officials told us they also use information obtained from field office inspections, audits, program reviews, employee and supervisor input, and executive management input, Enterprise Risk Management data, Division and Branch Compliance Committee meetings, and Department of Justice Office of Inspector General audits to identify risk and decide what audits and mitigations to conduct. However, the FBI could not provide documentation of how this information is used in these decisions as it pertains to Type I/II and Type III assessments.

³³(U//FOUO) The FBI could not provide an exact number of noncompliance instances for several reasons. In some instances, the FBI reported the substantial noncompliance did not indicate the specific assessment type, e.g. whether it was Type I/II, Type III or another type. In other instances, the FBI said the data were too burdensome to provide. In addition, the FBI altered how it was tracking assessment noncompliance in 2022 when it stopped identifying what type of assessment was involved in the noncompliance and only identified the category as "assessment." Also, an example of a minor deviation includes noncompliance that relates solely to administrative or peripheral requirements.

assessments, 18 pertained to Type III assessments, and 57 pertained to assessments generally.³⁴

(U//FOUO) Further, officials from the FBI Legal Compliance and Enterprise Risk Unit stated that instances of noncompliance are underreported, and self-reporting likely undercounts actual noncompliance.³⁵ The Legal Compliance and Enterprise Risk Unit reached this conclusion based on a comparison of noncompliance identified by FBI audits compared to the number of instances that were self-reported. An official in the Office of Integrity and Compliance told us they were unaware of other methods besides self-reporting to identify noncompliance. This official also said that the rate of noncompliance varied from year to year, and they were unsure why. Despite acknowledging that self-reporting likely underreports the amount of noncompliance with assessment policy, the FBI has not assessed if other more reliable tools could be used to identify noncompliance, separate from FBI audits.

Both our past work and Office of Management and Budget guidance recommend that federal agencies build a portfolio of high-quality, credible sources of evidence to support decision making.³⁶ According to Office of Management and Budget guidance, since different sources of evidence have varying degrees of credibility, the use of evidence requires an understanding of what conclusions can—and cannot—be drawn from the information. We have reported that using quality evidence allows the organization to assess the extent existing resources meet organizational needs for learning and decision making.

(U//FOUO) The FBI states it is neither feasible nor necessary for the agency to audit every DIOG section or DIOG-related policy or conduct a

³⁴The 57 instances of non-compliance pertaining to assessments generally is a result of a methodology change in 2022 when the FBI stopped identifying what type of assessment was involved in the noncompliance and only identified the category as “assessment.”

³⁵(U//FOUO) The FBI Legal Compliance and Enterprise Risk Unit’s mission is to ensure the FBI has processes and procedures to promote FBI compliance with both the letter and spirit of all applicable laws, regulations, rules, and policies. Furthermore, the FBI states it has an organizational request pending approval by the Office of Management and Budget, which includes integrating the part of the Office of Integrity and Compliance into the Inspection Division. The Legal Compliance and Enterprise Risk Unit has been reporting through the Inspection Division since May 30, 2025.

³⁶Office of Management and Budget Cir. No. A-11, § 240.13 (July 2024) and GAO-23-105460.

review of every program or field office and program annually. However, FBI officials have not assessed whether using self-reported instances of noncompliance is an effective tool to identify noncompliance or what other tools may exist besides inspections and reviews. Assessing whether tools besides self-reporting can be used to identify noncompliance outside the FBI's infrequent audits could help better position the FBI to understand the extent to which Type I/II and Type III assessments are meeting policy requirements. It could also serve as an additional resource to identify the need for further DIOG compliance audits for assessments.

(U//FOUO) The FBI Initiated Efforts to Track DOJ Recommendations Related to Agent's Assessment Practices but Has Not Identified Who Will Permanently Lead Them

(U//FOUO) The FBI has developed a new process to track implementation of recommendations from DOJ National Security Reviews but has not identified which office will be responsible permanently for carrying out this activity. Standards for Internal Control in the Federal Government state that to achieve an entity's objectives, management assigns responsibility and delegates authority to key roles throughout an entity.³⁷

(U//FOUO) When DOJ's National Security Reviews identify areas of noncompliance, they include recommendations for corrective actions to the field office. FBI headquarters staff previously did not track these recommendations, which the FBI reported makes it difficult to provide details on specific actions taken to address the recommendations, obstacles encountered, and how long it takes to address the recommendation without surveying the field offices.

(U//FOUO) In March 2025, in response to our inquiries, the FBI stated it planned to launch a new process to address recommendations from the National Security Reviews. The FBI noted that under the process, when the FBI's Office of the General Counsel National Security and Cyber Law Branch (NSCLB) receives a final National Security Review report, it will contact the FBI field office that received the recommendation or recommendations, including those regarding Type I/II assessments. The FBI further noted that if the field office has questions on how to implement the recommendation, the NSCLB and the relevant field office will discuss the recommendation and how to address it. According to the FBI, the field office will then carry out steps to address the recommendation and, if necessary, NSCLB and the field office will consult with the DOJ for further

³⁷GAO-25-107721.

guidance. FBI officials further stated that once the FBI resolves all steps, they will document the resolution of the recommendation.

(U//FOUO) As of June 2025, the FBI stated it has begun implementing this process. Following the March 2025 response to our inquiries, according to the FBI, the Strategic Projects Law Unit within the NSCLB began identifying and tracking recommendations made by the DOJ in the reviews, initially focusing on recommendations indicating the division needed to work with NSCLB on the disposition of information by flagging those recommendations to the field offices, and tracking and documenting the outcome.³⁸ However, the FBI said it is still finalizing aspects of this process. For instance, the FBI has not identified who will ultimately be responsible for implementing the process and who will be responsible for ensuring that recommendations beyond those specifically indicating the need for coordination with NSCLB will be addressed. The FBI officials state the process will continue to evolve in response to program experience. Identifying staff to lead the process will help the FBI continue its efforts and ensure the DOJ audit recommendations are implemented.

(U//FOUO) The FBI Does Not Analyze or Share the Results of DOJ's National Security Reviews Across Field Offices

(U//FOUO) The FBI does not identify and share useful and appropriate information from National Security Reviews with its other field offices. Prior work has found that when conducting an audit, it is important to highlight contributions of each audit in a lessons learned repository.³⁹

(U//FOUO) Our assessment of DOJ's National Security Reviews identified similar areas of noncompliance across multiple field offices. (U//FOUO) For example, the reviews identified that of the 988 Type I/II assessments and "information only" incidents reviewed from 2018 through 2024, approximately 5 percent included instances of insufficient authorized purposes and approximately 7 percent included instances of unauthorized investigative methods.⁴⁰ (U//FOUO) Further, we found these types of

³⁸(U//FOUO) In September 2025, the FBI stated that as of July 2025, the Strategic Projects Unit within NSCLB began tracking all DOJ recommendations, not only those that specifically require coordination with NSCLB.

³⁹Project Management Institute, Inc. *Process Groups: A Practice Guide* (2023). The Project Management Institute is a not-for-profit association that, among other things, provides standards for managing various aspects of projects, programs, and portfolios.

⁴⁰(U//FOUO) The DIOG states an FBI employee must be able to explain the authorized purpose and clearly defined objective, and reason the particular investigative methods were used to conduct the assessment. FBI employees who conduct assessments are responsible for ensuring that assessments are not pursued for frivolous or improper purposes and are not based solely on First Amendment rights or other the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject of the assessment, or a combination of only such factors.

findings occurred at multiple field offices. For example, 24 of the 56 FBI field offices reviewed from 2021 to 2024 (43 percent of all field offices open during these years) had at least one instance of using unauthorized investigative methods for an information only incident.⁴¹ Among these instances of field offices using unauthorized investigative methods for an information only incident, the most commonly employed unauthorized method—used by 18 of the field offices—was interviewing someone other than the complainant of the incident. In these instances, the FBI determined the field offices used investigative methods not permissible for an information only incident.

(U//FOUO) National Security Reviews offer corrective recommendations to field offices when the reviews identify a field office has committed an error when conducting an assessment or information only incident.

(U//FOUO) For example, two National Security Reviews found open assessments without an authorized purpose. Another review identified that the FBI opened two assessments that lacked an authorized purpose and, in both instances, conducted investigative activities based solely on the exercise of First Amendment-protected activities. In reports that found assessments were opened without an authorized purpose, each of these reviews stated the FBI should determine if the information obtained in the assessment should be destroyed and, if the assessment was still open at the time of review, close the unauthorized assessment. (U//FOUO) While multiple offices at FBI headquarters receive reports detailing the findings of each field office's National Security Review, the FBI does not summarize findings or recommendations from these reports or share such information with other field offices. According to DOJ, the FBI is encouraged to address the findings, whether through further distribution of the report or other means, as FBI determines would be useful and appropriate.

(U//FOUO) FBI officials stated they do not prepare any summary of the results of the National Security Review reports and do not disseminate them across field offices because DOJ has not historically found frequently reoccurring errors or trends across field offices and that the underlying circumstances of each case of noncompliance is unique. DOJ

⁴¹(U//FOUO) Examples of investigative methods only authorized for open assessments that FBI field offices employed for information only incidents include the use of a confidential human source, requesting information from a public or private entity, engaging in physical surveillance, and conducting interviews with individuals who were not the complainant of the incident. While these investigative methods may be authorized for assessments, they are not authorized for information only incidents.

officials told us that while they monitor findings from these reviews, they have not found persistent problems or meaningful trends. However, DOJ did not provide any analysis or documentation that supports this conclusion when we asked. DOJ officials said if these reviews find areas of concern that impact multiple field offices, FBI's National Security and Cyber Law Branch may inform operating divisions that oversee the assessments or inform relevant parts of the FBI through regular meetings with Chief Division Counsel officials across the FBI.

(U//FOUO) While DOJ stated it has not found persistent problems or meaningful trends from National Security Reviews, our analysis did find commonalities in the recommendations made to FBI field offices that may benefit those field offices that did not receive a review in a given year.

(U//FOUO) For example, we found that of the 15 FBI field offices that received a National Security Reviews in 2023, eight received an identical recommendation pertaining to noncompliance with the requirements for an authorized purpose. The recommendations from the DOJ reviewers stated that information obtained in the course of the assessments may have to be destroyed, including the removal of information from all FBI databases and systems. The decision to destroy any such information will be made on a case-by-case basis in conjunction with NSCLB. For example, a field office may be asked to destroy information from interviews that were conducted before an assessment was opened.

If the other 40 FBI field offices that did not receive a review that year could have seen this recommendation, they could potentially have received useful information and taken steps in advance of their own review to address the areas of noncompliance found in these reviews, as appropriate and consistent with FBI policy. Similar to how FBI shares information from its field office inspections, determining what information is useful and appropriate to share with other FBI field offices from DOJ National Security Reviews can help the FBI share lessons learned with other field offices that may encounter similar areas of noncompliance. This information can potentially help FBI field offices take proactive steps to avoid noncompliance.

Conclusions

(U//FOUO) Opening and conducting assessments is an important approach the FBI uses to identify and address emerging threats and evaluate intelligence information to ensure it appropriately identifies and categorizes national security threats. The DOJ and FBI use some of their resources to conduct audits to monitor compliance with FBI policies, but the FBI can do more to leverage these existing efforts. (U//FOUO) Given the FBI opened and closed approximately 127,000 Type I/II and Type III

assessment from 2018 to 2024, it is important for the FBI to follow its policies to help ensure it is protecting the security of the nation without impinging upon freedom of expression and other civil liberties. While the FBI relies on its staff to self-report instances of noncompliance, the FBI has indicated this method underreports the actual amount of noncompliance. Assessing whether tools besides self-reporting can be utilized to identify noncompliance would enable the FBI to better determine when additional compliance reviews of Type I/II and Type III assessments are necessary to identify and correct noncompliance.

(U//FOUO) In addition, while the FBI has created a new process to ensure that recommendations pertaining to assessments from DOJ National Security Reviews are tracked or resolved by headquarters in a more centralized way, it is still finalizing aspects of this process. For example, the FBI has not determined who will be permanently responsible for continuing the implementation of the process. Identifying who will permanently assume this responsibility will help the FBI continue the process and ensure the DOJ audit recommendations are implemented.

(U//FOUO) Finally, though the DOJ conducts audits of a sample of assessments, the FBI can do more to use these findings. (U//FOUO) For example, while multiple offices at FBI headquarters receive reports detailing what National Security Reviews find, the FBI does not summarize these findings or recommendations or share such information even though many of the recommendations in these reviews are identical and could potentially help other field offices before DOJ audits their field office. Determining what information is useful and appropriate to share with other FBI field offices from DOJ National Security Reviews can help the FBI share lessons learned with other field offices that may encounter similar areas of noncompliance. This information can potentially help FBI field offices take proactive steps to avoid noncompliance.

Recommendations for Executive Action

(U//FOUO) GAO is making the following three recommendations to the Director of the Federal Bureau of Investigation.

The Director of the FBI should assess whether tools besides self-reporting can be used to identify noncompliance of Type I/II and Type III assessments (recommendation 1).

The Director of the FBI should identify who will be responsible for permanently leading the new process to ensure that recommendations from DOJ's National Security Review are addressed (recommendation 2).

The Director of the FBI should identify and share useful and appropriate information from DOJ National Security Reviews with other field offices (recommendation 3).

Agency Comments

We provided a draft of this report to the DOJ and the FBI for review and comment. The FBI concurred with all three recommendations. The FBI and DOJ's National Security Division provided technical comments, which we incorporated as appropriate.

Because of the sensitive nature of the information contained in this product, we are only providing copies to the appropriate congressional committees, Attorney General and the Director of the Federal Bureau of Investigation with a need-to-know. On request, this product will also be made available to others with the appropriate need-to-know. If you or your staff have any questions about this report, please contact me at McNeilT@gao.gov. GAO staff who made key contributions to this report are listed in appendix II.

//SIGNED//

Triana McNeil,
Director, Homeland Security and Justice

List of Requesters

The Honorable Jamie Raskin
Ranking Member
Committee on the Judiciary
House of Representatives

The Honorable Robert Garcia
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Nancy Mace
Chair
Subcommittee on Cybersecurity, Information Technology, and
Government Innovation
Committee on Oversight and Government Reform
House of Representatives

Appendix I: Review and Approval Process for Assessments Involving a Sensitive Investigative Matter

(U//FOUO) The Federal Bureau of Investigation's (FBI) Domestic Investigations and Operations Guide (DIOG) states that Sensitive Investigative Matters (SIM) are investigative matters involving the activities of various individuals or organizations defined within the DIOG. The DIOG states that the phrase "investigative matter involving the activities of" is intended to focus on the behaviors or activities of the subject, target, or subject matter of the assessment. As described in the DIOG, the individuals and organizations encompassed in the SIM definition are:

- domestic public officials or domestic political candidates (involving corruption or a threat to national security),
- religious or domestic political organizations or an individual prominent in such organizations,
- the news media,
- an investigative matter with an academic nexus,¹
- or any other matter which, in the judgment of the official authorizing the investigation, should be brought to the attention of FBI headquarters and other Department of Justice officials.

(U//FOUO) The DIOG includes the requirements for legal reviews and executive approvals for assessments involving a SIM. The specific requirements depend on the on the type of assessment (i.e., Type I/II or Type III) and where the assessment is opened (i.e., an FBI field office or FBI headquarters).² The DIOG also sets approval requirements for Type I/II assessments involving a SIM that pertain to a presidential or congressional candidate or campaign.

¹(U//FOUO) An assessment that has an academic nexus is considered a sensitive investigative matter if it involves 1) a faculty member or administrator employed by any college or university located in the United States, provided the matter under assessment is related to the individual's position at the institution, or 2) a student association recognized and approved by the college or university at which the student association at issue is located, and the college or university is located in the United States. FBI, *Domestic Investigations and Operations Guide* (Washington, D.C.; Jan. 3, 2024).

²Type I/II assessments generally relate to information on activities—or the involvement or role of individuals, groups, or organizations relating to those activities—constituting violations of federal criminal law or threats to the national security, according to FBI policy. Type III assessments generally aim to identify, obtain, and utilize information about actual or potential national security threats or federal criminal activities, or the vulnerability to such threats or activities, per FBI policy.

Appendix I: Review and Approval Process for Assessments Involving a Sensitive Investigative Matter

(U//FOUO) Reviews and Approvals for Type I/II Assessments Involving a SIM. For Type I/II assessments involving a SIM opened by an FBI field office, the Chief Division Counsel and Special Agent-In-Charge must review and approve the assessment, respectively, per the DIOG. These tasks must be completed and the approval documented as soon as is practicable, but no later than 5 business days after the assessment is determined to involve a SIM, according to the DIOG.

(U//FOUO) For Type I/II assessments involving a SIM opened by FBI headquarters, the Office of General Counsel and Deputy Director are responsible for reviewing and approving the assessment, respectively.³ These tasks must be completed and the approval documented prior to opening the assessment.

(U//FOUO) Regardless of where the assessment is opened, in the event the FBI determines the assessment involves a SIM after the assessment has been opened, the review and approvals must be completed as soon as practicable, but no more than 5 business days after the determination. The approval must be documented within this time frame as well.

(U//FOUO) Reviews and Approvals for Type III Assessments Involving a SIM. For Type III assessments involving a SIM opened by an FBI field office, the Chief Division Counsel and the Special Agent-In-Charge must review and approve the assessment, respectively. For Type III assessments involving a SIM opened by FBI Headquarters, the Office of General Counsel and the Section Chief are responsible for reviewing and approving the assessment, respectively.

(U//FOUO) Regardless of where the assessment is opened, the review and approval must be completed prior to opening the assessment, or—in the event the FBI determines the assessment involves a SIM after the assessment has been opened—as soon as practicable, but no more than 5 business days after the determination. All approvals must be documented within these time frames as well.

³(U//FOUO) For Type I/II assessments opened at FBI headquarters involving a SIM, staff must additionally consult with the Assistant Directors-In-Charge or Special Agents-In-Charge of all affected field offices prior to opening the assessment, or—in the event the SIM arises after the assessment has already been opened—as soon as practicable but no more than 5 business days after determining the assessment involves a SIM. FBI, *Domestic Investigations and Operations Guide* (Washington, D.C.; Jan. 3, 2024).

Appendix I: Review and Approval Process for Assessments Involving a Sensitive Investigative Matter

(U//FOUO) Approvals for Type I/II Assessments Involving a Presidential or Congressional Candidate or Campaign. For a Type I/II assessment involving a candidate for president or vice president, a presidential campaign, or a senior presidential campaign staff member or advisor, the Deputy Director must approve opening the assessment, according to the DIOG.

(U//FOUO) The DIOG requires that a Type I/II assessment involving a declared congressional candidate or their campaign must be approved by an Operations Director if it was opened by an FBI field office.⁴ The Deputy Director must approve such assessments opened by FBI headquarters.

(U//FOUO) A Type I/II assessment involving activities related to illegal contributions to, donations to, or expenditures on behalf of a presidential or congressional campaign by foreign nationals must be approved by an Assistant Director if it was opened by an FBI field office, according to the DIOG. An Operations Director must approve such assessments opened by FBI headquarters, according to the DIOG.

(U//FOUO) The DIOG states that if any of the above activities become relevant to an assessment after it has been opened, FBI staff must begin seeking required approvals within 5 business days of making that determination. FBI staff must also document all approvals within this time frame.

(U//FOUO) Considerations for Officials Reviewing an Assessment Involving a SIM. The DIOG lists numerous factors that the reviewer and approving official should consider when determining whether to authorize an assessment involving a SIM. Per the DIOG, these factors include

- (U//FOUO) the seriousness or severity of the violation or threat being investigated;

⁴(U//FOUO) The DIOG states that Type I/II assessments involving a declared congressional candidate or their campaign opened by an FBI field office, or a Type I/II assessment involving activities related to illegal contributions to, donations to, or expenditures on behalf of a presidential congressional campaign by foreign nationals opened by FBI headquarters must be approved by an Executive Assistant Director. However, the FBI stated that, as of October 2025, it has an organizational request pending approval by congress that, if approved, will rename the Executive Assistant Directors to Operations Directors.

**Appendix I: Review and Approval Process for
Assessments Involving a Sensitive
Investigative Matter**

- (U//FOUO) the significance of the information sought to the violation or threat;
- (U//FOUO) the probability that the proposed course of action will be successful;
- (U//FOUO) the risk of public exposure, and if there is such a risk, the adverse impact or the perception of the adverse impact on civil liberties and public confidence;
- (U//FOUO) and the risk to the national security or the public welfare if the proposed course of action is not approved.

(U//FOUO) The DIOG also states that for assessments involving a SIM, particular care should be taken when considering whether the planned course of action is the least intrusive method if reasonable based upon the circumstances of the investigation.

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contact

Triana McNeil, McNeilt@gao.gov

**Staff
Acknowledgements**

In addition to the contact named above, Kevin Heinz (Assistant Director), James Cook (Analyst in Charge), James Ashley, Lauri Barnes, Benjamin Crossley, Dominick Dale, Amie Lesser, Amanda Miller Panko, Birch Synnott, Mary Turgeon, and Michael Volgman-Mercuri made key contributions to this report.

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 [X](#), [LinkedIn](#), [Instagram](#), and [YouTube](#).
Subscribe to our [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

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

A. Nicole Clowers, Managing Director, CongRel@gao.gov

General Inquiries

<https://www.gao.gov/about/contact-us>



Please Print on Recycled Paper.