



Evaluation of the U.S. Department of Justice's Efforts to Coordinate Information Sharing About Foreign Malign Influence Threats to U.S. Elections



EVALUATION AND INSPECTIONS DIVISION

24-080

JULY 2024



EXECUTIVE SUMMARY

Evaluation of the U.S. Department of Justice's Efforts to Coordinate Information Sharing About Foreign Malign Influence Threats to U.S. Elections

Introduction

Protecting the Integrity of U.S. elections is an important component of the U.S. Department of Justice's (Department, DOJ) overall mission to uphold the rule of law, keep our country safe, and protect civil rights. One type of threat to U.S. elections comes in the form of foreign malign influence, which the Federal Bureau of Investigation (FBI) defines as "subversive, covert (or undeclared) coercive, or criminal activities by foreign governments, nonstate actors, or their proxies to sow division, undermine democratic processes and institutions, or steer policy and regulatory decisions in favor of the foreign actor's strategic objectives."

In January 2017, the U.S. Intelligence Community issued an assessment stating that Russia's efforts to influence the 2016 U.S. presidential election demonstrated a "significant escalation in directness, level of activity, and scope of effort compared to previous operations." Similarly, the U.S. Senate Select Committee on Intelligence in 2019 and the U.S. House Permanent Select Committee on Intelligence in 2018 found, in part, that the Russian government historically has attempted to interfere in U.S. elections and attempted to interfere in the 2016 election through attacks on state voter registration databases and cyber operations targeting governments and businesses using tactics such as spear phishing, hacking operations, and social media campaigns. In 2017, the FBI established its Foreign Influence Task Force (FITF) to "identify and counteract the full range of malign foreign influence operations" targeting the United States, including operations targeting U.S. elections. DOJ's National Security Division (NSD) and U.S. Attorney's Offices (USAO) work with the FBI to combat foreign malign influence threats. Additionally, the Department and its components share information with other federal partners, states, and social media companies to counter foreign malign influence directed at U.S. elections.

The DOJ Office of the Inspector General (OIG) undertook this evaluation to assess the effectiveness of the Department's information-sharing system related to foreign malign influence directed at U.S. elections, evaluate the Department's oversight and management of its response, and identify any gaps or duplication among the Department's efforts in this area. We focused on the Department's information sharing with social media companies to evaluate the aspect of the Department's information-sharing system that the FITF developed following foreign malign influence directed at the 2016 U.S. presidential election.

Recommendations

In this report, we make two recommendations to ensure that DOJ takes a public and strategic approach to sharing information with social media companies in a manner that protects First Amendment rights to combat foreign malign influence directed at U.S. elections, thus strengthening public trust in the Department.

Results in Brief

We found that the FBI has developed an "intelligence sharing model," involving other members of the U.S. Intelligence Community and social media companies, but that neither DOJ nor the FBI had specific policy or guidance applicable to information sharing with social media companies. We also found that the DOJ components tasked with countering foreign malign influence directed at U.S. elections effectively share information with each other.

The Department Previously Lacked Guidance for Certain Types of Engagement with Social Media Companies

We found that neither DOJ nor the FBI had a specific policy or guidance applicable to information sharing with social media companies until February 2024.

At the time of our fieldwork, the Department shared information about foreign malign influence directed at U.S. elections by means of an “intelligence sharing model,” through which the FBI obtained information related to foreign malign influence actors from other U.S. Intelligence Community agencies and shared that information with social media companies. In some instances, the companies may have chosen to investigate further activity on their platforms. Upon receiving a court order obtained by DOJ, the companies were then able to provide information to the FBI. This could result in the development of new leads, which could help the FBI in its operational activities and potentially identify additional information that it could share with the companies.

FBI officials said that, in the absence of a specific policy or guidance, the FBI’s information-sharing method has been based on an “actor-driven versus content-driven” approach. DOJ and FBI officials told us that the FBI does not monitor social media content on platforms as it relates to foreign malign influence, nor does it investigate specific narratives spread online. Rather than using online content to identify foreign malign influence activity, the FBI told us that it acts based on intelligence developed during its ongoing investigations or received from other federal agencies concerning the activities of specific foreign actors. However, we also found during our document review that the FBI shared “content” information when the FBI had intelligence indicating that a foreign actor planned to promote specific themes or narratives with its social media activity. The FBI said that it relies on the social media companies to assess the information provided by the FBI and to determine whether to take any action based on its customer having violated the companies’ terms of service.

We also found that the Department does not have a comprehensive strategy guiding its approach to engagement with social media companies on foreign malign influence directed at U.S. elections and that it faces risks as a result. Specifically, the FBI maintains relationships with social media companies in the San Francisco area, where many social media companies are based, but lacks ongoing relationships with social media companies outside that area. Further, we found that the Department faces novel threats, such as the

expansion of foreign-owned social media platforms and the development of new technologies that could support foreign malign influence campaigns directed at U.S. elections.

While the FBI’s model and approach has put this framework in place, it nonetheless has an inherent risk arising from the fact that social media companies provide a forum for speech, which is subject to protection under the First Amendment from infringement by the government. While there are no apparent First Amendment implications from the FBI simply sharing information about foreign malign influence threats with social media companies, concerns may arise if that information is communicated in such a way that those communications could reasonably be perceived as constituting coercion or significant encouragement aimed at convincing the companies to act on the shared information in a way that would limit or exclude the speech of those who participate on their platforms. DOJ and the FBI issued a new standard operating procedure (SOP) in February 2024 that acknowledges this risk and takes steps to mitigate it. We believe that identifying a way to inform the public about this SOP and how it protects First Amendment rights would strengthen public trust in the Department and the FBI.

NSD, USAOs, and FBI Field Offices Effectively Share Information Regarding Foreign Malign Influence Cases Involving Threats to U.S. Elections

We found effective coordination within and among the three DOJ components tasked with sharing information regarding foreign malign influence directed at U.S. elections. Within DOJ, coordination on foreign malign influence directed at U.S. elections occurs at both a strategic case management level, where decisions about DOJ’s overall approach to combating foreign malign influence are made, and at a case investigative level, where FBI agents, Assistant U.S. Attorneys, and NSD attorneys coordinate weekly on the investigation and prosecution of individual cases. Officials we spoke to at each of the three DOJ components expressed positive views about their information-sharing relationships within DOJ pertaining to foreign malign influence directed at U.S. elections.

Table of Contents

Introduction.....	1
Background.....	2
Purpose and Scope of the OIG Evaluation.....	6
Results of the Evaluation.....	8
The Department Previously Lacked Guidance for Certain Types of Engagement with Social Media Companies.....	8
NSD, USAOs, and FBI Field Offices Effectively Share Information Regarding Foreign Malign Influence Cases Involving Threats to U.S. Elections	22
Conclusion and Recommendations.....	26
Conclusion.....	26
Recommendations	27
Appendix 1: Purpose, Scope, and Methodology.....	28
Standards	28
Purpose and Scope	28
Methodology.....	29
Appendix 2: The Mission, Structure, and Development of the Foreign Influence Task Force and the Role of the FBI’s Cyber Division	31
The Mission and Structure of the Foreign Influence Task Force.....	31
Additional Background on the FITF’s Development.....	31
The Role of the FBI’s Cyber Division in the FITF	31
Appendix 3: Databases and Systems Available to the FBI for Sharing Information.....	33
FBI Official System of Record	33
Methods for Sharing Information with Nonfederal Entities.....	33
Methods for Sharing Information within the U.S. Government.....	35
Method for Receiving Information from the General Public.....	36
Appendix 4: Overview of DOJ’s Mission to Counter Election Crimes.....	37
Appendix 5: DOJ’s Election-Related Information Sharing with Other Federal Agencies and State Government Officials.....	38
Coordination with the Department of Homeland Security	38
Coordination with Other Federal Agencies.....	38
Coordination with State Government Officials	39
Appendix 6: Descriptions of Laws and Policies Relevant to DOJ’s Mission to Counter Foreign Malign Influence.....	40

First Amendment to the U.S. Constitution.....	40
Statutes.....	40
Executive Order.....	41
Department of Justice Policies.....	41
FBI Policies	42
Appendix 7: The Department’s Response to the Draft Report.....	45
Appendix 8: OIG Analysis of the Department’s Response.....	52

Introduction

Protecting the integrity of U.S. elections is an important component of the U.S. Department of Justice's (DOJ, Department) overall mission to uphold the rule of law, keep our country safe, and protect civil rights. Additionally, according to the DOJ strategic plan, DOJ is responsible for investigating, disrupting, and prosecuting threats to U.S. national security, including foreign malign influence operations. Although elections are administered by states and their localities, DOJ has the primary responsibility for investigating foreign malign influence operations directed at elections (see the text box).

Concern about foreign malign influence targeting the United States dates back to our country's founding, when, during his famous farewell address in 1796, President George Washington warned against "insidious...foreign influence." Although foreign nations have targeted the United States with malign influence campaigns for centuries, these efforts have taken novel forms in recent years, particularly during and since the 2016 presidential election. In January 2017, the U.S. Intelligence Community issued an assessment stating that Russia's efforts to influence the 2016 presidential election demonstrated a "significant escalation in directness, level of activity, and scope of effort compared to previous operations."¹ Similarly, the U.S. Senate Select Committee on Intelligence in 2019 and the U.S. House Permanent Select Committee on Intelligence in 2018 found, in part, that the Russian government historically has attempted to interfere in U.S. elections and attempted to interfere in the 2016 election through attacks on state voter registration databases and cyber operations targeting governments and businesses using tactics such as spear phishing, hacking operations, and social media campaigns. In 2019, the U.S. Congress established the Foreign Malign Influence Center within the Office of the Director of National Intelligence. Two years earlier, the Federal Bureau of Investigation (FBI) had established the Foreign Influence Task Force (FITF) to "identify and counteract the full range of malign foreign influence operations" targeting the United States, including operations targeting U.S. elections. Three of the Department's components—the FBI, the National Security Division (NSD) and the U.S. Attorney's Offices (USAO)—work together to pursue the Department's mission to combat these foreign malign influence threats. Additionally, the Department and its components coordinate with non-DOJ entities, including members of the U.S. Intelligence Community, U.S. Department of Homeland Security (DHS), U.S. Department of the Treasury, state and local governments, and private sector entities (such as social media companies) to share information regarding foreign malign influence threats.

Foreign Malign Influence

The FBI defines foreign malign influence as "subversive, covert (or undeclared), coercive, or criminal activities by foreign governments, nonstate actors, or their proxies to sow division, undermine democratic processes and institutions, or steer policy and regulatory decisions in favor of the foreign actor's strategic objectives and to the detriment of its adversary."

Source: FBI training materials

The Office of the Inspector General (OIG) undertook this evaluation to assess the effectiveness and resilience of the Department's information-sharing system related to foreign malign influence directed at

¹ The U.S. Intelligence Community is composed of 18 executive branch agencies (such as the National Security Agency, the Central Intelligence Agency, and the FBI) and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States. For more information, see Office of the Director of National Intelligence (ODNI), "[Members of the IC](https://www.dni.gov/index.php/what-we-do/members-of-the-ic)," www.dni.gov/index.php/what-we-do/members-of-the-ic (accessed October 11, 2023).

U.S. elections, to evaluate the Department's oversight and management of its response to foreign malign influence directed at U.S. elections, and to identify any gaps or duplication among the Department's efforts in this area.

Background

Foreign Malign Influence

Foreign malign influence can take numerous forms and tactics and may vary by foreign actor and objective. According to the FBI, activities must be related to a foreign actor or proxy to be considered foreign malign influence, to include planning and pushing a foreign agenda at the expense of U.S. interests. Foreign malign influence operations are actions by foreign powers to influence U.S. policy, distort political sentiment and public discourse, or undermine confidence in democratic processes and values to achieve strategic geopolitical objectives. Although foreign influence operations involve a wide spectrum of foreign activities, it is the subversive, undeclared, criminal, or coercive nature of those activities that is the basis for the FBI's investigative interest. Examples of such activities include covert placement of media articles; economic coercion for advantage, bribery, or blackmail; cyber intrusions; campaign finance violations; and overt provision of funds to divisive groups.

Misinformation

An adversary uses false or misleading information. The adversary's intent can change *misinformation* to *disinformation*.

Disinformation

An adversary uses false or misleading information created or spread intentionally to alter a specific target audience's attitudes or behavior to benefit the information's creator.

Source: National Intelligence Council

Although foreign malign influence targets all aspects of American society, DOJ has stated that elections "are a particularly attractive target for foreign influence campaigns because they provide an opportunity to undermine confidence in a core element of our democracy: the process by which we select our leaders."² Foreign malign influence operations directed at elections may take many forms, including cyber operations targeting election infrastructure or political campaigns, covert influence operations aimed at assisting or harming political organizations or campaigns, misinformation and disinformation campaigns aimed at sowing discord, illicit campaign finance schemes, and violations of the Foreign Agent Registration Act (FARA) and related statutes (see the text box for the government's definitions of misinformation and disinformation).

Federal Bureau of Investigation

The FBI is the lead agency for investigating foreign malign influence operations. In accordance with usual FBI practice, foreign malign influence investigations are conducted at FBI field offices and managed at the program level from FBI headquarters in Washington, D.C. At FBI headquarters, the FITF identifies and oversees investigations of foreign malign influence operations targeting the United States. In this section, we discuss the creation and current role of the FITF, as well as the complementary roles played by the FBI's Cyber Division and field offices.

² DOJ, *Report of the Attorney General's Cyber Digital Task Force* (July 2018), Chapter 1, page 2.

The Foreign Influence Task Force

In 2017, the FBI created the FITF, within its Counterintelligence Division, as a direct result of Russia's malign influence during the 2016 U.S. presidential election.³ The former Assistant Director of the Counterintelligence Division explained that the FITF brought together staff with counterintelligence, cyber, and criminal investigative experience to work on foreign malign influence election threats. Following the 2018 midterm election, the FBI reviewed the effectiveness of the FITF and expanded the task force from focusing solely on Russian-based foreign malign influence to include foreign malign influence actors from China, Iran, and other global adversaries.⁴ Since this expansion, the FITF has focused on foreign malign influence generally, with foreign malign influence elections work comprising only a small part of the overall workload.

From an investigative standpoint, FITF program managers oversee counterintelligence cases dealing with foreign malign influence, including those with threats against U.S. elections, throughout the FBI's 56 field offices. FITF program managers work with their counterparts in other FBI headquarters divisions and field offices to deconflict cases, ensure coordination and tracking of all the major events in a case, and share information on foreign malign influence threats. These program managers also coordinate with liaisons from the FBI's partners in the U.S. Intelligence Community.

Cyber Division

The FBI's cyber mission, managed by the Cyber Division, is to investigate cyber attacks and cyber intrusions. Specific to elections, the Cyber Division investigates cyber attacks and illegal activity on American computer networks, including attacks targeting political campaigns, state election infrastructures, and private sector vendors of election equipment. The Cyber Division uses investigative, intelligence, and incident response resources to protect elections.⁵ For more information about the Cyber Division's mission and how it is distinct from the FITF, see [Appendix 2](#).

³ The FBI's counterintelligence mission, managed by the Counterintelligence Division, is to expose, prevent, and investigate foreign intelligence activities in the United States. This mission includes "detecting and lawfully countering actions of foreign intelligence services and organizations that employ human [such as spies] and technical [such as hackers] means to gather information about the U.S. that adversely affects our national interests," which encompasses combating foreign malign influence directed at U.S. elections.

⁴ More recently, Congress established a Foreign Malign Influence Center (FMIC) within ODNI in December 2019. According to its congressional charter, the FMIC "serves as the primary U.S. Government organization for analyzing and integrating all intelligence and other reporting possessed or acquired pertaining to foreign malign influence, including election security." The ODNI's website indicates that the FMIC partners with the FBI and other federal agencies to promote awareness of the foreign malign influence threat. The FMIC was activated in September 2022 and is considered the successor organization to the ODNI Election Threats Executive, established in 2019 and discussed later in this report.

The FBI began engaging with the FMIC at the time of the FMIC's inception and previously had engaged with the Election Threats Executive. The FBI continues to engage with FMIC staff; however, these interactions are not at the direction of specific guidance or law. We did not assess the FBI's interactions with the FMIC because we did not examine the FBI's activities in 2022 as part of this evaluation. For more information about the scope of our evaluation, see [Appendix 1](#).

⁵ The Cyber Division also notifies private sector partners of timely cyber threat information related to threats against critical infrastructure sectors using Private Industry Notifications (PIN) and FBI Liaison Alert System (FLASH) reports. The

Continued

Field Offices

Most FBI investigations are conducted at the FBI's 56 field offices located throughout the country. FBI field offices have Counterintelligence and Cyber squads that work investigations managed by the corresponding division at FBI headquarters to ensure strategic oversight and deconfliction with other investigations and U.S. Intelligence Community priorities.

Pursuant to policy, FBI field offices maintain relationships within their areas of responsibility to facilitate the FBI's investigative needs. This includes working with state and local governments, election officials, law enforcement agencies, private sector entities, and members of the public. For more information about DOJ's mission to counter election crimes, see [Appendix 4](#). For more information about DOJ's election-related information sharing with state government officials, see [Appendix 5](#).

Other DOJ Components

National Security Division

The mission of DOJ's NSD is to protect and defend the United States against the full range of national security threats, consistent with the rule of law. NSD is designed to ensure greater coordination between federal prosecutors and the FBI on one hand and other U.S. Intelligence Community agencies on the other. NSD's Counterintelligence and Export Control Section assists USAOs in the prosecution of foreign influence and interference cases, including FARA violations, while the Office of Law and Policy serves as the primary nexus for the development of DOJ policy on countering foreign malign influence. In response to its review of a draft of this report, the Department reported that NSD established the National Security Cyber Section in June 2023. This section is now primarily responsible for investigating and prosecuting foreign influence and interference cases that are "cyber-enabled," such as crimes in which online platforms, including social media platforms, are central to the commission of the offense.

U.S. Attorney's Offices

The USAOs enforce federal law by investigating and prosecuting cases nationwide in each of the 94 federal judicial districts. In coordination with NSD, USAOs assist FBI field offices in initiating legal process, as described below. USAOs ultimately decide whether to file criminal charges in foreign malign influence cases, in consultation with NSD.

Non-DOJ Partners

The FBI works with partners in the U.S. Intelligence Community, such as the National Security Agency, to share information about foreign malign influence threats to U.S. elections. U.S. Intelligence Community partners provide the FBI with information developed from their ongoing intelligence collection activities that may be useful to FBI investigations of foreign malign influence directed at U.S. elections or stakeholders. As an example, the FBI sends and receives information pertaining to foreign malign influence campaigns from the U.S. Department of Defense's Cyber Command and works with the U.S. Department of the Treasury to seek sanctions against foreign actors engaged in such campaigns. Additionally, the FBI communicates with

Cyber Division created PINs and FLASH reports in response to Executive Order 13636, which mandates that the federal government increase the volume, quality, and timeliness of cyber threat information shared with private industry. For more information about these reports, see [Appendix 3](#).

DHS in its mission to combat foreign malign influence and DHS's Cybersecurity & Infrastructure Security Agency is its main partner.

The FBI sometimes needs to share information related to foreign malign influence threats to U.S. elections with state governments because elections are administered by the states. However, FBI interaction with state governments related to combating foreign malign influence is limited as DHS is the states' primary federal partner related to election security. When the FBI does share information with states on foreign malign influence threats, sharing typically concerns cyber threats to state election systems. For more information about DOJ's election-related information sharing with other federal agencies and state government officials, see [Appendix 5](#).

Legal and Policy Framework

Below, we describe several existing policies that guide DOJ's efforts to share information about foreign malign influence directed at U.S. elections.⁶ We also describe several legal tools used in the investigation of all types of federal criminal cases that DOJ can use in its investigations of foreign malign influence. We discuss these policies and tools in greater detail, as well as additional laws and policies that are relevant to DOJ's foreign malign influence work, in [Appendix 6](#).

Executive Order 12333–U.S. Intelligence Activities

Executive Order (E.O.) 12333, originally issued in 1981 and amended by several subsequent executive orders, establishes the U.S. Intelligence Community and lays out the goals, directions, duties, and responsibilities for U.S. Intelligence Community agencies, including the FBI. One of these responsibilities is to prepare and provide intelligence in a manner that allows the full and free exchange of information, consistent with applicable law and presidential guidance.

The Executive Branch Notification Framework

In 2019, the federal government adopted a framework to ensure that appropriate members of Congress, state and local government officials, private sector entities, and the public are notified of covert foreign attempts to influence U.S. elections when such notification is necessary to protect U.S. national security and the integrity of U.S. elections. This framework complements existing legal and policy requirements to notify victims of foreign interference, including cyber intrusions and other criminal activities. According to the framework, DHS is responsible for making notifications relating to critical infrastructure, including election infrastructure, and the FBI is responsible for all other notifications.⁷ When a federal agency identifies a foreign interference campaign directed at a U.S. election, it is required to notify an interagency group

⁶ Upon reviewing a draft of this report, the FBI noted the existence of another policy, which is classified. This policy is not owned by the FBI but was formulated through an interagency process to establish principles and guidelines by which intelligence community members can analyze social media-related data in a manner that comports with constitutional protections.

⁷ DHS has identified 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on national security, economic security, public health or safety, or any combination thereof. One of those sectors, Government Facilities, includes the physical, electronic, and technological resources used to administer elections and report the results.

organized by the Office of the Director of National Intelligence (ODNI) and tasked with assessing foreign attempts at influencing U.S. elections.⁸

DOJ Policies

The Justice Manual lays out DOJ policy for the disclosure of foreign influence operations. The Justice Manual states that it is DOJ policy to alert the victims and unwitting targets of foreign influence activities, when appropriate and consistent with DOJ policies and practices and U.S. national security interests. Recognizing that it may not be possible to disclose all foreign influence operations because of investigative or operational concerns, Section 9-90.730 of the Justice Manual outlines several reasons for the potential disclosure of such operations, including to support arrests and charges, alert victims, inform relevant congressional committees, and alert the public or other affected individuals.

The FBI's primary source of guidance for investigations, including counterintelligence investigations such as investigations into foreign malign influence directed at U.S. elections, is the Domestic Investigations Operations Guide (DIOG). The DIOG outlines the various investigative steps FBI agents may take, including the type of factual basis needed for the FBI to begin taking preliminary investigative steps or open a full investigation, the techniques the FBI may use to collect information for the investigation, and the entities with which the FBI may share the information during the investigation.

Investigative Tools

When seeking information on foreign malign influence campaigns that use social media and technology platforms in the United States, the FBI has several tools to gain more information about the activity in coordination with local USAOs and NSD. We refer to these tools collectively as legal process. Legal process describes procedures that the FBI, in concert with USAOs and NSD, can initiate to compel third parties to produce evidence. For example, the FBI may seek a grand jury subpoena of social media and technology companies to acquire present subscriber information.⁹ If the FBI needs broader information, it may seek an order from a U.S. district court under 18 U.S.C. § 2703(d) for historical subscriber information as part of an ongoing criminal investigation under the Electronic Communications Privacy Act. If the FBI needs to acquire more detailed information, such as the content of messages, or to access evidence for an ongoing investigation, such as data stored on a computer or server, it may seek a search warrant issued by a U.S. district court.

Purpose and Scope of the OIG Evaluation

The OIG conducted this evaluation to assess the effectiveness and resilience of the Department's information-sharing system related to foreign malign election influence; assess the Department's oversight, management, and coordination of its activities to respond to foreign malign election influence; and identify any gaps or duplication of effort among these efforts during the 2016, 2018, and 2020 U.S. election cycles.

⁸ The interagency group organized by the ODNI, which includes the FBI and NSD, considers a number of factors when deciding whether to notify interested parties and the public about foreign attempts to influence U.S. elections. In this report, we do not evaluate the decisions that the federal government has made using this framework.

⁹ Subscriber information includes a user's name; address; phone connection records or session time records; length of service; telephone number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such services, such as a credit card or bank account number. 18 U.S.C. § 2703(c)(2). Subscriber information does not include the content of communications sent.

We did not examine these efforts during the 2022 U.S. election cycle because that election cycle was ongoing at the time of our fieldwork and we did not want to interfere with DOJ's activities.

We examined DOJ policies and practices related to its overall mission to combat foreign malign influence and how those policies and practices interfaced specifically with foreign malign influence threats directed at U.S. elections during the 2016, 2018, and 2020 election cycles. We also evaluated how the Department works with partner agencies at the federal, state, and local levels to send and receive information related to foreign malign influence threats to elections.

Due to limitations in the evidence available from the FBI, we did not evaluate the Department's sharing of information about all of the forms that foreign malign influence could take, such as cyber operations targeting election infrastructure or covert influence operations aimed at assisting or harming political organizations. We focused on the Department's information sharing with social media companies to evaluate the aspect of the Department's information-sharing system that the FITF developed following foreign malign influence directed at the 2016 U.S. presidential election because many FBI employees described those interactions to us and we concluded that those interactions were important.

The OIG did not evaluate the sharing of information related to election crimes that are domestic in origin, such as ballot fraud or campaign finance crimes unrelated to foreign malign influence directed at U.S. elections, nor did we evaluate the FBI's information sharing with social media companies with respect to domestic actors.¹⁰

We discuss the methodology of our evaluation in [Appendix 1](#).

¹⁰ Subsequent to the OIG's initiation of this evaluation, the FBI's engagement with social media companies became the subject of civil litigation. During that litigation, in addressing a preliminary injunction sought by the plaintiffs, the U.S. Court of Appeals for the Fifth Circuit found that FBI officials had "likely (1) coerced the platforms into moderating content, and (2) encouraged them to do so by effecting changes to their moderation policies, both in violation of the First Amendment." *Missouri v. Biden*, 83 F.4th 350, 388 (5th Cir. 2023). In response to a draft of this report, the Department stated that it disagreed with the Fifth Circuit's holding and noted that the Fifth Circuit had found that it could not say that the FBI's communications "were plainly threatening in tone or manner," but rather concluded only that "because the FBI wielded some authority over the platforms, the FBI's takedown requests can 'reasonably be construed' as coercive in nature."

On June 26, 2024, the U.S. Supreme Court reversed the Fifth Circuit's judgment, holding that the plaintiffs lacked sufficient standing to seek the preliminary injunction at issue. *Murthy v. Missouri*, 144 S. Ct. 1972 (2024). While the Supreme Court has issued its ruling on the preliminary injunction and remanded the case to the lower courts, the underlying litigation that gave rise to the request for a preliminary injunction remains ongoing, and, for that reason, to the extent the lawsuit includes allegations against the FBI relating to foreign influence on U.S. elections, the OIG did not include those allegations within the scope of this evaluation.

While there was some overlap between our evaluation and the litigation, the litigation was far broader than our scope. The litigation named as defendants a range of federal agencies, including the U.S. Departments of Health and Human Services, Homeland Security, and State, in addition to DOJ. We examined the effectiveness of DOJ's information sharing with many different entities, including social media companies, but only on the topic of foreign malign influence directed at U.S. elections.

Results of the Evaluation

The Department Previously Lacked Guidance for Certain Types of Engagement with Social Media Companies

In pursuit of DOJ's mission to combat foreign malign influence threats to U.S. elections, the FBI has developed a method for information sharing that includes other partner agencies in the U.S. Intelligence Community (IC) and social media companies. We found that at the time of our fieldwork neither the Department nor the FBI had a specific policy or guidance applicable to information sharing with social media companies.¹¹ We found that FBI communications to the social media companies focused on sharing information about social media and email accounts specifically attributed to foreign actors, but we also found that the FBI shared "content" information when the FBI had intelligence indicating that a foreign actor planned to promote specific themes or narratives with its social media activity.¹² Subsequent to the completion of our fieldwork, DOJ and the FBI jointly drafted a new standard operating procedure (SOP) formalizing steps for the FBI to follow when sharing information about specific foreign malign influence activities or accounts, such as particular posts or uploads of videos, with social media companies. While the SOP represents an improvement over the general guidance that existed at the time of our fieldwork, its sensitivity markings render it not suitable for public release. Finally, we found that the Department does not have a comprehensive strategy for engagement with social media companies regarding foreign malign influence issues.

This lack of policy and strategy created a potential risk because social media companies provide a forum for speech, which is subject to protection under the First Amendment from infringement by the government. While there are no apparent First Amendment implications from the FBI simply sharing information about foreign malign influence threats with social media companies, concerns may arise if that information is communicated in such a way that those communications could reasonably be perceived as constituting coercion or significant encouragement aimed at convincing those companies to act on the shared information in a way that would limit or exclude the speech of those who participate on their platforms.

The FBI Created an "Intelligence Sharing Model" to Share Foreign Malign Influence Threats to U.S. Elections with Social Media Companies

The FBI has developed a method for sharing information with social media companies about foreign malign influence actors to facilitate potential leads, which in turn can be helpful to both parties in identifying further information that can be shared (see Figure 1 below). As part of this method, the social media

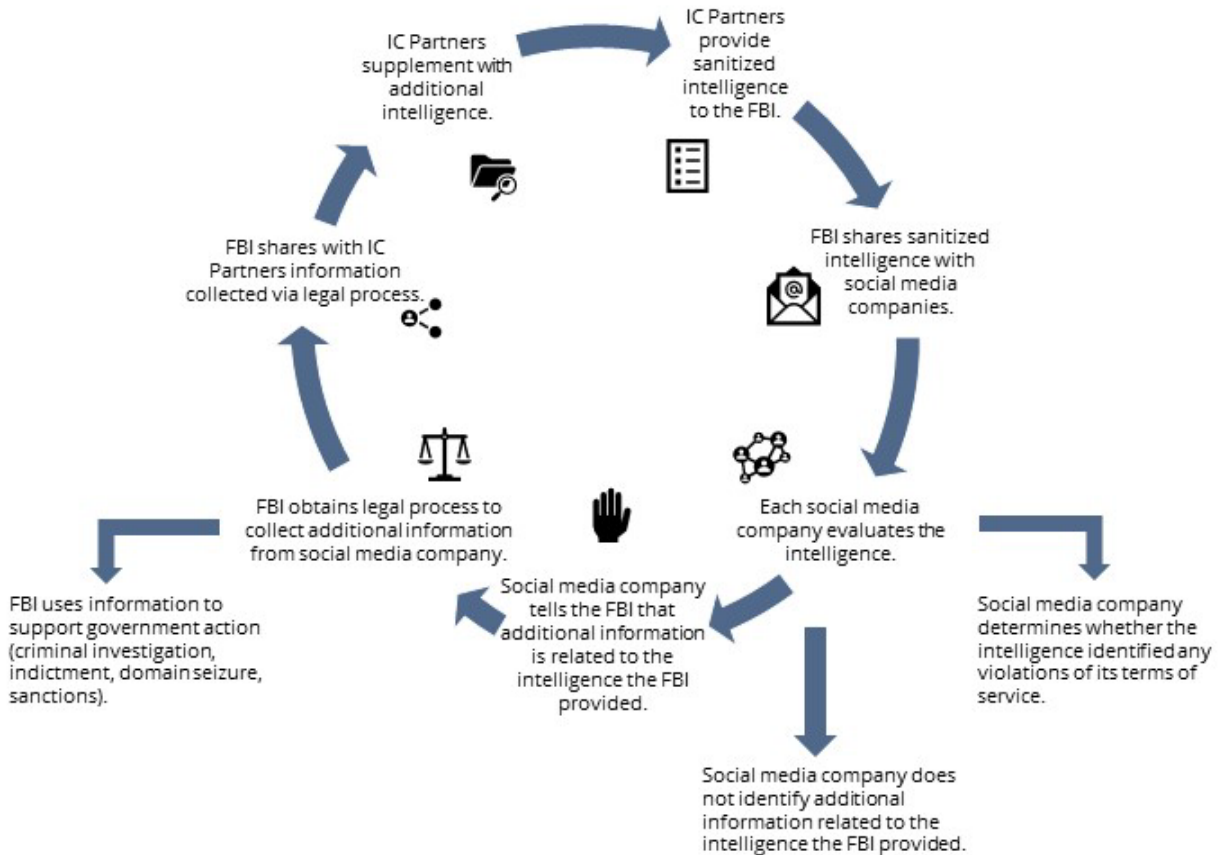
¹¹ The FBI also shares information about foreign malign influence directed at U.S. elections with DHS and state and local governments. This information sharing is primarily focused on cyber threats and is discussed in [Appendix 5](#).

¹² In this report, we use the term "actor" to refer to any information that confirms an actor's identity (such as account handles or Internet Protocol addresses). We use the term "content" to refer to any information that broadly relates to the information conveyed, or to be conveyed, by a foreign actor; this can include themes the FBI believes a foreign actor is using or plans to use or the information that the FBI believes is being or is likely to be shared. For example, the FBI identified specific hashtags and themes related to issues being debated during the 2020 presidential campaign that it believed specific foreign actors planned to use in social media activity to stoke tension and divisiveness in the United States.

companies also share information with the government, usually in the context of legal process obtained under 18 U.S.C. § 2703(d).¹³

Figure 1

The FBI's Intelligence Sharing Model for Sharing Foreign Malign Influence Information with Social Media Companies



Note: "Sanitization" refers to the editing of intelligence to protect sources, methods, capabilities, and analytical procedures to permit wider dissemination.

Source: OIG summarization of FBI and non-FBI interviewee statements

¹³ The FBI told us that social media companies may also provide tips to the FBI voluntarily and not in response to legal process. For example, the FBI stated that in the fall of 2023 one social media company identified multiple websites and social media accounts to the FBI that the social media company assessed as being related to a foreign malign influence operation.

We learned that the FBI maintains an important information-sharing relationship with IC Partners at the case level. To facilitate information sharing, a specific IC Partner has embedded staff (called “Embeds”) at the FBI, both in the field and at headquarters. These Embeds facilitate requests for “sanitization” of intelligence about foreign malign influence actors and share relevant U.S. Intelligence Community reporting with their FBI colleagues. FBI and IC Partner staff told us that having access to these Embeds is extremely helpful when investigating cases; the Embeds can help educate FBI personnel on the types of intelligence products the U.S. Intelligence Community can provide, facilitate access to information that would be otherwise unavailable to the FBI, and expedite the process for information sharing with external entities such as social media companies. One FBI Special Agent told us that assistance from an IC Partner Embed was crucial to his work on a case during the 2020 election because he could ask the IC Partner agency about information, which he could share with social media companies. An official with the IC Partner agency told us that the collaboration with the FBI is important because, unlike their agency, the FBI can take law enforcement action to prevent foreign interference in U.S. elections. This sentiment was echoed by the Foreign Influence Task Force (FITF) Section Chief, who noted that the FBI is the only U.S. Intelligence Community agency that can follow up with social media companies by serving legal process to acquire information about what foreign actors are doing on their platforms.

FBI officials told us that prior to and during the 2016 U.S. presidential election the FBI did not have effective, established relationships with major social media companies. Instead, during this time the FBI’s interactions with social media companies were mainly limited to communication about fraud, counterterrorism, and crimes against children. FBI officials told us that, after Russian attempts to interfere with the 2016 presidential election became public, social media companies contacted the FBI to learn more about what had happened. The companies also expressed interest in learning more about foreign malign influence activities on their platforms and obtaining information from the FBI to better understand the scope of these threats.

DOJ’s Disruption of an Iranian Cyber-Enabled Disinformation and Threat Campaign

The FBI used the foreign malign influence intelligence-sharing model to counter an attempt by two Iranian nationals to influence the 2020 U.S. presidential election. The FBI became aware that an online video threatening American voters—purportedly created by the Proud Boys, an organization described by media as a far-right extremist organization operating in the United States—was actually created by Iranian nationals seeking to influence American voters. These Iranian nationals also sent threatening messages to American voters using information obtained through a hack into a state’s voter website.

Because the U.S. Constitution does not apply to foreign actors operating outside the United States, the video and its content were not protected by the First Amendment. The FBI obtained technical information about the video that could help the social media company identify the video. The FBI then passed this information to the social media company, which identified and removed the Iranian video from its platform.

The FBI Director and the Director of National Intelligence later held a press conference to inform the public that the threats had been made by Iranian nationals. Subsequently, DOJ charged two Iranian nationals with numerous offenses related to computer fraud and intrusion, voter intimidation, and transmission of interstate threats, which exposes them to arrest and extradition to the United States if they travel outside Iran. Further, the U.S. Department of the Treasury designated the charged individuals and several of their associates for sanctions, blocking the Iranian actors from accessing property in the United States and prohibiting people in the United States from engaging in transactions with them.

Sources: DOJ, FBI, and Department of the Treasury

The FBI told us that it viewed the social media companies' interest in learning about the 2016 election interference as an opportunity to build relationships with those companies and that it sought the companies' feedback to identify potential areas for improvement. For example, according to an FBI attorney involved in the conversations, social media companies described the FBI's then practice of offering classified information as impractical due to the limited number of their employees having security clearances, which meant that the companies could not act on the information shared by the FBI. The FBI attorney further stated that social media companies appeared to view the FBI as adversarial rather than cooperative. FITF supervisors added that the social media companies also complained that the FBI seemed only to be asking for information from the companies, but not sharing information with the companies.

FBI officials told us that as a result of this feedback they decided to provide social media companies with unclassified information about foreign malign influence threats, with no expectation of reciprocity. The FBI first experimented with this new information-sharing approach in 2018 by offering several social media companies identifiers such as Internet Protocol (IP) addresses, social media handles, email addresses, or websites of accounts known to belong to foreign malign actors that may have violated the platforms' terms of service.¹⁴ Such violations could include a foreign actor setting up fake accounts, referred to as inauthentic behavior. The FBI further decided that it would offer this information to the companies with "no strings attached" and therefore did not ask the companies for any information in return. Between 2018 and June 2023, the FBI continued this practice by regularly providing social media companies with written information that provided identifiers known to belong to foreign malign actors.¹⁵

Social media companies have publicly stated that the FBI has shared foreign malign influence-related information with them. One company's website confirmed that the FBI sent it information prior to the 2018 congressional election about "online activity" on its platform that the FBI believed was "linked to foreign entities." The company stated that, having determined that the accounts linked to these foreign entities were "engaged in coordinated inauthentic behavior," it removed them from its platform because the

¹⁴ This method of information sharing represented the initial example of the more developed intelligence sharing model discussed above. For a description of the methods the FBI currently uses to share information with social media companies, see [Appendix 3](#).

¹⁵ The OIG examined documentation, which the FBI told us represented all of the meetings that the FBI held with social media companies between August 1 and November 3, 2020, to discuss foreign malign influence, including materials sent in advance of the meetings, as well as data the FBI provided to them. Further, the OIG reviewed what the FBI represented to us to be all of the files uploaded by the FBI to an encrypted file-sharing platform and shared with one or more social media companies regarding foreign malign influence directed at U.S. elections over this period.

Sometimes the FBI shared information about themes tied to foreign actors in addition to information about actors. For example, on October 13, 2020, the FBI shared 10 documents with 6 social media companies. Seven of the 10 documents provided information about Iranian actors, including social media handles and a series of hashtags that the FBI believed those actors might use to disseminate propaganda. One document provided information about Russian actors and anticipated behavior related to the publication of a book. Another provided links to FBI press releases about election crimes. The final document provided contact information for the FBI's San Francisco Field Office. We discuss the impact of such sharing more in the section [below](#).

The OIG did not examine records that were outside this 3-month window, those that had resulted from meetings hosted by agencies other than the FBI, or those whose content was beyond the scope of foreign malign influence information-sharing interactions (see the purpose and scope in [Appendix 1](#)). Further, the OIG did not evaluate the content shared during meetings beyond what was captured in meeting documentation or was relevant to the scope of this evaluation.

company bans that type of activity on its platform. A second company has publicly acknowledged that, based on information the FBI provided, the company removed from its platform accounts of Iranian nationals who were “attempting to disrupt the public conversation during the first 2020 US Presidential Debate.” FBI officials told us that the social media companies evaluated information the FBI provided and at times told the FBI that additional information about account connectivity could be shared if the FBI served legal process.¹⁶ The FBI did so and provided the information collected from the social media companies to other federal agencies. Representatives from one social media company described the FBI’s decision to share this information with them as a “key trust building moment,” because the information was “credible, actionable, and specific,” and the platform was able to take immediate action as a result.

The FBI also established routine quarterly meetings with certain social media companies to discuss foreign malign influence threats on the companies’ platforms.¹⁷ Officials from two companies testified at a September 2018 congressional hearing that their collaboration with the FBI, especially as it related to meeting with the FBI, had increased to help combat foreign influence operations. Another company official testified during a February 2023 congressional hearing that multiple technology companies had worked to build closer information-sharing relationships with the FBI.

These quarterly meetings with social media companies, which began after the 2018 midterm election and ended in mid-2023, were facilitated by the FBI’s San Francisco Field Office, whose Private Sector Engagement Squad serves as the official conduit between the FBI and private companies. The purpose of the meetings was for the FITF and the social media platforms to share threat indicator information, as well as strategic threat information about trends and themes both sides saw from foreign malign influence actors.¹⁸ The FBI met with each company individually, rather than in a group setting with industry competitors present, so that the companies would feel more comfortable discussing any challenges or potential threats they had experienced. Materials that we reviewed showed that in the 3 months leading up to the November 2020 presidential election the FBI held 29 such meetings with 13 different companies.

We also interviewed representatives from four social media companies, with which the FBI shared information to counter foreign malign influence ahead of the 2018 and 2020 elections, and learned that all four were generally satisfied with their interactions with the FBI during that timeframe. Two companies reported that the information-sharing process has improved over time, as both the FBI and the companies learned about foreign adversaries’ techniques; the two companies observed that the establishment of the FITF was helpful for standardizing the information-sharing process. One company said that the ability to share current information through these regular interactions is far more helpful to the platform than

¹⁶ See [Appendix 6](#) for more information about the types of legal process available to the FBI to obtain such information.

¹⁷ In response to a draft of this report, the FBI stated that the scheduling of routine meetings with specific companies was still operationally driven, either because the FBI was aware of threat indicators or other specific information that a foreign malign influence actor might leverage a company’s services or because a company had asked for engagement with the FBI on foreign malign influence. The FBI told us that it stopped meeting with social media companies due to the *Missouri v. Biden* litigation described above.

¹⁸ This voluntary sharing of high level trends and themes does not occur through legal process. The FBI is authorized to receive such information from private entities under Executive Order 12333.

reading government reports after the fact. Another company said that the quarterly meetings were helpful because they created a forum for the companies to ask questions of knowledgeable FBI personnel.

Given the importance to DOJ's mission of maintaining public trust and employing sensitive law enforcement authorities with consistency and objectivity, we asked FBI officials whether the foreign malign influence intelligence sharing model with social media companies had any effects—positive or negative—on the FBI's interactions with these same companies to facilitate other aspects of the FBI's work. The FBI officials stated that they were not aware of other FBI mission areas (unrelated to foreign malign influence or elections) that had been negatively affected. One official stated that he felt that the foreign malign influence election-related sharing had enhanced other FBI missions by building trust among the companies with which the FBI engages in information sharing.

The Department Followed Guidance for Sharing Foreign Malign Influence Information with Government Agencies or Victims of Cyber Attacks but Lacked Guidance for Sharing Threat Information with Social Media Companies

We found that DOJ followed general government-wide policies that guide information sharing in situations involving foreign malign influence and the FBI has additional policies applicable in certain specific situations. These general policies, which we describe below, govern the FBI's information sharing with other federal government agencies, with state and local governments, and with private sector entities when they are victims of cyberattacks such as unlawful intrusion of a computer network. However, at the time of our fieldwork, neither DOJ nor the FBI had policies covering the FBI's information sharing with social media companies on topics such as foreign malign influence directed at U.S. elections.

Coordination within the Federal Government

Sharing among IC partners, which includes the FBI, is established in Executive Order (E.O.) 12333, which permits broad information sharing. For example, Section 1.1(g) of the E.O. states that "all departments and agencies have a responsibility to prepare and to provide intelligence in a manner that allows the full and free exchange of information" consistent with applicable law and guidance.¹⁹ Although this information-sharing authority was in place during the 2016 election, the former Office of the Director of National Intelligence (ODNI) Election Threats Executive told us that the U.S. Intelligence Community has recognized that it did not fully share information that may have helped better defend U.S. elections against foreign influence operations.

We learned that the FBI, in coordination with other federal agencies, uses the Executive Branch Notification Framework to help guide the consistent, apolitical notification of victims of foreign malign influence campaigns. This framework governs when the federal government will provide notifications of foreign interference, as necessary to protect national security and the integrity of our elections, beyond circumstances in which notifications are provided under existing laws or policies. However, this framework does not cover the FBI's regular information sharing with social media companies on whose platforms foreign actors may spread disinformation. In 2019, DOJ collaborated with other IC partners and the National Security Council to develop this government-wide framework to ensure that appropriate members of Congress, state and local government officials, candidates and campaigns, private sector entities, and the

¹⁹ E.O. 12333, as amended by E.O. 13284, E.O. 13355, and E.O. 13470.

public are notified of foreign interference directed at U.S. elections when notification is necessary to protect U.S. national security and elections. Additionally, the FBI has developed an internal policy providing for the notification of individual targets of foreign influence operations, including both election and nonelection-related influence operations, through its Foreign Influence Defensive Briefing Board.²⁰

Coordination with State and Local Governments

We also learned of law and policy applicable to notifying state and local governments of foreign malign influence campaigns targeting them. Broadly, Section 1.6(e) of E.O. 12333 requires the heads of all member agencies of the U.S. Intelligence Community, which includes the FBI, to “facilitate, as appropriate, the sharing of information or intelligence, as directed by law or the President, to State, local, tribal, and private sector entities.”²¹ Further, we found that the FBI has established a policy for notifying state and local officials of cyber intrusions specifically affecting election infrastructure.²² The policy states that, in the event that a cyber intrusion affects a local election authority within a state, the FBI will notify both the affected local authority and the state’s chief election official to ensure that the FBI’s interactions regarding election security matters respect the roles of both state and local election authorities. For additional information about DOJ’s election-related information sharing with state government officials, see [Appendix 5](#).

Coordination with Victims of Cyber Attacks

We also found law and policy governing the notification of private sector entities when they are victims of cyberattacks. Specifically, E.O. 13636 mandates that the federal government increase the sharing of cyber threat information with the private sector.²³ To implement this E.O., the FBI provides Private Industry Notifications (PIN) that share general awareness of cyber threats and FBI Liaison Alert System (FLASH) reports that contain critical technical information to aid in threat neutralization. For more information on the FBI’s use of PINs and FLASH reports, see [Appendix 3](#).

Coordination with Social Media Companies

In contrast to the information-sharing methods noted above, we found that at the time of our fieldwork the FBI’s sharing of threat information with social media companies regarding foreign malign influence activity on their platforms was not governed by a specific DOJ or FBI policy or guidance. E.O. 12333 provides general authorization for the FBI to both send information to, and receive information from, private sector entities as part of its national security mission.²⁴ Further, the FBI Director has publicly emphasized that building strong relationships with the private sector, including social media companies, is a pillar of the FBI’s

²⁰ FBI Policy Notice 1166N, Defensive Briefing Policy Notice, September 8, 2021.

²¹ E.O. 12333.

²² The state and local notification policy provided supplemental guidance to the FBI’s existing cyber victim notification process, which is governed by the FBI’s Cyber Division Policy Guide. The state and local notification policy was superseded by a subsequent revision of the Cyber Division Policy Guide in 2022.

²³ E.O. 13636.

²⁴ E.O. 12333, Sections 1.4(g) and 1.6(e). E.O. 12333 permits the FBI to receive from private entities information that is not otherwise subject to legal process.

approach to combating foreign malign influence.²⁵ During congressional testimony, the FBI Director has also stated that the FBI must work with its partners to address the changing nature of foreign influence due to developments in communications technology and use of the Internet.²⁶ An FBI Section Chief told us that the FBI Director has articulated that the FBI has a duty to inform companies when foreign actors misuse their platforms.

FBI engagement with private sector entities, particularly media and communications outlets, can be sensitive in view of First Amendment considerations. While there are no First Amendment concerns that arise from information sharing in and of itself, the FBI must be mindful of the risk that its interactions with such entities, including any direct or indirect requests arising from the information sharing, could, depending on the precise nature of the interactions, reasonably be perceived as coercion or significant encouragement aimed at convincing the social media companies to limit or exclude speech posted by its customers, which may implicate First Amendment protections.²⁷

When we asked FBI officials during our fieldwork which policy guided the sharing of information with social media companies to combat foreign malign influence directed at U.S. elections, they told us that the First Amendment and the FBI Domestic Investigations Operations Guide (DIOG) provided the basis for the FBI's information sharing in this area but that no policy, guidance, or SOP specifically governed the sharing of foreign malign influence threat information with social media companies. The DIOG provides guidance on applying the First Amendment to FBI activities and acknowledges that it is not necessary for law enforcement action to totally undermine the exercise of First Amendment rights for the action to be unconstitutional. Rather, activities "significantly diminishing or lessening the ability of individuals to exercise these rights" without an authorized investigative purpose under the DIOG, would also be unconstitutional. The DIOG further states that the FBI cannot base any investigative activity solely on activities protected by the First Amendment (see [Appendix 6](#) for details).

The U.S. Attorney General's Guidelines for Domestic FBI Operations (Attorney General Guidelines) also provide guidance on how the FBI should apply the First Amendment.²⁸ The restrictions in the Attorney General Guidelines appear to go beyond the requirements of the First Amendment by prohibiting the FBI from "monitoring" the exercise of First Amendment rights if that is the sole purpose of the investigative

²⁵ E.O. 12333 requires the heads of U.S. Intelligence Community agencies, including the FBI, to "facilitate, as appropriate, the sharing of information or intelligence, as directed by law or the President, to state, local, tribal, and private sector entities" and calls upon U.S. Intelligence Community agencies to take into account the responsibilities and requirements of state, local, and tribal governments and, as appropriate, private sector entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.

²⁶ Christopher A. Wray, Director, Federal Bureau of Investigation, before the Committee on the Judiciary, U.S. Senate, concerning "[Oversight of the Federal Bureau of Investigation](#)" (August 4, 2022), www.judiciary.senate.gov/imo/media/doc/Testimony%20-%20Wray%20-%202022-08-04.pdf (accessed October 12, 2023).

²⁷ See, e.g., *Blum v. Yaretsky*, 457 U.S. 991, 1004 (1982): "[A] state normally can be held responsible for a private decision only when it has exercised coercive power or has provided such significant encouragement, either overt or covert, that the choice must in law be deemed to be that of the state."

²⁸ The Attorney General Guidelines establish Department policy governing the FBI's investigative activities within the United States. The Department issued this policy to balance the FBI's need to fully use its authorities and investigative methods to protect the United States from threats, including national security threats, against its need to respect privacy and avoid unnecessary intrusions into the lives of law-abiding people.

activity, regardless of whether the investigative activity directly infringes on those rights. Multiple FBI officials we interviewed confirmed the importance of the First Amendment to the FBI's approach to information sharing with social media companies. While the Attorney General Guidelines provide basic principles for FBI personnel to follow, they do not describe in detail how FBI personnel can ensure that First Amendment rights are protected when sharing information with private sector entities such as social media companies. Rather, the limited guidance focuses on investigative activities such as monitoring conversations of targets of investigations.

When we asked FBI officials during our fieldwork how they shared information with social media companies in the absence of a specific policy or guidance outlining the process, FBI officials articulated that the FBI's information-sharing method was based on an "actor-driven versus content-driven" approach. In explaining this approach, DOJ and FBI officials told us that, to protect First Amendment rights, the FBI does not monitor social media content on platforms as it relates to foreign malign influence, nor does it investigate specific narratives related to foreign malign influence being spread online. In the next section, however, we discuss instances in which the FBI shared "content" information in its communications with social media companies. Specifically, the FBI did so when it had intelligence indicating that a foreign actor planned to promote specific themes or narratives with its social media activity directed at Americans.

According to one FITF Unit Chief, rather than seeking online content that may indicate foreign malign influence activity, the FBI acted based on intelligence concerning the activities of specific foreign actors developed during its ongoing investigations or received from other federal agencies. When the FBI received threat information about a foreign malign influence operations on social media platforms, it may then have shared an unclassified version of relevant information with social media companies about the foreign malign influence activity on their platforms. This explanation matched our review of FBI presentations about the FITF's mission, which state that the "subversive, undeclared, criminal, or coercive nature of foreign malign influence activities" is the basis for the FBI's investigative interest. Representatives from one social media company said that the information the FBI shared matched what the company was already tracking, giving the company confidence that it and the FBI were on the same page.

Two FITF Unit Chiefs explained that foreign malign influence campaigns often sought to amplify speech made by people in the United States that is protected by the First Amendment. These officials explained that the FBI sought to determine whether suspicious activity on social media platforms, such as amplification, could be tied to a foreign actor and that the FBI's focus was the suspicious activity rather than the content that the foreign actors were amplifying.²⁹ According to the former Assistant Director of the FBI's Counterintelligence Division, social media companies may then have used this information to investigate foreign malign influence activity on their platforms and may have requested that the FBI serve the company with a court order before the company shared the results of its internal investigation with the FBI. See [Appendix 6](#) for more information on the legal processes through which the FBI can obtain information from social media companies.

²⁹ In response to a draft of this report, the FBI stated that the Counterintelligence Division's mission is to identify foreign attribution as it pertains to suspicious activity on social media platforms. If there is evidence of social media activity originating from a foreign actor, the Counterintelligence Division will investigate as necessary.

FBI officials told us that, because of First Amendment concerns, the FBI shared foreign malign influence information with social media companies without providing direction on what those companies should do with the information. FBI and DOJ officials expressed that the FBI and DOJ did not tell the companies to take specific action because they do not want to create a situation in which social media companies are acting as agents of the U.S. government. However, FBI officials also told us that the FBI provided information to social media companies about foreign malign influence actors using their platforms in ways that the FBI believed could violate the platforms' terms of service.³⁰ FBI officials told us that the FBI strove to understand companies' terms of service but the companies themselves made the determination about whether there had been an actual violation.³¹

An FBI attorney noted that it took a long time for the FBI to build trust with social media companies and to ensure that both FBI personnel and the companies understood the voluntary nature of the information-sharing relationship. When asked whether he thought that social media companies understood that the FBI is not directing them to take action, a DOJ National Security Division (NSD) attorney stated that, in his experience, social media companies had not been afraid to push back on FBI requests and require that the FBI provide legal process before they responded. During the OIG's review of a sample of communications about foreign malign influence between the FBI and social media companies during the 3 months preceding the 2020 U.S. presidential election, we found that one of the social media companies informed the FBI that it had taken no action based on information the FBI had provided. The OIG also identified documentation that another company had removed some accounts from its platform based on information the FBI had provided but did not remove others because the company had determined that the other accounts had not violated its terms of service.

The Department Lacked Clear Policy on Sharing, with Social Media Companies, Content Information, Such as Themes Tied to Foreign Actors

As noted above, we found that FBI communications to social media companies generally focused on foreign actors by sharing information about social media and email accounts specifically attributed to foreign actors while giving no direction on what to do with the information. However, we also found during our document review that the FBI shared "content" information when the FBI had intelligence indicating a foreign actor planned to promote specific themes or narratives with its social media activity directed at Americans.³²

³⁰ Further, these officials stated that the social media companies have tools that they can use to investigate potential foreign malign influence activity on their own platforms and determine the appropriate action based on their own policies.

³¹ Although multiple FBI officials similarly described this approach to the OIG, their description of the FBI's general practice may be in tension with the October 2023 decision of the U.S. Court of Appeals for the Fifth Circuit, referenced [above](#), which concluded, based on the factual record before that court, that the FBI had "urged the platforms to take down content." *Missouri v. Biden*, 83 F.4th 350, 388 (5th Cir. 2023), *rev'd sub nom. Murthy v. Missouri*, 144 S. Ct. 1972 (2024). In response to a draft of this report, the FBI made clear that it disagrees with the Fifth Circuit's conclusion.

³² In the documents we reviewed, the content information about foreign malign influence actors that the FBI shared with multiple social media companies simultaneously did not quote specific posts. We also identified instances in which the FBI shared a specific post associated with a foreign actor with a single social media company.

Continued

In response to this observation, the FITF Section Chief told us that the FBI's "actor-driven versus content-driven" model did not mean that the FBI would never share information about content with social media platforms, but rather that the identity as a foreign actor and their activities were driving the nature of the information shared, including about messages or themes that actor may be seeking to push on social media platforms. An FBI Assistant Special Agent in Charge (ASAC) told us that social media companies have asked the FBI about the themes the FBI saw in the activities of foreign actors. The ASAC told the OIG that this type of information was not something the FBI regularly shared with the companies, but that companies told the FBI that it would be helpful to know about themes in foreign actors' behaviors leading up to elections so that the social media companies could monitor their platforms for foreign malign influence activity. The ASAC also told the OIG that in some instances the FBI was able to share credible intelligence about foreign actors discussing the specific themes they were planning to promote to Americans on social media platforms.

Due to the complex nature of foreign influence campaigns and potential First Amendment implications of sharing content information with social media platforms, we believe that the Department should mitigate the inherent risks in this area. Unlike sharing with other government agencies, sharing content with private sector entities, particularly social media platforms, presents a unique set of challenges, as illustrated by the decision of the U.S. Court of Appeals for the Fifth Circuit, described [above](#).³³ Further, guidance on combating foreign malign influence published by the National Intelligence Council noted that, "because [foreign malign] influence campaigns are generally conducted with methods that could constitute speech, departments and agencies should take care to specifically define foreign malign influence activities to ensure protection of civil liberties."³⁴

DOJ and FBI officials we spoke with agreed that there were inherent risks involved in DOJ's mission to combat foreign malign influence directed at U.S. elections due to the sensitive First Amendment concerns related to speech on social media platforms. A former Deputy Assistant Attorney General in NSD told the OIG that DOJ must be sensitive about how it is perceived by others and share information carefully when working to combat foreign malign influence campaigns. He added that the framework for how DOJ works with social media platforms is not well understood by the public, which creates a potential for significant damage to DOJ's credibility and reputation. He noted that transparency is important when it comes to foreign malign influence and stated that he believed that it would be good if the public understood more clearly what the FBI and DOJ do when they meet with social media companies. Similarly, an FBI attorney acknowledged that because of the free speech implications the FBI operates in a "risky legal space" in its efforts to combat foreign disinformation campaigns. He stated that the FBI must ensure that it provides only "foreign [actor] account information" to social media companies to avoid partisan political appearances and legal issues.

Because our evaluation focused on the Department's information sharing about foreign malign influence threats to U.S. elections, we did not evaluate the extent to which the Department shared information about domestic actors with social media companies.

³³ The OIG notes that the Supreme Court recently issued another opinion addressing the First Amendment risks of government actors seeking to limit or control the actions of social media companies. *See Moody v. NetChoice LLC*, 144 S. Ct. 2383 (2024). This is an active and evolving area of federal jurisprudence.

³⁴ The National Intelligence Council supports the Director of National Intelligence's role as head of the U.S. Intelligence Community and is the U.S. Intelligence Community's center for long-term strategic analysis.

The FBI is aware of the risks and challenges associated with combating foreign malign influence and acknowledges them in presentations to DOJ stakeholders about the FITF's mission. In these materials, which provided a broad overview of the FBI's efforts to combat foreign malign influence, the FBI emphasized that such investigative matters are often politically sensitive and that influence activities are not "black and white" but take place in a "gray area."

DOJ and FBI officials we interviewed agreed that the FBI should continue sharing foreign malign influence election-related information with social media platforms to counter foreign threats. They believed that the national security risks associated with not sharing foreign malign influence threat actor information with social media platforms outweigh potential negative effects on the FBI's public image from continuing to share information. They expressed support for a policy or guidance that more clearly and transparently defined the FBI's mission, approach, and procedures for sharing information with social media companies. An FBI Intelligence Analyst in Charge told us that developing a policy could be a challenge because combating foreign malign influence directed at U.S. elections is a fluid space; but she acknowledged that a policy could help protect the FBI and ensure that the boundaries of FBI actions are clear. A former Deputy Assistant Attorney General in NSD and the former Assistant Director of the FBI's Counterintelligence Division agreed that there would be value in having a policy on the process for sharing information with social media companies. This assessment of the need to share information with social media companies in furtherance of critical national security goals underscores the importance of transparency and consistency; we believe that the development of a public-facing policy or guidance would be in the Department's interest.

Subsequent to the completion of our fieldwork, DOJ and the FBI jointly drafted a new SOP governing the FBI's transmission of foreign malign influence threat information to social media companies. The FBI implemented the SOP beginning in February 2024 and first provided a copy of the SOP to the OIG in response to its review of a draft of this report.³⁵ The SOP, which is marked as classified, formalized steps for the FBI to follow when sharing information about specific foreign malign influence activities or accounts, such as particular posts or uploads of videos, with social media companies. These steps include:

- criteria for determining that the information constitutes foreign malign influence,
- supervisory approval requirements, and
- standard language for inclusion with every disclosure and guidance governing the FBI's further engagement with social media companies that specifically recognize and address the First Amendment risks described above in this report.

We concluded that the SOP is an improvement over the general guidance that existed at the time of our fieldwork. For example, we determined that the supervisory approval requirements are targeted to the

³⁵ The FBI also provided a copy of an unclassified January 2024 National Security Council document titled "Interim Guidance Regarding Certain Engagement with Tech Companies Regarding Online Content." DOJ and the FBI incorporated the principles outlined in this guidance into the new SOP.

proper level and ensure both substantive and legal review. We also determined that the SOP describes criteria that information must meet to be eligible for sharing with social media companies.

Despite these improvements over the prior general guidance, we note that the SOP does not prohibit employees from using pre-populated or boilerplate criteria when documenting in the FBI's records the decision to disclose information to a social media company. We encourage the FBI to consider whether the SOP as currently drafted addresses this concern. Additionally, in view of its sensitivity markings, the FBI informed the OIG that the SOP is not suitable for public release. As we noted above, a former Deputy Assistant Attorney General in NSD articulated that DOJ's credibility and reputation are at risk when its activities are not well understood by the public. We therefore recommend that the Department identify a way that it can inform the public about the procedures it has put into place to transmit foreign malign influence threat information to social media companies while also protecting First Amendment rights.

The Department Lacked a Strategic Approach to Engagement with Social Media Companies to Address the Landscape of the Foreign Malign Influence Threat to U.S. Elections

Although officials we interviewed at the FBI and social media companies expressed satisfaction with their relationships to share information about foreign malign influence during the 2018 and 2020 election cycles, we found that the Department does not have a comprehensive strategy for engagement with social media companies regarding foreign malign influence issues. FBI officials and reports describe that novel threats, such as the expansion of foreign-owned social media platforms and the development of new technologies that could support foreign malign influence campaigns, pose risks to U.S. elections. Led by NSD, the Department established its first overall strategy to combat foreign malign influence in the 2018 Attorney General's Cyber Digital Task Force report, which provided general guidance for DOJ actions to expose and counter foreign influence threats and was subsequently incorporated into the Justice Manual.³⁶ The report broadly stated that "the Department maintains strategic partnerships with social media providers" without providing an approach to establishing and maintaining such partnerships. A former Deputy Assistant Attorney General in NSD who worked on the Cyber Digital Task Force's report told us that the Department's interactions with social media companies have been fluid and that traditionally the FBI has taken the lead on these interactions. During fieldwork, we identified three risk areas associated with the Department's lack of a strategic approach to relationships with social media companies.

First, the FBI maintains relationships with social media companies in the San Francisco Field Office's area of responsibility but lacks ongoing relationships with social media companies outside the San Francisco Bay Area. The FITF Section Chief told us that the FITF has had occasional contact with fewer than six companies located outside the San Francisco Field Office's area of responsibility to convey specific and discrete information, such as account handles, that may be relevant to a specific company. For companies located outside the San Francisco Bay Area, the FBI's information sharing through occasional contact to convey specific and discrete information is an approach that appears different than the more regular, trust building

³⁶ DOJ, *Report of the Attorney General's Cyber Digital Task Force* (July 2018). See [Appendix 6](#) for more information about the resulting section of the Justice Manual, including the principles that the Department will weigh when making disclosure decisions.

approach used for companies located inside the San Francisco Bay Area.³⁷ This differing approach can create risks if foreign malign influence actors begin using accounts on these platforms. Our review of FITF quarterly meeting records (discussed above) also demonstrated this area of risk. Records of one such meeting documented a social media company representative stating that his company had done research and had determined that a foreign actor was building contacts on smaller social media platforms with sympathetic audiences.³⁸ A former Assistant Director of the FBI's Counterintelligence Division stated that smaller social media companies could be targeted by foreign actors to spread messages specifically to appeal to the particular partisan lean of a platform's users. Other officials said that the FBI would benefit from establishing ongoing relationships with social media companies, including smaller companies, in other parts of the country. Some FBI officials, as well as representatives from one social media company, did note that the FBI may have more difficulty establishing information-sharing relationships with smaller companies that may not have dedicated security operations staff to address foreign malign influence threats.

Second, the increasing reach of foreign-owned social media platforms poses a challenge. FBI officials told us that having information-sharing relationships with these companies may pose national security risks. If a foreign malign influence campaign were to be conducted on foreign social media platforms, FBI officials told us, the FBI response would require a different approach than foreign malign influence campaigns on U.S.-based platforms. FBI officials stated that information sharing with such companies would be a challenge because the information could end up in the hands of a foreign adversary. Instead, the FBI might need to rely on assistance from foreign partner nations.

Third, as technology continues to develop, foreign actors may use sophisticated tools in foreign influence campaigns. FBI officials we interviewed expressed concern that foreign actors could use "deepfakes" to manipulate or generate content using artificial intelligence techniques to promote their influence campaigns targeting U.S. elections.³⁹ In January 2020 the FBI's Office of Private Sector disseminated a report, intended for wide distribution throughout the private sector, warning that foreign malign actors, who have technical resources beyond those available to individuals or rival political organizations, could post deepfake-generated content on social media to help candidates they perceive as favorable to their interests or to undermine candidates they perceive as threats. The report cautioned its recipients that if such content

³⁷ An ASAC from the FBI San Francisco Field Office described a three-pronged approach to information sharing focused on (1) engaging in multiple avenues of communication with companies to build trust using contact outside the regularly scheduled meetings or requests for investigative assistance, (2) building cooperation with companies to combat foreign malign influence directed at U.S. elections, and (3) understanding the unique culture of technology companies.

For example, we learned that appropriate attire for meetings in the technology industry is more casual than what is considered appropriate in other industries or the government. We also learned that conceptions of timeliness in responding to requests and inquiries varies significantly between the government and the technology industry.

³⁸ In response to a draft of this report, the FBI stated that sharing actionable, specific information related to companies being targeted has been critical to the FBI's efforts to build trust with social media companies. The FBI further stated that the nature of these relationships is voluntary and critical to their success and that it cannot force companies to engage regularly.

³⁹ A "deepfake" is a realistic photograph, audio, video, or other forgery most often created with artificial intelligence technology.

went viral it could amplify voters' misconceptions and undermine a targeted candidate's credibility with American voters.

We believe that DOJ, in particular the FBI, as both a law enforcement and an intelligence agency that leads the Department's interactions with social media companies, can do more to improve resiliency and address risks related to the evolving foreign malign influence threat landscape that is directed at U.S. elections. The Department should address the lack of strategic engagement with companies outside the San Francisco Bay Area, the rise of foreign-owned social media platforms, and evolving technologies that foreign actors may employ in their foreign malign influence campaigns. The lack of a comprehensive, Department-level strategy to coordinate information sharing with social media companies regarding foreign malign influence stands in contrast to other priority threat areas covered by DOJ's mission. Additionally, the lack of policy (discussed previously) and strategy creates a potential risk because social media companies provide a forum for speech, which is subject to protection under the First Amendment from infringement by the government.

As described previously, subsequent to the completion of our fieldwork, the Department and the FBI jointly drafted a new SOP governing the FBI's transmission of foreign malign influence threat information to social media companies and implemented that procedure beginning in February 2024. The Department and the FBI take the position that the Department's broad strategy for addressing foreign malign influence threats is discussed in the Justice Manual and the DIOG, with the new SOP essentially functioning as a strategy for engagement with social media companies on this topic. We evaluated the SOP to assess this position, and also evaluated a 2018 document, titled "Foreign Influence Task Force Mission and Strategy," which was quoted in the new SOP but had not been previously provided to the OIG for review.

We concluded that the SOP outlines a reasonable approach for the FBI to provide information to social media companies who are willing to interact with the FBI and with which the FBI has taken steps to establish contacts and a relationship. However, we believe that further work to develop a broader strategy will aid the Department and the FBI in addressing the potential risk that could result from foreign actors engaging in foreign malign influence activity on social media platforms with which the FBI is unable to communicate directly and with which it had not developed contacts or relationships. In our review of the "Foreign Influence Task Force Mission and Strategy" document, we found that the document contemplated some of the same risks we have identified; but it is not clear to us whether the FBI took actions to address those risks.

We therefore recommend that the Department develop and implement a comprehensive strategy to ensure that DOJ's approach to information sharing with social media companies to combat foreign malign influence directed at U.S. elections can adapt to address the evolving threat landscape while also addressing risks related to First Amendment rights.

NSD, USAOs, and FBI Field Offices Effectively Share Information Regarding Foreign Malign Influence Cases Involving Threats to U.S. Elections

We found effective coordination within and among NSD, USAOs, and the FBI, the three DOJ components tasked with sharing case information regarding foreign malign influence directed at U.S. elections. Within DOJ, coordination on foreign malign influence directed at U.S. elections occurs on two levels: (1) a strategic,

case management level, at which NSD guides decisions about DOJ's overall approach to combating foreign malign influence threats through prosecutions, and (2) a case-to-case, investigative level, at which FBI agents, Assistant U.S. Attorneys (AUSA), and NSD attorneys coordinate weekly on the investigation and prosecution of individual cases. Officials from NSD, USAOs, and the FBI told us that they communicated regularly and worked collaboratively as partners on foreign malign influence cases.

NSD Plays an Important Role in Sharing Foreign Malign Influence Information and Expertise

DOJ's NSD plays the primary role in sharing strategic information about foreign malign influence directed at U.S. elections by representing DOJ in interagency coordination, including coordination within the IC. At the strategic level, NSD interacts with the FBI and other IC partners through meetings hosted by the ODNI, as well as by the National Security Council. FBI engagement with other U.S. Intelligence Community agencies includes interagency meetings in which the FITF represents the interests of the FBI. According to the former ODNI Election Threats Executive, these interagency meetings included work on policy issues related to intelligence sharing leading up to the 2020 presidential election. NSD and the FBI also participate with other IC partners in discussions facilitated through the Executive Branch Notification Framework.⁴⁰ A former NSD Deputy Assistant Attorney General involved in these discussions said that the Framework creates an opportunity for agencies to discuss how to share information without appearing to take sides in U.S. elections.

NSD also serves as the primary DOJ component for legal expertise on combating foreign malign influence, both in crafting policy and by playing a leading role in prosecutions. NSD has a role in investigative, case-level information sharing at both headquarters and field levels. The FBI's DIOG requires that the FBI and NSD regularly meet to share information about national security threats and approaches for addressing such threats. The FITF is the lead FBI office for responding to foreign malign influence threats, and NSD's Counterintelligence and Export Control Section (CES) is the lead NSD office for responding to foreign malign influence threats. The Section Chief of the FITF and the Deputy Chief of the CES with responsibility for the foreign malign influence portfolio meet monthly to discuss relevant cases.⁴¹ FITF staff also reported effective engagement with NSD attorneys, including frequent coordination on sensitive cases. NSD's expertise facilitates effective foreign malign influence information sharing, including at high-level interagency meetings, in policy development, and through Department coordination on foreign malign influence investigations.

USAOs, NSD, and FBI Field Offices Effectively Coordinate to Share Information Regarding Foreign Malign Influence Cases Involving Threats to U.S. Elections

The Justice Manual identifies criminal provisions affecting, involving, or relating to national security and requires USAOs to consult with NSD's CES on cases involving these statutes, or otherwise affecting, involving, or relating to national security, when specific events, such as the need to request a search warrant, occur over the course of an investigation. This includes statutes that NSD officials told us are relevant to foreign malign influence investigations or recent indictments involving foreign malign influence

⁴⁰ We provided additional detail about the Executive Branch Notification Framework in the [Introduction](#) to the report.

⁴¹ The CES supervises the investigation and prosecution of cases affecting national security, foreign relations, and the export of military and strategic commodities and technology.

directed at U.S. elections.⁴² The acting CES Section Chief said that these consultation requirements ensure that the FBI and USAOs discuss foreign malign influence cases with NSD counsel but that coordination with USAOs occurs more frequently than the minimum requirements found in the Justice Manual. She added that, although NSD does not have to sign off on all forms of legal process for social media companies, it is usually aware that legal process is taking place. She emphasized that decision making is collaborative between NSD, FBI, and AUSAs in foreign malign influence cases.

The National Election Command Post

To facilitate coordinated information sharing in the weeks immediately preceding and after each national Election Day, FBI headquarters operates a National Election Command Post (NECP) in the Strategic Information and Coordination Center. The NECP is responsible for coordinating all FBI election-related operations, analyzing and disseminating intelligence, providing rapid DOJ consultation for FBI matters nationwide, facilitating real-time information sharing with other government agencies, and deconfliction. The 2020 NECP had staff from across FBI headquarters, including FITF personnel; DOJ attorneys to vet information being shared to various FBI field offices for action, particularly to FBI San Francisco for sharing with social media companies; and liaisons from five non-DOJ partner agencies. In addition to sharing information about foreign malign influence, the NECP also shared information relevant to cyber intrusions and information related to criminal violations of election law.

The FBI supplemented the NECP by requiring all field offices to establish a local election command post, including staff capable of addressing both domestic and foreign malign influence threats. These local command posts submitted tips received by each field office to the NECP for evaluation and acted on tips forwarded to the field office by the NECP. The FBI field office in San Francisco also established a dedicated communications channel with area technology and social media companies as part of its local election command post to share foreign malign influence threat information.

For information on the FBI Cyber Division's involvement in the NECP, see [Appendix 3](#), "Watch Floor and CyNERGY."

Source: FBI

NSD officials told us that NSD trial attorneys and AUSAs work as "equal partners" on foreign malign influence cases because foreign malign influence, including influence directed at U.S. elections, is a relatively new and high profile area. An AUSA we interviewed echoed this sentiment, stating that his USAO and NSD work together to make a collaborative decision about the role NSD will play in each case. One AUSA described the CES as the "overall coordinator" for foreign malign influence cases because NSD sees the "big picture" and facilitates coordination among the relevant FBI offices and USAOs. AUSAs we interviewed also emphasized the importance of involving NSD because NSD takes a higher, strategic view of the FBI's casework to ensure that all of DOJ's components are synchronized on an issue. For example, an AUSA told us that he briefs issues to NSD earlier than is required so that NSD is aware of emerging issues in foreign malign influence cases. Another AUSA told us that, when he authorizes the opening of a new counterintelligence or cyber national security case, including a foreign malign influence case, he informs the CES right away. Still another AUSA told us that his office participated in weekly calls during the 2016 presidential election to share case information with the CES.

The USAOs focus on information sharing specific to individual investigations. AUSAs and FBI agents described generally effective interactions between their offices to investigate ongoing foreign malign influence cases. AUSAs we interviewed told us that coordination is most effective when FBI staff involve

⁴² The Department has published the entire text of the Justice Manual on its website. See, for example, DOJ, Justice Manual § 9-90.000–[National Security](#), www.justice.gov/jm/jm-9-90000-national-security#9-90.020 (accessed July 26, 2023).

their offices early during investigations so that they may assist with the overall approach to a case and any early legal process requests. An FBI Special Agent said that one of the best ways to counter foreign malign influence is public exposure, which renders the foreign actor's activities less effective. He explained that the best way to achieve that exposure is for FBI Special Agents and AUSAs to begin working together as soon as possible with the goal of developing criminal charges that can be unsealed for the public.⁴³

An AUSA who has worked on investigations involving foreign malign influence threats directed at U.S. elections said that the local FBI field office and his USAO have "a very open dialogue." Another AUSA said that, during one investigation of foreign malign influence threats to the 2020 presidential election, coordination between the USAO and FBI Special Agents helped the government develop the evidence it needed to take disruptive action, before the election occurred, against a collection of websites controlled by a foreign malign actor.

⁴³ Indictments of foreign actors who are unlikely to be brought into U.S. custody are designed to disrupt foreign actors and their criminal networks by making the public aware of their foreign malign influence campaigns, restricting their ability to access financial assets, and limiting their travel to the United States or countries friendly to the United States due to the threat of prosecution.

Conclusion and Recommendations

Conclusion

The FBI developed an intelligence sharing model for sharing information related to foreign malign influence threats to U.S. elections with other members of the U.S. Intelligence Community and social media companies. However, we found that at the time of our fieldwork DOJ did not have guidance pertaining to the information that is shared with social media companies. This lack of guidance created potential risks for the FBI and the Department arising from the fact that social media is often used as a forum for protected political speech in connection with U.S. elections. DOJ and FBI officials acknowledged the sensitivity of the FBI's mission to combat foreign malign influence directed at U.S. elections and articulated that the FBI's information-sharing method is based on an "actor-driven versus content-driven" approach. In explaining this actor-driven approach, Department and FBI officials told us that the FBI does not monitor social media content on platforms as it relates to foreign malign influence, nor does it investigate social media activity based on specific narratives; rather, the FBI said that it acts on intelligence concerning the activities of foreign actors. However, the information the FBI shared with social media companies sometimes also described "content" information when the FBI had intelligence indicating that a foreign actor planned to promote specific themes or narratives with its social media activity.

The Department and the FBI jointly drafted a new standard operating procedure (SOP) governing the FBI's transmission of foreign malign influence threat information to social media companies and implemented it in February 2024. While this was an improvement over the prior general guidance, we note that the SOP does not prohibit employees from using pre-populated or boilerplate criteria when justifying a disclosure of information to a social media company. We encourage the FBI to consider whether the SOP as currently written addresses this concern. Additionally, in view of its sensitivity markings, the FBI informed the OIG that the SOP is not suitable for public release. Because DOJ's credibility and reputation are potentially impaired when its activities are not well understood by the public, we recommend that the Department identify a way that it can inform the public about the procedures it has put into place to transmit foreign malign influence threat information to social media companies in a manner that is protective of First Amendment rights. We also found that DOJ did not have a comprehensive strategy guiding its approach to engagement with social media companies on foreign malign influence directed at U.S. elections, resulting in varied approaches to its information-sharing relationships with social media companies depending on where those companies were based. Establishing a comprehensive strategy could help DOJ address the challenging threat landscape of foreign malign influence directed at U.S. elections and ensure that DOJ takes a cohesive approach to engagement with social media companies to combat the threat.

Although the FBI has traditionally served as the primary conduit for DOJ's interactions with social media companies, the National Security Division (NSD) is the primary DOJ component for crafting policy on combating foreign malign influence. We therefore believe that the Department should develop this policy or guidance to ensure that FBI efforts in sharing information with social media companies to combat foreign malign influence are cognizant of this risk and undertaken in a manner to mitigate it. In addition to contributing to DOJ's important mission to protect U.S. elections, policy and guidance that promotes doing so in a manner that recognizes the potential First Amendment implications would strengthen public trust in the Department.

Finally, we found that the FBI, NSD, and U.S. Attorney's Offices effectively coordinate the sharing of case information relating to foreign malign influence threats to U.S. elections at a strategic, case management level, at which decisions about DOJ's overall approach to combating foreign malign influence are made, and at the case level, at which FBI agents, Assistant U.S. Attorneys, and NSD attorneys coordinate daily on the investigation and prosecution of individual cases. Officials we spoke with at each of the three DOJ components tasked with sharing case information regarding foreign malign influence directed at U.S. elections expressed positive views about their information-sharing relationships within the Department pertaining to foreign malign influence directed at U.S. elections and emphasized that information sharing among the components facilitated the investigations' progress toward their objectives.

Recommendations

To address risks in DOJ's mission to combat foreign malign influence directed at U.S. elections, we recommend that the Department:

1. Develop an approach for informing the public about the procedures the Department has put into place to transmit foreign malign influence threat information to social media companies that is protective of First Amendment rights.
2. Develop and implement a comprehensive strategy to ensure that the Department of Justice's approach to information sharing with social media companies to combat foreign malign influence directed at U.S. elections can adapt to address the evolving threat landscape.

Appendix 1: Purpose, Scope, and Methodology

Standards

The OIG conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* (January 2012).

Purpose and Scope

The OIG conducted this evaluation to assess the effectiveness and resilience of the Department's information-sharing system related to foreign malign influence threats to U.S. elections and the Department's oversight, management, and coordination of its activities to respond to such threats, as well as to identify any gaps or duplication of effort among these efforts during the 2016, 2018, and 2020 U.S. election cycles. We did not examine these efforts during the 2022 U.S. election cycle because that election cycle was ongoing at the time of our fieldwork and we did not want to interfere with DOJ's activities. We also did not examine the sharing of information related to election crimes that are domestic in origin, such as ballot fraud or campaign finance crimes unrelated to foreign malign influence directed at U.S. elections, nor did we examine the FBI's information sharing with social media companies with respect to domestic actors.

Our fieldwork took place between October 2021 and April 2023.

Due to limitations in the evidence available from the FBI, we did not evaluate the Department's sharing of information about all of the forms that foreign malign influence could take, such as cyber operations targeting election infrastructure or covert influence operations aimed at assisting or harming political organizations. We focused on the Department's information sharing with social media companies to evaluate the aspect of the Department's information-sharing system that the Foreign Influence Task Force (FITF) developed following foreign malign influence directed at the 2016 U.S. presidential election because many FBI employees described these interactions to us and we concluded that those interactions were important.

Subsequent to the OIG's initiation of this evaluation, the FBI's engagement with social media companies became the subject of civil litigation. During that litigation, in addressing a preliminary injunction sought by the plaintiffs, the U.S. Court of Appeals for the Fifth Circuit found that FBI officials had "likely (1) coerced the platforms into moderating content, and (2) encouraged them to do so by effecting changes to their moderation policies, both in violation of the First Amendment." *Missouri v. Biden*, 83 F.4th 350, at 388 (5th Cir. 2023). In response to a draft of this report, the Department stated that it disagreed with the Fifth Circuit's holding and noted that the Fifth Circuit found that it could not say that the FBI's communications "were plainly threatening in tone or manner," but rather concluded only that "because the FBI wielded *some* authority over the platforms, the FBI's takedown requests can 'reasonably be construed' as coercive in nature." On June 26, 2024, the Supreme Court reversed the Fifth Circuit's judgment, holding that the plaintiffs lacked sufficient standing to seek the preliminary injunction at issue. *Murthy v. Missouri*, 144 S. Ct. 1972 (2024). While the Supreme Court has issued its ruling on the preliminary injunction and remanded the case to the lower courts, the underlying litigation that gave rise to the request for a preliminary injunction remains ongoing, and, for that reason, to the extent the lawsuit includes allegations against the FBI relating

to foreign influence on U.S. elections, the OIG did not include those allegations within the scope of this evaluation.

Methodology

Our methodology consisted of interviews of DOJ, other federal government, state, and local officials, including a site visit to the San Francisco Bay Area to meet with FBI, U.S. Attorney's Office (USAO), U.S. Department of Homeland Security (DHS), state, and local officials, as well as representatives from several social media companies. We also analyzed Department and FBI policies and examined records associated with the FBI's information-sharing activities.

Interviews and Observations

We conducted 93 interviews during this evaluation. The individuals whom we interviewed held their identified roles during that timeframe. As part of our fieldwork, we conducted a site visit to the FBI's San Francisco Field Office.

DOJ Interviews

At the FBI, we interviewed current and former staff in the Counterintelligence Division; the Office of the General Counsel; the FITF, including both Special Agents and Intelligence Analysts; the Cyber Division; and the Security Division. We requested demonstrations of databases that the FBI can use to share information, as well as examples of information related to foreign malign influence directed at U.S. elections that were shared using those databases. We provide additional information about these systems in [Appendix 3](#). We also interviewed FBI field division staff, including supervisors and Special Agents.

At the National Security Division, we interviewed current and former supervisory and nonsupervisory attorneys.

At the USAOs, we interviewed Assistant U.S. Attorneys who have worked on investigations and prosecutions involving foreign malign influence directed at U.S. elections.

Non-DOJ Interviews

We interviewed stakeholders in other federal agencies, including the Office of the Director of National Intelligence and DHS's Cybersecurity & Infrastructure Security Agency.

We interviewed officials at the agencies responsible for the certification of election results in five states.

We interviewed employees from four social media companies with whom the FBI regularly shared information on foreign malign influence directed at U.S. elections in the months leading up to the 2020 presidential election.

Policy and Document Review

To understand the rules and parameters for sharing information on foreign malign influence directed at U.S. elections, we reviewed executive orders, Department and FBI policies, and Department and FBI training materials related to the general topics of foreign malign influence and responding to election-related threats, including relevant sections of the March 2020 edition of the FBI's Domestic Investigations and Operations Guide.

To understand the FBI's practice of hosting quarterly bilateral meetings with social media companies and the type of information exchanged with those companies on the topic of foreign malign influence directed at U.S. elections, we reviewed records of all meetings that the FBI held with social media companies for this purpose between August 1 and November 3, 2020. We chose this date range because it encompassed the 90 days preceding a presidential election and interviewees had told us that communication between the FBI and social media companies is frequent close to an election. In addition to reviewing records of meetings, we also reviewed copies of all information about foreign malign influence shared with social media companies, either directly in connection with a bilateral meeting or in a separate communication, during that same 90-day period.

Appendix 2: The Mission, Structure, and Development of the Foreign Influence Task Force and the Role of the FBI's Cyber Division

The Mission and Structure of the Foreign Influence Task Force

The Foreign Influence Task Force's (FITF) mission and structure have developed since its creation. At the time of our evaluation, the FITF's mission is to protect democratic institutions and public confidence, develop a common operating picture, raise adversaries' costs, and reduce the threats presented by adversaries across the globe. The FITF brings together employees from the FBI's Counterintelligence, Cyber, Criminal Investigative, and Counterterrorism Divisions under a unified command structure.

Structurally, the FITF is led by a Section Chief from the Counterintelligence Division and an Assistant Section Chief from the Cyber Division. The FITF is divided into three units (one unit focusing on the Russian Federation, one on the People's Republic of China, and a third Global Unit focusing on all other foreign states), and each unit consists of Special Agents and Intelligence Analysts. Most Special Agents serve in a program manager role when assigned to the FITF.

Additional Background on the FITF's Development

Prior to the creation of the FITF, the FBI investigated foreign malign influence threats but no single FBI unit or team focused specifically on them. Instead, FBI headquarters divisions and their associated field division squads that focused on cyber, counterintelligence, or criminal threats would have performed the investigative work for a foreign malign influence case, typically based on a specific focus (such as an actor group or region) and with a nexus to that type of investigation.

FITF leadership explained that, during an expansion period, the FBI pulled together ad hoc teams to focus on non-Russian adversaries and that, after the election, instead of dispersing the teams and later reforming them for the next election, the FBI decided to maintain the teams year-round because foreign influence threats exist even between election cycles. During congressional testimony, the FBI Director stated that the FBI added resources to maintain a permanent "surge" capability on election and foreign influence threats to address the expanding focus and wider set of adversaries. The FBI also made the FITF Section Chief an executive leadership position due to the expansion of the FITF's mission.

The Role of the FBI's Cyber Division in the FITF

As described previously, the FITF operates within the Counterintelligence Division and consists of three units encompassing staff with counterintelligence and cyber experience who work on election-related foreign malign influence threats. FBI officials, including senior executives, praised the task force model as an effective means for coordinating the sharing of information about foreign malign influence issues.

Separately, the FBI Cyber Division's mission involves the investigation of computer intrusions, such as those perpetrated by nation-state actors, and sometimes includes election-related computer intrusions, such as the intrusion by Iranian nationals hacking into one U.S. state's voter database during the 2020 presidential

election. Cyber Division personnel assigned to these cases work with FITF personnel but are not assigned to the FITF. Additionally, the primary personnel responsible for interacting with social media companies, including liaising on behalf of the FITF, are field division personnel with cyber experience.

Example of a FITF Case Involving the Cyber Division

When foreign malign influence cases are conducted by FBI cyber squads in the field, the field agent will engage with a Cyber Division program manager, who then coordinates with a FITF program manager. For example, if there is a hack of a political campaign, the FITF will quickly engage with the FBI's Cyber Division. One Cyber Division official explained that, if a political campaign or email account is hacked, the Cyber Division will investigate the intrusion. However, if stolen nonpublic information is leaked to the public, the Counterintelligence Division will investigate the possibility of an influence operation.

Source: OIG interviews of FBI employees

The roles of the FITF and Cyber Division pertaining to foreign malign influence directed at U.S. elections can be roughly divided along lines of foreign activities that fall into the categories of influence and interference. The National Intelligence Council defines "election influence" to include overt and covert efforts intended to directly or indirectly affect a U.S. election, including candidates, political parties, voters or their preferences, or political processes. The National Intelligence Council defines "election interference" as a subset of election influence activities targeted at the technical aspects of the election, including voter registration, casting and counting ballots, or reporting results. FITF leadership told us that the FBI has also adopted these understandings of influence and interference. FITF personnel with counterintelligence experience focus on influence campaigns. FITF personnel with cyber experience, as well as personnel in the Cyber Division who are not part of the FITF, focus on interference, including foreign interference activities directed at U.S. elections.

FBI officials in the Counterintelligence Division and Cyber Division described their missions within the FITF to be distinct from each other, allowing them to clearly define their respective roles. Specifically, Cyber Division officials told us that malign interference, a subset of influence, can be thought of as an intrusion (or hack) of a computer system, whereas Counterintelligence Division officials explained that malign influence can be broad and include covert activity, such as espionage, attempts to influence voter opinions or confidence, or technical interference (hacking).

Appendix 3: Databases and Systems Available to the FBI for Sharing Information

As we discussed in the [Results of the Evaluation](#), the FBI held quarterly bilateral meetings with social media platforms for the primary purpose of sharing information about foreign malign influence threats on those platforms. Additionally, FBI officials described to us systems for receiving or distributing information that exist for other, broader, purposes, but which the FBI can use also for sharing information about foreign malign influence directed at U.S. elections when such a need arises. We describe these additional methods below.

FBI Official System of Record

Sentinel

Sentinel, in use since 2012, is the FBI's third-generation case management and official records management system.⁴⁴ It maintains records of the FBI's investigative and administrative activities in case files that document each case from inception to conclusion. Cases involving foreign malign influence directed at U.S. elections may be categorized in Sentinel as either:

- a counterintelligence investigation, overseen by the FBI's Counterintelligence Division, targeting a particular country's foreign malign influence activities, or
- a criminal investigation overseen by the FBI's Cyber Division focused on a specific cyber intrusion that is related to an election (including a campaign or candidate).

FBI employees told us that, while Sentinel can identify all cases that have been categorized as foreign malign influence, those cases have to be manually reviewed to identify the subset involving threats directed at U.S. elections.

In 2020 the FBI used Sentinel to manage the high volume of election-related incident and intelligence information reported to the FBI for approximately 1 week surrounding Election Day. The FBI reported that very little of this information involved foreign malign influence but stated that Sentinel could not quantify how many foreign malign influence-related tips it received and processed through this process.

Methods for Sharing Information with Nonfederal Entities

Teleporter

Teleporter is an encrypted file-sharing system that allows the FBI to share operational files with any entity with whom it maintains a trusted relationship, including federal, state, local, tribal, or foreign government

⁴⁴ Between 2006 and 2014, the OIG issued a series of 10 audits evaluating the FBI's planning for and implementation of Sentinel. A 2014 audit includes a complete list of all of the audits in the series. See DOJ OIG, [Audit of the Status of the Federal Bureau of Investigation's Sentinel Program](#), Audit Report 14-31 (September 2014), oig.justice.gov/reports/audit-status-federal-bureau-investigations-sentinel-program.

agencies, as well as private sector partners.⁴⁵ Teleporter is one of the features housed within the FBI's Law Enforcement Enterprise Portal, a secure platform providing web-based investigative tools and analytical resources for law enforcement. An FBI user of Teleporter uploads files to be shared, specifies recipients, sets a time limit during which the recipients are allowed to access the files, and sends the recipients an email containing a link to download the shared files. An FBI user of Teleporter also has the option to send a recipient an upload link that allows the recipient to provide a file to the FBI within a limited period of time. Recipients must be granted at least temporary access to Teleporter to download or upload files.

During the scope of our evaluation, the FBI used Teleporter to share, with social media platforms, foreign malign influence information such as Internet Protocol addresses, domain names, and social media handles associated with known foreign actors. The FBI also used Teleporter to accept tips voluntarily offered by social media platforms that were related to potential foreign malign influence activities on those platforms.

Non-Governmental Encrypted Messaging Application

In the fall of 2020, the FBI established a channel on an encrypted messaging application to communicate in real time with participants from the Foreign Influence Task Force (FITF), the FBI's San Francisco Field Office, the U.S. Department of Homeland Security (DHS), and seven social media platforms. The FBI established this channel for the limited purpose of sharing unclassified foreign malign influence threat information while the FBI's National Election Command Post (NECP) was active.⁴⁶ The channel was used between October 27 and November 7, 2020.

The FBI used the channel to share social media handles, domain names, or websites controlled by foreign actors, as well as themes foreign actors would use to conduct influence operations. The FBI required that this information be preapproved in Sentinel by an FBI Office of the General Counsel attorney and an operational Unit Chief for recordkeeping purposes. Additionally, the FBI prohibited the dissemination of any identifying information about U.S. persons via the channel.

Private Industry Notifications/FBI Liaison Alert System Reports

Executive Order (E.O.) 13636 required the federal government to increase the volume, quality, and timeliness of cyber threat information shared with private industry. To meet this goal, the FBI's Cyber Division writes Private Industry Notifications (PIN) and FBI Liaison Alert System (FLASH) reports to provide threat information to private sector partners and to request that those partners provide the FBI with information about any cyber targeting activity identified using this data. Both PINs and FLASH reports

⁴⁵ The FBI's Criminal Justice Information Services Division provides a variety of support services for law enforcement. Teleporter is a tool hosted on the division's Law Enforcement Enterprise Portal that allows operations-related files to be shared and moved between law enforcement and partner communities and is available to anyone who maintains a trusted relationship with the FBI. Any individual may be granted temporary access to Teleporter to upload or download files.

⁴⁶ An FBI Assistant Special Agent in Charge told us that the FBI had originally planned to establish for the 2020 election a joint command post in which these participants would have been in the same room; but the coronavirus disease 2019 pandemic forced the FBI to instead use a virtual common space. The FBI and the other participating entities agreed to use the nongovernmental encrypted messaging application for this purpose because the application is not owned by any of the social media companies that participated in the channel.

contain only unclassified, actionable information and are designed to aid in threat neutralization. PINs provide contextual information about ongoing or emerging cyber threats, and FLASH reports provide technical indicators gleaned through investigations or intelligence. PINs and FLASH reports may be distributed narrowly to specific recipients or broadly to the general public, depending on the nature of the threat information being shared.

The lead author of a PIN or a FLASH report is an analyst from an FBI Cyber Division headquarters intelligence unit, in coordination with the FBI's Counterintelligence Division if the report covers a nation-state actor. The FBI identified five products, including PINs and FLASH reports, that it has released since August 2020 discussing cyber nation-state threats that may affect U.S. elections.

Methods for Sharing Information within the U.S. Government

Intelligence Information Reports

The FBI uses Intelligence Information Reports (IIR) to share raw, unevaluated intelligence information, obtained by the FBI through its investigations and activities, with other federal government partners, to include the U.S. Intelligence Community. IIRs are used by federal agencies to quickly share raw intelligence (information that does not include the FBI's or other agencies' analytical assessment or judgments). IIRs are drafted and distributed by the FBI field office that collected the intelligence being shared. A FITF Supervisory Intelligence Analyst stated that the FITF sent guidance to the field offices before the 2020 election advising them to write and disseminate IIRs if they found information related to foreign malign influence.

Each IIR is tagged to identify the intelligence requirements that are relevant to the information the IIR contains, thereby directing the attention of specific U.S. Intelligence Community personnel toward that IIR even though it is disseminated more broadly.⁴⁷ Officials from the FBI's Directorate of Intelligence stated that the FBI cannot quantify the extent to which the FBI uses IIRs to share information about foreign malign influence directed at U.S. elections because there is no single requirement, or specific combination of requirements, that could reliably identify this category of information.

Pulse

Pulse is a database, managed by agencies in the U.S. Intelligence Community, that stores 31 types of intelligence product. The database has multiple channels for each participating agency to publish intelligence products and offers keyword search capabilities. Individuals working throughout the U.S. Intelligence Community can access Pulse, but the products each individual user can view vary depending on the user's security clearance and access level.

Chronicle

Chronicle is a resource available to U.S. Intelligence Community agencies that the FBI uses to share bulk, raw data with those agencies. Specifically, the FBI uses Chronicle to share actionable technical details, such

⁴⁷ An intelligence requirement is any topic about which the U.S. Intelligence Community needs to collect information and is authorized to commit resources to do so.

as tips provided voluntarily by the private sector or information obtained from the private sector via legal process, before any public announcements are made based on that information.

Watch Floor and CyNERGY

The FBI belongs to the National Cyber Investigative Joint Task Force, a partnership of more than 30 federal law enforcement, intelligence, and defense agencies to coordinate, integrate, and share information to support cyber threat investigations. As part of its role on the task force, the FBI operates a 24/7 command center, known as the Watch Floor, to facilitate interagency sharing of reports of cyber incidents and to direct the reports it receives to relevant FBI investigative units. The Watch Floor can tag reports as election related, but the tag encompasses reports related to foreign malign influence, as well as reports related to other types of election-related threats.

During significant cyber incidents and events, the FBI also activates its Cyber Division Event Coordination Center and staffs it with subject matter experts, relevant to the specific event, to review and process any event-related reports received by the Watch Floor. The FBI activated the Cyber Division Event Coordination Center for 1 week surrounding Election Day 2020 and staffed it with individuals with election-related expertise. The Cyber Division Event Coordination Center constituted the Cyber Division's participation in the FBI's NECP, which was responsible for the overall coordination of all FBI election-related operations. This same group of experts was also on standby around Super Tuesday 2020 and Inauguration Day 2021.

CyNERGY is an interagency database hosted by the FBI to help federal agencies track cyber incidents and coordinate notifications to the targets of cyber intrusions, which could include incidents related to elections. This tracking is required under E.O. 13636. At the time of our fieldwork, the FBI had finalized memoranda of understanding with DHS's Cybersecurity & Infrastructure Security Agency, the National Security Agency, and the U.S. Department of the Treasury to allow those agencies to access and contribute to the database. At that time, the FBI was in the process of establishing memoranda of understanding to allow CyNERGY access to additional federal agencies.

Method for Receiving Information from the General Public

Internet Crime Complaint Center

The FBI Cyber Division's Internet Crime Complaint Center (IC3) Unit maintains the FBI's IC3 database. Created in 2000, the IC3 database serves as the nation's central hub for reporting cybercrime. Through an online system, members of the public may submit complaints, which are analyzed by the FBI to determine how the FBI should respond.

Staff from the IC3 Unit worked with the FITF and the FBI's Election Fraud Working Group to develop keywords that could be used to categorize a complaint submitted to the IC3 database as election related. These keywords cover both potential foreign malign influence directed at U.S. elections and election-related threats that are not connected to foreign malign influence. The FBI stated that, out of thousands of complaints submitted to the IC3 database in 2020, it categorized 63 complaints, not all of which were related to foreign malign influence, as related to the election.

Appendix 4: Overview of DOJ's Mission to Counter Election Crimes

In addition to combating foreign malign influence directed at U.S. elections, DOJ has a broader mission to combat election crimes. Federal law criminalizes threatening violence against election officials or staff, as well as intimidating or bribing voters; buying and selling votes; impersonating voters; intentionally lying about the time, place, or manner of an election to prevent qualified voters from voting; altering vote tallies; stuffing ballot boxes; and marking ballots for voters against their wishes or without their input. Federal law also contains special protections for the rights of voters and provides that they can vote free from interference, including intimidation, and other acts designed to prevent or discourage people from voting or voting for the candidate of their choice. The task of investigating violations of this framework of election laws is handled by several DOJ components, including the FBI, U.S. Attorney's Offices (USAO), the Criminal Division, and the Civil Rights Division.

- In 2021 the Department created an Election Threats Task Force to focus on addressing threats of violence against election workers. The task force evaluates allegations and reports of threats against election workers and works with USAOs and FBI field offices throughout the country to investigate and prosecute these offenses, as appropriate. The task force includes several entities within DOJ, including the Criminal, Civil Rights, and National Security Divisions and the FBI, as well as key interagency partners such as the U.S. Department of Homeland Security.
- Each FBI field office has designated at least one Special Agent and one Intelligence Analyst as Election Crimes Coordinators to lead their office's efforts to assess allegations of election crimes, investigate threats, and gather intelligence. The Election Crimes Coordinators also serve as the point of contact for state and local officials in their office's area of responsibility and conduct outreach and establish relationships with local law enforcement.
- Prior to each federal election, USAOs appoint District Election Officers responsible for overseeing the handling of Election Day complaints of voting rights concerns, threats of violence against election officials or staff, and elections fraud in consultation with DOJ headquarters divisions such as the Criminal and Civil Rights Divisions.
- The Civil Rights Division's Voting and Criminal Sections enforce various federal statutes regarding elections. The Voting Section monitors elections and receives complaints about violations of federal voting statutes, while the Criminal Section conducts investigations and coordinates with the FBI to pursue criminal violations such as voter intimidation and suppression.
- The Criminal Division's Public Integrity Section addresses election crimes in several areas. The section deals with election fraud crimes and ballot fraud, including vote buying; multiple voting; submission of false registration or false ballots; altering votes; bribery; and disinformation as to the time, place, or manner of voting. The section is responsible for prosecuting cases of voter intimidation or suppression not handled by the Civil Rights Division, such as the targeting of political groups, which are not protected by the Civil Rights Act. The section also prosecutes campaign finance crimes, including prosecutions of foreign entities that violate campaign finance laws.

Appendix 5: DOJ's Election-Related Information Sharing with Other Federal Agencies and State Government Officials

In addition to the relationships among DOJ, the National Security Agency, and social media companies that we discussed in the body of the report, DOJ maintains relationships with other government agencies in its efforts to combat foreign malign influence directed at U.S. elections. Within the federal government, DOJ also maintains relationships with the U.S. Department of Homeland Security (DHS) and the U.S. Department of the Treasury. DOJ also has limited interaction with state and local governments.

Coordination with the Department of Homeland Security

We learned that DOJ's primary partner at DHS is the Cybersecurity & Infrastructure Security Agency (CISA). CISA and DOJ work together on several common missions, including cyber incident response, election security, and countering foreign malign influence operations. As it pertains to countering foreign malign influence operations, CISA officials told us that CISA focuses on promoting resiliency through providing accurate information about elections to the public. In its efforts to promote resiliency, CISA interacts with state and local election officials, including Secretaries of State. CISA officials told us that CISA and DOJ coordinate daily because their missions to combat foreign malign influence align.

A CISA official told us that CISA and the FBI work together on incident response, with the FBI taking the lead on criminal investigations while CISA focuses on remediation and incident management. CISA officials told us that the FBI is effective at pulling together other federal partners to provide assistance in support of CISA's role during cyber intrusion incidents, in addition to connecting CISA with private sector companies with whom the FBI has established relationships. A CISA official told us that the FBI also lends its credibility and resources, which is important because CISA is a newer agency. For example, a CISA official told us that, if CISA identifies a suspicious Internet Protocol (IP) address during an incident response, it can coordinate with the FBI, which can search Sentinel for any information on the IP address.⁴⁸ If the FBI already has information about the IP address, it may be an indication that the new incident could be more serious.

Homeland Security Information Network

The Homeland Security Information Network is a DHS-sponsored system for sharing sensitive but unclassified information among federal, state, local, territorial, tribal, international, and private sector partners. One use of this system in 2020 was to allow federal, state, local, and territorial agencies to monitor, analyze, and respond to election-related threats and incidents.

Coordination with Other Federal Agencies

We also learned that DOJ may work with the U.S. Department of the Treasury to seek sanctions against foreign malign influence actors as a mitigation or disruption technique, but we did not explore this relationship in significant detail. Several DOJ staff told us that sanctions can be a very effective tool in combating foreign malign influence, particularly when it is unlikely that the United States will gain custody over a foreign malign influence actor. To facilitate this interagency relationship, the FBI maintains a detailee

⁴⁸ For a description of the FBI's use of Sentinel for information sharing, see [Appendix 3](#).

at the Department of the Treasury's Office of Foreign Assets Control, which coordinates sanctions matters between the two agencies. Foreign Influence Task Force (FITF) program managers may work through the FBI detailee at the Office of Foreign Assets Control to seek sanctions against foreign investigative targets.

Another federal agency relationship that the OIG did not explore in significant detail was DOJ's and the FBI's relationship with the U.S. Department of Defense. FBI officials told us that the Department of Defense's U.S. Cyber Command has at times given the FBI information that was actionable for the FBI or its private sector partners. In these cases, the FBI acted as a conduit for relevant information shared to social media companies, with the Cyber Command providing information to the FITF, which then passed relevant information to the FBI's San Francisco Field Office for dissemination to private sector partners.

Coordination with State Government Officials

We found that state and local governments had limited interaction with the FBI regarding foreign malign influence directed at U.S. elections. We interviewed officials from a judgmental sample of five states representing variety in size, geographic region, and partisan preference in the 2020 U.S. presidential election. Interaction between state-level governments and the FBI was more extensive than that with county-level governments, but the bulk of the interaction that states had with the FBI did not appear to be related to foreign malign influence. Most of the states expressed that their main federal partner for election security was DHS/CISA, not the FBI.

In describing their interactions with the FBI related to countering foreign malign influence directed at their elections, state officials expressed that they had good relationships with the FBI. State officials we interviewed placed emphasis on protecting against cyber intrusions and other attacks on physical infrastructure, rather than focusing on responding to general foreign malign influence campaigns. Further, state officials told us that they did not need certain details from FBI intelligence on foreign malign influence operations directed at their elections. For example, state officials told us that attribution information detailing which foreign actor was attacking their elections was not critical to their responses. Rather, state officials had concerns, such as gaining information needed to take protective measures and ensuring the continued integrity of their elections.

States reported that their primary points of contact with the FBI were Election Crimes Coordinators, FBI agents at field offices who handle election crimes that are domestic in origin, although states did have some contact with the FBI's Cyber Division, largely due to the emphasis on cyber security mentioned above. (See [Appendix 2](#) for more information about the distinct missions of the FITF and the Cyber Division.) Some states also reported contact with their local U.S. Attorney's Offices (USAO), but most states' communication with USAOs regarding foreign malign influence was limited.

Some of the state officials we interviewed had trouble fully differentiating their state's interactions with the FBI and other parts of the federal government, particularly DHS. However, although the depth of the relationship with the FBI varied, state officials were confident that they could reach out to the FBI if needed and emphasized that an important element of their relationship with the FBI is the delivery of actionable information that could be used to secure their election systems and reassure voters.

Appendix 6: Descriptions of Laws and Policies Relevant to DOJ's Mission to Counter Foreign Malign Influence

During our fieldwork, Department and FBI officials identified federal laws, executive orders, DOJ and FBI policies, and investigative tools that establish parameters for DOJ's and the FBI's ability to collect information related to foreign malign influence threats, including threats directed at U.S. elections, and their obligations to disseminate information related to this mission. We describe these laws, orders, and policies below.

First Amendment to the U.S. Constitution

"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

Statutes

The following statutes were either identified by interviewees as relevant to foreign malign influence investigations or charged in recent indictments involving foreign malign influence directed at U.S. elections.

22 U.S.C. § 611 et seq.–Foreign Agents Registration Act

The Foreign Agents Registration Act (FARA) requires certain agents of foreign principals who are engaged in political activities or other activities specified under the statute to make periodic public disclosure of their relationship with the foreign principal, as well as activities and receipts and disbursements in support of those activities. Disclosure of the required information facilitates evaluation by the government and the American people of the activities of such persons in light of their function as foreign agents. The FARA Unit of the DOJ National Security Division's (NSD) Counterintelligence and Export Control Section (CES) is responsible for the administration and enforcement of the FARA.

18 U.S.C. § 951–Agents of Foreign Governments

18 U.S.C. § 951 requires agents operating under the control of foreign governments or foreign officials, other than diplomats, to notify the U.S. Attorney General before acting. Registration under the FARA serves as the requisite notification for the purposes of this statute.

18 U.S.C. § 594–Intimidation of Voters

18 U.S.C. § 594 prohibits intimidating, threatening, or coercing anyone, or attempting to do so, for the purpose of interfering with an individual's right to vote or not vote in any election held solely or in part to elect a federal candidate.

18 U.S.C. § 1030–Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act contains seven types of criminal activity relating to computers: obtaining national security information; accessing a computer and obtaining information; trespassing in a government computer; accessing a computer to defraud and obtain value; intentionally damaging by

knowing transmission, recklessly damaging by intentional access, or negligently causing damage and loss by intentional access; trafficking in passwords; and extortion involving a computer.

18 U.S.C. § 371–Conspiracy to Defraud the United States

The general conspiracy statute, 18 U.S.C. § 371, makes it a crime “if two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose.” The purpose of the statute is to protect governmental functions from frustration and distortion through deceptive practices. According to the U.S. Supreme Court in *Hass v. Henkel*, 216 U.S. 462, 479 (1910), § 371 reaches “any conspiracy for the purpose of impairing, obstructing or defeating the lawful function of any department of Government,” which includes federal elections.

18 U.S.C. § 875–Interstate Communications

18 U.S.C. § 875 prohibits the transmission of threatening interstate communications. Among other provisions, the statute prohibits transmitting in interstate or foreign commerce “any communication containing any threat to kidnap any person or any threat to injure the person of another.”

Executive Order

Executive Order 12333–U.S. Intelligence Activities

Executive Order (E.O.) 12333, originally issued in 1981 and amended by several subsequent executive orders, establishes the U.S. Intelligence Community and lays out various standards of operations for IC agencies, including the FBI. E.O. 12333 establishes the FBI’s authority to investigate threats to national security and to conduct intelligence activities. Specifically, it requires the FBI to collect, analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and DOJ missions, in accordance with procedural guidelines approved by the Attorney General, after consultation with the Director of National Intelligence. E.O. 12333 also requires the FBI to conduct counterintelligence activities and establish relationships with foreign partner agencies as needed to conduct its foreign intelligence and counterintelligence missions.

Department of Justice Policies

Justice Manual § 9-90.730–Disclosure of Foreign Influence Operations

The Justice Manual contains publicly available DOJ policies and procedures. Section 9-90.730, regarding the disclosure of foreign influence operations, provides a framework for the Department to evaluate whether to disclose foreign malign influence operations to victims and the public. Information collected by the Department concerning foreign malign influence operations may be disclosed to support arrests and charges for federal crime; alert victims of federal crimes arising out of foreign influence operations; alert unwitting recipients of foreign government-sponsored covert support, as necessary to assist in countering the threat; alert technology companies or other private sector entities to foreign influence operations when their services are used to disseminate covert foreign government propaganda or disinformation, or to provide other covert support to political organizations or groups; alert relevant congressional committees to significant intelligence activities; and alert the public or other affected individuals when the federal or national interests in doing so outweigh any countervailing considerations.

In determining whether and how to make these notifications, the Justice Manual directs the Department to be mindful of several important principles and policies. The Justice Manual requires that partisan political considerations must play no role in efforts to alert victims, other affected individuals, or the American public to foreign influence operations against the United States. Such efforts must not be for the purpose of conferring any advantage or disadvantage on any political or social group or any individual or organization. In considering whether and how to disclose foreign malign influence operations, the Justice Manual requires the Department to protect intelligence sources and methods, investigations, and other U.S. government operations. Accordingly, the Department will publicly identify foreign malign influence operations only when the Department can with high confidence attribute those activities to a foreign government. Responses to disinformation or other support or influence by unknown or domestic sources not acting on behalf of a foreign government is beyond the scope of the DOJ policy on disclosing foreign influence operations. When a criminal or national security investigation during an election cycle is at issue, the Justice Manual and other DOJ policies require the Department and its components to adhere to longstanding policies regarding the timing of charges or overt investigative steps.

The Attorney General’s Guidelines for Domestic FBI Operations

The Attorney General’s Guidelines for Domestic FBI Operations (Attorney General Guidelines) establish Department policy governing the FBI’s investigative activities within the United States. The Attorney General Guidelines authorize the “permissive sharing” of information obtained or produced by the FBI within the FBI and DOJ, as well as with other federal, state, local, or tribal agencies and the U.S. Intelligence Community if related to their responsibilities. According to the Attorney General Guidelines, the FBI has a responsibility to provide information as consistently and fully as possible to agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to national security except as limited by specific constraints on such sharing.

The Attorney General Guidelines also prohibit investigating, collecting, or maintaining information on U.S. persons solely for the purpose of monitoring activities protected by the First Amendment.

FBI Policies

Domestic Investigations and Operations Guide

The Domestic Investigations and Operations Guide (DIOG) applies to all investigative activities and intelligence collection activities conducted by the FBI within the United States, in the U.S. territories, or outside the territories of all countries. The DIOG does not apply to investigative and intelligence collection activities of the FBI inside foreign countries.

Application of the First Amendment to FBI Activities

The DIOG places limitations on FBI investigative activities based on an application of the First Amendment. According to the DIOG, “the FBI may lawfully collect, retain, and consider the content of constitutionally protected speech, so long as (i) the collection is logically related to an authorized investigative purpose; (ii) the collection does not actually infringe on the ability of the speaker to deliver his or her message; and (iii) the method of collection complies with the least intrusive method policy.” The DIOG further states that law enforcement activity that diminishes a person’s ability to communicate protected speech may interfere with that person’s First Amendment rights and thus may not be undertaken by the FBI solely for the purpose of

interfering with the person's freedom of speech. Despite these restrictions, the DIOG clarifies that, "despite the high standard for interfering with free speech or punishing those engaged in it, the law does not preclude FBI employees from observing and collecting any of the forms of protected speech and considering its content—as long as those activities are done for a valid law enforcement or national security purpose and are conducted in a manner that does not unduly infringe upon the ability of the speaker to deliver his or her message."

Assessments and Investigations

The FBI categorizes its investigative activities as assessments, preliminary investigations, or full investigations, depending on the level of factual certainty (referred to as predication) on which an activity is based. 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. Although "no particular factual predication" is required to open an assessment, the basis of an assessment cannot be arbitrary or groundless speculation, nor can an assessment be based solely on the exercise of First Amendment-protected activities. If the FBI develops factual predication of possible criminal or national threat activity, it may open a preliminary or full investigation. A preliminary investigation is investigative activity based on any allegation or information indicative of possible criminal activity or threats to national security. A full investigation is investigative activity when there is an articulable factual basis that activity constituting a federal crime or a threat to national security has or may have occurred, is or may be occurring, or will or may occur. The investigation may obtain information relating to the activity or the involvement or role of an individual, group, or organization in such activity.

While the FBI is permitted to conduct limited information gathering prior to the opening of an assessment or formal investigation, the opening of an assessment or investigation allows FBI staff to employ a variety of investigative tools. The investigative tools available to FBI staff vary depending on the type of assessment or investigation.

Commonly Used Investigative Tools for Combating Foreign Malign Influence Directed at U.S. Elections

Grand Jury Subpoenas

In criminal cases, prosecutors present evidence to a grand jury, which then determines whether there is probable cause to believe that an individual has committed a crime and should be put on trial. During certain FBI assessments, the FBI may coordinate with a local U.S. Attorney's Office (USAO) and NSD to issue grand jury subpoenas to obtain subscriber or customer information from providers of electronic communication services or remote computing services, such as email providers and social media platforms. The FBI may also work with the USAO and NSD to obtain grand jury subpoenas during an investigation, including for subscriber as well as other information relevant to the investigation. In certain jurisdictions, the sharing of information obtained via grand jury subpoena may be restricted by court rulings, requiring further consultation with the USAO and DOJ, including NSD, before the sharing of such information with other federal agencies, such as IC partners. Federal Rule of Criminal Procedure 6(e) imposes secrecy requirements on most information occurring before a grand jury but allows federal prosecutors to share foreign intelligence, counterintelligence, and terrorism-related threat information.⁴⁹ It is DOJ's policy that such information must be shared to the fullest extent permissible by law and in a manner consistent with

⁴⁹ Federal Rule of Criminal Procedure 6(e).

the rule. There are no FBI supervisory approval requirements associated with issuing grand jury subpoenas, but all grand jury subpoenas must be issued by the USAO handling the assessment or investigation.

2703(d) Orders

Section 2703 of the Electronic Communications Privacy Act (ECPA) provides several mechanisms for the government to obtain electronic information.⁵⁰ One such method, a 2703(d) court order, is commonly used in the FBI's mission to combat foreign malign influence directed at U.S. elections. Agents seeking a 2703(d) order do not need supervisory approval, but work with an Assistant U.S. Attorney and NSD to request the court order. To obtain such an order, the FBI must offer specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. A court order authorized by 18 U.S.C. § 2703(d) may be issued by any federal magistrate, district court, or equivalent state court judge.⁵¹

According to the ECPA, when a court issues a 2703(d) order, a provider of an electronic communication service or remote computing service must disclose the subscriber's name, address, local and long distance telephone records, or records of session times and durations; length of service (including the start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and the means or source of payment for the service (including any credit card or bank account number).⁵² Interviewees stated that one benefit of a 2703(d) order is that returns from the order are not governed by Federal Rule of Criminal Procedure 6(e), simplifying the FBI's ability to share the collected information with others. FBI agents can use a § 2703(d) order to obtain account logs and historical transactional records from social media and other online accounts, which can help the FBI determine whether a foreign intelligence agent controls additional accounts.⁵³ The FBI uses returns from a 2703(d) order to develop probable cause for a search warrant.

Search Warrants

Access to the contents of electronic storage requires a search warrant issued by a federal court under § 2703(a) of the ECPA. The FBI can obtain the full contents of a network account with a search warrant, allowing the FBI to acquire any information on an account that may not have already been obtained through subpoenas or 2703(d) orders. A search warrant to acquire electronic storage information can be issued to a provider without notice to the customer or subscriber. Agents seeking a search warrant coordinate with the USAO or DOJ headquarters in certain instances, such as investigations pertaining to violations of statutes overseen by NSD's CES. A search warrant in this context differs from a Title III search warrant. Title III search warrants can be used to provide real-time information from an account and are not frequently issued in cases involving foreign malign influence directed at a U.S. election.

⁵⁰ The ECPA protects wire, oral, and electronic communications while those communications are being made, when they are in transit, and when they are stored on computers. The Act applies to emails, telephone conversations, and data stored electronically.

⁵¹ 18 U.S.C. §§ 2703(d), 2711(3).

⁵² 18 U.S.C. § 2703(c)(2).

⁵³ A § 2703(d) order issued by a federal court has effect outside the district of the court that issued it, meaning that a 2703(d) order may compel providers to disclose information even if that information is stored outside the district of the issuing court.

Appendix 7: The Department's Response to the Draft Report




U.S. Department of Justice
Office of the Deputy Attorney General

Office of the Deputy Attorney General

950 Pennsylvania Ave., N.W.
RFK Main Justice Bldg.
Washington, D.C. 20530

MEMORANDUM

TO: Allison Russo
Assistant Inspector General
Evaluation and Inspections Division
Office of the Inspector General

FROM: George D. Turner 
Associate Deputy Attorney General
Office of the Deputy Attorney General

DATE: July 12, 2024

SUBJECT: Department of Justice's Response to Formal Draft Report, "Evaluation of the U.S. Department of Justice's Efforts to Coordinate Information Sharing About Foreign Malign Influence Threats to U.S. Elections"

The Department of Justice (DOJ) appreciates the opportunity to provide a response to the Formal Draft Report prepared by the Office of the Inspector General (OIG), transmitted to DOJ on May 30, 2024, entitled "Evaluation of the U.S. Department of Justice's Efforts to Coordinate Information Sharing About Foreign Malign Influence Threats to U.S. Elections" (Formal Draft Report). This response reflects the consolidated input of relevant DOJ components, including the Federal Bureau of Investigation (FBI), National Security Division (NSD), Executive Office for United States Attorneys, and Civil Division.

Below, we address the two recommendations contained in the Formal Draft Report. The Department concurs with both recommendations, as explained more fully herein.

First Recommendation

The first recommendation calls for DOJ to "[d]evelop an approach for informing the public about the procedures the Department has put into place to transmit foreign malign influence threat information to social media companies that is protective of First Amendment rights." As reflected in the Formal Draft Report, following the district court's July 2023 decision in *Missouri v. Biden*, DOJ worked over several months to develop a standard operating procedure (SOP) for sharing foreign malign influence (FMI) information with social media companies that serves and promotes two fundamental DOJ priorities: combatting FMI operations

posing a threat to U.S. national security, and protecting the vital First Amendment rights of Americans. Recognizing that FMI threats are constantly evolving, the SOP is designed to be an adaptive document. The first iteration of the SOP was implemented in early February 2024, and DOJ—through FBI—has been actively sharing FMI threat information with social media companies pursuant to the SOP since then.

We concur with OIG’s first recommendation, as we believe it will be beneficial to ensure that the public is aware that DOJ’s sharing of information with social media companies about potential FMI threats to national security, including election interference, is undertaken pursuant to carefully calibrated protocols that protect First Amendment rights. We will address this recommendation by making publicly available a detailed summary version of the SOP and posting that summary on DOJ’s website by July 31, 2024. We will also further inform the public about the SOP through DOJ’s planned outward-facing actions responsive to OIG’s second recommendation, as discussed below.

As background with respect to the SOP, in July 2023, a Louisiana district court issued an injunction in *Missouri* restricting FBI’s engagement with social media companies based on the judge’s view that such engagement was likely violative of the First Amendment because it involved allegedly coercive requests to remove content from the companies’ platforms. In September 2023, the Fifth Circuit upheld a modified version of the injunction. *Missouri v. Biden*, 83 F.4th 350 (5th Cir. 2023). The Supreme Court subsequently stayed the injunction in October 2023. On June 26, 2024, the Supreme Court reversed the Fifth Circuit’s judgment, holding that the plaintiffs lacked standing to seek such an injunction. *Murthy v. Missouri*, No. 23-411 (June 26, 2024).

Following the October 2023 stay, DOJ began developing a standardized approach for sharing FMI information with social media companies that continued to appropriately account for First Amendment considerations. Over several months, DOJ worked to formulate such guidance, which ultimately resulted in the SOP.

The SOP reflects the fundamental premise, rooted in longstanding Supreme Court precedent, *see, e.g., Bantam Books, Inc. v. Sullivan*, 372 U.S. 58 (1963); *Blum v. Yaretsky*, 457 U.S. 991 (1982), that it is permissible and appropriate for FBI to share FMI information with social media companies, as long as it is clear that ultimately it is up to the company whether to take any action, such as removing content or barring users, based on the shared information. The SOP includes, among other things, the following principles, guidance, and protocols:

- The SOP recognizes the critical importance both of DOJ being able to share FMI threat information with social media companies in order to carry out DOJ’s national security mission, and of doing so in a manner that does not infringe upon on any applicable First Amendment protections.
- The SOP defines what constitutes FMI with reference to specific categories of FMI activity and information.

- The SOP requires that certain conditions must be met for FBI to share FMI information with a social media company, including that the FBI personnel has identified specific, credible, and articulable facts that provide high confidence for assessing that the information at issue relates to activity attributable to a foreign government, foreign non-state actor, or their proxy engaged in an FMI operation.¹
- The SOP requires that communications with social media must include a standardized caveat explaining that FBI does not request or expect the receiving company to take any particular action based on the shared information.
- The SOP specifies procedures for how FBI personnel can appropriately respond to follow-up questions or requests from social media companies seeking additional information from FBI after receiving FMI information.

Since the SOP went into effect in early February 2024, FBI has been actively sharing FMI threat information with social media companies on a continuing basis pursuant to the SOP. We look forward to informing the public about the SOP by posting a summary version of the SOP on our website, and to further highlighting and explaining the SOP to the public as part of the planned actions discussed below in response to the second recommendation.

Second Recommendation

The second recommendation calls for DOJ to “[d]evelop and implement a comprehensive strategy to ensure that the Department of Justice’s approach to information sharing with social media companies to combat foreign malign influence directed at U.S. elections can adapt to address the evolving threat landscape.” While we concur with this recommendation, we note that, over the course of several years and as further outlined below, DOJ has already developed and is actively implementing a strategic approach (which includes the SOP) for sharing information with social media companies and combatting the inherently fluid threat of FMI directed at our elections. We plan to address this recommendation by taking a series of additional actions by August 31, 2024 to further refine and strengthen our strategy, including:

- **Development and Release of Strategic Principles.** DOJ will set forth in a public manner the principles reflecting DOJ’s strategy for sharing FMI information with social media companies to combat the evolving threat landscape.
- **Resumption of FBI’s Regular Meetings with Social Media Companies.** As part of that strategy, FBI will resume regular meetings in the coming weeks with social media companies to brief and discuss potential FMI threats involving the companies’ platforms.

¹ The Formal Draft Report suggests that the SOP might permit FBI employees to use “pre-populated or boilerplate criteria when justifying a disclosure of information to a social media company.” Formal Draft Rpt. at 27. To the contrary, and as set forth above, the SOP requires FBI employees to identify specific, credible, and articulable facts—which must be reflected in the report transmitted to the social media company—supporting a high-confidence FBI assessment that the shared information relates to an FMI threat.

FBI will conduct these meetings—as FBI did before pausing the meetings in summer 2023 due to the now-vacated *Missouri* injunction (*see infra* at 5)—in a manner that is entirely consistent with applicable First Amendment principles. As has been FBI’s practice, FBI will conduct these engagements with social media companies located across the country, depending on the circumstances and nature of the potential threats.

- **Outreach by FBI Field Offices to Social Media Companies.** FBI will instruct FBI Field Offices in the coming weeks to conduct outreach—in coordination with the FBI’s Foreign Influence Task Force (FITF)—to any identified social media companies located in their areas of responsibility, to develop contacts at those companies and ensure they are aware of the SOP and DOJ’s overall approach for engaging with social media companies regarding FMI threat information.
- **Engagements by Senior Officials.** In the coming months, senior DOJ officials will highlight and explain, during public engagements with relevant stakeholders and the public, DOJ’s strategy for information sharing with social media companies to combat FMI directed at our elections.
- **Launch of DOJ Website Page.** DOJ plans to launch a new section on its website dedicated to ensuring public awareness of DOJ’s strategy for engaging with social media companies regarding FMI. The website page will collect and highlight in a single location relevant resources, guidance, and other materials, including the summary of the SOP discussed above.

As background, the U.S. Intelligence Community (USIC) has publicly described how the FMI operations of hostile state actors from China, Iran, and Russia directly threaten U.S. national security. *See* Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 5, 2024), at 12, 17, 20. Congress has specifically recognized that FMI poses a serious threat to national security, finding in 2019 that foreign actors have used social media platforms to engage in FMI activities that threaten U.S. national security, and likely will continue to do so. 50 U.S.C. § 3369. Congress found, among other things, that foreign adversaries were deploying “information warfare operations [involving] the weaponization of social media platforms with the goals of intensifying societal tensions, undermining trust in governmental institutions within the United States, its allies and partners in the West, and generally sowing division, fear, and confusion.” 50 U.S.C. § 3369(a)(2). Congress also found that “[b]ecause these information warfare operations are deployed within and across private social media platforms, the companies that own these platforms have a responsibility to detect and facilitate the removal or neutralization of foreign adversary networks operating clandestinely on their platforms.” *Id.* § 3369(a)(7). The statute further states that “information from law enforcement and the intelligence community is also important in assisting efforts by these social media companies to identify foreign information warfare operations.” *Id.* § 3369(b)(2).

Since well before those Congressional findings, DOJ, acting through the FBI, has been working to combat FMI. In the fall of 2017, the FBI Director established FITF to combat the emerging FMI threat. As set forth in FITF’s Mission and Strategy framework, referenced in the Formal Draft Report, FITF is a multi-division FBI section comprised of operational and

analytical personnel from the FBI's Counterintelligence, Cyber, and Criminal Investigative Divisions with the authority and mandate to identify, investigate, and combat FMI operations targeting U.S. democratic institutions, with specific focus on the U.S. electoral process. FITF serves as FBI's central coordination point for the USIC and international partners for engaging in a whole-of-government approach to combatting FMI threats. The FBI, principally through FITF, is the DOJ component responsible for engaging with social media companies—including through information sharing—regarding FMI threats.

FITF's formative Mission and Strategy document expressly includes the strategic priority of sharing FMI threat information with social media companies, while also highlighting the imperative of not infringing upon First Amendment rights. As set forth in that strategy framework, FITF's key lines of effort since its inception have included: (a) "Lead the engagement with social media and Internet technology providers to enable an effective dialogue focused on 1) understanding and leveraging the visibility and capabilities of these providers, and 2) providing actionable direction to enable self-monitoring and mitigation efforts of those organizations' platforms"; and (b) "Develop a clear strategic messaging framework to define USG's posture for specific key audiences [including] Internet technology and social media providers." The strategic framework further provides that, in carrying out its mission, FITF must "protect the rights embodied in the Constitution" and, in particular, avoid engaging in any investigative activities "based upon speech protected under the First Amendment."

As DOJ has developed and deployed its strategy for engaging with social media companies about FMI, we have also drawn on and implemented guidance from an array of other sources, including guidance specifically directed at ensuring that First Amendment rights are protected. For example, all of FBI's investigative activity, including information sharing with social media companies, must adhere to the Attorney General Guidelines on Domestic Investigations (AGG-DOM) and the FBI Domestic Investigations and Operations Guidance (DIOG). Both documents reinforce the core principle that FBI must protect the rights and liberties of all Americans. The AGG-DOM provides that all investigative activities "must be carried out in conformity with the Constitution and all applicable statutes," and specifically prohibits "investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment." AGG-DOM § I(C)(3). The DIOG expands on this principle and includes a section dedicated to requirements related to protecting First Amendment activity. The DIOG notes that "[n]o investigative activity . . . may be taken solely on the basis of activities that are protected by the First Amendment," and that "even 'monitoring' the exercise of First Amendment rights" is prohibited. DIOG §§ 5-2, 4-3. The DIOG also provides that "when First Amendment rights are at stake, the choice and use of investigative methods should be focused in a manner that minimizes potential infringement of those rights." *Id.* § 4-19.

Further, the Justice Manual (JM) sets forth DOJ policy principles regarding the disclosure of foreign influence operations. *See* JM § 9-90.730. As set forth in the JM, it is "the Department's policy to alert the victims and unwitting targets of foreign influence activities, when appropriate and consistent with the Department's policies and practices, and with our national security interests." *Id.* Recognizing that it is often not possible or prudent to publicly disclose FMI operations because of investigative considerations, the JM provides a strategic

framework for DOJ to evaluate whether, when, and under what circumstances to disclose FMI operations. This strategic approach includes that DOJ may disclose FMI threat information “[t]o alert technology companies or other private sector entities to foreign influence operations where their services are used to disseminate covert foreign government propaganda or disinformation, or to provide other covert support to political organizations or groups.” *Id.*²

As part of DOJ’s strategy for engagement with social media companies, following the 2018 midterm elections, FBI established a practice of regularly meeting with social media companies to discuss potential FMI threats on the companies’ platforms. FITF coordinated and led the meetings, which involved an array of social media companies located in the San Francisco area given the cluster of such companies based there, as well as other social media companies located in other regions. These meetings afforded a valuable opportunity for two-way discussion, enabling FBI and social media companies to share information that both sides were seeing on the companies’ platforms relating to potential threat indicators and trends. FBI met with each company individually, rather than in a group setting with industry competitors present, to facilitate the most fulsome and productive engagement regarding potential threat information implicating the company’s platform. FBI met with each company on a quarterly basis, and also met with companies more frequently depending on threat-specific factors—such as when a particular company requested to discuss potential FMI threats with FBI, and when FBI was aware of information indicating that an FMI actor was poised to leverage a company’s platform in furtherance of FMI operations. However, in summer 2023, FBI suspended these regular meetings with social media companies following the issuance of the injunction in *Missouri*. As set forth above, and in light of the Supreme Court’s recent decision, FBI will resume these meetings—which are both important to DOJ’s national security mission and fully consistent with the First Amendment—on an expedited basis, and will conduct these meetings with social media companies located across the country.

As reflected in the Formal Draft Report, another key prong of DOJ’s strategy for sharing FMI threat information with social media companies over the past several years has been, and remains, providing specific threat-related data to social media companies on a continuous basis. Specifically, FBI obtains information from the USIC relating to FMI actors leveraging particular online platforms, and FBI then promptly shares that information with the relevant social media company. This strategic approach combats FMI threats in multiple critical ways, including by enabling the company to remove or otherwise regulate the content on its platform, to the extent the company elects to do so, and by facilitating further investigation of the FMI actors involved—including through the company’s gathering of additional relevant information pursuant to legal process served by FBI. As set forth above, in early February 2024, DOJ implemented the SOP, which established the existing framework for this prong of DOJ’s information-sharing strategy, consistent with applicable First Amendment principles.

² Footnote 6 of the Formal Draft Report references a separate classified guidance document, which was formulated in 2019 through an interagency process and was not issued by DOJ. This guidance articulated principles for other government agencies’ efforts to combat FMI operations, and has been provided to OIG.

As the foregoing reflects, DOJ has developed and is actively implementing an evolving, multi-faceted, strategic approach for sharing FMI threat information with social media companies that is creative, impactful, and protective of First Amendment rights. Nevertheless, we welcome OIG's recommendation, as we continuously strive to enhance our strategy and inform the public about our work, and we will address the recommendation through the planned series of actions outlined above.

Appendix 8: OIG Analysis of the Department's Response

The OIG provided a draft of this report to the Department for its comment. The Department's response is included in [Appendix 7](#) to this report. The OIG's analysis of the Department's response and the actions necessary to close the recommendations are discussed below.

Recommendation 1

Develop an approach for informing the public about the procedures the Department has put into place to transmit foreign malign influence threat information to social media companies that is protective of First Amendment rights.

Status: Resolved.

Department Response: The Department concurred with the recommendation and stated that it would be beneficial to ensure that the public is aware that DOJ's sharing of information with social media companies about potential foreign malign influence threats to national security, including election interference, is undertaken pursuant to carefully calibrated protocols that protect First Amendment rights. The Department stated that it would prepare a summary of the Department's procedures for sharing foreign malign influence threat information with social media companies and will post that summary on the DOJ website by July 31, 2024.

OIG Analysis: The Department's proposed actions are responsive to the recommendation. By October 23, 2024, please provide a copy of the public summary of the Department's procedures for sharing foreign malign influence threat information with social media companies and documentation that the summary was posted on the DOJ website.

Recommendation 2

Develop and implement a comprehensive strategy to ensure that the Department of Justice's approach to information sharing with social media companies to combat foreign malign influence directed at U.S. elections can adapt to address the evolving threat landscape.

Status: Resolved.

Department Response: The Department concurred with the recommendation and stated that it would take a series of additional actions by August 31, 2024, to further refine and strengthen its strategy for sharing information with social media companies and combating the inherently fluid threat of foreign malign influence directed at U.S. elections. The Department's planned actions include developing and publicly releasing strategic principles for sharing foreign malign influence information with social media companies, resuming regular meetings with social media companies to discuss potential foreign malign influence threats involving those companies' platforms, instructing FBI field offices and the FBI's Foreign Influence Task Force (FITF) to conduct outreach to social media companies within their areas of responsibility in accordance with the Department's overall strategy for these engagements, highlighting the Department's strategy during public engagements with relevant stakeholders, and launching a new section on the DOJ website to ensure public awareness of the Department's strategy and guidance.

OIG Analysis: The Department's proposed actions are responsive to the recommendation. By October 23, 2024, please provide documentation of:

- the Department's strategic principles, as described above;
- any meetings the FBI has held with social media companies since the date of this report to discuss potential foreign malign influence threats involving the companies' platforms;
- efforts undertaken by FBI field offices and the FITF to conduct outreach to social media companies since the date of this report, in line with the Department's strategic principles for sharing foreign malign influence information with social media companies;
- engagement by senior DOJ officials with relevant stakeholders, including participants, dates, locations, and topics of discussion; and the webpage that the Department created to publicize these initiatives.