The Privacy and Civil Liberties Oversight Board



Government Efforts to Counter Domestic Terrorism by Targeting Disinformation on Social Media

Staff Report

November 18, 2026

[THIS PAGE INTENTIONALLY LEFT BLANK]



THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

GOVERNMENT EFFORTS TO COUNTER DOMESTIC TERRORISM BY TARGETING DISINFORMATION ON SOCIAL MEDIA

STAFF REPORT

NOVEMBER 18, 2026



Privacy and Civil Liberties Oversight Board

Beth A. Williams, Board Member

TABLE OF CONTENTS

Executive Summary **1**

I. Introduction **5**

A. Project Overview 7

B. Investigative Scope and Methodology 7

1. Foreign Malign Influence and Disinformation 8

2. Agencies 9

C. Report Organization 10

II. Background **12**

A. World War II and Cold War Efforts to Counter Foreign Disinformation 12

B. 2016 to 2020: Renewed Efforts to Counter Foreign Malign Interference 13

C. 2021 to 2024: Expansion of Government Counter-Disinformation and Growing Concerns 18

1. Expansion of Government Counter-Disinformation Efforts Domestically 18

2. Concerns Over Government Counter-Disinformation Efforts and Subsequent Contraction 24

D. 2025 to Present: Executive Orders and Legislative Developments 28

III. Discussion **30**

A. The Government Failed to Provide Evidence of a Nexus Between Disinformation and Domestic Terrorism 31

1. "Disinformation" Often Relies on Subjective Interpretation 33

2. Counter-Disinformation Efforts Were Diffused Across Numerous Agencies and Components 35

B. Concerns with Counter-Disinformation Engagements 37

1. Countering Foreign Disinformation Can Have National Security Value, But Presents Risks 37

2. Counter-Disinformation Engagements Were *Ad Hoc* and Lacked Transparency 39

3. Policies Regarding Evaluating the Foreignness of Speakers Were Inconsistent Across the Government 42

4. Counter-Disinformation Efforts Failed to Consider Whether Targeted Speech Was Otherwise Protected 45

C. Existing Policies Related to Social Media Engagement Were Insufficient for Counter-Disinformation Efforts 46

1. General Policies 46

2. Policies Relating to Government Engagement with Social Media Companies 48

D. The Impacts of EO 14149 on Government Counter-Disinformation Activities 58

1. Recent Consent Decrees Have Curtailed Some Agencies' Future Communications with Social Media Companies 60

E. Risks to Free Speech Remain 61

IV. Conclusion 63

V. Recommendations 64

Appendix A: Separate Statement of Member Beth A. Williams A-1

Appendix B: Counter-Disinformation Inventory B-1

Appendix C: Disinformation Countermeasures C-1

Appendix D: PCLOB Correspondence with DHS D-1

EXECUTIVE SUMMARY[1]

In 2021, the White House issued a National Strategy in which it publicly asserted that "a crisis of disinformation and misinformation" (collectively referred to herein as "disinformation"[2]), "often channeled through social media platforms," was fueling "extreme polarization" that could lead to domestic terrorism.[3] Consistent with this strategy, Executive Branch officials engaged directly with social media companies[4] to share what they deemed to be disinformation, with the goal of causing these platforms to limit the spread of such material. They encouraged the social media companies to label content as false, limit the ability to find content through search, and, in some cases, completely remove the content or the speakers' accounts from their platforms altogether. Although the government had previously engaged with social media companies, the 2021 National Strategy provided explicit domestic terrorism justifications for such action.[5]

[1] The initiation of this oversight project was approved by a quorate Board in November 2022. This Report reflects the analysis of the Privacy and Civil Liberties Oversight Board's staff (PCLOB) but has not been voted on or approved by a quorate Board. Per the Board's Sub-Quorum Policy, adopted October 23, 2024, all conditions for publication of this Report have been met. *See* PRIV. & C.L. OVERSIGHT BD., *Sub-Quorum Authorities and Operations when Position of Chair is Vacant*, Policy 102-01, § 6.1.C (2024), https://documents.pclob.gov/prod/DynamicImages/Generic/59b039ee-73ef-44fc-a80d-862d10a2ca84/102-01~1.PDF. PCLOB thanks the departments and agencies mentioned herein, and especially their privacy and civil liberties leadership, for their cooperation and assistance with PCLOB's questions and requests.

[2] According to a 2024 report from the U.S. Government Accountability Office, the Intelligence Community (IC) defines "misinformation" in its *IC Lexicon for Foreign Malign Influence* as "false, inaccurate, or misleading information that is spread regardless of the intent to deceive. "Disinformation" is defined as "false or misleading information deliberately created or spread with the intend to deceive or mislead." U.S. GOV'T ACCOUNTABILITY OFF., GAO-24-107600, FOREIGN DISINFORMATION: DEFINING AND DETECTING THREATS 8 (2024), https://www.gao.gov/assets/gao-24-107600.pdf. Although different, this Report collectively refers to both as "disinformation" because government countermeasures largely did not distinguish. "Disinformation" in this Report refers to information government actors deemed to be disinformation; PCLOB has not independently investigated these claims, and the use of this term should not suggest that PCLOB agrees with this characterization.

[3] WHITE HOUSE, NATIONAL STRATEGY FOR COUNTERING DOMESTIC TERRORISM 29 (2021), https://www.govinfo.gov/content/pkg/GOVPUB-PR-PURL-gpo174845/pdf/GOVPUB-PR-PURL-gpo174845.pdf [hereinafter the 2021 DT STRATEGY] ("These efforts speak to a broader priority: enhancing faith in government and addressing the extreme polarization, fueled by a crisis of disinformation and misinformation often channeled through social media platforms, which can tear Americans apart and lead some to violence. … We will work toward finding ways to counter the influence and impact of dangerous conspiracy theories that can provide a gateway to terrorist violence.") ("[Domestic terrorists' ideologies] can, in some instances, connect and intersect with conspiracy theories and other forms of disinformation and misinformation.").

[4] PCLOB uses the term "social media companies" to collectively reference social media companies, social media platforms, file upload platforms, and gaming platforms.

[5] 2021 DT STRATEGY, *supra*, at 29. *See also* DEP'T OF HOMELAND SEC., OFF. OF INTEL. & ANALYSIS, HOMELAND THREAT ASSESSMENT 2024 6-7 (2023), https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf; OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 12 (2024), https://archive.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

These government efforts had few safeguards and operated with minimal transparency.[6] The government's informal outreach, which was often intended to—and did—prompt social media companies to take action, was largely conducted *ad hoc*. No government entity engaged in counter-disinformation efforts had formal policies or procedures[7] for identifying and protecting Americans' lawful speech with respect to this work.[8] Specifically, there were no policies governing engagement with social media companies that required agencies to distinguish U.S. person speech from that of foreign actors.[9] And there was no requirement that officials seek attorney or high-level approval before encouraging the suppression of speech. In many cases, government actors encouraged suppression of speech having nothing to do with violence or the incitement of violence.

There also was no serious effort to determine whether specific disinformation—or even disinformation writ large—was in fact "fuel[ing]" domestic terrorism, as the White House strategy claimed. The strategy did not cite or point to evidence that countering disinformation would mitigate domestic terror threats.[10] In fact, the strategy's 2021 Implementation Plan *tasked* the government with producing a report "within the next six months" to "[e]nhance the U.S. Government's understanding" of how disinformation "relate[d] to the domestic terrorism threat."[11] PCLOB repeatedly requested this report but was given no indication that it was ever produced.

---

[6] *See* STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF THE FED. GOV'T, FINAL REPORT 1553, https://judiciary.house.gov/media/press-releases/final-report-weaponization-federal-government [hereinafter WEAPONIZATION SUBCOMMITTEE FINAL REPORT]. *See e.g.,* U.S. DEP'T OF JUST., OFF. OF THE INSPECTOR GENERAL, EVALUATION OF THE U.S. DEPARTMENT OF JUSTICE'S EFFORTS TO COORDINATE INFORMATION SHARING ABOUT FOREIGN MALIGN INFLUENCE THREATS TO U.S. ELECTIONS i-ii (2024), https://oig.justice.gov/sites/default/files/reports/24-080.pdf [hereinafter DOJ OIG REPORT ON FMI].

[7] The Federal Bureau of Investigation (FBI) states that it did not have such a policy because its "efforts were never focused on countering disinformation," but that it did have a requirement to distinguish and identify foreign actors in the course of its work countering FMI. Responses to PCLOB from the FBI (Sep. 2026).

[8] PCLOB uses "American" for consistency with Executive Order (EO) 14149 ("The First Amendment to the United States Constitution, an amendment essential to the success of our Republic, enshrines the right of the American people to speak freely in the public square without Government interference."). Exec. Order. No. 14149 § 1.

[9] According to the State Department (State), a relevant policy, *Department Guidance Concerning Engaging Online Platforms Regarding the Removal or Retention of Content on Third-Party Accounts*, was shared with its staff on April 14, 2021. However, State did not produce this policy to PCLOB, and thus PCLOB was unable to independently review and assess the policy's applicability and potential safeguards. State advises that this policy included a discussion of freedom of expression and the First Amendment, a required consultation with lawyers, and other requirements to ensure compliance with the First Amendment. Responses to PCLOB from State (Oct. 2026).

[10] The government did not cite evidence in the 2021 National Strategy or concurrently with its release. Nor, despite many requests, did the government provide PCLOB evidence the government considered at the time to support this claim.

[11] 2021 DT STRATEGY, *supra,* at 18 ("The intelligence and law enforcement communities will enhance the government's understanding of how foreign malign influence operations and the dissemination of disinformation, including by foreign governments, relate to the domestic terrorism threat we face."); WHITE HOUSE, STRATEGIC IMPLEMENTATION PLAN FOR COUNTERING DOMESTIC TERRORISM 5,

Over the past four years, PCLOB has examined these governmental efforts to combat disinformation, analyzing both the basis for tying these actions to domestic terrorism and the civil liberties implications of doing so. This accords with the Board's statutory purpose: to "analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties."[12]

PCLOB has concluded that civil liberties are at risk when the government encourages the suppression of lawful, protected speech under the justification of combating domestic terrorism.[13] This includes false speech and speech the government deems to be disinformation. While the government has historically played a role in combating foreign malign influence (FMI),[14] the government steps beyond its proper bounds in seeking censorship for disfavored views expressed by U.S. persons.

The government failed to provide either to the public or to PCLOB its justification for concluding that a "crisis of disinformation" fueled domestic terrorism.

This Report concludes that the government failed to provide either to the public or to PCLOB its justification for concluding that a "crisis of disinformation" fueled domestic terrorism. It further regularly failed to distinguish between foreign and domestic origins in its counter-disinformation efforts and failed to establish sufficient safeguards in its dealings with social media companies concerning presumed disinformation.

https://www.dni.gov/files/ODNI/documents/DIG/DIG-Declassified-Strategic-Implementation-Plan-for-CT-April2025.pdf [hereinafter 2021 IMPLEMENTATION PLAN] ("Enhance the U.S. Government's understanding of how foreign state and non-state information operations, particularly disinformation, relate to the domestic terrorism threat") ("Measure of Performance 1.3.ld: Provide an internal report for U.S. Government stakeholders on key findings regarding this potential threat within the next six months.").

[12] 42 U.S.C. §2000ee(c)(1).

[13] In conducting its evaluation, this Report distinguishes between constitutionally protected speech, and unprotected speech, which may include speech by foreigners abroad or speech that is an incitement to imminent lawless action or otherwise unlawful. *See, e.g., United States v. Verdugo-Urquidez*, 494 U.S. 259, 265 (1990).

[14] DOJ OIG REPORT ON FMI, *supra*. 50 U.S.C. § 3059(f)(2) defines "foreign malign influence" as "any hostile effort undertaken by, at the direction of, or on behalf of or with the substantial support of, the government of a covered foreign country with the objective of influencing, through overt or covert means— (A) the political, military, economic, or other policies or activities of the United States Government or State or local governments, including any election within the United States; or (B) the public opinion within the United States."

PCLOB provides the following recommendations to guide future government efforts:

1. **The government should ensure Executive Order 14149 is fully implemented**. Executive Order (EO) 14149, *Restoring Freedom of Speech and Ending Federal Censorship*, prohibits government censorship of Americans, however the absence of formal agency policies and procedures creates a risk of inappropriate engagement with social media companies.[15] All relevant agencies should draft and revise existing policies to implement the principles of EO 14149 regarding social media engagement, foreignness determinations, and agency training.
2. **The government should improve transparency and oversight around its policies and communications with social media companies.** Agencies should publish their social media engagement policies and any guidance or policies implementing EO 14149, as well as policies concerning FMI and attribution, to the extent consistent with national security. Agencies should also publish regular transparency reports informing the public of their engagements with social media companies regarding perceived disinformation.
3. **The government should develop uniform terminologies**. To the extent the government continues efforts to counter foreign disinformation, relevant departments and agencies should develop and adopt uniform definitions.
4. **The government should ensure that any related grantmaking is carefully circumscribed**. Agencies should ensure that their grantmaking processes are conducted in accordance with EO 14332, *Improving Oversight of Federal Grantmaking*, which requires agencies to ensure grantmaking aligns with the President's priorities and does not impose harm to Americans such as through the previous funding of "social media censorship tools."[16] To further transparency, agencies should also publish relevant information about any related grants on their websites.
5. **Free speech protections and safeguards should be codified.** The government should take steps to guarantee free speech protections endure, including by enacting key restrictions and protections into law.

[15] Exec. Order No. 14149 § 2.
[16] Exec. Order No. 14332, § 1, https://www.whitehouse.gov/presidential-actions/2025/08/improving-oversight-of-federal-grantmaking/. Specifically, the EO requires funding opportunity announcements and discretionary grants to, among other things, undergo "interagency coordination to determine whether the subject matter of a particular funding opportunity announcement has already been addressed by another agency announcement," "demonstrably advance the President's policy priorities," and comply with Gold Standard Science (which is explained in EO 14303).

I. INTRODUCTION

Foreign efforts to influence or deliberately deceive Americans have been a concern since the nation's founding.[17] At various times throughout history, however, the American government has endeavored to curb even the speech of its own people. This was especially so when the speech was deemed to run counter to national security. The Sedition Act of 1798 forbade writing "false, scandalous, and malicious" statements against the U.S. government.[18] The Sedition Act of 1918 criminalized, among other things, "any disloyal, profane, scurrilous, or abusive language about the form of government of the United States."[19]

If these acts had not, respectively, expired and been repealed, they would undoubtedly be held unlawful today.[20] But the boundaries of government control over speech continue to be debated. The government has warned that foreign adversaries are exploiting the internet and social media—widely disseminating harmful disinformation via social media platforms as a psychological weapon for geopolitical influence.[21] And as recently as 2021, the White House issued a strategy where it claimed that "a crisis of disinformation and misinformation often channeled through social media platforms," was fueling domestic terrorism.[22] The next year, the Department of Homeland Security (DHS) asserted that such speech can "undermine public trust in government institutions to encourage unrest, which could potentially inspire acts of violence."[23]

---

[17] George Washington, Washington's Farewell Address to the People of the United States, (Sept. 19, 1796), *reprinted by* U.S. Senate Hist. Off., at 20-21 (2017), https://www.senate.gov/artandhistory/history/resources/pdf/Washingtons_Farewell_Address.pdf. ("Against the insidious wiles of foreign influence ... the jealousy of a free people ought to be constantly awake, since history and experience prove that foreign influence is one of the most baneful foes of republican government.").

[18] The Sedition Act of 1798, 1 Stat. 596 596 (1798).

[19] Sedition Act of 1918, ch. 75, § 1, 40 Stat. 553, 553 (1918).

[20] *Brandenburg v. Ohio*, 395 U.S. 444, 449 (1969) (wherein the Supreme Court held that a statute "purport[ing] to punish mere advocacy and to forbid, on pain of criminal punishment, assembly with others…falls within the condemnation of the First and Fourteenth Amendments").

[21] DEP'T OF HOMELAND SEC., DEPARTMENT OF HOMELAND SECURITY STRATEGIC FRAMEWORK FOR COUNTERING TERRORISM AND TARGETED VIOLENCE, 27 (Sept. 2019), https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf [hereinafter DHS STRATEGIC FRAMEWORK]. GAO-24-107600, FOREIGN DISINFORMATION: DEFINING AND DETECTING THREATS, *supra,* at 1.; Emily Harding, *A Russian Bot Farm Used AI to Lie to Americans. What Now?*, CTR. FOR STRATEGIC & INT'L STUD. (July 16, 2024), https://www.csis.org/analysis/russian-bot-farm-used-ai-lie-americans-what-now; Giulia Alesse, *The Weaponization of Disinformation in Modern Geopolitics*, ATLAS INST. FOR INT'L AFF. (June 13, 2025), https://atlasinstitute.org/the-weaponization-of-disinformation-in-modern-geopolitics/.

[22] 2021 DT STRATEGY, *supra*, at 29.

[23] *Summary of Terrorism Threat to the U.S. Homeland*, DEP'T OF HOMELAND SEC. (Feb. 7, 2022), https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-february-07-2022.

The government may, of course, affirmatively communicate its own views and policy preferences and rebut information it believes to be false. But the range of government response to perceived disinformation—including "fact-checking" and requesting companies remove content (post takedowns) or users (deplatforming)—vary in their intrusiveness and civil liberties impacts.[24] These impacts may be compounded when the government's involvement is indirect and not transparent.

This Report examines recent government efforts to counter what it determined to be disinformation. This includes a discussion of strategies and policies related to domestic terrorism and government engagement with social media companies regarding disinformation, focusing specifically on suppression mechanisms such as notifications or "flagging," or encouraging post takedowns, demotions (or shadow bans), and deplatforming by social media companies. The Report does not adjudicate the lawfulness of these actions or opine on whether government involvement was unlawfully coercive or persuasive.[25] Rather, the Report approaches the topic from a policy perspective, evaluating government engagement from counterterrorism and civil liberties objectives. The Report analyzes whether the government provided adequate basis to link disinformation to domestic terrorism and whether it distinguished between countering FMI and countering domestic speech deemed harmful. It also discusses the risks to civil liberties, and assesses what, if any, safeguards were in place to mitigate these risks.[26] Finally, the Report discusses EO 14149, *Restoring Freedom*

[24] *See* Appendix C for descriptions of countermeasures and their potential First Amendment impacts.

[25] "Unlawful coercion" has not been clearly defined by the Supreme Court. "To identify coercion, [the Fifth Circuit in *Murthy*] asked whether 'the government compelled the [private party's] decision by . . . intimating that some form of punishment will follow a failure to comply.' … The court explained that the Government significantly encourages a private party's choice when it exercises 'active, meaningful control, whether by entanglement in the party's decision-making process or direct involvement in carrying out the decision itself.'" *Murthy v. Missouri*, 603 U.S. 43, 55 (2024). Because the Supreme Court did not reach the merits, it expressed no view as to whether the Fifth Circuit correctly articulated the standard for when the Government transforms private conduct into state action. *See also id.* at 99-100 (Alito, J. dissenting, "The principle recognized in *Bantam Books* and *Vullo* requires a court to distinguish between permissible persuasion and unconstitutional coercion, and in *Vullo*, we looked to three leading factors that are helpful in making that determination: (1) the authority of the government officials who are alleged to have engaged in coercion, (2) the nature of statements made by those officials, and (3) the reactions of the third party alleged to have been coerced."); *see also Nat'l Rifle Assoc. of America v. Vullo*, 602 U.S. 175, 201 (2024) (Jackson, J. concurring, ("[*Bantam Books*] does *not* hold that government coercion alone violates the First Amendment." (emphasis in original)).

[26] Not all FMI involves disinformation; other FMI methods include covert campaign financing, economic blackmail, intellectual property theft, and laundering money to divisive local activist groups. *SEE* DOJ IG REPORT ON FMI, *supra,* at iii. Government experts have argued that foreign malign disinformation can sow societal division and discord, undermine trust in democratic institutions, and advance foreign state/non-state actors' policy interests. OFF. OF THE DIR. OF NAT'L INTEL., FOREIGN MALIGN INFLUENCE CAMPAIGNS ON SOCIAL MEDIA PLATFORMS TARGETING ELECTIONS FOR FEDERAL OFFICE 1 (2022), https://www.dni.gov/files/FMIC/documents/products/FMI-Social-Media-Platforms-Targeting-Elections-Oct2022.pdf; Senator Marco Rubio, Americans need to know how social media companies handle foreign disinformation (YouTube, Sept. 18, 2024), https://www.youtube.com/watch?v=ifB-J2nKt8E.

of Speech and Ending Federal Censorship, issued in January 2025, and provides recommendations to strengthen protections going forward.

A. Project Overview

The Privacy and Civil Liberties Oversight Board was established in its current form by the Implementing Recommendations of the 9/11 Commission Act of 2007.[27] The Board's mission is to ensure that efforts by the Executive Branch to protect the nation from terrorism are appropriately balanced with the need to protect privacy and civil liberties.[28] In 2022, the Board initiated an oversight project to review the Executive Branch's policies and activities to counter domestic terrorism. The Board approved the project to focus on two simultaneous and distinct workstreams: the impact on First Amendment rights (the First Amendment workstream), and the impact on privacy and civil liberties of particular groups such as those with shared racial, religious, political, or ideological affiliations (the Shared Affiliations workstream). This Report is produced pursuant to the First Amendment Workstream.[29]

B. Investigative Scope and Methodology

This Report discusses the government's efforts to counter and suppress disinformation as part of its strategy to combat domestic terrorism. It focuses on the government's engagement with social media companies, assessing the privacy and civil liberties impacts of these actions. Specifically, PCLOB examined government strategies to counter disinformation, reviewed the actions taken, and assessed whether policies or safeguards were in place to protect First Amendment activities. The analysis includes FMI-related disinformation.[30]

[27] Pub. L. No. 110-53, § 801, 121 Stat. 266, 352 (2007).
[28] 42 U.S.C. § 2000ee(c).
[29] *See Countering Domestic Terrorism and its Impacts on Privacy and Civil Liberties*, PRIV. & C.L. OVERSIGHT BD., https://www.pclob.gov/OversightProjects ("The Board will examine how the Government's activities to counter domestic terrorism intersect with First Amendment rights. This will focus on how the Government, in its efforts to counter domestic terrorism: Distinguishes First Amendment-protected speech and activity, including political, religious, and protest speech or activity, from domestic terrorism, and how that distinction is reflected in the Government's policy and training; Ensures that operational personnel comply with such policy and training as they execute mission activities, including and with respect to communities of color, religious communities, and political groups; Collects, retains, analyzes, and disseminates publicly accessible online activity; Defines, identifies, evaluates, seeks to counter, and seeks to suppress mis- and disinformation; Engages with and/or directs social media companies and other third parties regarding domestic terrorism and all the categories of speech and activities referenced above, and the resulting impact on individual users' or groups' speech; and Distinguishes the speech of foreign actors from that of U.S. persons.").
[30] DOJ OIG REPORT ON FMI, *supra,* at iii. Other FMI methods such as covert campaign financing, economic blackmail, and intellectual property theft are not included in the scope of this Report.

1. Foreign Malign Influence and Disinformation

While the government considers countering FMI to be distinct from countering disinformation, the two efforts can overlap.[31] FMI includes a range of hostile efforts undertaken by foreign governments to—overtly or covertly—influence U.S. policy or public opinion.[32] In particular, foreign malign actors may create, disseminate, or amplify disinformation against the interest of the United States (foreign disinformation). These operations are often conducted via social media platforms, where Americans may exercise their free speech rights the most. In recent years, the government increasingly undertook a broadly construed campaign to counter what it labeled as "mis-, dis-, and mal-information" or "MDM" often in the name of countering foreign actors, engaging directly with social media platforms to share what it deemed to be disinformation.[33]

Misinformation is defined as "false, inaccurate, or misleading information that is spread regardless of the intent to deceive."[34] Disinformation is defined as "false or misleading information deliberately created or spread with the intent to deceive or mislead." Malinformation is commonly referred to as otherwise true information that is taken out of context or amplified for deceptive purposes.[35]

Both disinformation and FMI have been applied broadly to capture a range of similar operations and activities, including those by state and non-state actors. However, only FMI is defined by law; it captures many activities that are unrelated to disinformation, such as cyberattacks on critical infrastructure or election interference.[36] Disinformation spread by foreign actors is a type of FMI activity that can threaten national security. For example, targeted disinformation campaigns by nation states may seek to sow discord or undermine an election. Given this overlap, the possibility that foreign malign actors might work to encourage domestic terrorism, and the need to examine how the government distinguishes

---

[31] Responses to PCLOB from ODNI (Aug. 2026).

[32] 50 U.S.C. § 3059(f)(2) defines FMI as "any hostile effort undertaken by, at the direction of, or on behalf of or with the substantial support of, the government of a covered foreign country [defined under 50 U.S.C § 3059(f)(1)] with the objective of influencing, through overt or covert means—(A) the political, military, economic, or other policies or activities of the United States Government or State or local governments, including any election within the United States; or (B) the public opinion within the United States." The National Intelligence Council in the *IC Lexicon* defines FMI as "[s]ubversive, undeclared (including covert and clandestine), coercive or criminal activities by foreign governments, non-state actors, or their proxies to affect another nation's popular or political attributes, perceptions, or behaviors to advance their interests"). GAO-24-107600, FOREIGN DISINFORMATION: DEFINING AND DETECTING THREATS, *supra*, at 5. Examples of other FMI activities include subverting American elections, "economic coercion for advantage, bribery, or blackmail; cyber intrusions; campaign finance violations; and overt provision of funds to divisive groups." DOJ IG REPORT ON FMI, *supra* at i.

[33] GAO-24-107600, FOREIGN DISINFORMATION: DEFINING AND DETECTING THREATS, *supra, at* 8.

[34] *Id.*

[35] *Id. See, e.g., Malinformation*, MERRIAM-WEBSTER, https://www.merriam-webster.com/slang/malinformation (last visited Oct. 14, 2026). *See also, We're in This Together. Mis-, Dis-, and Malinformation Stops with You,* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, (*https://www.cisa.gov/sites/default/files/2022-12/election-disinformation-toolkit_508_0.pdf* (last accessed Nov. 11, 2026).

[36] 50 U.S.C. § 3059(f)(2).

foreign from domestic actors, PCLOB also examined counter-disinformation efforts occurring within the auspices of FMI response.

2. Agencies

PCLOB engaged with key agencies involved in the government's counter-disinformation activities that are listed in the recently declassified *Strategic Implementation Plan for Countering Domestic Terrorism* (2021 Implementation Plan), the implementing guidance for the *National Strategy for Countering Domestic Terrorism* (2021 DT Strategy) (see Table 1 below).[37] These agencies included DHS, the Federal Bureau of Investigation (FBI), the Department of Justice (DOJ), the Office of Director of National Intelligence (ODNI), and the Department of State (State). While each of these agencies engaged in counter-disinformation activities, their roles and the scope of their efforts varied. Some developed or led active countermeasures, while others provided funding for research efforts or participated in interagency or public-private sector information sharing efforts. PCLOB also examined correspondence between the White House and social media companies that was subsequently made public.

Table 1. Key Agencies Involved in Counter-Disinformation Activities[38]

Agency	Office or Component
DHS	• Cybersecurity and Infrastructure Security Agency • Office of Intelligence & Analysis • Office of Strategy, Policy, and Plans (including Center for Prevention Programs and Partnerships) • Disinformation Governance Board
DOJ	• Office of Justice Programs (including National Institute of Justice) • FBI's Foreign Influence Task Force
ODNI	• Foreign Malign Influence Center
State	• Global Engagement Center • Office of the Under Secretary for Public Diplomacy and Public Affairs • United States Agency for International Development

In preparing this Report, PCLOB gathered information from several of these agencies through multiple requests for information, briefings, questions and responses. Agencies varied in their

[37] 2021 IMPLEMENTATION PLAN, *supra*; 2021 DT STRATEGY, *supra*. PCLOB did not engage with the Central Intelligence Agency, Department of Education, or Department of Health and Human Services because there was not sufficient indication that such agencies were involved in countering disinformation for the purposes of counterterrorism.

[38] *See* IMPLEMENTATION PLAN, *supra*. PCLOB identified relevant sub-components of each agency. Departments' or agencies' own views of their work may not align. For example, ODNI states that FMIC did not conduct disinformation activities, which they view as separate from countering FMI. As explained herein, PCLOB recognizes an overlap.

responsiveness.[39] PCLOB also met with numerous civil society representatives over multiple sessions and conducted an extensive review of open-source material, including thousands of pages of publicly available government documents and documents disclosed in conjunction with related litigation.

This Report also includes an inventory of government counter-disinformation efforts by DHS and DOJ, including the FBI (see Appendix B for the full inventory).

C. Report Organization

Section II provides a brief overview of the government's past counter-disinformation activities, which historically focused on FMI. This section describes the recent expansion of the government's activities to include a domestic focus, and a subsequent contraction of efforts following EO 14149.

Section III analyzes the government's role in countering disinformation, discusses both the government's stated national security benefits and the civil liberties risks of such action, and lists the range of potential countermeasures. This section also briefly discusses the currently unfolding environment of renewed counter-FMI work and related considerations regarding disinformation posted online. It discusses the relative absence of formal policies on counter-disinformation activities, the creation of an FBI FMI social media engagement policy in 2024, and subsequent developments.

Section IV contains PCLOB's conclusions about government social media engagement in conjunction with its domestic terrorism counter-disinformation efforts.

Section V contains PCLOB's recommendations about the government's approach to countering disinformation.

[39] Two Board Members initially requested information from DHS relevant to this Report in August 2022, but DHS provided no information. *See* Appendix D. After the project was formally opened in November 2022, the request was treated as an official Board request. PCLOB received briefings from DHS and the FBI and sent formal requests for information to DHS, the FBI, State, DOJ, and ODNI in 2024 and 2025. DOJ, the FBI, and DHS's Cybersecurity and Infrastructure Security Agency (CISA) provided material and responded to PCLOB questions, with DOJ providing funding details about disinformation-related grants. No other agencies provided funding information. In February 2025, ODNI provided a blanket denial for all of PCLOB's requests for information (stating that the National Counterterrorism Center (NCTC), National Counterintelligence and Security Center, Foreign Malign Influence Center (FMIC), and Cyber Threat Intelligence Integration Center "are not involved in any work aimed at preventing and/or countering mis-, dis-, and mal-information (MDM) within the DT context"), PCLOB Correspondence with ODNI (Feb. 24, 2025). ODNI later provided policies which are described below. As discussed above, State reported that it had a relevant policy but did not produce this policy to PCLOB.

Appendix A contains the separate statement of Member Beth A. Williams.

Appendix B contains an inventory of known counter-disinformation efforts by DHS and DOJ, including the FBI, related to domestic terrorism. It also includes a brief description of DOJ counter-disinformation funding to third parties.

Appendix C contains descriptions of the types of countermeasures the government can employ to counter disinformation online, including the associated impacts on speech.

Appendix D contains the letter of Chair Sharon Bradford Franklin and Member Beth A. Williams to Secretary of Homeland Security Alejandro Mayorkas in August 2022 regarding DHS's counter-disinformation efforts and DHS's July 2023 response.

II. BACKGROUND

Countering disinformation can take a variety of forms: from public governmental statements rebutting the disinformation, to active countermeasures such as pressuring social media companies to throttle or deplatform accounts posting the disinformation. Over much of the twentieth century, the government focused on countering foreign disinformation largely through transparency efforts and counter-messaging.[40] More recently, there has been a turn toward the inclusion of domestic speech and suppression efforts. [41]

A. World War II and Cold War Efforts to Counter Foreign Disinformation

In 1938, Congress passed the Foreign Agents Registration Act (FARA) to counter Nazi and fascist propaganda networks operating covertly inside the United States.[42] As initially enacted, "FARA responded to foreign influence concerns by creating a system designed 'to identify agents of foreign principals who might engage in subversive acts or in spreading foreign propaganda and to require them to make public record of the nature of their employment.'"[43] Rather than banning speech, FARA operated by exposing networks and increasing public transparency; it has been amended several times since its passage.

Following the attack on Pearl Harbor, President Franklin D. Roosevelt established the Office of War Information (OWI) in June 1942 "in recognition of the right of the American people and of all other peoples opposing the Axis oppressors to be truthfully informed about the common war effort."[44] OWI's stated goal was "to ensure an accurate and consistent flow of information from the Government to the public."[45] OWI originally operated both abroad and domestically, but its domestic branch "was virtually abolished a year after its creation" because of funding cuts.[46] While OWI operated to amplify government speech, it is not reported to have made efforts to limit domestic speech.[47] OWI was terminated in September 1945.

---

[40] Also known as counter-narratives. For a more fulsome description of various countermeasures, *see* Appendix C.
[41] While not an exhaustive list, this section highlights some of the key counter-FMI measures of the twentieth century.
[42] 22 U.S.C. § 611-621; Jacob R. Straus, *Foreign Agents Registration Act (FARA): Background and Issues for Congress*, CONG. RSCH. SERVICES, https://www.congress.gov/crs-product/R46435.
[43] *Foreign Agents Registration Act (FARA): Background and Issues for Congress, supra* (citing *Vierick v. United States*, 318 U.S. 236, 241 (1943) and H.Rept. 104-339, p. 1, at 5-8 (1995)).
[44] GEN. SERVICES ADMIN. & NAT'L ARCHIVES, PRELIMINARY INVENTORY OF THE RECORDS OF THE OFFICE OF WAR INFORMATION 1 (1967), https://www.archives.gov/files/research/foreign-policy/related-records/rg-208-owi-preliminary-inventory.pdf.
[45] *Id.*
[46] INFORMATION CONTROL AND PROPAGANDA: RECORDS OF THE OFFICE OF WAR INFORMATION v (David H. Culbert eds., 1986), https://www.lexisnexis.com/documents/academic/upa_cis/3447_InfoControlPropaPt2SerA.pdf.
[47] While there were concerns at the time about what the Domestic Branch would do, the Branch focused mostly on war news distribution and the motion picture industry and lost most of its funding in 1943. *See* Marja Roholl, *An Invasion of a Different Kind: The U.S. Office of War Information and "The Projection of America" Propaganda in the Netherlands, 1944-1945*, in Media, Memory, and Projections of Democracy 19-20 (2018), https://brill.com/display/book/edcoll/9789004292017/BP000003.xml; Phillip W. Stewart, *A Reel Story of World War II*, NAT'L ARCHIVES (2015), https://www.archives.gov/publications/prologue/2015/fall/united-newsreels.html; Cedric Larson, *The Domestic Motion Picture Work of the Office of War Information* 3 Hollywood Q. 434, 435

During the Cold War, in 1953, President Eisenhower created the United States Information Agency (USIA).[48] In many ways a successor to OWI, USIA operated to promote American democratic and cultural values in foreign countries.[49] The Smith-Mundt Act of 1948, as amended in 1972, prohibited the distribution of covered materials within the United States.[50] In 1985, Congress enacted a related restriction, providing no funds appropriated to USIA could be used "to influence public opinion in the United States."[51]

In 1981, the Reagan Administration created the Active Measures Working Group, which tasked experts from the Central Intelligence Agency (CIA), the FBI, State, Department of Defense (DOD), and the USIA with identifying and exposing Soviet disinformation campaigns.[52] The working group published highly detailed, unclassified reports describing the Soviet techniques, neutralizing the impact of the Soviet disinformation campaigns.[53] The Active Measures Working Group effectively ceased in 1989 without any redistribution of its duties.[54]

USIA was officially terminated in 1999 and many of its statutory functions were integrated into State.[55] In 2013, both of the domestic prohibitions were amended to clarify that State could continue to disseminate Smith-Mundt covered materials online to foreign audiences abroad even if domestic U.S. audiences are inadvertently exposed to such material on the internet.[56]

B. 2016 to 2020: Renewed Efforts to Counter Foreign Malign Interference

Over the past two decades, Russia, largely through its Internet Research Agency (IRA), reportedly began leveraging many of its previous Soviet Cold War disinformation techniques using social media and the internet.[57] The U.S. Senate Select Committee on Intelligence released a report in 2019 concluding that the IRA used fake profiles (or bots) to spread disinformation, seeking to

(1948), https://womenfilmeditors.princeton.edu/wp-content/uploads/2019/10/The_Domestic_Motion_Picture_Work_of_the_OWI_Cedric_Larson.pdf.
[48] Steve D. Boilard, *United States Information Agency*, EBSCO, https://www.ebsco.com/research-starters/history/united-states-information-agency.
[49] *Id.*
[50] Pub. L. No. 80-402, § 2, 62 Stat. 6 (1948); Pub. L. No. 92-352, § 204, 86 Stat. 494 (codified at 22 U.S.C. § 1461).
[51] Pub. L. No. 99-93, § 208, 99 Stat. 431 (1985) (codified at 22 U.S.C. § 1461-1a).
[52] Steve Abrams, *Beyond Propaganda: Soviet Active Measures in Putin's* Russia, 15 CONNECTIONS: THE Q. J., 5, 10 (2016), https://connections-qj.org/system/files/15.1.01_abrams.pdf.
[53] *See id.* at 11-12, FLETCHER SCHOEN & CHRISTOPHER J. LAMB, DECEPTION, DISINFORMATION AND STRATEGIC COMMUNICATIONS: HOW ONE INTERAGENCY GROUP MADE A MAJOR DIFFERENCE 3-4, 116 (Nicholas Rostow, ed., 2012), https://ndupress.ndu.edu/portals/68/documents/stratperspective/inss/strategic-perspectives-11.pdf.
[54] DECEPTION, DISINFORMATION AND STRATEGIC COMMUNICATIONS, *supra,* at 96; Catherine A. Theohary, *Information Warfare: Issues for Congress,* CONG. RSCH. SERVICES (2018), https://www.congress.gov/crs-product/R45142.
[55] *Reform and Restructuring of U.S. Foreign Affairs Agencies: Public Diplomacy in the Department of State*, DEP'T OF STATE (1999), https://1997-2001.state.gov/outreach/publicaffdip/fs_990930_merger.html.
[56] Pub. L. No. 112-239, § 1078. 126 Stat. 1957-1958 (2013).
[57] Calder Walton, *What's Old Is New Again: Cold War Lessons for Countering Disinformation*, 5 TEXAS NAT'L SEC. REV. 51, 64 (2022), https://tnsr.org/2022/09/whats-old-is-new-again-cold-war-lessons-for-countering-disinformation/.

enflame existing social divisions in the United States around domestic issues, such as police violence, gun control, race, and immigration.[58]

During this time, China was also understood to be leveraging social media for information warfare. In 2015, China reportedly expanded its use of social media disinformation campaigns when it reorganized the People's Liberation Army (PLA), "which included the establishment of the PLA Strategic Support Force (PLASSF) as a new, separate service stood up with a mission focus on the conduct of information warfare."[59] In the event of a crisis or conflict, China could target the United States with disinformation campaigns.[60]

In response, the government began a renewed focus on counter-disinformation efforts, establishing new or rebranded component offices[61] with explicit counter-FMI missions, and surged funding for such efforts.[62] In 2016, Congress passed the Countering Foreign Propaganda and Disinformation Act as part of the National Defense Authorization Act for Fiscal Year 2017.[63] This law mandated that the State Department establish the Global Engagement Center (GEC) to "lead, synchronize, and coordinate" federal efforts to "understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining United States national security interests."[64] The law also required the President to "designate a senior official" to develop and ensure guidance for the GEC on relevant privacy and civil liberties laws.[65]

In 2017, the FBI established the Foreign Influence Task Force (FITF), which was "specifically charged with identifying and combating foreign influence operations targeting democratic institutions and values inside the United States."[66] FITF was housed within the FBI's Counterintelligence Division "and composed of agents, analysts, and professional staff from the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative Divisions" of the FBI.[67]

---

[58] *See id. See also, Senate Intel Committee Releases Bipartisan Report on Russia's Use of Social Media,* U.S. SENATE SELECT COMM. ON INTEL. (Oct. 8, 2019), https://www.intelligence.senate.gov/2019/10/08/press-senate-intel-committee-releases-bipartisan-report-russia-e2-80-99s-use-social-media/.

[59] Scott W. Harold, Nathan Beauchamp-Mustafaga, & Jeffrey W. Hornung, *Chinese Disinformation Efforts on Social Media*, RAND CORPORATION ix (2021), https://www.rand.org/pubs/research_reports/RR4373z3.html.

[60] *Id.* at x-xi.

[61] Component offices refer to subordinate offices or agencies within a given department.

[62] *See* DOJ OIG REPORT ON FMI, *supra*, at 1 (explaining how, prior to the 2016 Election, there were few coordinated efforts to counter Russian disinformation and other FMI efforts).

[63] National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, 130 Stat. 2000 (2016), https://www.congress.gov/bill/114th-congress/senate-bill/2943.

[64] *Id.* at § 1287(a).

[65] *Id.* at § 1287(c)(2). A senior official was designated by the Secretary of State in 2017 following a Presidential delegation of authoring allowing him to do so. *See* MEMORANDUM ON DELEGATION OF AUTHORITY TO THE SECRETARY OF STATE UNDER THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2017, 2 PUB. PAPERS 1717 (Jan. 17, 2017); PCLOB Correspondence with State (Oct. 28, 2026).

[66] Nikki Floris, *Securing America's Elections: Oversight of Government Agencies,* FED. BUREAU OF INVESTIGATION (Oct. 22, 2019), https://www.fbi.gov/news/speeches-and-testimony/securing-americas-elections-oversight-of-government-agencies-102219; DOJ OIG REPORT on FMI, *supra,* at 1; *Combating Foreign Influence*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/investigate/counterintelligence/foreign-influence [https://web.archive.org/web/20240719084414/https://www.fbi.gov/investigate/counterintelligence/foreign-influence] (last visited July 29, 2026).

[67] *Oversight of Government Agencies, supra.*

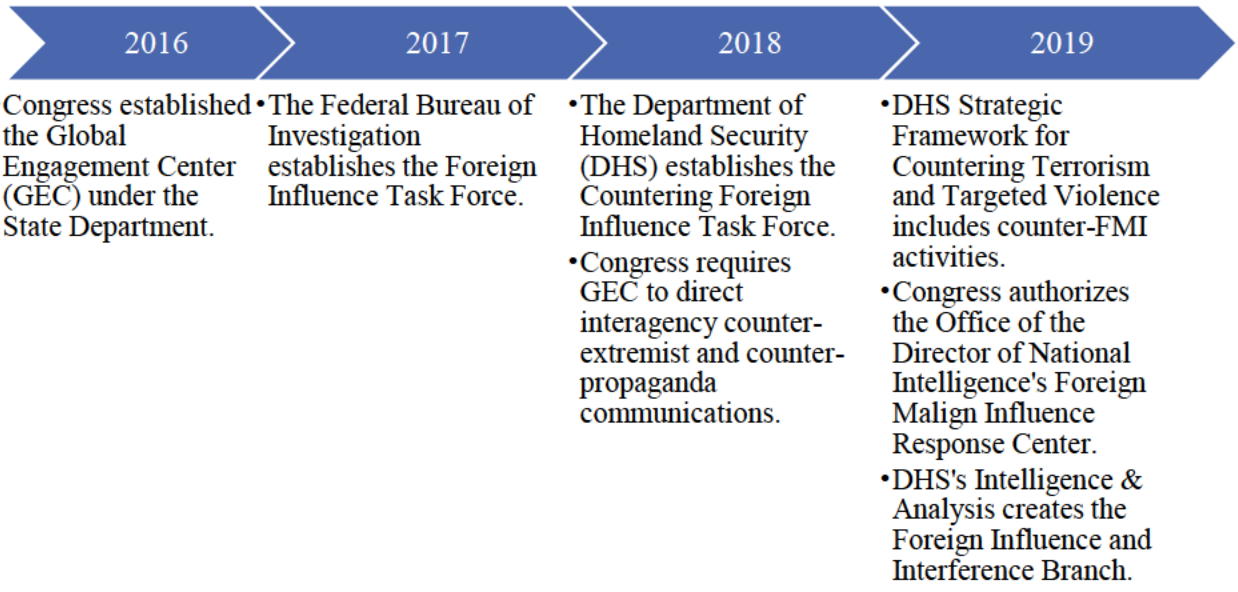
FITF's efforts were initially focused on Russian FMI operations but were later expanded to focus on those originating from China, Iran, and other global adversaries.[68]

In 2018, DHS established a dedicated counter-foreign disinformation team called the Countering Foreign Influence Task Force, which comprised staff from DHS's Cybersecurity and Infrastructure Security Agency (CISA) and Office of Intelligence and Analysis (I&A). The Countering Foreign Influence Task Force "developed threat intelligence and engaged with stakeholders" leading up to the 2020 elections.[69] It also started "notifying social media platforms or appropriate law enforcement officials when voting-related disinformation appeared in social media."[70] For example, emails from CISA officials to Facebook and Twitter (now X) in 2020 show that CISA communicated with platforms and had meetings about what the platforms were doing to combat election disinformation, including potentially contributing to a "Misinformation Reporting Portal" being developed by a non-profit connected to CISA.[71]

DHS's I&A also created a Foreign Influence and Interference Branch in 2019 "to organize and create analytical products about disinformation."[72] However, according to the DHS Office of Inspector General (OIG), the Foreign Influence and Interference Branch "did not directly counter disinformation; but rather, it shared information on the current threat environment."[73]

[68] DOJ OIG REPORT ON FMI, *supra*; *Combating Foreign Influence*, *supra*; *Oversight of Government Agencies, supra*.
[69] DEP'T OF HOMELAND SEC., OFF. OF INSPECTOR GEN., DHS NEEDS A UNIFIED STRATEGY TO COUNTER DISINFORMATION CAMPAIGNS, 5 (Aug. 10, 2022), https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-58-Aug22.pdf [hereinafter DHS NEEDS A UNIFIED STRATEGY].
[70] *Id.*
[71] The Parties' Joint Statement on Discovery Disputes at 100-118, *Missouri v. Biden,* 680 F. Supp. 3d 630 (W.D. L.a., 2022) (No. 71-9). The portal was not established. STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF "DISINFORMATION" PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS' POLITICAL SPEECH 30 (Nov. 6, 2023), https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/EIP_Jira-Ticket-Staff-Report-11-7-23-Clean.pdf [hereinafter THE WEAPONIZATION OF "DISINFORMATION" PSEUDO-EXPERTS AND BUREAUCRATS].
[72] DEP'T OF HOMELAND SEC., OFF. OF INSPECTOR GEN., DHS ACTIONS RELATED TO AN I&A INTELLIGENCE PRODUCT DEVIATED FROM STANDARD PROCEDURES (REDACTED) 2 (Apr. 26, 2022), https://www.oig.dhs.gov/sites/default/files/assets/2022-05/OIG-22-41-Apr22-Redacted.pdf; DHS NEEDS A UNIFIED STRATEGY, *supra,* at 6.
[73] DHS NEEDS A UNIFIED STRATEGY, *supra,* at 6.

Figure 1: Government Counter-Disinformation Efforts, 2016-2019



In its 2019 Strategic Framework for Countering Terrorism and Targeted Violence (DHS Strategic Framework), DHS stated an objective of "build[ing] resilience to malign information operations initiated by foreign states and foreign non-state actors."[74] DHS listed its priority actions for achieving this objective as developing a media or information literacy toolkit "to raise awareness of disinformation targeting communities" in the United States and to bolster information sharing with partners about foreign disinformation campaigns.[75] These efforts were in furtherance of the agency's broader goal of preventing domestic terrorism and targeted violence.

Later in 2019, Congress passed legislation authorizing ODNI's Foreign Malign Influence Center (FMIC) as the primary agency for integrating and disseminating FMI-related intelligence, although funding for FMIC was not appropriated by Congress until 2022 and FMIC did not start operations until September 2022.[76] Congress also amended the GEC's establishing provision in the National Defense Authorization Act for Fiscal Year 2019 "to clarify and strengthen GEC's authorities" and expanded the purpose of the GEC to include "direct[ing]" federal efforts to counter foreign state

[74] DHS STRATEGIC FRAMEWORK, *supra,* at 8, 10, 11, 27.
[75] *Id.* at 27.
[76] Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020, Pub. L. No. 116-92 § 2709 (codified as 50 U.S.C. § 3059). Responses to PCLOB from ODNI (Aug. 2026).

and non-state propaganda and disinformation.[77] Congress imposed evaluation requirements on the GEC to assess the effectiveness of its activities.[78]

In 2020, the FBI's FITF led the government's outreach efforts to social media companies in response to FMI campaigns ahead of the 2020 presidential election. According to a 2024 archived version of the FBI's website, one way FITF promoted its mission was "by providing foreign malign influence (FMI) threat information to companies hosting social media (Social Media Platforms) so that they may, based on their independent judgment, initiative, and decision-making process, take steps to mitigate such threats."[79] Throughout 2020, FITF coordinated regular "Election Integrity" calls through the FBI's San Francisco Field Office between government entities—including CISA, FBI elements, DOJ's National Security Division, and ODNI—and social media company representatives.[80] Agendas and notes from these calls suggest that the government would provide updates regarding FMI and cyber threats and discuss the actions companies took to communicate accurate election information.[81]

According to documents produced during the *Murthy v. Missouri* (formerly *Missouri v. Biden*) litigation, FITF claimed that, as part of this engagement, it "d[id] not perform narrative or content-based analysis;"[82] however, there were instances when FBI personnel working with the FITF, after conducting reviews of FBI or government holdings, flagged specific posts or content as likely foreign disinformation to a social media company for its review pursuant to the platform's internal content moderation policies.[83]

---

[77] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 § 1284 (*cf.* National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328 § 1287); Matthew C. Weed, *Termination of the State Department's Global Engagement Center,* CONG. RSCH. SERVICES (Dec. 26, 2024), https://www.congress.gov/crs-product/IN12475.

[78] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 § 1284.

[79] *Providing Foreign Malign Influence Threat Information to Social Media Platforms*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/investigate/counterintelligence/foreign-influence/providing-foreign-malign-influence-threat-information-to-social-media-platforms [https://web.archive.org/web/20240812110937/https:/www.fbi.gov/investigate/counterintelligence/foreign-influence/providing-foreign-malign-influence-threat-information-to-social-media-platforms] (last visited July 29, 2026). *See also*, *Foreign Malign Influence*, FED. BUREAU OF INVESTIGATION, https://www.justice.gov/archives/voting/foreign-malign-influence and WEAPONIZATION SUBCOMMITTEE FINAL REPORT, *supra,* at 1553.

[80] WEAPONIZATION SUBCOMMITTEE FINAL REPORT, *supra,* at 1299-1385. *See also*, Zoom Videotaped Dep. of Elvis Chan at 18-20, 23-28, *Missouri v. Biden,* 680 F. Supp. 3d. 630 (W.D. La. 2022) (No. 204-1) and Mem. Ruling on Req. for Prelim. Inj. at 58-61, *Missouri v. Biden*, 680 F. Supp. 3d 630 (W.D. La. 2022) (No. 293).

[81] WEAPONIZATION SUBCOMMITTEE FINAL REPORT, *supra,* at 1299, 1320.

[82] Second Am. Compl., Ex. Q, at 34, *Missouri v. Biden,* 680 F. Supp. 3d 620 (W.D. La. 2022) (No. 84-2).

[83] DOJ OIG REPORT ON FMI, *supra,* at 17. On October 4, 2020, for example, an FBI supervisory special agent forwarded to Facebook a CISA tip about a Facebook page with misleading information on local voting, reminding Facebook to "take whatever steps" were needed and to let the FBI know if any actions were taken as a result. In another case, during an October 14, 2020 meeting between FITF and Twitter, Twitter told the FBI that a recent takedown of Iranian government cyberwarfare group "was based on information previously provided by the FBI." The FBI notes for the meeting claimed that "they attributed these accounts" to the Iranian group "because of their behavior, such as tweeting about social justice and racial issues like Black Lives Matters." *See* WEAPONIZATION SUBCOMMITTEE FINAL REPORT, *supra,* at 1097 and 1266.

In the run up to the 2020 elections, DHS, CISA, and State Department's GEC interacted with the Election Integrity Partnership (EIP), a consortium of nongovernmental organizations.[84] According to a 2021 presentation by the leader of the EIP, the project was established to "try to fill the gap of the things that the Government could not do themselves" because federal agencies lacked "the funding and the legal authorizations."[85] Though the EIP's centralized ticketing infrastructure, external participants—including state and local elections officials and, at times, federal personnel—submitted "tickets" flagging online narratives and specific domestic social media posts.[86] EIP staff analyzed these inputs and forwarded systemic policy violations to content moderation teams at major social media companies.[87] In 2021, the EIP shifted focus and launched the Virality Project, adapting the same structural pipeline to monitor domestic narratives concerning COVID-19 vaccine skepticism.[88]

C. 2021 to 2024: Expansion of Government Counter-Disinformation and Growing Concerns

1. Expansion of Government Counter-Disinformation Efforts Domestically

In 2021, the government formally expanded its focus from foreign disinformation to countering "misinformation, disinformation, and malinformation" more generally.[89] In January 2021, CISA replaced its portion of the Countering Foreign Influence Task Force with the Misinformation, Disinformation, and Malinformation team (MDM team), which was created to "promote more flexibility to focus on general MDM."[90] The MDM team, according to one CISA official quoted in a DHS OIG report, "counter[ed] all types of disinformation, to be responsive to current events."[91] For example, the MDM team not only focused on election disinformation, but a broader set of topics, such as disinformation about the COVID-19 pandemic, vaccines, and how social media bots operated in the disinformation space. [92]

---

[84] WEAPONIZATION SUBCOMMITTEE FINAL REPORT, *supra,* at 931.
[85] Censorship Laundering: How the U.S. Department of Homeland Security Enables the Silencing of Dissent, Hearing Before the Subcomm. on Oversight, Investigations, & Accountability of the House Comm. on Homeland Sec., (2023), https://www.congress.gov/event/118th-congress/house-event/115901/text.
[86] *Id.*
[87] *Id.*
[88] *Id.*
[89] *See, e.g.*, WHITE HOUSE, FACT SHEET: THE BIDEN-HARRIS ADMINISTRATION IS TAKING ACTION TO RESTORE AND STRENGTHEN AMERICAN DEMOCRACY, (Dec. 8, 2021), https://www.presidency.ucsb.edu/documents/fact-sheet-the-biden-harris-administration-taking-action-restore-and-strengthen-american (announcing its efforts "Combating Misinformation and Disinformation," not specific to FMI). MDM appears to have been first introduced as a framework for understanding information operations in 2017 in a report for the Council of Europe report (2017). *See* Claire Wardle & Hossein Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, COUNCIL OF EUR., 20 (2017), https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html.
[90] DHS NEEDS A UNIFIED STRATEGY, *supra,* at 7.
[91] *Id.*
[92] *Mis, Dis, Malinformation,* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/mdm [https://web.archive.org/web/20220429060805/https://www.cisa.gov/mdm] (last visited July 29, 2026); DHS NEEDS A UNIFIED STRATEGY, *supra,* at 7.

In June 2021, the White House released its DT Strategy, which directly linked disinformation and domestic terrorism, and which was intended in part to "complement the U.S. Government's coordinated activities to recognize, understand, and counter terrorist propaganda and disinformation."[93] The 2021 DT Strategy stated that the government needed to address "extreme polarization, fueled by a crisis of disinformation and misinformation often channeled through social media platforms, which can tear Americans apart and lead some to violence."[94]

The 2021 DT Strategy stated that the government needed to address "extreme polarization, fueled by a crisis of disinformation and misinformation often channeled through social media platforms, which can tear Americans apart and lead to some violence."

Following the release of the 2021 DT Strategy, the White House issued the recently declassified 2021 Implementation Plan.[95] Among other things, the 2021 Implementation Plan identified roles of specific agencies engaged in the 2021 DT Strategy. The 2021 Implementation Plan required:

1) The FBI, State, DHS, and the CIA to "enhance the U.S. Government's understanding of how foreign state and non-state information operations, particularly disinformation, relate to the domestic terrorism threat" by "provid[ing] an internal report" to government stakeholders "on key findings regarding this potential threat within the next six months."[96]
2) DHS, with support from the Department of Education, State, and United States Agency for International Development (USAID), to provide funding for research on and to facilitate development of "evidence-based digital literacy programs" and an update on relevant findings or evaluations of digital literacy programming.[97]
3) The FBI, National Counterterrorism Center (NCTC), and DHS to conduct information sharing with "relevant technology and other private-industry companies" on "[domestic terrorism]-related and associated transnational terrorist online content" and to "as

[93] 2021 DT STRATEGY, *supra*.
[94] 2021 DT STRATEGY, *supra*. *See also* Statement of John Cohen, Coordinator for Counterterrorism, Dept. of Homeland Sec, Confronting Violent White Supremacy (Part VI): Examining the Biden Administration's Counterterrorism Strategy, Hearing Before the Subcomm. on CR. & C.L. of the House Comm. on Oversight & Reform, (2021), https://www.congress.gov/117/meeting/house/114074/documents/HHRG-117-GO02-Transcript-20210929.pdf ("Online content, disinformation, false narratives, and conspiracy theories spread by foreign nation-states, international terrorist groups, and extremist thought leaders fuel much of the violence we are experiencing in the country today. Domestic and foreign threat actors purposely seek to exploit the fractures in our society, the anger and discord in our political discourse to sow discord and inspire acts of violence.").
[95] 2021 IMPLEMENTATION PLAN, *supra*.
[96] *Id.* at 5. It is unclear whether this report was ever produced. The FBI did not have any corresponding documents to provide PCLOB. Responses to PCLOB from DOJ and the FBI (Sept. 21, 2026).
[97] *Id.* at 7. Note, the Department of Education's Institute of Education Sciences (an independent research arm of the Department) funded at least one digital literacy program called "Agents of Influence" in 2023 and 2024. *See Agents of Influence*, INST. OF EDUC. SCIENCES, DEP'T OF EDUC. (last visited May 20, 2026), https://ies.ed.gov/use-work/awards/agents-influence; *Agents of Influence,* INST. OF EDUC. SCIENCES, DEP'T OF EDUC. (last visited May 20, 2026), https://ies.ed.gov/use-work/awards/agents-influence-0. This report does not further detail the Department of Education's counter-disinformation efforts. It is unclear whether this report was ever produced.

appropriate and as expeditiously as possible and on a consistent basis […] ensure appropriate review of information intended for sharing with technology companies, such as legal, privacy, civil rights, and civil liberties review."[98] The FBI, NCTC, and DHS were directed to produce an update "on how engagements have developed, including whether there is improved information sharing."[99]

The White House referenced the 2021 DT Strategy in its 2022 National Security Strategy to explain how the government was addressing domestic extremists.[100] The 2022 National Security Strategy stated that the government was "confronting the long-term contributors to domestic violent extremist threats" by "addressing the crisis of disinformation and misinformation, often channeled through social and other media platforms, that can fuel extreme polarization and lead some individuals to violence."[101]

DHS further attempted to formalize and unify its counter-disinformation strategy throughout 2021. In September 2021, DHS's Under Secretary for Office of Strategy, Policy, and Plans and the Senior Counselor for National Security wrote a memo to the DHS Secretary about "organizing DHS efforts to counter disinformation," with a list of models DHS could use to structure its counter-disinformation efforts.[102] This resulted in the short-lived Disinformation Governance Board (DGB) (discussed further below).

Parts of DHS's efforts included interfacing directly with social media companies. A briefing memo for a meeting between the same DHS Under Secretary and executives of Twitter described it as "an opportunity to discuss operationalizing public-private partnerships between DHS and Twitter," including "that Twitter become involved in Disinformation Governance Board Analytic Exchanges on Domestic Violent Ext[r]emism [sic] (DVE) and Irregular Migration."[103]

In 2021, CISA established the Protecting Critical Infrastructure from Misinformation & Disinformation Subcommittee (MDM Subcommittee) of the CISA Cybersecurity Advisory Committee (CSAC).[104] A December 2022 CISA toolkit included "domestic extremist groups"

[98] 2021 IMPLEMENTATION PLAN, *supra,* at 9.
[99] *Id.* at 9. It is unclear whether this report was ever produced.
[100] WHITE HOUSE, NATIONAL SECURITY STRATEGY 31 (Oct. 2022), https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.
[101] *Id.*
[102] U.S. DEP'T OF HOMELAND SEC., ORGANIZING DHS EFFORTS TO COUNTER DISINFORMATION 1, 3 (Sept. 13, 2021), https://www.hawley.senate.gov/wp-content/uploads/files/2022-06/2022-06-07%20DOCS%20ONLY%20CEG%20JH%20to%20DHS%20(Disinformation%20Governance%20Board)%5B1%5D.pdf.
[103] SENS. CHARLES GRASSLEY & JOSH HAWLEY, LETTER TO DHS SEC. ALEJANDRO MAYORKAS (June 7, 2022), https://www.grassley.senate.gov/imo/media/doc/grassley_hawley_to_deptofhomelandsecuritydisinformationgovernanceboard.pdf. The document listed the operationalization of public-private partnerships under the "Key Objectives:" header.
[104] *See CISA Cybersecurity Advisory Committee Factsheet,* CISA CYBERSECURITY ADVISORY COMM., https://www.cisa.gov/sites/default/files/publications/CSAC_Factsheet_5-19-22_508c.pdf?_sp=3ab15d44-7646-4d97-92ee-dc96908008f7 (last visited July 29, 2026). CSAC is "an independent advisory body" comprised on public and private leaders and provides "recommendations to the CISA Director." *CISA Cybersecurity Advisory Committee,* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/resources-tools/groups/cisa-

along with foreign states as the "primary malign actors associated with the spreading of election-related MDM."[105] Similar to the 2020 example cited above, other investigations into counter-disinformation activities have highlighted that government entities may have continued flagging specific posts or accounts for take-down consideration by social media companies on the grounds that the accounts or posts spread FMI content. The U.S. House Judiciary Select Subcommittee on the Weaponization of the Federal Government (Weaponization Subcommittee), for example, reported that in 2022, an FBI[106] assistant legal attaché in Ukraine sent a number of emails to Facebook staff requesting review of accounts suspected of spreading Russian disinformation.[107] One read: "I have a few more Instagram and [Facebook] accounts that according to the [Security Service of Ukraine] spread Russian disinformation. For your review and action as deemed appropriate."[108] While most accounts listed in a spreadsheet attached to the email appeared to belong to foreign nationals or entities, the FBI flagged at least one as being located in the United States.[109] It is unclear what the company's response to this request was; according to the Subcommittee "[i]t appears that Meta did not immediately take noticeable action against these accounts."[110]

During this period, several Executive Branch entities also enhanced funding for counter-disinformation related grants, including a range of countermeasures. The White House's newly-created Information Integrity Research and Development Interagency Working Group published a Roadmap "to coordinate and guide federally funded [research and development] in information integrity."[111] The Roadmap adopted a new term, "corrupted information," to encompass "information that is inaccurate, misleading, deceptive, or inauthentically amplified within the context presented to the information consumer and that may cause harm to individuals, communities, institutions, or society at large, regardless of the author's or the distributor's intent."[112] While some research priorities were focused on foreign state manipulations and illegal activity, others were broader. Citing the 2021 DT Strategy, the Roadmap stated that two priorities of the Administration were to "mitigate threats that misinformation and disinformation pose to

cybersecurity-advisory-committee (last visited July 29, 2026). The MDM Subcommittee was a subcommittee of that advisory group. *CISA Cybersecurity Advisory Committee Factsheet*, *supra*.

[105] *See We're in This Together. Mis-, Dis-, and Malinformation Stops with You, supra*.

[106] This is consistent with the FBI's stated focus of countering FMI. *See supra* note 7.

[107] STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE FBI'S COLLABORATION WITH A COMPROMISED UKRAINIAN INTELLIGENCE AGENCY TO CENSOR AMERICAN SPEECH 6-17 (July 10, 2023), https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/fbi-sbu-staff-report-7.10.23-sm.pdf. PCLOB did not have access to the primary source documents when preparing this report. This except was included in the House Subcommittee Report.

[108] *Id.* at 10.

[109] *Id.*

[110] *Id.* at 12.

[111] NAT'L SCI. & TECH. COUNCIL, ROADMAP FOR RESEARCHERS ON PRIORITIES RELATED TO INFORMATION INTEGRITY RESEARCH AND DEVELOPMENT (Dec. 2022), https://www.nitrd.gov/pubs/Roadmap-Information-Integrity-RD-2022.pdf (*see* "About This Document").

[112] *Id.* at 11 ("The principal reason for using corrupted information is that there is currently no umbrella term that focuses specifically on the potential to cause harm, regardless of intent."). *See also id.* at C-3 (finding "[t]he comparable use of corrupted information by organized criminal groups and violent extremists grew exponentially during the COVID-19 pandemic.").

public safety and national security" and to "[a]ddress disinformation and *domestic and* foreign malign activities used to sow division and conflict."[113]

DHS's Center for Prevention Programs and Partnerships (CP3), which worked to prevent targeted violence and terrorism in the United States, funded the Targeted Violence and Terrorism Prevention (TVTP) program.[114] Through TVTP, CP3 funded a number of programs from 2021-2022 that promoted countering disinformation and media literacy in countering domestic terrorism and violent extremism.[115] Indeed, the link between disinformation and domestic terrorism was made explicit in such funding opportunities. For example, CP3 funded the Veterans Preventing Misinformation and Violence program, which focused on preventing extremism among veterans in part by educating veterans about disinformation aimed at them by foreign and domestic actors.[116] CP3 also funded Lewis University's How2Inform, which "was developed to combat online misinformation with navigating violent online content and critical thinking tools and resources."[117]

In April 2022, DHS announced the formation of the Disinformation Governance Board (DGB),[118] an internal working group with the explicit goal of "ensuring [Americans' freedom of speech, civil rights, civil liberties, and privacy] protections are appropriately incorporated across DHS's disinformation-related work and that rigorous safeguards are in place."[119] In May 2022, DHS directed the Homeland Security Advisory Council (HSAC), which provided advice and recommendations to the DHS Secretary, to establish a subcommittee on Disinformation Best Practices and Safeguards.[120]

---

[113] *Id.* at 10 (italics added).
[114] *Who We Are*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/cp3-who-we-are (last visited July 7, 2026); *What We Do*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/cp3-what-we-do (last visited July 7, 2026).
[115] See a list of TVTP grantees at *Targeted Violence and Terrorism Prevention Grantee Results*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/tvtp-grantee-results (last accessed July 7, 2026).
[116] *Targeted Violence Prevention for the Veteran and Military Family Community*, NAT'L CONSORTIUM FOR THE STUDY OF TERRORISM & RESPONSES TO TERRORISM, https://www.start.umd.edu/training/targeted-violence-prevention-veteran-and-military-family-community (last visited July 29, 2026); *View Grant Opportunity, DHS-22-TTP-132-00-01,* GRANTS.GOV, https://www.grants.gov/search-results-detail/339426 (last visited July 29, 2026).
[117] *Targeted Violence and Terrorism Prevention Grantee Results*, Department of Homeland Security, https://www.dhs.gov/tvtp-grantee-results (last accessed July 7, 2026); HOW2INFORM, https://h2i.info/ (last visited July 7, 2026). DOJ's Office of Justice Programs (OJP) also funded a wide range of external programs related to criminal justice, including violence prevention research that addressed disinformation and domestic terrorism. *See About Us,* OFF. OF JUST. PROGRAMS, https://www.ojp.gov/about (last visited July 29, 2026). Appendix B presents a full list of disinformation-related funding provided to PCLOB by DOJ.
[118] Bridget Johnson, *DHS Standing Up Disinformation Governance Board Led by Information Warfare Expert,* HOMELAND SECURITY TODAY (Apr. 27, 2022), https://www.hstoday.us/federal-pages/dhs/dhs-standing-up-disinformation-governance-board-led-by-information-warfare-expert/.
[119] *Fact Sheet: DHS Internal Working Group Protects Free Speech and Other Fundamental Rights When Addressing Disinformation That Threatens the Security of the United States*, DEP'T OF HOMELAND SEC. (May 2, 2022), https://www.dhs.gov/archive/news/2022/05/02/fact-sheet-dhs-internal-working-group-protects-free-speech-other-fundamental-rights.
[120] Notice, 87 Fed. Reg. 32047 (May 26, 2022), https://www.federalregister.gov/documents/2022/05/26/2022-11279/homeland-security-advisory-council-new-projects; *Homeland Security Advisory Council,* DEP'T OF HOMELAND SEC. https://www.dhs.gov/homeland-security-advisory-council (last visited May 20, 2026).

In June 2022, CISA's MDM Subcommittee released its first formal recommendations, advising CISA to work with election officials "to identify and address" election-related disinformation.[121] It did not distinguish between foreign and domestic sources.[122] The FBI's FITF also continued to flag specific posts or accounts for take-down consideration by social media companies on the grounds that the accounts or posts spread FMI content.[123]

In addition, ODNI's Foreign Malign Influence Response Center, which had previously been renamed by statute to the Foreign Malign Influence Center (FMIC), commenced operations on September 23, 2022.[124] The FMIC led intelligence efforts to communicate with the media, private sector, and stakeholders "including election officials, civil society leaders, and the American people" about FMI campaigns against U.S. elections.[125]

[121] *Report to the CISA Director: Protecting Critical Infrastructure from Misinformation and Disinformation,* CISA CYBERSECURITY ADVISORY COMM., 1 (June 22, 2022), https://www.cisa.gov/sites/default/files/publications/June%202022%20CSAC%20Recommendations%20%E2%80%93%20MDM_0.pdf.

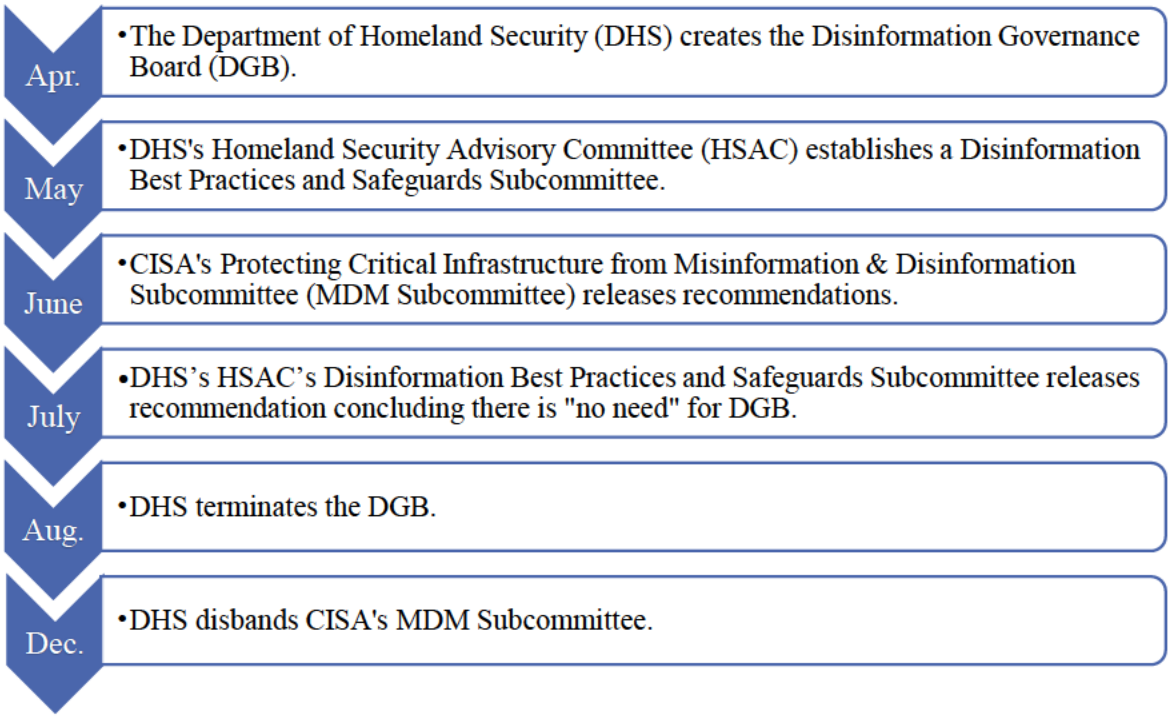
[122] *Id.* CSAC also released brief recommendations in Sept. 2022 where they did talk specifically about foreign disinformation. *Report to the CISA Director: Protecting Critical Infrastructure from Misinformation and Disinformation, Information Sharing Around Foreign Adversary Threats to Elections,* CISA CYBERSECURITY ADVISORY COMM., 3 (Sept. 13,2022), https://www.cisa.gov/sites/default/files/publications/CSAC_MDM_September_2022_Final_Recommendations_09132022-508.pdf.

[123] *See* THE FBI'S COLLABORATION WITH A COMPROMISED UKRAINIAN INTELLIGENCE AGENCY, *supra,* at 12.

[124] James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 § 6307 (Pub. L. 117–263); Responses to PCLOB from ODNI (Aug. 2026). The FMIC was never operational as the Foreign Malign Influence Response Center. Responses to PCLOB from ODNI (Oct. 2026)

[125] *Election Security: U.S. Government's Efforts to Protect the 2024 U.S. Election from Foreign Malign Influence*, DEP'T OF STATE (Sept. 6, 2024), https://2021-2025.state.gov/briefings-foreign-press-centers/protecting-the-2024-election-from-foreign-malign-influence/.

Figure 2: DHS Efforts to Counter Disinformation (2022)



2. Concerns Over Government Counter-Disinformation Efforts and Subsequent Contraction

The announcement of the creation of the DGB in April 2022 elicited bipartisan concern and criticism about the government's role in countering disinformation and its impact on Americans' First Amendment rights.[126] In May 2022, DHS Secretary Mayorkas directed HSAC to review the ways in which the agency "can most effectively and appropriately address disinformation that poses a threat to the homeland, while increasing transparency and protecting free speech, civil rights, civil liberties, and privacy."[127] In June 2022, this group issued an interim recommendation that there was "no need for a Disinformation Governance Board" without detailing why.[128]

[126] *See, e.g.*, PROTECT DEMOCRACY, KNIGHT FIRST AMEND. INST. AT COLUM. UNIV., & ELEC. FRONTIER FOUND., LETTER TO DHS RE: SIGNIFICANT CONCERNS REGARDING THE "DISINFORMATION GOVERNANCE BOARD" (May 3, 2022), https://www.documentcloud.org/documents/21850086-letter-to-mayorkas-re-disinformation-governance-board_may-3-2022/; REP. JAMES COMER ET AL., LETTER TO DHS RE: DISINFORMATION GOVERNANCE BOARD (Apr. 29, 2022), https://oversight.house.gov/wp-content/uploads/2022/04/Letter-to-DHS-re-Disinformation-Governance-Board-04292022.pdf.

[127] HOMELAND SEC. ADVISORY COUNCIL, DISINFORMATION BEST PRAC. & SAFEGUARDS SUBCOMM., FINAL REPORT 6, 24 (Aug. 24, 2022), https://www.dhs.gov/sites/default/files/2022-08/22_0824_ope_hsac-disinformation-subcommittee-final-report-08242022.pdf; HOMELAND SEC. ADVISORY COUNCIL, DISINFORMATION BEST PRAC. & SAFEGUARDS SUBCOMM., FINAL INTERIM RECOMMENDATION 2 (July 18, 2022), https://www.dhs.gov/sites/default/files/2022-07/22_0718_ope_final-interim-recommendation-disinformation-best-practices-safeguards-subcommittee_0.pdf.

[128] FINAL INTERIM RECOMMENDATION, *supra*, at 4.

Their final report, issued in August 2022, stated, "it is our assessment that the underlying work of Department components on this issue is critical."[129] However they noted DHS "does not have a broad remit to address all inaccurate information or disinformation, nor does it have the authority to silence or sanction anyone's speech."[130] In August 2022, DHS terminated the DGB based on HSAC's recommendation.[131]

In August 2022, two PCLOB Board Members sent a letter to the DHS Secretary requesting information on how DHS counters disinformation.[132] The members cited a DHS fact sheet which stated that "[f]or nearly 10 years, different agencies across DHS have worked to address disinformation that threatens our homeland security."[133] DHS did not respond for almost a year and did not produce any of the requested information.[134]

In 2023, the U.S. House of Representatives Judiciary Committee created the Weaponization Subcommittee to investigate, among other things, how Executive Branch agencies provide information to the private sector "to facilitate action against American citizens."[135] The Weaponization Subcommittee held hearings and released reports on a number of topics, including government engagement with social media companies on disinformation.[136]

In October 2023, the Supreme Court agreed to hear a case assessing the lawfulness of the government's counter-disinformation efforts and communications with social media companies. In *Murthy v. Missouri*, two states and five individual social media users sued the government, claiming that the government engaged in a censorship campaign when federal officials reached

[129] FINAL REPORT, *supra,* at 12.
[130] *Id.* at 13.
[131] *Following HSAC Recommendation, DHS terminates Disinformation Governance Board,* DEP'T OF HOMELAND SEC. (Aug. 24, 2022), https://www.dhs.gov/archive/news/2022/08/24/following-hsac-recommendation-dhs-terminates-disinformation-governance-board; FINAL REPORT, *supra,* at 12. *See also Hawley Leads Letter Demanding DHS Release Documents on Disinformation Governance Board,* JOSH HAWLEY (May 23, 2022), https://www.hawley.senate.gov/hawley-leads-letter-demanding-dhs-release-documents-disinformation-governance-board/.
[132] CHAIR SHARON BRADFORD FRANKLIN AND MEMBER BETH A. WILLIAMS, LETTER TO DEPARTMENT OF HOMELAND SECURITY SECRETARY ALEJANDRO MAYORKAS (Aug. 4, 2022), *see* Appendix D. The letter became a request by the full Board when the *Countering Domestic Terrorism and its Impacts on Privacy and Civil Liberties* project was approved later that year. *See* DEP'T OF HOMELAND SEC., DEPARTMENT OF HOMELAND SECURITY RESPONSE TO PCLOB'S AUGUST 2022 LETTER TO SECRETARY MAYORKAS (July 20, 2023) at n.1, *see* Appendix D.
[133] LETTER TO DEPARTMENT OF HOMELAND SECURITY SECRETARY ALEJANDRO MAYORKAS, *supra*; *Fact Sheet: DHS Internal Working Group Protects Free Speech and Other Fundamental Rights When Addressing Disinformation That Threatens the Security of the United States*, DEP'T OF HOMELAND SEC. (May 2, 2022), https://www.dhs.gov/news/2022/05/02/fact-sheet-dhs-internal-working-group-protects-free-speech-other-fundamental-rights.
[134] DEP'T OF HOMELAND SEC., DEPARTMENT OF HOMELAND SECURITY RESPONSE TO PCLOB'S AUGUST 2022 LETTER TO SECRETARY MAYORKAS (July 20, 2023), *see* Appendix D.
[135] *Select Subcommittee on the Weaponization of the Federal Government*, H. COMM. ON THE JUDICIARY, *Background*, U.S. SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T, https://weaponization-judiciary.house.gov/about/background (last visited June 17, 2026).
[136] *Select Subcommittee on the Weaponization of the Federal Government*, H. COMM. ON THE JUDICIARY, https://judiciary.house.gov/subcommittees/committee-judiciary-118th-congress/select-subcommittee-weaponization-federal (last visited June 17, 2026); WEAPONIZATION SUBCOMMITTEE FINAL REPORT, *supra,* at iii, 1872.

out to social media companies to remove certain content.[137] The government argued that the plaintiffs failed to show any injury traceable to the government "as opposed to third-party social media companies."[138]Around this time, CISA's work countering disinformation also came under scrutiny.[139] In 2023, the organization Foundation for Freedom Online published a report showing that CISA removed references to domestic disinformation and "domestic threat actors" from its website, perhaps in response to backlash about perceived government involvement in domestic disinformation.[140] Also in 2023, the House Committee on the Judiciary and the Weaponization Subcommittee released an interim staff report about "censorship efforts" encouraged by CISA.[141] At some point before March 2024, CISA moved its standalone MDM team into its Election Security and Resilience team.

[137] Third Am. Compl. at 7-8, 11, *Missouri v. Biden*, 680 F. Supp. 3d 630 (W.D. La. 2022) (No. 268).
[138] Defs.' Mot. to Dismiss for Lack of Subject-Matter Jurisdiction and Failure to State a Claim at 23, *Missouri v. Biden*, F. Supp. 3d 630 (W.D. La, 2022) (No. 35). The Supreme Court held in June 2024 that the plaintiffs lacked standing. The Court remanded the case back to the lower courts for further proceedings consistent with its opinion. *Murthy v. Missouri*, 603 U.S. 43 (2024).
[139] *See* STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE Judiciary, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A "CYBERSECURITY" AGENCY COLLUDED WITH BIG TECH AND "DISINFORMATION" PARTNERS TO CENSOR AMERICANS 17 (June 26, 2023), https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/cisa-staff-report6-26-23.pdf [hereinafter THE WEAPONIZATION OF CISA]; *See also* Subcomm. on Oversight, Investigations, and Accountability Hearing, "Censorship Laundering Part II: Preventing the Department of Homeland Security's Silencing of Dissent" (Dec. 13, 2023), https://homeland.house.gov/hearing/censorship-laundering-part-ii-preventing-the-department-of-homeland-securitys-silencing-of-dissent/.
[140] FOUND. FOR FREEDOM ONLINE, DHS QUIETLY PURGES CISA "MIS, AND DIS AND MALINFORMATION" WEBSITE TO REMOVE DOMESTIC CENSORSHIP REFERENCES 1 (Mar. 2023), https://www.foundationforfreedomonline.com/wp-content/uploads/2023/03/FFO-FLASH-REPORT-REV.pdf; *see Mis, Dis, Malinformation*, *supra.* In September 2024, CISA told PCLOB, "CISA does not do counter-MDM work in the context" of countering domestic terrorism, but instead "focus[es] on educating election infrastructure officials on how to navigate foreign influence operations and disinformation related risks." Email from CISA to PCLOB (Sept. 20, 2024).
[141] THE WEAPONIZATION OF CISA, *supra,* at 5.

Figure 2: Events Relevant to Government Counter-Disinformation Efforts, 2021-2024



According to a 2024 DHS OIG report, CISA "discontinued its efforts to work directly with social media companies to counter disinformation after the 2022 election."[142] In 2024, CISA represented to PCLOB staff that CISA does not monitor social media for disinformation, however it did, as of October 2024, engage in public awareness campaigns and resilience building and development overseas to combat disinformation by foreign extremists.[143]

The FBI paused contact about foreign disinformation with social media companies "for more than half a year."[144] After receiving interim guidance from the National Security Council (NSC) *Regarding Certain Engagement with Technology Companies Regarding Online Content* in January 2024, the FBI resumed contact in March 2024 and resumed "normal call engagements" in September 2024.[145]

[142] DEP'T OF HOMELAND SEC., OFF. OF THE INSPECTOR GEN., FINAL REPORT: DHS IMPROVED ELECTION INFRASTRUCTURE SECURITY, BUT ITS ROLE IN COUNTERING DISINFORMATION HAS BEEN REDUCED 4 (Sept. 17, 2024), https://www.oig.dhs.gov/sites/default/files/assets/2024-09/OIG-24-52-Sep24.pdf.
[143] PCLOB Notes on CISA Team Meeting, (Oct. 15, 2024). CISA also told PCLOB that "CISA does not engage in MDM activities related to combatting domestic terrorism." Email from CISA to PCLOB, (Mar. 20, 2025).
[144] Responses to PCLOB from the FBI (Sept. 2026).
[145] Responses to PCLOB from the FBI (Sept. 2026).

D. 2025 to Present: Executive Orders and Legislative Developments

In January 2025, President Donald Trump issued EO 14149, *Restoring Freedom of Speech and Ending Federal Censorship*, which critiqued actions taken by the previous administration to combat "misinformation," "disinformation," and "malinformation," by "censoring Americans' speech on online platforms, often by exerting substantial coercive pressure on third parties, such as social media platforms, to moderate, deplatform, or otherwise suppress speech that the Federal Government did not approve," in a "manner that advanced the Government's preferred narrative about significant matters of public debate."[146] EO 14149 "[p]rohibit[ed] the [g]overnment from unconstitutionally abridging the speech of Americans" and required the government to "take appropriate action to correct past misconduct by the Federal Government related to censorship of protected speech."[147] It also mandated that the Attorney General investigate "the activities of the Federal Government over the last 4 years" that are counter to the EO, and required heads of agencies to cooperate with the DOJ's investigation into the matter.[148]

In January 2025, President Trump issued EO 14149, *Restoring Freedom of Speech and Ending Federal Censorship*, which critiqued actions taken by the previous administration to combat "misinformation," "disinformation," and "malinformation," by "censoring Americans' speech on online platforms, often by exerting substantial coercive pressure on third parties, such as social media platforms, to moderate, deplatform, or otherwise suppress speech that the Federal Government did not approve," in a "manner that advanced the Government's preferred narrative about significant matters of public debate."

Relatedly, President Trump issued a Presidential Memorandum, *Addressing Risks from Chris Krebs and Government Censorship*, which required a "comprehensive evaluation of all of CISA's activities over the last 6 years" focusing on activities that were counter to the aims of EO 14149.[149]

With respect to legislative developments since 2025, the National Defense Authorization Act (NDAA) for Fiscal Year 2026 (FY26) gave State's Under Secretary for Public Diplomacy statutory responsibility—similar to that previously given the now-terminated GEC—to "lead, synchronize, and coordinate efforts to recognize, understand, expose, and counter foreign information manipulation and malign activities, including through efforts to limit the foreign propaganda and

[146] Exec. Order No. 14149 § 2.
[147] *Id.* at § 2(d).
[148] *Id.* at § 3(b) ("The Attorney General, in consultation with the heads of executive departments and agencies, shall investigate the activities of the Federal Government over the last 4 years that are inconsistent with the purposes and policies of this order and prepare a report to be submitted to the President, through the Deputy Chief of Staff for Policy, with recommendations for appropriate remedial actions to be taken based on the findings of the report.").
[149] Memorandum on Addressing Risks From Chris Krebs and Government Censorship (Apr. 9, 2025) ("Upon completing these reviews, the Attorney General and the Secretary of Homeland Security shall prepare a joint report to be submitted to the President, through the Counsel to the President, with recommendations for appropriate remedial or preventative actions to be taken to fulfill the purposes and policies of Executive Order 14149.").

disinformation efforts of adversaries, and coordinate those efforts across Federal departments and agencies."[150] The FY26 NDAA also directs the Under Secretary to "oppose censorship by foreign adversaries."[151]

[150] National Defense Authorization Act for Fiscal Year 2026, Pub. L. No. 119-60, § 5401(4), 139 Stat. 1596-1597 (2025).
[151] *Id.*

III. DISCUSSION

The 2021 DT Strategy and its ensuing implementation memorandum blurred the lines between foreign and domestic speech, and between protected and unprotected speech.[152] As discussed above, the government has historically responded to threats posed by foreign disinformation campaigns, especially those that were believed to impact national security, enflame domestic tensions, or undermine democratic institutions and processes. The government often counters foreign efforts through means of transparency such as those described above, including through criminal indictment.[153]

The 2021 DT Strategy and its ensuing implementation memorandum blurred the lines between foreign and domestic speech, and between protected and unprotected speech.

Attempts to suppress domestic speech, however, have long been disfavored or rejected—even when the government believes such speech to be false or harmful.[154] But the ease by which messages may now be transmitted to large numbers of people in short periods of time appears to

[152] The Supreme Court has not ruled whether foreign disinformation is protected speech. In *Lamont v. Postmaster General***,** 381 U.S. 301 (1965), the Court struck down an act that required the Postmaster General to detain and deliver only upon the addressee's request unsealed foreign mailings of communist political propaganda. But the Court based its ruling on "narrow grounds" due to the burden placed on the addressee. ("Nor do we reach the question whether the standard here applied could pass constitutional muster. Nor do we deal with the right of Customs to inspect material from abroad for contraband. We rest on the narrow ground that the addressee, in order to receive his mail, must request in writing that it be delivered."). In *Holder v. Humanitarian Law Project*, 561 U.S. 1 (2010), the Supreme Court upheld the federal ban on providing "material support" to foreign terrorist organizations, even when that support consisted entirely of legal speech, suggesting that the government in certain instances may lawfully restrict cross-border communication.

[153] DOJ has a practice of announcing indictments publicly. *See, e.g., Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System*, DEP'T OF JUST. (Feb. 16, 2018), https://www.justice.gov/archives/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere (indicting foreign agents for "information warfare against the United States," with the stated goal of "spread[ing] distrust towards the candidates and the political system in general"). *Two RT Employees Indicted for Covertly Funding and Directing U.S. Company that Published Thousands of Videos in Furtherance of Russian Interests*, DEP'T OF JUST. (Sept. 4, 2024), https://www.justice.gov/archives/opa/pr/two-rt-employees-indicted-covertly-funding-and-directing-us-company-published-thousands (indicting two RT employees for "creat[ing] and distribut[ing] content to U.S. audiences with hidden Russian government messaging'"). *See also Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm,* DEP'T OF JUST. (July 9, 2024), https://www.justice.gov/archives/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners (seizing "of two domain names and the search of 968 social media accounts used by Russian agents to create an AI-enhanced social media bot farm that spread disinformation in the United States and abroad") and *Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere,* DEP'T OF JUST. (Sept. 4, 2024), https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence (seizing "of 32 internet domains used in Russian government-directed foreign malign influence campaigns").

[154] *See, e.g., United States v. Alvarez*, 567 U.S. 709 (2012) (plurality) (invalidating the Stolen Valor Act, a federal law prohibiting false statements about receiving military decorations or medals).

[R]ecent government efforts to counter disinformation for purposes including preventing domestic terrorism often lacked appropriate justification, failed to assess the First Amendment impacts of such efforts, and lacked privacy and civil liberties safeguards.

have heightened governmental concern about the potential harms of disinformation.[155] Nevertheless, recent government efforts to counter disinformation for purposes including preventing domestic terrorism often lacked appropriate justification, failed to assess the First Amendment impacts of such efforts, and lacked privacy and civil liberties safeguards.

A. The Government Failed to Provide Evidence of a Nexus Between Disinformation and Domestic Terrorism

The 2021 DT Strategy promoted counter-disinformation efforts to prevent domestic terrorism without pointing to evidence that disinformation contributed to domestic terrorism. Neither the 2021 DT Strategy nor the follow-on Implementation Plan cited to any articles or evidence to support the proposition that disinformation was contributing to domestic terrorism. The government also failed either to provide to PCLOB or to make public analyses on how disinformation "relate[s] to the domestic terrorism threat."[156]

Underscoring the government's insufficient justification for the connection between disinformation and domestic terrorism, the 2021 Implementation Plan *tasked* four agencies—the FBI, CIA, State, and DHS—with "[e]nhanc[ing] the U.S. Government's understanding of how foreign state and non-state information operations, particularly disinformation, relate to the domestic

The 2021 Implementation Plan *tasked* four agencies—the FBI, CIA, State, and DHS—with "[e]nhanc[ing] the U.S. Government's understanding of how foreign state and non-state information operations, particularly disinformation, relate to the domestic terrorism threat." It directed them to "provide an internal report for U.S. Government stakeholders on key findings regarding this potential threat within the next six months." Despite repeated requests, PCLOB has not been provided with this report, and relevant agencies cannot say if it was ever produced.

[155] *See e.g.,* 2021 DT STRATEGY, *supra,* at 21 ("The widespread availability of domestic terrorist recruitment material online is a national security threat whose front lines are overwhelmingly private sector online platforms, and we are committed to informing more effectively the escalating efforts by those platforms to secure those front lines.").

[156] PCLOB requested responsive documentation but was not provided with any response. LETTER FROM BOARD MEMBER BETH A. WILLIAMS TO ATTORNEY GENERAL PAMELA BONDI (Mar. 13, 2026) (requesting any "analyses by the FBI, CIA, State Department, and DHS, in accordance with Section 1.1.2.d of the Strategic Plan [2021 Implementation Plan]). DHS confirmed that they were not aware of any "evidence or analysis provided […] to the White House/NSC to support the 2021 National Strategy for Countering Domestic Terrorism citing disinformation as a contributor to domestic terrorism." Responses to PCLOB from DHS (Oct. 2026).

terrorism threat."[157] It directed them to "provide an internal report for U.S. Government stakeholders on key findings regarding this potential threat within the next six months." Despite repeated requests, PCLOB has not been provided with this report, and relevant agencies cannot say if it was ever produced.

While a full review of the research linking disinformation to domestic terrorism is beyond the scope of this Report, PCLOB reviewed recent available academic literature on this subject. Some studies have found that exposure to violent content might play a role in mobilizing someone towards violence, but this is highly context dependent.[158] Drawing a direct causal link between disinformation on social media and offline violence remains tenuous at best, and the government has not made public or provided to PCLOB analyses, intelligence reports, or other products on which it relied to develop its policies.

Other studies suggest that digital media use *in general* is associated with increased polarization.[159] However, as stated above, linking online content, specifically disinformation, to violence is challenging and remains contested.[160] Overall, the research reveals the impracticalities of asserting anything beyond possible correlation between specific forms of online disinformation and future terrorist violence or support for violence.[161]

---

[157] 2021 IMPLEMENTATION PLAN, *supra.*

[158] *See* Thomas Frissen, *Internet, The Great Radicalizer? Exploring Relationships Between Seeking for Online Extremist Materials and Cognitive Radicalization In Young Adults*, 114 COMPUTERS IN HUM. BEHAV., (2021), https://doi.org/10.1016/j.chb.2020.106549 (concluding that radicalization to violence occurs in a phased approach whereby numerous factors – such as prior criminal activity and moral disengagement – interact with exposure to violent content online; however, the behavior of actively seeking out violent content is correlational but not causal here).

[159] *See generally* Philipp Lorenz-Spreen, Lisa Oswald, Stephan Lewandowsky, et al., *A Systematic Review of Worldwide Causal and Correlational Evidence On Digital Media and Democracy*, 7 NATURE HUM. BEHAV. 74–101 (2023), https://doi.org/10.1038/s41562-022-01460-1; Pramukh Nanjundaswamy Vasist, et al., *The Polarizing Impact of Political Disinformation and Hate Speech: A Cross-country Configural Narrative*, 17 INFO. SYS. FRONTIERS, 1-26 (2023), https://doi.org/10.1007/s10796-023-10390-w. The FBI's 2027 Budget Request states that domestic terrorists employ social media "to recruit new adherents, plan and rally support for in-person actions, and disseminate materials encouraging radicalization and mobilization to violence," but does not mention disinformation. *See* FED. BUREAU OF INVESTIGATION, FY 2027 FBI BUDGET REQUEST TO CONGRESS 13 (Mar. 2026), https://www.justice.gov/jmd/media/1434246/dl?inline.

[160] *See* Ghayda Hassan, et al., *Exposure to Extremist Online Content Could Lead to Violent Radicalization: A Systematic Review of Empirical Evidence*, 12 INT'L J. OF DEV. SCI., 12 1-2, 71-88 (2018), https://doi.org/10.3233/DEV-170233 (stating "the link between exposure to violent radical material online and violent radical behavior online and/or offline remains unknown, largely due to the lack of integration of available empirical evidence into a meaningful whole for policy, research, and prevention purposes"). *See also* Kate Cox, Theodora Ogden, Victoria Jordan, and Pauline Paille, *COVID-19, Disinformation and Hateful Extremism: Literature Review Report*, RAND EUROPE, (Mar. 2021), https://assets.publishing.service.gov.uk/media/60c8681bd3bf7f4bd323e1e8/RAND_Europe_Final_Report_Hateful_Extremism_During_COVID-19_Final_accessible.pdf (discussing the difficulties of determining causality with exposure to misinformation and hateful incidents).

[161] The government's ability to discern what is disinformation while retaining public trust is also suspect, as government overreach and violations of civil liberties may often themselves, be drivers of extremist violence. *See* James A. Piazza, *Fake News: The Effects of Social Media Disinformation on Domestic Terrorism*, 15 DYNAMICS OF ASYMMETRIC CONFLICT 1, 55–77, https://doi.org/10.1080/17467586.2021.1895263.

Nevertheless, government agencies and officials drew connections between disinformation concerning politically divisive issues and the possibility of future violence.[162] For example, in 2020, DHS assessed that Russia and Iran spread disinformation about the origins of COVID-19 to sow discord and distrust in government, which could lead to domestic terrorism.[163] In October 2021, DHS circulated a threat assessment entitled, "Threats to Public Schools Likely Elevated Due to Opposition of Mask and Vaccine Mandates, Perception of Critical Race Theory" (CRT).[164] With "medium confidence," DHS attributed threats to school personnel as being due to "misinformation and disinformation related to CRT curriculum, and upcoming school board elections" and the approval of a COVID vaccine for children.[165] DOJ has noted that the threat assessment relied in part on a letter by the National School Boards Association as a source.[166]

A report published by ODNI in March of 2021 stated that "[n]ewer sociopolitical developments—such as narratives of fraud in the recent general election, the emboldening impact of the violent breach of the U.S. Capitol, conditions related to the COVID-19 pandemic, and conspiracy theories promoting violence—will almost certainly spur some DVEs [domestic violent extremists] to try to engage in violence this year."[167] In neither of these reports did the agencies reference specific examples where consumption of disinformation led to violent behavior domestically.

1. "Disinformation" Often Relies on Subjective Interpretation

Rather than focusing primarily on FMI as they had in the past, various entities within the Executive Branch expanded their strategies to counter what they called "MDM." The terms mis-, dis-, and

[162] The inclination to draw a causal link between divisive rhetoric by some members of the public and extremist acts committed by others—thereby forming a basis to argue for the removal or censorship of that rhetoric—is not unique to this point in time. As discussed in the Scope and Methodology section, the focus on the recent period reflects the public discussion surrounding nonpublic communications between government officials and online platforms.
[163] U.S. DEP'T OF HOMELAND SEC., HOMELAND THREAT ASSESSMENT 17-18 (Oct. 2020), https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf. ("Another motivating force behind domestic terrorism that also poses a threat to the Homeland is anti-government/anti-authority violent extremism. These violent extremists, sometimes influenced by anarchist ideology, have been associated with multiple plots and attacks, which included a significant uptick in violence against law enforcement and government symbols in 2020. This ideology is also exploited by hostile nation-states, which seek to promote it through disinformation campaigns and sow additional chaos and discord across American society…").
[164] DEP'T OF JUST., WEAPONIZATION WORKING GROUP, THE 2026 REPORT TO EXPOSE THE WEAPONIZATION OF GOVERNMENT AGAINST PARENTS IN SCHOOLS 19, 261 (Oct. 5, 2026), https://www.justice.gov/opa/media/1464216/dl?inline. (The Appendix of the DOJ report provides the DHS threat assessment from 2021, which states, "We assess that violent individuals who oppose mask mandates, vaccine requirements, and CRT as a topic of classroom learning, will increasingly pose a threat to school personnel over the next six months due to the expected approval of a COVID-19 vaccine for children ages 5-11, continued misinformation and disinformation related to CRT curriculum, and upcoming school board elections.").
[165] *Id.* at 19.
[166] *Id.*
[167] OFF. OF THE DIR. OF NAT'L INTEL., DOMESTIC VIOLENT EXTREMISM POSES HEIGHTENED THREAT IN 2021 2 (Mar. 1, 2021), https://www.dni.gov/files/ODNI/documents/assessments/UnclassSummaryofDVEAssessment-17MAR21.pdf. DVEs are defined as "an individual based and operating primarily within the territorial jurisdiction of the United States who seeks to further their ideological goals wholly or in part through unlawful acts of force or violence." *See* FED. BUREAU OF INVESTIGATION & DEP'T OF HOMELAND SEC., DOMESTIC TERRORISM: DEFINITIONS, TERMINOLOGY, AND METHODOLOGY (Nov. 2020), https://www.fbi.gov/file-repository/fbi-dhs-domestic-terrorism-definitions-terminology-methodology.pdf/view.

mal-information are not defined by federal statute. Nor have they been uniformly defined by government policy.[168] Even if applied consistently, the terms may encompass information that is disputed, out of context, incomplete, not objectively false, or only subjectively considered misleading. Indeed, "malinformation" was defined by CISA as *true* information "based on fact, but used out of context to mislead, harm, or manipulate."[169] While most agencies within the Intelligence Community (IC) have used the National Intelligence Council's *IC Lexicon for Foreign Malign Influence,* which does not include malinformation as a concept, other agencies used their own definitions, which were often different from those contained in existing policies.[170] Some definitions were overbroad or simply wrong, and did not distinguish between foreign and domestic speech.[171] Broad definitions of a problem vest the government with wide discretion to leverage its power. Such sweeping authority, accompanied by vague or ill-defined terms, heightens the potential for government abuse in the name of countering domestic terrorism. In the absence of a defined threat and narrow, uniformly-adopted definitions, the government struggles to identify its legitimate objectives and evaluate its efforts consistent with First Amendment protections and civil liberties.[172]

Broad definitions of a problem vest the government with wide discretion to leverage its power. Such sweeping authority, accompanied by vague or ill-defined terms, heightens the potential for government abuse in the name of countering domestic terrorism.

[168] For example, several agencies PCLOB investigated defined "disinformation" differently. *See e.g.,* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, DISINFORMATION STOPS WITH YOU, https://www.cisa.gov/sites/default/files/publications/disinformation_stops_with_you_infographic_set_508.pdf ("is deliberately created to mislead, harm, manipulate a person, social group, organization, or country"); HOMELAND THREAT ASSESSMENT 2024, *supra,* at 6 ("false or misleading information that is deliberately created or spread with the intent to deceive or mislead"); DOJ OIG Report on FMI, *supra,* at 2 ("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"). Most agencies within the Intelligence Community have adopted the National Intelligence Council's definition of "disinformation" as well. *See* GAO-24-107600, FOREIGN DISINFORMATION: DEFINING AND DETECTING THREATS, *supra*, at 8 ("False or misleading information deliberately created or spread with the intent to deceive or mislead."). As discussed previously, the 2022 charter for DHS's Disinformation Governance Board (DGB) stated that the purpose of the DGB was "to guide and support the Department's efforts to address mis-, dis-, and malinformation that threatens homeland security (MDM)." DEP'T OF HOMELAND SEC., DHS DISINFORMATION GOVERNANCE BOARD CHARTER 7 (Feb. 24, 2022), https://americansforprosperity.org/wp-content/uploads/2023/03/DHS-Disinfo-Board-Interim-Response-12-9-22.pdf. The charter provided no definition for these terms.

[169] DISINFORMATION STOPS WITH YOU, *supra*.

[170] GAO-24-107600, FOREIGN DISINFORMATION: DEFINING AND DETECTING THREATS, *supra*.

[171] In 2021, a DHS internal memo used "disinformation" to reference "any of the mis-, dis-, or mal-information, or other terms of art that refer to false information that is intentionally or inadvertently injected into the information environment." ORGANIZING DHS EFFORTS TO COUNTER DISINFORMATION, *supra,* at 1.

[172] Such was the case involving the FBI's COINTELPRO program, whereby First Amendment-protected activities were sometimes labeled as furthering foreign propaganda efforts, justifying agency activities to discredit Americans, like Dr. Martin Luther King Jr. *See* SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, U.S. SEN., BOOK IV: SUPPLEMENTARY DETAILED STAFF REPORTS ON FOREIGN AND MILITARY INTELLIGENCE, S.Rep. No. 94-755, 94TH CONG.III.D (1976). Specifically, the FBI used unlawful techniques to investigate civil rights leaders and activists, who were alleged to have been furthering the foreign

It is also unclear *who* is determining what content or information is "disinformation;" and what, if any, internal review process exists to ensure decisions are not made in a political or discriminatory fashion.[173] This concern is magnified when the subjective definition of "disinformation" is connected to domestic terrorism. Indeed, the government divides domestic terrorism actors by ideology, such as anti-government and anti-authority violent extremism and racially and ethnically motivated violent extremism.[174] Because the government links domestic terrorism with ideology, countering disinformation could overlap with otherwise lawful beliefs or behaviors. For example, discourse surrounding the origins of the COVID-19 virus could subjectively be labeled as disinformation. [175]

Countering disinformation, as it is broadly defined, with respect to specific groups based on ideology therefore presents heightened risks. The risks posed by subjective terminologies—and the ability for agencies to apply disinformation (and FMI) and domestic terrorism terminologies broadly—were aggravated by the fact that broad or ill-defined authorities also allow agencies to justify almost anything as a threat that warrants agency attention. DHS's statutory authorities allow for extensive information sharing efforts on many different types of threats and issues.[176] Similarly, CISA's statutory authorities enable it to work on threats to critical infrastructure, a concept which is itself subject to broad interpretation.[177]

2. Counter-Disinformation Efforts Were Diffused Across Numerous Agencies and Components

The risks discussed above were exacerbated by the sheer number of agencies and components involved in counter-disinformation work. The White House's Information Integrity Research and Development Interagency Working Group worked on efforts to combat "misinformation and

ideology of communism, in the name of countering domestic security threats. The Committee found that Americans' rights were violated under specific programs focused on countering foreign influence, *Id.* at 215 ("Nor was this the only First Amendment right violated by the Bureau. In addition to attempting to prevent people from joining or continuing to be members in target organizations, the Bureau tried to "deter or counteract" what it called "propaganda"- the expression of ideas which it considered dangerous. Thus, the originating document for the "Black Nationalist" COINTELPRO noted that "consideration should be given to techniques to preclude" leaders of the target organizations "from spreading their philosophy publicly or through various mass communication media.""").

[173] Throughout this investigation, no agency produced information relevant to the issue of how "disinformation" is labeled and reviewed, and whether there is any redress process for impacted parties.

[174] *See also* FED. BUREAU OF INVESTIGATION & DEP'T OF HOMELAND SEC., STRATEGIC INTELLIGENCE ASSESSMENT AND DATA ON DOMESTIC TERRORISM, (June 2023), https://www.fbi.gov/file-repository/counterterrorism/fbi-dhs-domestic-terrorism-strategic-report-2023.pdf/view; *See also* DEP'T OF JUSTICE, JUSTICE MANUAL, rule 9-2.137 (Nov. 2022).

[175] *See e.g., Summary of Terrorism Threat to the U.S. Homeland, supra.* ("There is widespread online proliferation of false or misleading narratives regarding unsubstantiated widespread election fraud and COVID-19.").

[176] *See* 6 U.S.C. § 481-486.

[177] *See* 6 U.S.C. § 652(c) and NATIONAL SECURITY MEMORANDUM ON CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE/NSM-22 (Apr. 20, 2024) [hereinafter NSM-22]. *See also* Maggie Miller, *Cyber agency beefing up disinformation, misinformation team*, THE HILL (Nov. 10, 2021) (quoting the then-CISA Director, "One could argue we're in the business of critical infrastructure, and the most critical infrastructure is our cognitive infrastructure, so building that resilience to misinformation and disinformation, I think, is incredibly important.").

disinformation" and received input from 26 different federal agencies and offices.[178] The 2021 Implementation Plan itself tasked six agencies with this work in addition to the Domestic Policy Council at the White House; these included the FBI, CIA, State, DHS, Department of Education, and USAID.[179]

Within DHS alone, the DGB charter revealed that multiple entities were involved in the counter-disinformation space, including the Management Directorate, Office of Intelligence and Analysis, Science and Technology Directorate, CISA, Federal Emergency Management Agency, and U.S. Customs and Border Protection. The charter provided that "Department Components will lead on operational responses to MDM in their relevant mission spaces."[180] A 2022 DHS OIG report identified additional components engaged in counter-disinformation work.[181]

Risks were exacerbated by the sheer number of agencies and components involved in counter-disinformation work. The White House's Interagency Working Group for "Information Integrity Research and Development" included 26 different federal agencies and offices in efforts to combat "misinformation and disinformation."

DOJ's Counterintelligence and Export Control Section and National Security Cyber Section of the National Security Division worked on investigating and prosecuting foreign government-operated social media operations directing disinformation to U.S. audiences.[182] DOJ's National Institute of Justice (NIJ) funded a range of disinformation-related grants.[183]The FBI's FITF served as the FBI's central coordinating entity for counter-FMI activities until February 2025.[184][185]

Other agency units targeted foreign malign actors who used a variety of tactics, including disinformation, to influence the United States. In ODNI, FMIC's mission is to serve "as the primary U.S. government organization for integrating intelligence pertaining to FMI, including on election security."[186] State's GEC was focused on countering foreign state and non-state

[178] *See* ROADMAP FOR RESEARCHERS ON PRIORITIES RELATED TO INFORMATION INTEGRITY RESEARCH AND DEVELOPMENT, *supra,* at 8.
[179] 2021 IMPLEMENTATION PLAN, *supra,* at § 1.3.1d, 2.1.2, and 4.1.1d.
[180] DHS DISINFORMATION GOVERNANCE BOARD CHARTER, *supra.*
[181] DHS NEEDS A UNIFIED STRATEGY, *supra,* at 8, 12.
[182] DOJ OIG REPORT ON FMI, *supra,* at 4. The report states "NSD's [Counterintelligence and Export Control Section] is the lead NSD office for responding to foreign malign influence threats." *Id.* at 23.
[183] *See, e.g., NIJ FY22 Research and Evaluation on Domestic Radicalization and Violent Extremism,* NAT'L INST. OF JUST., https://nij.ojp.gov/funding/opportunities/o-nij-2022-171193 (last visited July 31, 2026). NIJ made two awards for 2022: *Understanding and Responding to Domestic Extremism Financing* and *Understanding the Complete Spectrum of the Left-Wing and Environmental Movement: A Data Driven Approach* – the proposals can be read at the above link.
[184] *Combating Foreign Influence, supra;* U.S. DEP'T OF JUST., OFF. OF THE ATT'Y GEN., GENERAL POLICY REGARDING CHARGING, PLEA NEGOTIATIONS, AND SENTENCING 4 (Feb. 5, 2025), https://www.justice.gov/ag/media/1388541/dl.
[185] *See* Background section for examples from the House Subcommittee Weaponization report of FBI personnel working with FITF flagged specific posts or content with a social media company for its review.
[186] Michael E. DeVine, *The Intelligence Community's Foreign Malign Influence Center,* CONG. RSCH. SERVICES (Nov. 27, 2024), https://www.congress.gov/crs-product/IF12470.

disinformation "targeting the United States and U.S. interests."[187] The GEC had its own Counterterrorism Division focused on countering terrorist propaganda and a Technology Engagement Division whose activities included "working with social media companies and the tech industry."[188] USAID provided counter-disinformation training to its employees and funded disinformation-related programs[189] USAID also funded the Consortium for Elections and Political Process Strengthening's Counter Disinformation Guide, a global database of organizations, projects, and donors working on efforts to counter disinformation.[190]

The absence of specific social media engagement policies may have contributed to *ad hoc* government counter-disinformation efforts that lacked transparency and threatened Americans' civil liberties.

B. Concerns with Counter-Disinformation Engagements

Until 2024, no agency that was a subject of PCLOB's investigation had a formal policy regarding engagement with social media companies concerning disinformation.[191] The absence of specific social media engagement policies may have contributed to *ad hoc* government counter-disinformation efforts that lacked transparency and threatened Americans' civil liberties.

1. Countering Foreign Disinformation Can Have National Security Value, But Presents Risks

The government often premised previous counter-disinformation efforts on the need to counter FMI, explaining that foreign actors may post disinformation to sow discord and distrust.[192] Efforts to counter FMI have taken a number of forms, including "debunking" or producing accurate information. For example, Customs and Border Protection has combated border crossing

[187] Matthew C. Weed, *Global Engagement Center: Background and Issues,* CONG. RSCH. SERVICES 1 (Aug. 4, 2017), https://www.congress.gov/crs-product/IN10744.
[188] GAO-24-107600, FOREIGN DISINFORMATION: DEFINING AND DETECTING THREATS, *supra*, at 6; Interim Staff Report on H. Comm. on Small Business, Small Business: Instruments and Casualties of the Censorship-Industrial Complex 11 (2024), https://smallbusiness.house.gov/uploadedfiles/house_committee_on_small_business_-_cic_report_september_2024.pdf.
[189] *See* 22 U.S.C. § 6592 ("The Administrator of the Agency for International Development, appointed pursuant to section 2384(a) of this title, shall report to and be under the direct authority and foreign policy guidance of the Secretary of State.").
[190] *Countering Disinformation Guide*, GLOBAL DEMOCRACY COALITION (last accessed Oct. 8, 2026), https://globaldemocracycoalition.org/library/countering-disinformation-guide/; *Grant to Consortium for Elections & Political Process Strengthening,* USASPENDING.GOV, https://www.usaspending.gov/award/ASST_NON_AID521LA1700002_7200 (last visited Oct. 8, 2026).
[191] As part of its investigation, PCLOB requested Government policies regarding social media engagement from ODNI, DHS, State, and DOJ. CISA had specific protocols for information sharing for the time periods around the 2018 and 2020 elections. As discussed above, State reported that it issued a policy in 2021 about engaging online platforms regarding content on third-party user accounts but not specifically with respect to the topic of foreign disinformation. In its 2024 review, the DOJ Office of the Inspector General found that while DOJ components shared FMI information with each other effectively, "neither DOJ nor the FBI had a specific policy or guidance applicable to information sharing with social media companies until February 2024." DOJ IG REPORT ON FMI, *supra,* at i.
[192] DOJ IG REPORT ON FMI, *supra,* at iii.

disinformation by launching a digital ad campaign, "Say No to the Coyote," to communicate that smugglers are lying, and that entering the United States illegally is a crime.[193] Such efforts can alert the public to foreign sources seeking to mislead them in ways that harm U.S. national security.

In 2022, the Department of War (then DOD), acknowledged a Chinese disinformation campaign against an Australian company seeking to establish production capacity for rare earth minerals in Texas.[194] The campaign "used inauthentic social media and forum accounts, including those posing as residents in Texas to feign concern over environmental and health issues surrounding the plant, including via posts to a public social media group predisposed to be receptive to that content."[195] In response, the Department of War "provide[d] accurate information" about supply chain investments and publicized an agreement to "establish a [new] modern and world class" rare earth element processing facility which would conform with all federal, state, and local government environmental and health safety regulations.[196]

The government has also used criminal indictments and economic sanctions to counter foreign disinformation, thus providing public transparency around FMI efforts targeting the United States. For example, on November 18, 2021, DOJ unsealed an indictment charging two affiliates of "Emennet Pasargad," an Iranian cyber security company, for their involvement in an FMI campaign, which disseminated "threatening email messages to intimidate and interfere with voters; creating and disseminating a video containing disinformation about purported election infrastructure vulnerabilities; attempting to access, without authorization, several states' voting-related websites; and successfully gaining unauthorized access to a U.S. media company's computer network that, if not for successful FBI and victim company efforts to mitigate, would have provided the conspirators another vehicle to disseminate false claims after the election."[197] In its press release, DOJ stated that the allegations in the unsealed indictment "illustrate how foreign disinformation campaigns operate and seek to influence the American public" and reaffirmed that the government has several tools to disrupt FMI efforts, including bringing criminal charges. On September 27, 2024, the Treasury Department announced that it sanctioned several related actors.[198]

---

[193] FINAL REPORT, *supra.* at 21.
[194] *Reports of Disinformation Campaign Against Rare Earth Processing Facilities,* DEP'T OF WAR (June 28, 2022), https://www.war.gov/News/Releases/Release/Article/3077280/reports-of-disinformation-campaign-against-rare-earth-processing-facilities/.
[195] *Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance*, MANDIANT THREAT INTEL. (June 28, 2022), https://cloud.google.com/blog/topics/threat-intelligence/dragonbridge-targets-rare-earths-mining-companies.
[196] *Reports of Disinformation Campaign Against Rare Earth Processing Facilities, supra.*
[197] *Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election*, DEP'T OF JUST. (Nov. 18, 2021), https://www.justice.gov/archives/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed.
[198] *Treasury Sanctions Iranian Regime Agents Attempting to Interfere in U.S. Elections,* DEP'T OF TREASURY (Sep. 27, 2024), https://home.treasury.gov/news/press-releases/jy2621.

In a 2024 case, DOJ indicted two employees of Russia Today, a media outlet operating in the United States that is funded and directed by the Russian government, for using almost $10 million to "covertly finance and direct [...] online content creation" across several social media platforms on issues such as immigration, inflation, and foreign policy to influence American public opinion and amplify domestic divisions.[199]

Transparency and counter speech—whether through affirmative government speech debunking false claims, criminal indictment, or other means—can provide countermeasures to foreign disinformation with minimal impact on Americans' free speech.

Transparency and counter speech—whether through affirmative government speech debunking false claims, criminal indictment, or other means—can provide countermeasures to foreign disinformation with minimal impact on Americans' free speech.[200] The cases above present specific examples.

2. Counter-Disinformation Engagements Were *Ad Hoc* and Lacked Transparency

Formal policies faithfully enforced are crucial to the protection of privacy and civil liberties because they help ensure that the government operates fairly and consistently. Transparency of policies and activities ensures public trust and prevents abuse by opening government operations to public oversight. Many government engagements with social media companies regarding disinformation, however, occurred through private communication, and lacked both specific governing policies and appropriate legal review or supervision by accountable leadership officials.[201]

[199] *Press Release: Two RT Employees Indicted For Covertly Funding And Directing U.S. Company That Published Thousands Of Videos In Furtherance Of Russian Interests,* DEP'T OF JUST. (Sept 4, 2024), https://www.justice.gov/usao-sdny/pr/two-rt-employees-indicted-covertly-funding-and-directing-us-company-published.

[200] The Department of Justice recently issued a press release suggesting it would actively enforce federal laws designed to enforce transparency around foreign influence. *See Liability for Unregistered Foreign Agents,* DEP'T OF JUST. (Sept. 16, 2026), https://www.justice.gov/opa/pr/liability-unregistered-foreign-agents ("Two such federal laws — the Foreign Agents Registration Act, known as FARA, and 18 U.S.C. § 951 — impose disclosure or notification obligations when a person acts in the United States as an agent of a foreign principal or foreign government. These obligations aid in stopping foreign governments or their representatives from using undisclosed agents, intermediaries, false affiliations, covert funding, or other deceptive activities to illegally influence public debate, suborn sedition, or interfere with official proceedings. Both citizens and noncitizens are reminded that anyone who violates FARA or § 951 may face federal civil or criminal liability. If a person acts as an agent of any foreign power to carry out any public activity, including (but not limited to) public demonstrations designed to further the propaganda or other goals of the foreign power, he or she must register with or notify the appropriate federal authorities. Failure to do so may result in significant civil or criminal sanctions, up to and including a maximum of five years in prison.").

[201] *See* discussion below of FBI policies issued in 2024 addressing some of these issues.

Formal policies faithfully enforced are crucial to protection of privacy and civil liberties because they help ensure that the government operates fairly and consistently.

In 2021, for example, White House officials attempted to convince Facebook to change its approach to what they had determined to be COVID-19 related disinformation.[202] White House staff suggested, in email communications with Facebook, that the platform was at least in part responsible for political violence and pressured it to make an "algorithmic shift."[203] Days later, a White House official reiterated this position in an email requesting clarification on why certain vaccine-related content had not been removed or demoted: "And we've gone a million rounds on this in other contexts to pardon what may seem like deja vu [sic]…. Not for nothing but last time we did this dance, it ended in an insurrection," referring to the violence at the U.S. Capitol on January 6, 2021.[204] These communications, connecting the failure to suppress disinformation with violence, were made public years later.

Similarly, in 2021, White House staff expressed concern about books promoting anti-vaccination stances during the COVID-19 pandemic.[205] A series of emails revealed that Amazon Web Services (AWS) staff attempted to navigate "negative feedback" and "criticism" from the government, creating the need for a "high priority" response.[206] AWS staff temporarily placed an *ad hoc* "extremist" Do Not Promote tag normally reserved for books containing extremist content on the backend for 43 books.[207] The Do Not Promote tag restricts the promotion of content on the platform but does not prevent the material from being purchased.[208] Eventually, AWS created a

[202] J.A., Ex. A at 666-671 (Emails between Facebook staff and the White House), *Murthy v. Missouri*, 603 U.S. 43 (2024), https://www.supremecourt.gov/DocketPDF/23/23-411/293781/20231219192444120_23-411%20J.A.%20-%20Murthy%20FILE.pdf.

[203] *See, e.g.,* J.A., Ex. A at 670-671 (Email from the White House to Facebook staff), *Murthy v. Missouri*, 603 U.S. 43 (2024), https://www.supremecourt.gov/DocketPDF/23/23-411/293781/20231219192444120_23-411%20J.A.%20-%20Murthy%20FILE.pdf. In an April 9, 2021 email, a White House official wrote, "[A]t the end of the day, I care mostly about what actions and changes you're making to ensure you're not making our country's vaccine hesitancy problem worse …. In the electoral context, you tested and deployed an algorithmic shift that promoted quality news and information about the election …. You only did this, however, after an election that you helped increase skepticism in, and an insurrection which was plotted, in large part, on your platform. And then you turned it back off. I want some assurances, based on data, that you are not doing the same thing again here." *Id.* at 671.

[204] *Id.* at 697-698. Subsequent internal Facebook emails suggest that Facebook employees found the tenor of these communications upsetting—describing it as "harassment" and "terribly galling," however, the company ultimately did not feel completely strong-armed into complying with all the demands made. WEAPONIZATION SUBCOMMITTEE FINAL REPORT, *supra,* at 642 (Ex. 76) (emails from a Meta official to others at Facebook about the conversations with the White House). In responses to the Administration, Facebook staff cited the platform's policies, rather than the preferences of Government officials, as authoritative. *Id*. at 576 (Ex. 63) (emails between Facebook's staff about how "there is likely a significant gap between what the [White House] would like us to remove and what we are comfortable removing" based on Facebook's content policies).

[205] *Id.* at 869-873 (Ex. 131) (emails among Amazon employees about changes to "address negative feedback we're getting from the Whitehouse's (sic) Coronavirus Taskforce").

[206] *Id.*

[207] *Id.*

[208] *Id.* at 871-873 (Exhibit 131).

specific classifier for "anti-vax content" and updated their standard operating procedures regarding anti-vaccination content on the platform. The email exchanges, however, suggest AWS staff acted in response to substantial pressure from White House staff through informal channels. Specifically, AWS staff's initial response was to expand the use of a deplatforming tool to address content not clearly connected to the counter-extremist goals for which it was originally created.[209]

Transparency of policies and activities ensures public trust and prevents abuse by opening government operations to public oversight. Government engagement with social media companies regarding disinformation, however, appeared to occur behind the scenes, lacking both specific governing policies and appropriate legal review or supervision by accountable leadership officials.

From a civil liberties perspective, these efforts were highly problematic. First, the government did not publicly acknowledge at the time, either to Congress or through public disclosure,[210] that it was engaging in these sorts of counter-disinformation efforts (i.e., pressuring companies to either remove content or deprioritize particular books). Not until documents were disclosed in the lower courts for the *Murthy* case and were released as part of a congressional investigation did the government publicly convey the extent of its engagement with social media companies on counter-disinformation work. Even after the disclosure of these documents, the government has not fully explained how it did, or whether it continues to, flag social media posts containing disinformation to social media companies or what policies, if any, it follows for these engagements.

Nor did these communications explain why the requested speech suppression was justified for national security or to prevent violence. Instead, they illustrate the dangers of subjective interpretations of what constitutes disinformation.

[209] *Id.* at 870-871 (Ex. 131). Internal discussion notes appearing to be from Facebook's Product Policy team entertain the analogous scenario to that within AWS, "stemming from the continued criticism to our approach from the US administration" to "Covid and vaccine misinformation." Brief of Rep. Jim Jordan et al. as Amici Curiae Supporting Appellees, Ex. 9 at 94, *Missouri v. Biden,* 83 F.4th 350 (5th Cir. 2023) (No. 224-1). The notes suggest that the team considered counting COVID-19 "misinformation and harm" and vaccine "widely debunked hoaxes" "as severe strikes," subjecting them to more rapid adverse treatment. The notes state, however: "We do not recommend this measure, as we reserve severe strikes for the worst integrity violations (e.g., terrorism, CEI [child exploitation images], human exploitation)." WEAPONIZATION SUBCOMMITTEE FINAL REPORT, *supra,* at 321 (Ex. 29) (document from Facebook employees listing policy options and recommendations on how "be more aggressive against COVID and vaccine misinformation").

[210] For example, Meta provides semi-annual reports on government requests for user data, including legal process and emergency disclosure requests on their website, *See Government requests for user data*, META TRANSPARENCY CTR., https://transparency.meta.com/reports/government-data-requests/ (last visited July 2, 2026).

3. Policies Regarding Evaluating the Foreignness of Speakers Were Inconsistent Across the Government

Constitutional protection for speech is determined in part by the identity and location of the speaker.[211] While Americans' freedom of speech is protected by the First Amendment, speech by a non-U.S. person located outside the United States is not constitutionally protected.[212] Determining the location, nationality, or identity of the source of online content or activity is crucial, therefore, to the protection of Americans' speech.

The process for determining the location, nationality, or identity of the source of online content or activity is referred to as attribution.[213] Attribution can be based on technical indicators, such as the IP address of the source, contextual and linguistic information, and other sources of intelligence.[214] Because sophisticated foreign actors often use techniques to obscure their physical location, attribution can be difficult—even for social media companies.[215] Attribution can be even more difficult for the government, which typically lacks back-end access to companies' data about social media users' locations.

In order to determine foreign attribution, some agencies have used methods such as:

- Using "computerized analyses of social media networks, linguistic and regional expert analyses, and assessing foreign media narratives;"
- Assessing posts' "content and associated data such as location or timestamps;"

---

[211] *See Agency for Int'l Dev. v. Alliance for Open Society Int'l, Inc.,* 591 U.S. 430, 433 (2020) ("It is long settled as a matter of American constitutional law that foreign citizens outside U. S. territory do not possess rights under the U. S. Constitution.").

[212] Even then, exceptions such as incitement to imminent violence, described below, may apply. Other permutations of speakers and locations may present more difficult questions, such as when a person located in the United States repeats foreign-originating speech or when a U.S. citizen claims the right to hear foreign-originating speech.

[213] Traditionally, the term "attribution" referred to identifying the source of cyber-attacks or exploitations. *See,* e.g., David D. Clark and Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SEC. J. 1-2, https://harvardnsj.org/wp-content/uploads/sites/13/2011/03/Vol.-2_Clark-Landau_Final-Version.pdf. Attributing social media campaigns or influence operations has similarities to traditional attribution but also relies on different types of information and evidence. *See*, e.g., James Pamment and Victoria Smith, *Attributing Information Influence Operations,* NATO STRATEGIC COMMUNICATIONS CTR. OF EXCELLENCE, 4 (2022), https://stratcomcoe.org/publications/attributing-information-influence-operations-identifying-those-responsible-for-malicious-behaviour-online/244; DEPT. OF HOMELAND SEC., PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM, COMBATTING TARGETED DISINFORMATION CAMPAIGNS, 15, (2021), https://www.dhs.gov/sites/default/files/publications/phase_ii_-_combatting_targeted_disinformation.pdf.

[214] *Attributing Information Influence Operations*, *supra*, at 15.

[215] Joyce Hakmeh, Harriet Moynihan, and Nayana Prakash, *Holding state-sponsored hackers and other cyber proxies to account,* CHATHAM HOUSE, 2 (2026), https://www.chathamhouse.org/sites/default/files/2026-03/2026-03-25-holding-cyber-proxies-to-account-hakmeh-et-al_0.pdf ("The wide variety of Russian or Russia-linked cyber proxies, differing in their organization, motivation and relationship to the state, creates a spectrum of threat actors that complicates attribution and benefits Russia by enabling calibrated deniability and facilitating the evasion of sanctions."). Internal Facebook communications preceding the 2020 election, for example, reveal that in response to a proposal to remove leaked information "when linked to a foreign interference operation for a government," the conclusion was that they "would often not have the evidence...." WEAPONIZATION SUBCOMMITTEE FINAL REPORT, *supra,* at 1388-1389 (Ex. 81) (email among Facebook employees in September 2020 asking what Facebook would do with leaked information linked to an FMI operation).

- Analyzing "social media content by filtering for certain words or phrases, searching for inconsistencies in profile information, and looking for evidence of nonhuman behavior;"
- Identifying proxy sources (e.g., troll farms) and cyber-enabled sources (e.g., spoofed websites). [216]

These methods of attribution, however, are complicated, time-consuming and can be unreliable, especially without back-end data.[217]

Notwithstanding that the government initially premised much of its counter-disinformation work on the threat of FMI, PCLOB's investigation could not determine whether and to what extent the government actually engaged in foreignness determinations before flagging content for social media companies.[218] No policy was provided to PCLOB that required them to do so before 2024, and even then only the FBI's FMI policy required such determinations.[219] In addition, neither the White House nor CISA appeared to differentiate between information originating in the U.S. versus abroad in their counter-disinformation efforts.[220]

---

[216] GAO-24-107600, FOREIGN DISINFORMATION: DEFINING AND DETECTING THREATS, *supra,* at 11 (addressing State, DHS's I&A, and DOD).

[217] *See* Camille François, Actors, Behaviors, Content: A Disinformation ABC, ANNENBERG PUB. POL'Y CTR., UNI. OF PENNSYLVANIA, 2-3 (Sep. 2019), https://www.annenbergpublicpolicycenter.org/wp-content/uploads/ABC_Framework_TWG_Francois_Sept_2019.pdf ("Throughout the technology industry, detection and enforcement of this vector of viral deception campaigns rely on the cat-and-mouse game of a) identifying threat actors willing and able to covertly manipulate public discourse and b) keeping those actors from leveraging social media to do so, as they refine their strategies to evade detection."). Another important issue is how the government should appropriately identify or respond to online foreign speech that is then re-posted domestically. The agencies currently treat this as domestic speech.

[218] In July 2024, the DOJ Office of Inspector General (OIG) published an Evaluation of the U.S Department of Justice Efforts to Coordinate Information Sharing About Foreign Malign Threats to U.S. Elections. Because the OIG's evaluation focused on DOJ's information sharing about FMI threats to U.S. elections, it did not evaluate the extent to which DOJ shared information about domestic actors with social media companies. In the report, a former DOJ Deputy Assistant Attorney General 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. DOJ OIG REPORT ON FMI, *supra*.

[219] *But see* GAO-24-107600, FOREIGN DISINFORMATION: DEFINING AND DETECTING THREATS, *supra,* at 5 (stating that as of September 2024, "State, DHS, and DOD officials told us they do not counter the actions of U.S. citizens who create or spread disinformation. Instead, these agencies either focus on countering disinformation threats that have a foreign origin, or they broadly distribute accurate information to educate the public, set the record straight, or build resilience to disinformation."). The report did not explain how these agencies were able to or systematically attempted to distinguish foreign from domestic speech.

[220] *See* THE WEAPONIZATION OF THE "DISINFORMATION" PSEUDO-EXPERTS AND BUREAUCRATS, *supra*, at 33. (In depositions, the former CISA director acknowledged: "[W]e certainly would look to the intelligence community if they made a determination on foreign threat actor intelligence. But, again, as these things pop up, […] it doesn't necessarily matter whether it's foreign or domestic. Again, our authorities are rooted in the Homeland Security Act, which enables us to act on domestic or foreign threats. And, again, they don't come waving a flag" and "I don't recall the moment in time or the periods of time within which we were thinking about the distinction between domestic and foreign interference."). PCLOB did not have access to the primary source document. This excerpt was included in the House Subcommittee Report. Similarly, DHS connected the amplification of disinformation regarding the 2020 presidential election and COVID-19 pandemic by domestic as well as foreign actors to threats and acts of violence without information on source origin or attribution. *Summary of Terrorism Threat to the U.S.*

The FBI stated that it does engage in foreignness determinations (or attribution of foreign actors) before flagging accounts for social media companies.[221] The FBI also stated that it derives activity "based off of technical indicators and would only become content informed post foreign adversary identification."[222] This means that the FBI would be "content agnostic" until foreignness is confirmed.[223] This is consistent with findings by the DOJ OIG, who reported that officials confirmed that the FBI takes an "actor-driven versus content-driven approach" and does not monitor social media content on platforms as it relates to FMI, nor does it investigate specific narratives related to FMI being spread online.[224]

Based on PCLOB's review of documents shared with the agency, in 2023, DOJ began developing a standard operating procedure (SOP), later implemented in 2024, for disseminating FMI information with social media companies. Described in more detail below, part of the SOP required employees to identify "specific, credible, and articulable facts that provide high confidence for assessing that the [FMI] activity is attributed to a foreign government, foreign nonstate actor or their proxy."[225] It does not discuss how a "proxy" who is a domestic speaker should be addressed, however.

The lack of policies requiring attribution, combined with the failure to provide safeguards or checks, most certainly contributed to a negative impact on the civil liberties of domestic speakers.

To be sure, foreign malign actors routinely attempt to disguise their efforts as domestic speech to avail themselves of Americans' free speech protections.[226] This likely paved the way from a policy focused on countering FMI, including foreign disinformation, to a broader "counter-disinformation" effort. But the lack of policies requiring attribution, combined with the failure to provide safeguards or checks, most certainly contributed to a negative impact on the civil liberties of domestic speakers.

Homeland, supra. Videotaped Dep. of Brian J. Scully at 15-16, *Missouri v. Biden,* 680 F. Supp. 630 (W.D. La. 2022) (No. 209-1). ("So CISA does not do attribution. We didn't do analysis of what we received from election officials. So we would not know what percentage were foreign derived.") *Id.* at 122-123. *See also* GAO-24-107600, FOREIGN DISINFORMATION: DEFINING AND DETECTING THREATS, *supra,* at 7 ("CISA officials told us they do not distinguish between disinformation threats originating in the U.S. or abroad because they focus on building resilience to foreign malign influence operations to reduce risks to U.S. election infrastructure.").

[221] Responses to PCLOB from the FBI (Sept. 2026).

[222] *Id.*

[223] *Id.* For example, an online social media account posing as an American but run by a known or attributed foreign adversary (or its proxies) might be flagged by the FBI regardless of whether it was posting true information or disinformation. *Id.*

[224] DOJ OIG REPORT ON FMI, *supra,* at 16.

[225] FED. BUREAU OF INVESTIGATION, *Providing Foreign Malign Influence Threat Information, supra.*

[226] FMI PRIMER, DEP'T OF STATE, FOREIGN MALIGN INFLUENCE CTR. 1 (Apr. 2024), https://www.dni.gov/files/FMIC/documents/products/04-25-24_Report_FMI-Primer-Public-Release.pdf.

4. Counter-Disinformation Efforts Failed to Consider Whether Targeted Speech Was Otherwise Protected

Just as foreign speech lacks constitutional protection, so too do certain "'historic and traditional categories [of expression]."[227] While the Supreme Court has rejected "as 'startling and dangerous' a 'free-floating test for First Amendment coverage . . . [based on] an *ad hoc* balancing of relative social costs and benefits,'" it has permitted content-based restrictions in several instances.[228] These include: advocacy intended and likely to incite imminent lawless action; obscenity; speech integral to criminal conduct; fraud or defamation; true threats; and narrow categories of false statements that inflict legally cognizable harm, such as fraudulent conspiracy to deprive citizens of their right to vote.[229]

There are many situations in which speech on social media would not be protected, regardless of the speaker. Laws prohibit the creation and dissemination of child sexual abuse material (CSAM),[230] for example, or the threat of mass violence at a U.S. location.[231] Federal law also prohibits conduct intended to deceive the public as to the time, place, and manner of elections.[232]

As discussed above, however, the social media contact policies provided to PCLOB did not expressly require government actors to consider whether the speech they considered to be disinformation fell within these specific categories.[233] Nor did processes exist for making these determinations.[234] As a result, documents that are now publicly available, some of which are

[227] *See United States v. Alvarez*, 567 U.S. 709, 716-17 (2012) (listing categories of speech that can be subject to restriction).
[228] *Id.*
[229] THE FIRST AMENDMENT: CATEGORIES OF SPEECH, CONG. RSCH. SERVICES (Mar. 28, 2024), https://www.congress.gov/crs_external_products/IF/PDF/IF11072/IF11072.4.pdf. A recent case raising these issues involves the removal by Apple of the "ICEBlock" application from the App store. Plaintiffs allege this removal was the result of pressure from the federal government. Defendants argue the speech was not protected, as it could result in the doxxing of federal agents. While the government's arguments at this stage focus on lack of standing and failure to plead a claim, the case may also raise questions about lawful speech if a purpose of the app is to obstruct law enforcement operations or incite violence. *See Aaron v. Bondi*, Case 1:25-cv-04250-DLF (D.D.C. 2026); *see also Rosado v. Bondi*, No. 1:26-cv-01532 (No. 26 C 1532 at 1-3, 6-7) (N.D. Ill. 2026).
[230] *See* 18 U.S.C. § 2251, 2252(2).
[231] 18 U.S.C. § 875(c) ("Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.").
[232] 18 U.S.C. § 245(2)(b)(1)(A) ("Whoever…intimidates or interferes with, or attempts to injure, intimidate or interfere with any person…voting or qualifying to vote…")
[233] Paradoxically, the charter of the Disinformation Governance Board suggests the DGB's purpose was to bring some order and "governance" to the wide array of counter-disinformation activities already happening across DHS. Such activities pre-dated the Board and presumably continued after the Board's swift dissolution. In addition to "lead[ing] on MDM-related operational responses and other efforts to counter MDM in their relevant mission spaces," the Board envisioned its role as "developing MDM-related guidance, best practices, and recommendations regarding: compliance with applicable constitutional, statutory, and regulatory obligations; [and] standards for and implementation of appropriate privacy, civil rights, and civil liberties protections[.]" *See* ORGANIZING DHS EFFORTS TO COUNTER DISINFORMATION, *supra, at* 1, 3.
[234] Legal challenges to the government's counter-disinformation engagements with social media companies have not assessed the content of the speech the government has sought to influence. *See., e.g., Murthy v. Missouri*, 603 U.S.

Documents that are now publicly available… show the government took steps to seek the suppression of relatively broad types of speech without concluding that they constituted "true threats" or incitement of "imminent lawless action."

described above, show the government took steps to seek the suppression of relatively broad types of speech without concluding that they constituted "true threats" or incitement of "imminent lawless action."[235]

C. Existing Policies Related to Social Media Engagement Were Insufficient for Counter-Disinformation Efforts

While the government had general policies governing First Amendment protections and information sharing, almost no agency had specific policies governing counter-disinformation engagements with social media companies before 2024.[236]

1. General Policies

a. Executive Order 12333

Agencies within the IC are governed by EO 12333.[237] Published in 1981, and amended by several subsequent executive orders, EO 12333 provides the framework for the government's intelligence activities, and requires certain procedures, protections, and oversight to protect privacy and civil liberties.[238] It establishes that the IC is only "authorized to collect, retain, or disseminate information concerning" U.S. persons if permitted by an agency's Attorney General guidelines and if the information falls under one of the categories outlined under EO 12333.[239] It "provides general authorization for the [IC agencies] to both send information to, and receive information from, private sector entities as part of its national security mission."[240] However, it does not dictate specific rules for doing so.

43, 51-53, 56 (2024) (Supreme Court analysis of several counter-disinformation fact patterns discussed earlier in this report).

[235] PCLOB does not express a view as to the legality of these actions. From a policy perspective, even if the social media companies acted as final decisionmaker, considerations of when the Government seeks to exert influence should respect the values of free speech and civil liberties.

[236] As discussed further below, CISA had specific policies for the time periods surrounding Election Day in 2018 and 2020. *See also* DOJ OIG Report on FMI ("Neither DOJ nor the FBI had a specific policy or guidance applicable to information sharing with social media companies until February 2024.").

[237] Exec. Order No. 12333.

[238] *Id.*

[239] *Id.* at § 2.3. Among other categories, Section 2.3 of EO 12333 permits collection, retention, dissemination of information concerning U.S. persons that is "publicly available or collected with the consent of the person concerned." The type of information discussed in this Report—publicly viewable social media posts—could presumably fall into this category. *Id.* at § 2.3(a).

[240] DOJ OIG REPORT ON FMI, *supra*, at 14.

b. Attorney General Guidelines

EO 12333 requires each IC element that collects, retains, or disseminates information concerning U.S. persons conduct such activities only in compliance with the Attorney General's approval, in consultation with the DNI.[241] Each such agency therefore has Attorney General Guidelines which, among other things, direct how the intelligence and information collected may be used and shared.[242] Like EO 12333, the Attorney General's Guidelines provide high-level guidance and do not specifically address disinformation or engagement with social media companies.

For example, the *Attorney General's Guidelines for Domestic FBI Operations* states that "the FBI must conduct its investigations and other activities in a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into the lives of law abiding people."[243] The Guidelines mandate that all FBI activities under the Guidelines must be "carried out in conformity with the Constitution and all applicable statutes, executive orders, Department of Justice regulations and policies and Attorney General Guidelines."[244] They expressly "do not authorize investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States."[245] Under its authorities to protect national security, the FBI is authorized to "provid[e] threat information and warnings" to other government entities and private entities.[246]

In describing these Attorney General Guidelines, the DOJ OIG recently explained that while they "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 foreign targets."[247]

ODNI's Attorney General Guidelines also require ODNI to perform its activities consistent with the Constitution and the laws of the United States, executive orders, and other presidential directives.[248] The Guidelines prohibit ODNI from collecting, accessing, obtaining, or maintaining, information concerning a U.S. person solely for monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States.[249]

Other agencies' Attorney General Guidelines contain similar high-level protections. DHS's I&A Program Guidelines prohibit personnel "under all circumstances from engaging in any intelligence

[241] Exec. Order No. 12333 § 1.3.
[242] *Id.*
[243] DEP'T OF JUST., THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 5 (2008).
[244] *Id.* at 13.
[245] *Id.*
[246] *Id.* at 8.
[247] DOJ OIG REPORT ON FMI, *supra*, at 16.
[248] OFF. OF THE DIR. OF NAT'L INTEL., INTELLIGENCE ACTIVITIES PROCEDURES APPROVED BY THE ATTORNEY GENERAL PURSUANT TO EXECUTIVE ORDER 12333 § 1.5 (Dec. 2020).
[249] *Id.*

activities, including the dissemination of information to the White House, for the purpose of affecting the political process in the United States, for the sole purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States. . ."[250] I&A personnel must be "regularly train[ed]" on "the civil rights, civil liberties, and privacy protections that apply" to United States person information.[251]

c. FBI Domestic Investigations and Operations Guide (DIOG)

The FBI also has a *Domestic Investigations and Operations Guide* (DIOG), an operational manual that puts the FBI's Attorney General Guidelines into practice for Bureau personnel.[252] It contains several sections devoted to First Amendment protections, which, among other things, discuss constitutionally protected speech.[253] The DIOG states that "individuals in the United States (and organizations comprised of such individuals) do not forfeit their First Amendment rights simply because they also engage in criminal activity or in conduct that threatens national security.[254] For example, an organization suspected of engaging in acts of domestic terrorism may also pursue legitimate political goals and may also engage in lawful means to achieve those goals."[255]

The DIOG does not mention disinformation or contacts with social media companies, but it does state that the FBI's activities must be done "for a valid law enforcement or national security purpose" and must be "conducted in a manner that does not unduly infringe upon the ability of the speaker to deliver his or her message" or "the ability of the audience to hear it."[256]

2. Policies Relating to Government Engagement with Social Media Companies

Since at least 2018, various components of the government have issued guidance regarding government engagement with social media companies.[257] While some were related to terrorism, the policies did not discuss disinformation or establish rules for protected speech deemed to be "disinformation."

---

[250] DEP'T OF HOMELAND SEC., OFF. OF INTEL. & ANALYSIS, INTELLIGENCE OVERSIGHT PROGRAM AND GUIDELINES 2 (Jan. 2017).
[251] *Id.* at 5.
[252] FED. BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE (2024).
[253] *Id.* at § 4.2.
[254] *Id.*
[255] *Id.*
[256] *Id.* at § 4.2.1.
[257] In 2015, DOJ's National Security Division drafted a memorandum entitled "Legal Limitations on U.S. Government Requests to Remove Content on Public Websites." It does not purport to be guidance governing officials' actions, and it is unclear if it was disseminated, and if so, to whom. The memorandum "considers the legal limitations on U.S. Government officials' requests that private technology companies remove content generated by their users, in particular content that may promote or facilitate terrorist activity." The memorandum did not mention disinformation and did not distinguish between foreign and domestic speech; it assumed that the speech and speaker were protected by the First Amendment. It concluded that "[g]overnment officials may educate technology companies regarding the problems or hazards that content that promotes or facilitates terrorist activity presents, and they may request that companies voluntarily take down such content from public websites. However, government officials should not explicitly or implicitly threaten the company with punishment in the form of adverse regulation, prosecution, or other sanctions.… Nor should the officials harass or intimidate the companies." DEP'T OF JUST., LEGAL LIMITATIONS ON U.S. GOVERNMENT REQUESTS TO REMOVE CONTENT ON PUBLIC WEBSITES (2015).

a. National Security Council

i. U.S. Guiding Principles for Engaging Technology Companies on the Use of the Internet for Terrorist Purposes (NSC, 2018)

In 2018, the NSC issued principles "intended to guide U.S. department and agency engagements with technology companies to support the companies' efforts to reduce the use of the internet for terrorist purposes and to prevent and counter terrorism online."[258] The guidelines related to terrorism generally and not domestic terrorism specifically[259] and openly encouraged government persuasion:

> Keeping in mind that companies are independent and not agents of the U.S. Government, departments and agencies may encourage technology companies to undertake or enhance voluntary measures to address the use of the internet for terrorist purposes, provided that departments and agencies avoid any explicit or implicit suggestion that [the government] will take coercive or punitive action against companies, whether through regulation, punishment, or other sanctions, if companies fail to comply with such requests. Such engagements should focus on encouraging and persuading companies voluntarily to take steps to enhance or enforce their own terms of service or terms of use, which generally prohibit using their platforms for terrorist purposes such as mobilization to commit violent acts, recruitment of individuals to terrorist organizations, or other criminal acts.[260]

Because "no department or agency is the U.S. government lead for these issues," the NSC assumed the "policy guidance and coordination" role.[261] The 2018 Guiding Principles acknowledged that "automated tools (e.g., artificial intelligence) used to analyze user data as well as flag and remove content in order to enforce company policies, particularly when overly broad criteria are used, could have negative implications for free expression and privacy" and stated that the government "should continue to advocate for human oversight and/or other mechanisms to ensure responsible use of automated tools."[262]The 2018 NSC principles did not reference disinformation and did not distinguish between foreign or domestic-origin terrorist content. They also did not discuss specific speech protections beyond advising agencies to avoid coercing private companies.[263]

---

[258] NAT'L SEC. COUNCIL, U.S GUIDING PRINCIPLES FOR ENGAGING TECHNOLOGY COMPANIES ON THE USE OF THE INTERNET FOR TERRORIST PURPOSES 1 (2018).

[259] This was consistent with the 2018 National Strategy to Counter Terrorism, which related to both foreign and domestic terrorism. *See* WHITE HOUSE, NATIONAL STRATEGY FOR COUNTERTERRORISM 2 (2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/10/NSCT.pdf.

[260] *Id.*

[261] *Id.* at 2.

[262] *Id.* at 1.

[263] The Guidelines stated that "[d]iscussions with companies regarding whether particular terrorist use of the Internet or accounts contravene federal criminal laws (such as material support, threats, or incitement to imminent violence) is the sole responsibility of the Department of Justice, including the Federal Bureau of Investigation." *Id.*

ii. Guiding Principles for Engaging Technology Companies on the Use of their Platforms to Host Terrorist Propaganda (NSC, May 2021)

In May 2021, the NSC issued updated Guiding Principles that were similar in tone and content to the 2018 document.[264] Like 2018, "these principles [were] intended to guide U.S. department and agency engagements with technology companies to support the companies' efforts to reduce the use of their platforms for hosting terrorist propaganda."[265] They did not mention disinformation or domestic terrorism specifically, and they continued the policy of "robust engagement between the Government and the private sector" technology companies that focused on "encouraging and persuading companies voluntarily to take steps to enhance or enforce their own terms of service or terms of use" to remove terrorist content from their platforms.[266]

iii. Regarding Certain Engagement with Technology Companies Regarding Online Content (January 2024) and the Framework for Engagement with Technology Companies Regarding Online Content (August 2024)

In January 2024, after the injunction in the *Murthy* litigation which had restricted certain communications with social media companies was stayed, NSC released interim guidance (2024 Interim Guidance) "to relevant departments and agencies to inform their direct engagement with technology companies on national security concerns and online content."[267] Unlike the previous guiding principles, the 2024 Interim Guidance was not limited to terrorism. Its stated purpose was to inform the direct engagement of relevant departments and agencies with technology companies "on national security and online content," but it noted "the same principles could be applied to a range of appropriate non-national security-focused engagements between relevant departments and agencies and technology companies."[268] Nevertheless, it repeatedly cited terrorism and violent extremism as reasons for government interaction with social media companies. The 2024 Interim Guidance asserted the responsibility of the U.S government to engage "appropriately" with technology companies to combat "grave threats" such as "terrorism and violent extremism, foreign election interference, marketing of deadly drugs like fentanyl, and more."[269] While avoiding the terms "disinformation" or "MDM," the 2024 Interim Guidance permitted government actors to notify technology companies of "false or misleading information designed to subvert U.S. national security efforts with respect to foreign conflicts."[270]

---

[264] NAT'L SEC. COUNCIL, GUIDING PRINCIPLES FOR ENGAGING TECHNOLOGY COMPANIES ON USE OF THEIR PLATFORMS TO HOST TERRORIST PROPAGANDA (2021).
[265] *Id.* at 1.
[266] *Id.*
[267] NAT'L SEC. COUNCIL, INTERIM GUIDANCE REGARDING CERTAIN ENGAGEMENT WITH TECHNOLOGY COMPANIES REGARDING ONLINE CONTENT 1 (Jan. 11, 2024). Although the final draft was circulated throughout the Administration by NSC staff, the interim guidance document was drafted collaboratively by NSC staff members and attorneys for many departments and agencies.
[268] *Id.*
[269] *Id.* at 2.
[270] *Id.* at 3.

The 2024 Interim Guidance stated that the government's engagement with social media companies could be both general and focused. Higher-level engagement would not be focused on "specific online content," but would instead be "aimed at educating and informing companies about evolving online threats such as … efforts to radicalize and mobilize Americans and others to engage in terrorism or violent extremism. . ."[271] In more "focused" engagements, the U.S. Government would "notify company personnel about specific content on their platforms that raises national security or other concerns" such as "online postings deliberately and explicitly intended to inspire Americans to join or support terrorist groups and lead them to kill or injure their fellow citizens. . . "[272] The NSC directed that both the general and focused engagements were permissible if such engagements were consistent with an agency's authorities and "so long as it is clear that the companies are free to make their own choices about what, if anything, those companies will do in response to the information they have received, and that no adverse consequences will result from whatever action the companies may or may not take."[273] With respect to the focused engagements concerning specific content, the NSC Guidance concluded it was permissible "*so long as U.S. Government participants do not coerce the companies to take any particular action with respect to any First Amendment-protected speech*."[274]

The 2024 Interim Guidance is notable for several reasons. As with the previous guiding principles, the 2024 Interim Guidance repeatedly directs the avoidance of explicit government coercion. It acknowledges that "even arguable instances" of government coercion to remove First Amendment-protected content "can have harmful effects."[275] But despite this recognition, the 2024 Interim Guidance does not explain what speech is First Amendment-protected (i.e., differentiating unlawful content such as CSAM or true threats), and does not distinguish between foreign and domestic speech. Indeed, it specifically permits government officials to notify technology companies about "false or misleading information designed to subvert U.S. national security efforts with respect to foreign conflicts," without consideration of whether the speech is made by Americans or by foreign actors.[276]

Also absent from the 2024 Interim Guidance is any instruction to confirm either the actual threat posed by the online speech or the "false or misleading" nature of it before raising it to the attention

[271] *Id.* at 2. This guidance was crafted for "relevant departments and agencies."
[272] *Id.*
[273] *Id.*
[274] *Id.* (emphasis in original). The Guidance suggested that: "When discussing particular posts, accounts, categories of posts, or content moderation policies with technology companies, it may be prudent to make the following disclaimer, either in writing or verbally:
'We are [sending this communication/sharing this information] with the understanding that [you/the technology company] will make your own independent determination as to whether and how to respond. No adverse action will be taken by [insert communicating department/agency] based on [your/its] decision about whether or how to respond.'" Id. at 3.
[275] *Id.* at 1-2.
[276] *Id.* at 3. While the purpose of the NSC Guidance might have been to limit legal exposure, no other companion policy guidance was issued directing prudential consideration of these issues.

of social media companies. And, except for specific limitations on government outreach about online content concerning interference with U.S. elections, the 2024 Interim Guidance sets no limits with respect to the speech that may be flagged for social media companies.[277] Despite the recognition of the "harmful effects" of coercion, the document does not mention the potential negative civil liberties effects of the types of government interaction it endorses.[278] The 2024 Interim Guidance states that it "will be reassessed in light of the [decision in *Murthy v Missouri*] and updated as appropriate."[279]

In August 2024, after the Supreme Court released its decision in *Murthy*, the NSC issued a *Framework for Engagement with Technology Companies Regarding Online Content* (2024 Framework).[280] The 2024 Framework stated that it "summarizes existing guidelines for relevant departments and agencies to inform their direct, voluntary engagements with technology companies on national security concerns and online content."[281] However, as with the 2024 Interim Guidance, it added that "the same principles could be applied to a range of appropriate non-national security focused engagements between relevant departments and agencies and technology companies."[282] Unlike the 2024 Interim Guidance, the 2024 Framework did not specifically mention the *Murthy* case.

The 2024 Framework is largely similar to the 2024 Interim Guidance with respect to policy and content.[283] Like the 2024 Interim Guidance, it did not distinguish between foreign and domestic speech. Nor did it distinguish between foreign and domestic security threats "necessitat[ing]" engagement with technology companies: "terrorism and violent extremism, foreign election interference, foreign malign influence, marketing of deadly drugs like fentanyl, and more…."[284]

The 2024 Framework, however, changes a key word in its operative language. Whereas the 2024 Interim Guidance states that engagement with technology companies about specific content on their platforms is generally permissible "*so long as U.S. Government participants do not* ***coerce*** *the companies to take any particular action with respect to any First Amendment-protected speech*," the 2024 Framework states content-specific engagement is permissible "*so long as U.S. Government participants do not* ***compel*** *the companies to take any particular action with respect to any First Amendment-protected speech*."[285] The 2024 Framework defines compulsion "in this

[277] *Id.*
[278] *Id.* at 4.
[279] *Id.* at 2.
[280] NAT'L SEC. COUNCIL, FRAMEWORK FOR ENGAGEMENT WITH TECHNOLOGY COMPANIES REGARDING ONLINE CONTENT (Aug. 2024).
[281] *Id.* at 1.
[282] *Id.*
[283] *Id.*
[284] *Id.*
[285] INTERIM GUIDANCE REGARDING CERTAIN ENGAGEMENT WITH TECHNOLOGY COMPANIES REGARDING ONLINE CONTENT, *supra,* at 2 (bold not in original); FRAMEWORK FOR ENGAGEMENT WITH TECHNOLOGY COMPANIES REGARDING ONLINE Content, *supra*, at 2 (bold emphasis added).

context" to mean "either coercive threats or equivalent significant encouragement—that is, positive inducements that overwhelm the recipient's independent judgment and render its decisions fairly attributable to the government."[286]

To PCLOB's knowledge, the 2024 Framework remains operative.

b. National Counterterrorism Center

i. NCTC Guidance on Outreach to the Private/Non-Governmental Sector (ODNI, February 2019)[287]

In February 2019, NCTC issued generalized guidance (NCTC Guidance) "govern[ing] outreach to non-governmental entities conducted by NCTC personnel acting in their official capacity."[288] The NCTC Guidance is not specific to engagement with social media companies and does not discuss domestic terrorism or disinformation. Instead, it provides high-level guidance for "articulat[ing] the purpose and intended outcome of the engagement, including which of NCTC's missions the engagement will help to advance." It directs officers to "obtain Group Chief approval prior to pursuing the engagement" and request guidance from NCTC Legal "[i]f a private sector entity contacts an NCTC officer to request an engagement or briefing—or if an NCTC officer is proactively seeking to engage with a private sector or non-governmental entity."[289]

c. Department of Homeland Security

i. Protocol for Election Day Information-Sharing by the Countering Foreign Influence Task Force (DHS, November 5, 2018)

On November 5, 2018, the DHS Office of the General Counsel and the Privacy Office issued guidance "regarding Election Day information-sharing activities" by DHS's Countering Foreign Influence Task Force (2018 Protocol).[290] The protocol explained that because the Countering Foreign Influence Task Force expects that in the period surrounding Election Day, "they will

[286] FRAMEWORK FOR ENGAGEMENT WITH TECHNOLOGY COMPANIES REGARDING ONLINE Content, *supra*, at 1.
[287] In addition to this policy, as PCLOB explained in its 2024 report on NCTC, in 2022 Congress curtailed NCTC's activities in support of domestic counterterrorism. PCLOB assessed that, consistent with congressional direction, NCTC had ceased the issuance of analytic contributions and products concerning terrorist threats without an identified foreign nexus. NCTC adopted internal guidance in 2023 to ensure compliance with the congressional direction. While the guidance did not pertain specifically to disinformation, it requires supervisor and legal review prior to outreach engagements related to domestic terrorism. PRIV. & C.L. OVERSIGHT BD., REPORT ON THE NATIONAL COUNTERTERRORISM CENTER 9-11, 21 n.117 (Dec. 10, 2024), https://documents.pclob.gov/prod/Documents/OversightReport/4ce093a4-d28d-4996-a35b-c11d18e19018/PCLOB%20FY2024%20NCTC%20REPORT%20-%20Completed%20508%20-%20Dec%2017%202024.pdf; *see also* NAT'L COUNTERTERRORISM CTR., NCTC GUIDANCE ON PROHIBITION ON NCTC ASSESSMENTS WITH NO FOREIGN NEXUS IN THE CLASSIFIED ANNEX TO THE INTELLIGENCE AUTHORIZATION ACT (June 2024); Responses to PCLOB from ODNI (Oct. 2026).
[288] NAT'L COUNTERTERRORISM CTR., NCTC GUIDANCE ON OUTREACH TO THE PRIVATE/NON-GOVERNMENTAL Sector 1 (Dec. 2018).
[289] *Id.* at 2.
[290] DEP'T OF HOMELAND SEC., PROTOCOL FOR ELECTION DAY INFORMATION-SHARING BY THE COUNTERING FOREIGN INFLUENCE TASK FORCE (Nov. 5, 2018).

receive information relating to social media posts that attempt to cause electoral fraud," the Countering Foreign Influence Task Force will plan to "serve as a 'switchboard,' using its relationships to provide this information to appropriate social media companies and suggesting that representatives of those companies consider reaching out to affected state of local officials directly."[291] The 2018 Protocol did not refer specifically to disinformation but it did give an example of the type of post it would pass to social media companies, "e.g. suggesting that people should not try to vote because polling places have run out of ballots."[292]

The 2018 Protocol provided actions the Countering Foreign Influence Task Force should take to protect privacy, such as asking the originating source to remove personally identifying information that is not necessary to understand the threat.[293] It also provided "First Amendment Protection Guidance," which included requiring the Task Force to make clear to all Election Day stakeholders from whom it receives information and with whom it shares information that "DHS makes no recommendations about how the information it shares should be handled."[294] The 2018 Protocol also stated explicitly that "[t]his protocol applies to information shared with DHS *that solely relates to foreign influence*."[295]

ii. Protocol for Sharing Elections-Related Information That Threatens Critical Infrastructure (CISA, October 29, 2020)

On October 29, 2020, DHS issued a new protocol to govern the upcoming election-related switchboarding (2020 Protocol).[296] This time, the protocol was issued by CISA's Office of the Chief Counsel and the Privacy Office.[297] Whereas the 2018 Protocol was specific to the Countering Foreign Influence Task Force, the 2020 Protocol related to CISA, including the Countering Foreign Influence Task Force.[298] In 2020, it was CISA that "plan[ned] to serve as a 'switchboard,' rather than the Countering Foreign Influence Task Force. [299] The 2020 Protocol now referred specifically to receiving "elections-related misinformation and disinformation that threatens critical infrastructure."[300]

The 2020 Protocol contained similar "privacy protection" and "First Amendment protection" guidance.[301] It differed from the 2018 Protocol, however, in two significant ways. First, it incorporated a new term, "qualifying information."[302] Under the 2020 Protocol, CISA would only

[291] *Id.* at 1.
[292] *Id.*
[293] *Id.*
[294] *Id.* at 2.
[295] *Id.* at 1, note 1 (emphasis added).
[296] DEP'T OF HOMELAND SEC., PROTOCOL FOR SHARING ELECTIONS-RELATED INFORMATION THAT THREATENS CRITICAL INFRASTRUCTURE (Oct. 29, 2020).
[297] *Id.*
[298] *Id.*
[299] *Id.* Based on the DHS OIG report from 2022, CISA had at least a standard disclaimer used for social media engagement. DHS NEEDS A UNIFIED STRATEGY, *supra,* at 6, n. 22.
[300] PROTOCOL FOR SHARING ELECTIONS-RELATED INFORMATION THAT THREATENS CRITICAL INFRASTRUCTURE, *supra.*
[301] *Id.* at 1-2.
[302] *Id.* at 1.

share reports about information that met three criteria: "(1) the information was reported by a trusted source ["a trusted source is an entity that is well-positioned to evaluate the particular information reported, including its truth or falsity (e.g. a local election official reporting information that conveys false facts about the time, place, or manner of voting in that jurisdiction)"]; (2) the information relates to elections; and (3) the information threatens critical infrastructure or access to critical infrastructure."[303]

Second, unlike the 2018 Protocol, the 2020 Protocol contained no limitation applying it only to information shared with DHS that solely relates to foreign influence.

d. Federal Bureau of Investigation

i. FBI FMI Standard Operating Procedure (FBI Counterintelligence Division, 2024) and Guidance for Engagement with Social Media Platforms (DOJ Office of the General Counsel, August 9, 2024)

In February 2024, shortly after the NSC released its 2024 Interim Guidance, the FBI's Counterintelligence Division issued an internal SOP titled *Providing Foreign Malign Influence Threat Information to Social Media Platforms* (FBI SOP).[304] The FBI SOP referenced and quoted the 2024 Interim Guidance, but unlike the NSC Guidance, the FBI SOP was limited to interactions with social media concerning FMI. The FBI SOP recognized countering FMI operations, including disinformation, as a priority and stated that an appropriate reason to disclose FMI threat information is to "alert technology companies" when their platforms are being used to disseminate "covert foreign government propaganda or disinformation or to provide other covert support to political organizations or groups."[305] Its stated purpose was to provide "procedures to be followed, in coordination with FITF, when an FBI employee seeks to share information regarding specific FMI activities or accounts, such as particular posts or uploads of videos, with Social Media Platforms."[306] The FBI SOP made clear that it did not apply "to general threat awareness briefings, or to communications regarding service of legal process, threats to life, or any other non-FMI activity, as otherwise covered in the [previous] November 4 guidance."[307]

The FBI SOP defined FMI as "subversive, covert (or undeclared), coercive, or criminal activities by foreign governments, nonstate actors, or their proxies designed to sow division, undermine democratic processes and institutions, or steer policy and regulatory decisions in favor of the foreign actors' strategic objectives and to the detriment of their adversaries."[308]

[303] *Id.*
[304] *Providing Foreign Malign Influence Threat Information, supra*. The FBI Office of the General Counsel had provided prior guidance on engagement with social media companies during the pendency of the *Murthy* litigation. *Id.* at 3. The FBI SOP supplemented that guidance.
[305] *Id.* at 5. ("One of the ways the FBI supports this mission is by providing FMI threat information to Social Media Platforms so that they may, in their discretion, take steps to mitigate such threats.") *Id.* at 1.
[306] *Id.* at 3
[307] *Id.* at 3-4.
[308] *Id.* at 4-5

The FBI SOP authorized sharing of FMI information with social media companies under certain conditions. These conditions included requirements that FBI personnel:[309]

- Determine that the activities under investigation were conducted covertly by or directed by a foreign government for FMI purposes;
- Identify specific, credible, and articulable facts that provided high confidence demonstrating so;
- Record that information in an appropriate system of records that could be later referenced;
- Obtain attorney and supervisor approval; and
- Caveat their communications with social media companies with specific language stating that the FBI did not request or expect the company to take any particular action based on the shared FMI information.

The FBI SOP further provided that any meetings with social media companies that would result in the FBI sharing information about specific content or accounts or that relate to content moderation required pre-approval by the National Security and Cyber Law Branch.[310] Meetings initiated by social media platforms had to be documented in a case file.[311]

In August 2024, the FBI's Office of General Counsel issued further guidance entitled *Guidance for Engagement with Social Media Platforms* (FBI Social Media Guidance).[312] Unlike the February 2024 SOP, this guidance applied to all FBI engagement with social media companies, not just FMI.[313] The FBI Social Media Guidance, which followed the June 2024 decision by the Supreme Court in *Murthy*, stated that it remains the FBI's "responsibility to ensure that any communication between the FBI and the private sector clearly respect First Amendment-protected free speech."[314]

The FBI Social Media Guidance listed categories of communications that did not require attorney approval.[315] For example, communications regarding threats to life or CSAM would not need FBI OGC prior approval. Communications regarding FMI and cyber intrusions also did not need OGC approval provided certain conditions were met.[316] In addition, the FBI Social Media Guidance

[309] DOJ IG REPORT ON FMI, *supra,* at 46-47.
[310] *Providing Foreign Malign Influence Threat Information, supra,* at 7.
[311] *Id.*
[312] DEP'T OF JUST., OFF. OF THE GEN. COUNSEL, GUIDANCE FOR ENGAGEMENT WITH SOCIAL MEDIA PLATFORMS (Aug. 9, 2024).
[313] *Id.*
[314] *Id.* at 1.
[315] *Id.* at 2-3.
[316] *Id.* The conditions included that the communication did not: "a) suggest that a company's terms of service should change, b) suggest that specific content be removed from or altered on a social media platform or, in the case of a domain registrar, webhost, virtual private server provider or similar entity, suggest that a third-party public-facing website or content be moderated or removed, or c) opine about what content could potentially be posted by others in the future without an articulable basis and a need for the third party to know."

required caveat language to be added to certain communications.[317] Similar to the FBI SOP caveat language, this disclaimer stated that the FBI did not request or expect particular action to be taken with regard to the information and that no adverse action to the company would be taken by the FBI as a result of the company's decision.[318] The FBI Social Media Guidance also required all substantive communications and engagements with social media companies be "appropriately documented and serialized to the appropriate case file consistent with the DIOG, FBI policy, and any guidance from the relevant Division."[319]

From a free speech perspective, the FBI's SOP and Social Media Guidance, taken together, are an improvement but remain insufficient. The fact that the FBI promulgated formal policies concerning social media engagement, especially as it relates to disinformation, is a positive step forward. The clear requirement of communicated language disclaiming coercion or adverse consequences is important, if truthful and enforced. So too are the requirements for record-keeping, which allow for auditing and oversight of FBI engagement with social media companies; and for some attorney or supervisor approvals, which promote accountability. The requirement that FMI be attributed to foreign actors or their proxies with high confidence is also crucial, although the SOP does not offer guidance as to how speech by a domestic "proxy" of a foreign power would be treated.

The FBI Social Media Guidance, however, does not itself contain express protection for lawful domestic speech. As discussed above, the DIOG, the FBI's operations manual, contains several sections devoted to First Amendment protections.[320] The FBI states that all its actions must comply with the provisions in the DIOG, including those actions taken under the FBI Social Media Guidance or the FBI SOP.[321] The DIOG contains First Amendment, privacy, and civil liberties protections, and prohibits investigating, collecting, or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment. But it does not offer specific guidance on how those provisions would apply to flagging protected speech for social media companies. The NSC 2024 Framework, discussed above, presumes such action is consistent with the First Amendment and arguably encourages it. If the FBI takes a contrary position—i.e. that the DIOG *prohibits* it from flagging lawful domestic speech for social media companies even if the FBI deems the engagement to be related to an authorized purpose—that prohibition is not adequately spelled out in its policies.[322].

---

[317] *Id.* at 3-4.
[318] *Id.*
[319] *Id.* at 2.
[320] DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE, *supra,* at § 4.2. It also states that the FBI's collection of First Amendment protected speech must be done "for a valid law enforcement or national security purpose" and must be "conducted in a manner that does not unduly infringe upon the ability of the speaker to deliver his or her message" or "the ability of the audience to hear it."
[321] PCLOB Correspondence with the FBI (Oct. 23, 2026).
[322] The Social Media Guidance suggests OGC approval *is* required if the FBI "suggest[s] that specific content be removed or altered on a social media platform." GUIDANCE FOR ENGAGEMENT WITH SOCIAL MEDIA PLATFORMS, *supra.* It does not mention throttling or deplatforming. Such approval could of course be withheld. The FBI states that "it would be prohibited from doing this because of the DIOG. It would not flag lawful domestic speech solely based on the speech. The FBI would only engage with a social media company if it deems that the engagement was

After listing categories of speech for which approvals are not needed, the FBI Social Media Guidance states, "[f]or all other types of communications, please consult with OGC."[323] The FBI SOP, on the other hand, contains layers of conditions that must be met before communication with a social media company is made, but it applies only to *foreign* malign influence. Illogically, on its face, the FBI SOP appears to provide more specific guardrails and protection to foreign speech than the Social Media Guidance does for domestic speech.

As drafted, the FBI's policies do not explicitly preclude the FBI from "notifying" social media companies about domestic speech it finds problematic. There is no requirement that the speech be somehow illegal or constitute a grave or imminent threat, and no prescribed method for making that determination. Nor are approvals required, other than the general ones described. The policies also do not require any transparency, whether to Congress, the DOJ OIG, or the public. Given the serious public concerns about communications between the federal government and social media companies concerning pressure to deplatform, remove, or minimize content, transparency, provided consistently with the needs of national security, would play an important role in restoring trust.

D. The Impacts of EO 14149 on Government Counter-Disinformation Activities

The government's counter-disinformation efforts were dramatically curtailed in early 2025. Following EO 14149 in January 2025,[324] the government suspended several existing agency components and activities engaged in or related to countering disinformation: [325]

- In February 2025, the Attorney General dissolved the FBI's FITF. [326]
- In April 2025, the National Science Foundation announced that it was no longer funding disinformation research, pursuant to the requirements of the EO.[327]

---

related to an authorized purpose not based purely on first amendment protected activity." PCLOB Correspondence with the FBI (Oct. 23, 2026).

[323] GUIDANCE FOR ENGAGEMENT WITH SOCIAL MEDIA PLATFORMS, *supra.*

[324] Relatedly, EO 14332, *Improving Oversight of Federal Grantmaking* also provided additional guidance to agencies engaged in grantmaking to ensure external funding decisions are aligned with presidential priorities and do not fund "initiatives that compromise public safety or promote anti-American values. Exec. Order No. 14332, § 4 (b)(ii)(D). The preamble of the EO also discusses how grantmaking has been used to fund censorship activities.

[325] Most of the post-EO 14149 impacts relate to the suspension or cancellation of funding opportunities for work or research pertaining to disinformation. A comprehensive inventory and analysis of such funding obligations is beyond the scope of this report. Given that most funding opportunities and obligations related to disinformation research and work were suspended or cancelled since the issuance of the EO, additional discussion is not provided herein.

[326] GENERAL POLICY REGARDING CHARGING, PLEA NEGOTIATIONS, AND SENTENCING, *supra, at* 4. Additionally, at DOJ, OJP, which awards and administers grants, terminated 384 awards pursuant to 2 C.F.R. 200.340(a)(4) because they were determined to "no longer effectuate[] the program goals or agency priorities." The Department has advised that "[n]one of these terminations were made pursuant to EO 14149." Responses to PCLOB from the FBI (Sept. 2026). PCLOB is not aware how many of these related to disinformation.

[327] *Updates on NSF Priorities,* U.S. NAT'L SCI. FOUND. (Apr. 18, 2025), https://www.nsf.gov/updates-on-priorities (last updated July 30, 2025). "Per the [EO] announced January 20, 2025, NSF will not prioritize research proposals that engage in or facilitate any conduct that would unconstitutionally abridge the free speech of any American

- In April 2025, the Secretary of State announced the closure of the Counter Foreign Information Manipulation and Interference hub, whose duties had previously fallen within those of the GEC, whose legislative mandate had terminated in December 2024.[328]
- In May 2025, the DHS Secretary testified to Congress that CISA would no longer focus on disinformation.[329]
- In July 2025, State took over responsibility for administrating all ongoing foreign assistance programs previously administered by USAID.[330]
- In July 2025, DHS terminated all awarded grants for the CP3's TVTP program, which funded programs from 2021-2022 that promoted media literacy in countering domestic terrorism and violent extremism.[331]
- In August 2025, the Director of National Intelligence released a memo on "ODNI 2.0" which called for "refocusing functions with the" FMIC, asserting it was "used by the previous administration to justify the suppression of free speech and to censor political opposition."[332]

Additionally, in April 2025, ODNI declassified the 2021 Implementation Plan, in which the previous administration linked the need to counter disinformation to domestic terrorism threats.[333] The Attorney General's investigative findings of the previous administration's counter disinformation activity, required under EO 14149, have not yet been published. More recent

citizen. NSF will not support research with the goal of combating "misinformation," "disinformation," and "malinformation" that could be used to infringe on the constitutionally protected speech rights of American citizens across the United States in a manner that advances a preferred narrative about significant matters of public debate."

[328] Sec'y Marco Rubio, *Press Statement: Protecting and Championing Free Speech at the State Department* (Apr. 16, 2025), https://www.state.gov/protecting-and-championing-free-speech-at-the-state-department; Victor Nava, *Biden admin 'rebranding' State Dept's controversial Global Engagement Center under new name – with same employees: report,* NEW YORK POST (Jan. 2, 2025), https://nypost.com/2025/01/02/us-news/biden-admin-rebranding-state-depts-shuttered-gec-under-new-name-with-same-staff-report/.

[329] Liz Landers, *DHS Secretary Noem tells Congress cybersecurity agency is no longer focused on misinformation,* WRTV (May 6, 2025), https://www.wrtv.com/politics/dhs-secretary-noem-tells-congress-cybersecurity-agency-is-no-longer-focused-on-misinformation.

[330] Mary Kekatos and Chris Boccia, *USAID programs now being run by State Department as agency ends operations,* ABC NEWS (July 1, 2025), https://abcnews.go.com/Health/usaid-programs-now-run-state-department-agency-ends/story?id=123373289.

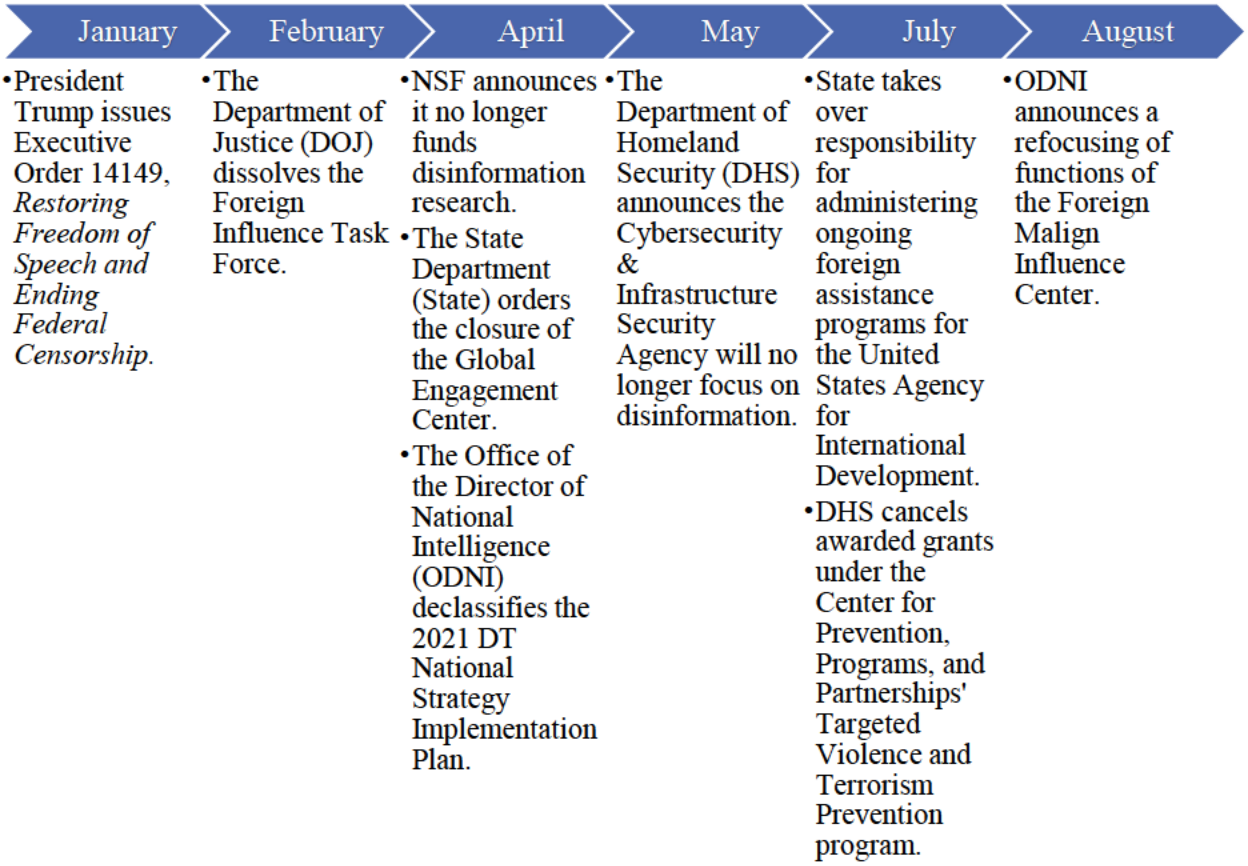
[331] *DHS Axes Wasteful, Misdirected Grants, Saves Taxpayers $18.5M,* U.S. DEPT. OF HOMELAND SEC. (July 17, 2025), https://www.dhs.gov/news/2025/07/17/dhs-axes-wasteful-misdirected-grants-saves-taxpayers-185m.

[332] *DNI Gabbard Launches ODNI 2.0: Reduce Bloat by over 40% and Save Taxpayers $700+ Million Per Year,* OFF. OF THE DIR. OF NAT'L INTEL. (Aug. 20, 2025), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2025/4100-pr-24-25; OFF. OF THE DIR. OF NAT'L INTEL., FACT SHEET: ODNI 2.0 LAUNCH, https://www.dni.gov/files/ODNI/documents/ODNI-20-Fact-Sheet.pdf (last visited May 20, 2026).

[333] OFF. OF THE DIR. OF NAT'L INTEL., DECLASSIFIED STRATEGIC IMPLEMENTATION PLAN FOR COUNTERING DOMESTIC TERRORISM FROM THE BIDEN ADMINISTRATION, https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-awareness-materials/cyber-training-series/11378-newsroom/dig/4064-dig-strat-impl-plan-ct-biden [https://web.archive.org/web/20260318234422/https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-awareness-materials/cyber-training-series/11378-newsroom/dig/4064-dig-strat-impl-plan-ct-biden]; 2021 IMPLEMENTATION PLAN, *supra*.

government activities are discussed in Section VI. Figure 4 provides a brief summary of the impact of EO 14149 in 2025.

Figure 4: The Impact of Executive Order 14149 in 2025.



1. Recent Consent Decrees Have Curtailed Some Agencies' Future Communications with Social Media Companies

Government counter-disinformation efforts were further restricted in March 2026 after several federal agencies entered into two separate consent decrees to resolve civil actions in which the plaintiffs alleged the government had infringed on "the constitutionally protected speech of American citizens," prior to the issuance of EO 14149.[334] Neither agreement conceded the accuracy of the plaintiffs' claims. The first consent decree stipulates that the Surgeon General, the Centers for Disease Control and Prevention, and CISA shall not a) threaten social media companies with punishment if they do not remove, delete, suppress, or reduce social-media content containing protected free speech or b) unilaterally direct or veto social media content moderation decisions.[335] The second consent decree requires State, and its now-terminated GEC, to abstain from knowingly or intentionally suppressing, censoring, demonetizing, and

[334] Consent Decree at 2, *Missouri v. Biden*, 680 F. Supp. 3d 630 (W.D. La. 2022) (No. 478); Consent Decree at 5, *The Daily Wire, LLC v. U.S. Dep't of State,* 733 F. Supp. 3d 566 (E.D. Tex. 2024) (No. 131).
[335] Consent Decree at 3, *Missouri v. Biden*. The social media platforms covered by this agreement are limited to Facebook, Instagram, Twitter or X, LinkedIn, and YouTube.

The risk remains that combating foreign malign influence, if not appropriately cabined and checked, could impact domestic speech.

downgrading constitutionally protected speech, including through a) actions taken via third parties, b) awards, c) grants, or d) funding of efforts which would result in suppression, censorship, demonetization and downgrading of constitutionally protected speech.[336] State also has to remove online materials concerning fact-checking, media literacy, and countering propaganda and disinformation tools and technologies. [337]

The consent decrees are limited in several ways. First, they apply only to the federal agencies that were parties to the lawsuit. Thus, they do not bind the FBI, DHS, ODNI, White House, or other government actors. Second, the latter consent decree is not indefinite and only remains operative until January 31, 2036. Further, because the consent decrees were entered into in March 2026, after the issuance of EO 14149, which prohibited the counter-disinformation activities covered, it is unclear what, if any, immediate impact they will have. Should EO 14149 be amended or withdrawn in the future, the decrees may have more concrete effect.

E. Risks to Free Speech Remain

While the government has undertaken significant efforts to curtail counter-disinformation work since EO 14149 went into effect (see Sec. III.D for a discussion), PCLOB assesses that risks to civil liberties remain.

As an initial matter, agency implementation of EO 14149 does not appear to be formalized. PCLOB was not provided agency policies or implementation guidance that prohibit agency personnel or funds from being used to "engage in or facilitate any conduct that would unconstitutionally abridge the free speech" of Americans.[338]

Moreover, because the policy against encouraging the suppression of speech was issued as an EO, rather than through legislation or regulation, it is subject to simple reversal in the future. The broad authorities of certain agencies to combat domestic terrorism could be used to justify potential future efforts to suppress speech.

Finally, with various agencies continuing counter-FMI activities, the risk remains that countering such influence, if not appropriately cabined and checked, could impact domestic speech.[339] As

[336] *Id.* at 3.
[337] *Id.* at 3-8, *The Daily Wire, LLC*. The agreement also requires the State Department to train all employees, contractors, and grantees on the Department's First Amendment limitations and provide an annual letter to the plaintiffs confirming compliance with the consent decree.
[338] Exec. Order No. 14149 § 2.
[339] State reports to PCLOB that in March 2026 it sent a cable to U.S. embassies and consulates with guidance on how to counter foreign disinformation seeking to undermine American interests, including on the social media platform X, in ways that uphold the principle of free speech. State further reported that in July 2026 it sent a cable updating its 2021 policy on engagement with online platforms regarding third-party user content, which both expanded the policy's reach and further restricted the parameters for any such engagements. State told PCLOB that

discussed above, the transition from countering FMI to countering broad categories of speech, both foreign and domestic, can be precipitous.[340] Even when steps have been taken to underscore that counter-foreign disinformation activities be conducted consistent with First Amendment considerations, the government recognizes no formal prohibition against encouraging social media platforms to limit speech.

"[k]ey elements of this updated policy were outlined within a new subchapter of the Department's Foreign Affairs Manual (FAM), at 10 FAM 355," and that "Senior State Department officials, including the Secretary of State, have emphasized that counter speech and more speech is the best remedy to counter foreign propaganda." PCLOB was not provided these cables or manual for review and so could not independently verify their content. Responses to PCLOB from State (Oct. 2026)

[340] 2021 DT STRATEGY, *supra*. *See also* Statement of John Cohen, Coordinator for Counterterrorism, Dept. of Homeland Sec, Confronting Violent White Supremacy (Part VI): Examining the Biden Administration's Counterterrorism Strategy, Hearing Before the Subcomm. on CR. & C.L. of the House Comm. on Oversight & Reform, (2021), https://www.congress.gov/117/meeting/house/114074/documents/HHRG-117-GO02-Transcript-20210929.pdf ("Online content, disinformation, false narratives, and conspiracy theories spread by foreign nation-states, international terrorist groups, and extremist thought leaders fuel much of the violence we are experiencing in the country today. Domestic and foreign threat actors purposely seek to exploit the fractures in our society, the anger and discord in our political discourse to sow discord and inspire acts of violence."). *See also* DOJ IG REPORT ON FMI, *supra,* at iii.

IV. CONCLUSION

If used to combat online threats from adverse nation-states and their foreign proxies, government counter-disinformation efforts could serve important national security functions. PCLOB's investigation revealed, however, that recent efforts to suppress speech through engagement with social media companies were often conducted without respect to whether the speech was protected or whether the speaker was foreign or domestic. PCLOB's investigation found several notable problems with the government's efforts.

First, the government failed to provide evidence to the public or to PCLOB regarding the counterterrorism value of countering disinformation online, as connections to past and future threats of violence were not demonstrated. While some academic research indicates there is a relationship between online disinformation and future terrorist violence, this relationship is complex and proving causation is challenging. In any event, PCLOB was not provided any indication that the government reviewed or relied on this research to justify its policies or actions.

Second, the subjective terminologies and definitions used to address disinformation—especially when they are connected to domestic terrorism terminologies based on ideology—may result in government overreach in countering disinformation and impact civil liberties.

Countering foreign disinformation may be crucial to national security, but so too is the responsibility to protect Americans' free speech.

Third, engagements with social media platforms were often *ad hoc*, lacked transparency, and did not regularly assess foreignness and protected speech. The government often engaged third party social media companies, even when the government lacked adequate policies and procedures to govern those engagements. Key agencies lacked or failed to provide to PCLOB agency guidance or policies for engaging social media companies on disinformation matters. The policies PCLOB was provided were insufficient in important respects. This general deficiency of policies and safeguards within the government may have contributed to the *ad hoc* and non-transparent nature of engagements with social media companies. The policies PCLOB did analyze failed to explain how agency personnel distinguish foreign from domestic speech online or provide guidance on how personnel should determine whether such speech is protected.

Countering foreign disinformation may be crucial to national security, but so too is the responsibility to protect Americans' free speech. Ensuring strict and enduring prohibitions around government efforts to suppress protected speech, as well as establishing rigorous safeguards and transparency for combating foreign malign influence are crucial.

V. RECOMMENDATIONS

The following are recommendations for future government engagement with social media companies with respect to perceived disinformation.

RECOMMENDATION 1:

The government should ensure EO 14149 is fully implemented.

EO 14149 prohibits government actors and agencies from engaging in, facilitating, or using any federal resources to abridge the protected speech of Americans, but further regulations and guidance are necessary to implement the EO fully. The absence of formal agency policies and procedures creates risk of inappropriate engagement with social media companies. The government should ensure that it does not contribute to suppressing protected speech on social media, especially when it justifies such efforts by combating domestic terrorism.

All relevant agencies should draft and revise existing policies to implement the principles of EO 14149 regarding social media engagement, foreignness determinations, and agency training. Agency policies should state that personnel are prohibited from engaging with social media companies in order to encourage the suppression of protected speech. Such policies should have strict processes requiring foreign attribution of the speech and, if domestic, a determination of a violation of U.S. law. They should also include requirements for high-level approvals and records of each action to assist in future auditing. These policies should be posted on agency websites and otherwise publicly available, to the extent consistent with national security and applicable law.

Social Media Engagement. As described in Section III, formal policies and procedures regarding engagement with social media companies concerning disinformation were sparse and insufficient. Existing procedures did not restrict government personnel from identifying protected speech for social media companies. Absent formal agency policies and procedures, the government risks inappropriately engaging social media companies and negatively impacting protected speech. Thus, relevant departments and agencies should formalize procedures to govern engagement with social media companies. And, as discussed above, the FBI should ensure that relevant prohibitions that they understand to be covered by the DIOG are incorporated in the FBI Social Media Guidance.

All relevant agencies should implement policies and safeguards that include:

- Whether and to what extent and purpose suspected foreign disinformation or other unprotected speech on a social media platform can be raised with social media companies;
- Processes and rules to guide agency personnel in communicating with social media companies; and
- Disclaimer language in communications with social media companies to clarify that speech moderation decisions rest solely with the company, not with the government, that no

particular action is required by the receiving party, and that the government will take no adverse actions against the company based on its moderation decision.

Attribution Standards and Other Unprotected Speech. Any such policies should also provide standards for assessing the foreignness of information or content in cases where engagement with social media companies is contemplated. Flagging domestic speech risks negatively impacting the free speech of Americans. Therefore, in cases where the agency may be communicating with social media companies regarding content on their platforms, agencies should develop and regularly evaluate policies and procedures for determining the foreignness of the speaker.

If the speech is determined to be domestic, the policies should be consistent with EO 14149 and should, at a minimum, include clear standards for determining if the speech is otherwise unprotected (e.g., incitement to imminent violence, true threats).

Training. These relevant policies and procedures should be developed into guidance and training for agency personnel to facilitate appropriate engagement with social media companies. Such training may focus on topics pertaining to unprotected speech or how officials should log communications from such engagements to promote transparency efforts.

RECOMMENDATION 2:

The government should improve transparency and oversight around its policies and communications with social media companies.

To foster public trust and help maintain government credibility, agencies should provide transparency regarding their engagements with social media companies regarding perceived disinformation. To the extent consistent with national security and applicable law, agencies should disclose this information in regular transparency reports. Such reports could include: (a) the date of the engagement; (b) the nature or purpose of the engagement; (c) a description of any action the agency seeks, encourages, or directs the platform to take; (d) the justification for the platform to take the desired or directed action; (e) the outcome of the foreignness determination and (f) the resulting action taken by the company (if known).

Agencies should publish their social media engagement policies and any guidance or policies implementing EO 14149. To the extent consistent with national security and applicable law, agencies should also publish their policies concerning FMI and guidance on attribution. A commitment to publishing such policies fosters public dialogue and ensures that any future changes to the policies will also be known to the public.

RECOMMENDATION 3:

The government should develop uniform terminologies.

As described in Section III, the terms mis-, dis-, and mal-information are not defined by federal statute, and agencies often use different definitions. Using subjective, broad, or ill-defined terms heightens the potential for government censorship in the name of countering domestic terrorism. To the extent the government continues efforts to counter foreign disinformation, relevant departments and agencies should develop and adopt uniform definitions and related concepts.[341] A clearly defined foreign threat and uniformly adopted definitions will help ensure the government properly identifies its legitimate objectives and promotes outcomes that are consistent with civil liberties protections.

RECOMMENDATION 4:

The government should ensure that any related grantmaking is carefully circumscribed.

EO 14149 directs that no taxpayer resources be "used to engage in or facilitate any conduct that would unconstitutionally abridge the free speech of any American citizen."[342] However, taxpayer money has been used in the past to fund counter-disinformation grants which may have negatively impacted protected speech. To the extent agencies have not done so already, agencies should ensure that their grantmaking processes are conducted in accordance with EO 14332, *Improving Oversight of Federal Grantmaking*. EO 14332 requires agencies to ensure grantmaking aligns with the President's priorities and does not impose harm to Americans, such as through the previous funding of "social media censorship tools."[343] To further transparency, agencies should also publish relevant information about any related awarded grants on their websites, to the extent consistent with national security and applicable law. In addition, agencies involved in any disinformation-related funding opportunities that involve human subjects should develop processes to provide a heightened internal review of privacy and civil liberties protections that exceed the requirements under 45 CFR Part 46, which governs the ethical treatment of study participants.[344]

---

[341] As discussed in Section IV, despite the National Intelligence Council's development and dissemination of the *IC Lexicon for Foreign Malign Influence*, many agencies have used their own, distinct definitions of disinformation and FMI. *See* GAO-24-107600, FOREIGN DISINFORMATION: DEFINING AND DETECTING THREATS, *supra*.

[342] Exec. Order 14149, Sec. 2(c), https://www.whitehouse.gov/presidential-actions/2025/01/restoring-freedom-of-speech-and-ending-federal-censorship/.

[343] Exec. Order 14332, Sec. 1, https://www.whitehouse.gov/presidential-actions/2025/08/improving-oversight-of-federal-grantmaking/.

[344] For example, Institutional Review Board (IRB) approvals of research require some level of review for ensuring the confidentiality and general welfare of subjects. *See e.g.,* 45 CFR 46.111(a)(7) ("where appropriate, there are adequate provisions to protect the privacy of subjects…") and 45 CFR 46.111(b) (and that "[w]hen some or all of the subjects are likely to be vulnerable to coercion or undue influence, such as children, prisoners, individuals with impaired decision-making capacity, or economically or educationally disadvantaged persons, additional safeguards have been included in the study to protect the rights and welfare of these subjects").

RECOMMENDATION 5:

Free speech protections and safeguards should be codified.

The government should take steps to guarantee free speech protections endure, including by urging Congress to enact key restrictions and protections into law.[345] Enshrining the principles of EO 14149 in statute and codifying the above protections, as well as requiring agencies to formalize procedures governing their engagement with social media companies, would guard against future abuses stemming from the government's efforts to counter disinformation.

[345] Such efforts should acknowledge the government's continued ability to speak publicly when it seeks to respond to disinformation.

APPENDIX A:
SEPARATE STATEMENT OF MEMBER BETH A. WILLIAMS

"It is error alone which needs the support of government. Truth can stand by itself."
– *Thomas Jefferson*

I extend my thanks to the current and former staff members who contributed to this project since it was opened more than four years ago. Their hard work and thoughtful analysis are evident in this Report. I write separately to underscore several points.

Speech suppression is an extreme response to perceived disinformation. As the Report explains, there exists a range of government responses to disinformation that vary in their intrusiveness and civil liberties impact. Affirmative government speech is, and has historically been, a generally accepted and appropriate reaction to information the government considers to be wrong and dangerous. The government may state what it believes to be true and do so with the full authority it can bring to bear. But government efforts to encourage third party social media platforms privately to "enforce their own terms of service" by removing speech or deplatforming accounts with which the government does not agree are highly concerning. As the Report explains, publicly available documents now confirm that government actors took steps to encourage social media platforms to suppress broad types of speech without considering the origin of the speech, and without considering whether the speech was protected. They did not, for example, only target speech that constituted a true threat or incited imminent lawless action.

Compounding the civil liberties concerns, these government efforts to suppress speech largely occurred privately—often through direct communication between government officials and social media platforms. Were it not for lawsuits that forced discovery of these communications, the public likely never would have known the scope of the government's involvement.

Avoidance of explicit government coercion is insufficient to protect civil liberties. Government lawyers responded to the lawsuits and the revelation of the (at best, unseemly) emails as they would be expected to do: by issuing guidance to ensure future communications were lawful. That primarily meant advising agencies and actors not to be coercive. The clear thrust of many of these policies was that the Executive Branch believed that it was both appropriate—and in many instances advisable—for government actors to persuade social media companies to monitor or limit certain speech so long as the communications were framed as suggestions.

It is of course questionable whether social media platforms would ever really find such communication from the White House to be a suggestion, no matter how many disclaimers are appended. But even if they did, that does not make those communications good policy.[346] And it would undoubtedly be terrible policy for the government to send to social media platforms secret lists of statements they believe to be wrong, accompanied by secret lists of accounts purveying these wrong statements. Whether such actions are lawful or not, the government should not be in the business of policing Americans' speech.

Whether such actions are lawful or not, the government should not be in the business of policing Americans' speech.

If a bright line did exist that limited government counter-disinformation efforts to countering only foreign malign influence, it faded quickly. In 2021, the White House assumed as fact that a "crisis of disinformation and misinformation" was fueling domestic terrorism.[347] White House personnel sent messages suggesting that social media platforms' failure to remove or limit disinformation would lead to violence. These government actors appeared to have little concern about whether the speaker was foreign or domestic.[348] As a White House-created working group's own Roadmap stated, the priorities were to "mitigate threats that misinformation and disinformation pose to public safety and national security" and to "[a]ddress disinformation and *domestic and foreign* malign activities used to sow division and conflict."[349]

The social media engagement practices that were utilized first to counter FMI were easily translated to countering domestic terrorism, with little evident concern for the repercussions. The risk that the need to fight terrorism would be used to justify curtailing civil liberties is well-recognized. Indeed, it is the reason that the 9/11 Commission recommended the creation of PCLOB.[350] And it is why the Commission recommended that "[t]he burden of proof for retaining a particular governmental power should be on the executive, to explain (a) that the power actually materially enhances security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties. If the power is granted, there must be adequate

[346] *See* Jennifer Senior, *In Conversation: Antonin Scalia*, NEW YORK MAGAZINE, (Oct. 4, 2013), https://nymag.com/news/features/antonin-scalia-2013-10/ ("A lot of stuff that's stupid is not unconstitutional.").
[347] WHITE HOUSE, NATIONAL STRATEGY FOR COUNTERING DOMESTIC TERRORISM 29 (2021), https://www.govinfo.gov/content/pkg/GOVPUB-PR-PURL-gpo174845/pdf/GOVPUB-PR-PURL-gpo174845.pdf
[348] The FBI arguably maintained this distinction. As discussed in the Report, the FBI stated that it does engage in foreignness determinations (or attribution of foreign actors) before flagging accounts for social media companies. *See supra* section III(B)(3).
[349] NAT'L SCI. & TECH. COUNCIL, ROADMAP FOR RESEARCHERS ON PRIORITIES RELATED TO INFORMATION INTEGRITY RESEARCH AND DEVELOPMENT 10 (Dec. 2022), https://www.nitrd.gov/pubs/Roadmap-Information-Integrity-RD-2022.pdf (emphasis added).
[350] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 395 (2004), https://www.9-11commission.gov/report/911Report.pdf.

guidelines and oversight to properly confine its use."[351] Here, it is not at all clear that disinformation fueled domestic terrorism, or that it did so on any significant scale. The government certainly has not provided PCLOB with support for that contention. Nor is it evident that government efforts to suppress such speech would enhance national security.

The Report correctly concludes that adequate guidelines and oversight do not currently exist to confine the government in any future efforts. Executive Order 14149 sets a clear direction against government efforts to pressure social media platforms to curtail speech. But prohibitions on attempts to suppress Americans' lawful speech are not clearly stated in current agency policy and are not codified into law. That makes it relatively easy for the government to reverse course in the future and resume the types of counter-disinformation efforts described in this Report.

Americans should not have to suspect—or fear—that the government is encouraging private companies to censor their speech. To effectively protect a nation, the government must perpetually prove itself worthy of trust.

I urge that the Report's recommendations be fully implemented.

[351] *Id.* at 394-95.

APPENDIX B: COUNTER-DISINFORMATION INVENTORY

This appendix describes the objectives and activities of agencies involved in the counter-disinformation space from 2018-2026. It focuses on the Department of Homeland Security (DHS) and the Department of Justice (DOJ) (including the Federal Bureau of Investigation (FBI)), two agencies listed in the 2021 Implementation Plan with a primary focus on countering domestic terrorist threats.[352]

It is comprised of two parts: (a) a narrative overview of each agency's respective counter-disinformation activities and (b) an agency-specific breakdown of funding decisions made to counter-disinformation.

For this investigation, PCLOB inventoried active countermeasures, formal partnerships with government and non-government entities, and external funding for research and programming.

> **Countermeasures** include activities pursued to prevent or respond to disinformation, such as debunking or fact-checking efforts on social media or engaging in community resilience building efforts. Countermeasures include training, outreach, community engagement, online activities, or general intelligence and information sharing efforts.
>
> **Partnerships** constitute formal and informal arrangements whereby agencies enter into an agreement to share resources, intelligence, personnel, or expertise to combat disinformation or collectively engage in active disinformation countermeasures.
>
> **External Funding** refers to financial agreements (e.g., contracts, grants, cooperative agreements) that agencies enter into with other entities to fulfill some defined obligation, such as research on the efficacy of disinformation countermeasures.

PCLOB's investigation consisted of formal requests for information (RFIs) to relevant departments and agencies, and extensive open-source research. The RFIs included requests for policies, procedures, guidance, and programmatic information to discern the activities pursued by the government to combat disinformation, as well as any relevant safeguards in place to ensure Americans' free speech rights are protected. In subsequent engagements, PCLOB requested additional information, clarified existing knowledge gaps, and requested agency briefings on specific programs, policies, or activities.

[352] WHITE HOUSE, STRATEGIC IMPLEMENTATION PLAN FOR COUNTERING DOMESTIC TERRORISM, https://www.dni.gov/files/ODNI/documents/DIG/DIG-Declassified-Strategic-Implementation-Plan-for-CT-April2025.pdf. The FBI (and DOJ as a result) and DHS are the lead agencies tasked with countering terrorist threats within the homeland.

External engagement with agencies commenced in August 2023 and continued for three years through October 2026. As discussed in the Report, agencies varied significantly in their responsiveness.

Counter-Disinformation Activities

Department of Homeland Security

Cybersecurity and Infrastructure Security Agency

Established in 2018, the Cybersecurity & Infrastructure Security Agency (CISA) provides substantive analysis of cyber and critical infrastructure threats, including threats to election security.[353] DHS established a Countering Foreign Influence Task Force that same year, composed of CISA's Election Security Initiative division and DHS's Intelligence & Analysis (I&A) staff, focused on foreign disinformation threats to election security leading up to the 2020 elections.[354] According to DHS's Office of Inspector General (OIG), CISA "also started notifying social media platforms or appropriate law enforcement officials when voting-related disinformation appeared in social media."[355]

Also in the run up to the 2020 elections, DHS, CISA, and State Department's Global Engagement Center interacted with the Election Integrity Partnership (EIP), a consortium of nongovernmental organizations, to "try to fill the gap of the things that the Government could not do themselves" because federal agencies lacked "the funding and the legal authorizations."[356] External participants, including federal, state, and local election officials, submitted "tickets" flagging online narratives and specific domestic social media posts through the EIP's centralized ticketing system.[357] EIP staff analyzed these inputs and forwarded systemic policy violations to content moderation teams at major social media companies.[358] In 2021, DHS transitioned the Countering Foreign Influence Task Force to the Mis-, Dis-, and Malinformation team (MDM team), which was "charged with building national resilience to MDM and foreign influence activities."[359]

---

[353] Cybersecurity and Infrastructure Security Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168 (2018).
[354] DEP'T OF HOMELAND SEC., OFF. OF INSPECTOR GEN., DHS NEEDS A UNIFIED STRATEGY TO COUNTER DISINFORMATION CAMPAIGNS, 5 (Aug. 10, 2022), https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-58-Aug22.pdf [hereinafter DHS NEEDS A UNIFIED STRATEGY].
[355] *Id.*
[356] STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF THE FED. GOV'T, FINAL REPORT 931, https://judiciary.house.gov/media/press-releases/final-report-weaponization-federal-government; Censorship Laundering: How the U.S. Department of Homeland Security Enables the Silencing of Dissent, Hearing Before the Subcomm. on Oversight, Investigations, & Accountability of the House Comm. on Homeland Sec., (2023), https://www.congress.gov/event/118th-congress/house-event/115901/text.
[357] Censorship Laundering, *supra.*
[358] *Id.*
[359] *Mis, Dis, Malinformation,* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/mdm [https://web.archive.org/web/20220429060805/https://www.cisa.gov/mdm] (last visited July 29, 2026); DHS NEEDS A UNIFIED STRATEGY, *supra,* at 7.

According to an archived version of CISA's website, the MDM team engaged with external partners, including social media companies, and worked "on a variety of projects to build resilience against malicious information activities."[360] The MDM team not only focused on election disinformation, but broader disinformation-related topics, such as disinformation about the COVID-19 pandemic and how social media bots operate in the disinformation space.[361]

In June 2021, DHS created the CISA Cybersecurity Advisory Committee (CSAC), an independent advisory body which comprised subject matter experts in non-profit and for-profit fields.[362] CSAC advised CISA on its cybersecurity mission.[363] CSAC established a Protecting Critical Infrastructure from Misinformation & Disinformation Subcommittee (MDM Subcommittee).[364] The MDM Subcommittee issued formal recommendations in June[365] and September[366] 2022. In December 2022, the MDM Subcommittee disbanded, and the CSAC 2023 strategic plan stated the MDM Subcommittee "will stand down, as they have successfully answered their taskings and provided recommendations to CISA."[367]

[360] *Mis, Dis, Malinformation, supra.*
[361] *Id.*; DHS NEEDS A UNIFIED STRATEGY, *supra,* at 7.
[362] *CISA Cybersecurity Advisory Committee,* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/resources-tools/groups/cisa-cybersecurity-advisory-committee (last visited July 29, 2026).
[363] *Id.*
[364] STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FED. GOV'T OF THE H. COMM. ON THE Judiciary, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A "CYBERSECURITY" AGENCY COLLUDED WITH BIG TECH AND "DISINFORMATION" PARTNERS TO CENSOR AMERICANS 6 (June 26, 2023), https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/cisa-staff-report6-26-23.pdf. It may be more accurate to say that the CISA Director established the MDM Subcommittee. *See* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, CYBERSECURITY ADVISORY COMMITTEE CHARTER 4 (Sept. 3, 2021), https://www.cisa.gov/sites/default/files/publications/CISA%20Cybersecurity%20Advisory%20Committee%20Charter_508%20Compliant.pdf.
[365] CISA CYBERSECURITY ADVISORY COMMITTEE, REPORT TO THE CISA DIRECTOR: PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION AND DISINFORMATION 1 (June 22, 2022), https://www.cisa.gov/sites/default/files/publications/June%202022%20CSAC%20Recommendations%20%E2%80%93%20MDM_0.pdf. ("The initial recommendations outlined below focus primarily on mis- and disinformation (MD) about election procedures and election results. Future recommendations may seek to address the potential impacts on other critical functions and some of the unique challenges in identifying and countering malinformation.").
[366] CISA CYBERSECURITY ADVISORY COMMITTEE, REPORT TO THE CISA DIRECTOR: PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION AND DISINFORMATION, INFORMATION SHARING AROUND FOREIGN ADVERSARY THREATS TO ELECTIONS 3 (Sept. 13, 2022), https://www.cisa.gov/sites/default/files/publications/CSAC_MDM_September_2022_Final_Recommendations_09132022-508.pdf. ("The MDM Subcommittee submitted a first set of recommendations in June 2022. The recommendations outlined below aim to emphasize and add further detail to key points and provide additional items for consideration.").
[367] CISA CYBERSECURITY ADVISORY COMMITTEE, DECEMBER 6, 2022 MEETING SUMMARY 1 (Dec. 6, 2022), https://www.cisa.gov/sites/default/files/publications/CSAC_December-Quarterly-Meeting-Summary_508_01062023_0.pdf.

In addition to the MDM Subcommittee, CISA established a Joint Managing Mis/Disinformation Working Group, a part of CISA's Election Infrastructure Subsector (EIS).[368]According to CISA's website, the working group most recently convened on June 18, 2024.[369] The Joint Managing Mis/Disinformation Working Group produced resource documents for state and local election officials responding to the impact of disinformation on elections.[370]

CISA also funded the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), a partnership between CISA, EIS Government Coordinating Council, and the Center for Internet Security (CIS), an IT non-profit where EI-ISAC is housed.[371] According to CIS, EI-ISAC "support[ed] the rapidly changing cybersecurity needs of U.S. elections offices."[372] EI-ISAC published a document for the 2020 election on how to report disinformation to the organization. The document stated that EI-ISAC would forward such reports "to our partners" at CISA.[373]

By March 2024, CISA had moved the standalone MDM team into the Election Security and Resilience subdivision. In September 2024, CISA told PCLOB, "CISA does not do counter-MDM work in the context" of countering domestic terrorism, but instead "focus[es] on educating election infrastructure officials on how to navigate foreign influence operations and disinformation related risks."[374] A 2024 DHS OIG report stated that, while CISA "is focused on resources that educate

[368] *Government Services and Facilities – Election Infrastructure Subsector Working Groups*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/resources-tools/groups/government-services-and-facilities-election-infrastructure-subsector-working-groups (last visited July 13, 2026) (see the agendas for June 30, 2022 to March 26, 2024 meetings of the "Joint Election Infrastructure Working Group to Build Voter Guidance," which lists the previous title of the group as the "Joint Managing Mis/Disinformation Working Group"). *See also, Joint Managing Mis/Disinformation Working Group*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/resources-tools/groups/joint-managing-misdisinformation-working-group (last visited Aug. 8, 2026).
[369] *Government Services and Facilities – Election Infrastructure Subsector Working Groups*, *supra.*; *Joint Managing Mis/Disinformation Working Group*, *supra.*
[370] CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, MIS-, DIS-, AND MALINFORMATION: PLANNING AND INCIDENT RESPONSE GUIDE FOR ELECTION OFFICIALS, https://web.archive.org/web/20240910011545/https://www.cisa.gov/sites/default/files/2022-11/mdm-incident-response-guide_508.pdf (last visited Aug. 6, 2026); CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, RUMOR CONTROL PAGE START-UP GUIDE, https://web.archive.org/web/20240910094423/https://www.cisa.gov/sites/default/files/2023-01/rumor-control-startup-guide_508.pdf (last visited Aug. 6, 2026).
[371] *Election Infrastructure Information Sharing and Analysis Center*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/ei-isac (last visited Aug. 8, 2026); *Join the EI-ISAC,* CISA, https://www.cisa.gov/resources-tools/groups/join-ei-isac (last visited July 13, 2026).
[372] *About Us*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/about-us (last visited Aug. 6, 2026).
[373] CTR. FOR INTERNET SEC. AND EI-ISAC, REPORTING MISINFORMATION TO THE EI-ISAC, https://web.archive.org/web/20240119005552/https:/www.eac.gov/sites/default/files/partners/EI_ISAC_Reporting_Misinformation_Sheet102820.pdf (last visited Aug. 8, 2026).
[374] Email from CISA to PCLOB (Sept. 20, 2024).

election partners and help to identify disinformation," it "discontinued its efforts to work directly with social media companies to counter disinformation after the 2022 election."[375]

CISA also explicitly told PCLOB that they do not monitor social media for disinformation, however CISA did, as of October 2024, engage in public awareness campaigns and resilience building and development overseas in the context of combatting disinformation by foreign extremists.[376] According to a September 2024 report by the Government Accountability Office, CISA did not "distinguish between disinformation threats originating in the U.S. or abroad because [it] focus[ed] on building resilience to foreign malign influence operations to reduce risks to U.S. election infrastructure."[377]

On January 16, 2025, then-CISA Director Jen Easterly dissolved the MDM team "with resources absorbed into the broader election mission."[378] In May 2025, then-DHS Secretary Kristi Noem testified to Congress that CISA would no longer focus on disinformation.[379]

Office of Strategy, Policy, and Plans

Within the DHS Office of Strategy, Policy, and Plans, the Center for Prevention Programs and Partnerships (CP3) worked to prevent targeted violence and terrorism in the United States. In particular, CP3 funded the Targeted Violence and Terrorism Prevention (TVTP) program which awards grants for recipients to conduct training, community outreach, and public-health focused prevention programming.[380] In July 2025, DHS discontinued $18.5 million in appropriations for TVTP grants it claimed had "no legitimate nexus to protecting the homeland from the threat of terrorism."[381] In previous years, CP3 funded a number of disinformation and media literacy programs intended to counter domestic terrorism and domestic violence extremism.[382]

---

[375] DEP'T OF HOMELAND SEC., OFF. OF THE INSPECTOR GEN., FINAL REPORT: DHS IMPROVED ELECTION INFRASTRUCTURE SECURITY, BUT ITS ROLE IN COUNTERING DISINFORMATION HAS BEEN REDUCED 4 (Sept. 17, 2024), https://www.oig.dhs.gov/sites/default/files/assets/2024-09/OIG-24-52-Sep24.pdf.
[376] PCLOB Notes on CISA Team Meeting, (Oct. 15, 2024).
[377] U.S. GOV'T ACCOUNTABILITY OFF., GAO-24-107600, FOREIGN DISINFORMATION: DEFINING AND DETECTING THREATS 8 (2024), https://www.gao.gov/assets/gao-24-107600.pdf. It is illegal to send out knowingly false information about the time, place, or manner of voting to prevent people from properly casting their ballots, regardless of the speaker. However, it is not clear that CISA limited the information it flagged for social media companies solely to these categories.
[378] PCLOB Correspondence with CISA (Mar. 12, 2025).
[379] Liz Landers, *DHS Secretary Noem tells Congress cybersecurity agency is no longer focused on misinformation,* WRTV (May 6, 2025), https://www.wrtv.com/politics/dhs-secretary-noem-tells-congress-cybersecurity-agency-is-no-longer-focused-on-misinformation.
[380] *Who We* Are, DEP'T OF HOMELAND SEC., https://www.dhs.gov/cp3-who-we-are (last visited July 13, 2026); *What We Do*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/cp3-what-we-do (last visited July 13, 2026).
[381] *DHS Axes Wasteful, Misdirected Grants, Saves Taxpayers $18.5M,* U.S. DEPT. OF HOMELAND SEC. (July 17, 2025), https://www.dhs.gov/news/2025/07/17/dhs-axes-wasteful-misdirected-grants-saves-taxpayers-185m.
[382] See a list of TVTP grantees at *Targeted Violence and Terrorism Prevention Grantee* Results, Dep't of Homeland Sec., https://www.dhs.gov/tvtp-grantee-results (last accessed July 13, 2026).

For example, CP3 funded the Veterans Preventing Misinformation and Violence program, a joint venture between the University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism and the non-profit organization We the Veterans.[383] The program focused on preventing extremism among veterans in part by educating them about foreign and domestic actors' disinformation attempts targeting veterans.[384] CP3 also funded Lewis University's How2Inform, which "was developed to combat online misinformation with navigating violent online content and critical thinking tools and resources."[385] CP3 also funded Embry-Riddle Aeronautical University's Building Resilient Communities program where participants learned how radicalization can develop through disinformation and extremist content.[386]

DHS's fiscal year 2026 budget justification to Congress eliminated funding for the TVTP grants, and Congress did not add funding back into the full-year appropriations bill signed by the President on April 30, 2026.[387]

Intelligence and Analysis

I&A provides intelligence collection and analysis to support DHS's mission.[388] A 2022 final report from the Homeland Security Advisory Council (HSAC) Subcommittee on Disinformation Best Practices and Safeguards (2022 HSAC Report) explained that, I&A "identifies the spread of disinformation through all-source intelligence research ... to establish narratives, tactics, techniques, and procedures used by known foreign actors and domestic violent extremists."[389] Finished intelligence products are shared with federal, state, local, and tribal partners as needed.[390]

---

[383] *Targeted Violence Prevention for the Veteran and Military Family Community*, NAT'L CONSORTIUM FOR THE STUDY OF TERRORISM & RESPONSES TO TERRORISM, https://www.start.umd.edu/training/targeted-violence-prevention-veteran-and-military-family-community (last visited July 29, 2026); *View Grant Opportunity, DHS-22-TTP-132-00-01,* GRANTS.GOV, https://www.grants.gov/search-results-detail/339426 (last visited July 29, 2026).
[384] *See* NAT'L CONSORTIUM FOR THE STUDY OF TERRORISM, *supra*.
[385] *Targeted Violence and Terrorism Prevention Grantee Results*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/tvtp-grantee-results (last accessed July 13, 2026); HOW2INFORM, https://h2i.info/ (last accessed July 13, 2026).
[386] *Targeted Violence and Terrorism Prevention Grantee Results*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/tvtp-grantee-results (last accessed July 13, 2026); *Building Resilient Communities*, EMBRY-RIDDLE AERONAUTICAL UNI., https://commons.erau.edu/resilient-communities/ (last accessed Sept. 13, 2026).
[387] DEP'T OF HOMELAND SEC., FISCAL YEAR 2026 BUDGET IN BRIEF 8, 28, https://www.dhs.gov/sites/default/files/2025-07/2025_07_03_ocfo_fy-2026-budget-in-brief.pdf; Homeland Security and Further Additional Continuing Appropriations Act, 2026, Pub. L. No. 119-86 140 Stat. 773 (2026).
[388] *Office of Intelligence and Analysis*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/office-intelligence-and-analysis (last visited Aug. 6, 2026).
[389] HOMELAND SEC. ADVISORY COUNCIL, DISINFORMATION BEST PRAC. & SAFEGUARDS SUBCOMM., FINAL REPORT 9 (Aug. 24, 2022), https://www.dhs.gov/sites/default/files/2022-08/22_0824_ope_hsac-disinformation-subcommittee-final-report-08242022.pdf.
[390] *Id.*

As of 2025, I&A was divided into five primary subcomponents (or offices), with the Office of Analysis and the Office of Partnerships most relevant to this Report.[391] The Office of Analysis "produce[d] primarily strategic intelligence products for DHS stakeholders, including senior government officials, federal partners, and state, local, tribal, territorial, and private sector professionals."[392] The Counterterrorism Center (CTC), the Cyber Intelligence Center (CIC), and the Nation-State Threat Center (NST) served as three of the analytic branches under the Office of Analysis.[393] CTC synthesizes counterterrorism intelligence and shares relevant intelligence to state, local, international, private sector, and IC partners.[394] The 2022 HSAC Report stated, "CTC does collect open-source information on the threats of domestic violent extremists (DVE)," and "this collection may surface disinformation narratives or trends associated with identified DVE threat actors."[395]

CIC conducted and delivered finished intelligence on cyber threat analysis.[396] As part of its mission, CIC "collect[ed] information on foreign malign influence activity, analyzing both official traditional and social media channels backed by foreign states and proxy websites and forums."[397] Under CIC, I&A created a Foreign Influence and Interference Branch (FIIB) in 2019 "to organize and create analytical products about disinformation."[398] However, according to DHS OIG, the FIIB "did not directly counter disinformation; but rather, it shared information on the current threat environment."[399] NST provides intelligence about the nation-threat space to inform the decisions of DHS and its partners.[400] One of the four branches within NST is the Counterintelligence & Malign Influence Branch.[401]

Disinformation Governance Board

DHS announced the formation of the Disinformation Governance Board (DGB) in April 2022.[402] The DGB's charter states that its purpose is to "guide and support the Department's efforts to

[391] DEP'T OF HOMELAND SEC., OFF. OF INTEL. & ANALYSIS, POLICY MANUAL 2025 11 (Jan. 16, 2025), https://www.dhs.gov/sites/default/files/2025-03/25_0313_ia_office-of-intelligence-and-analysis_policy-manual.pdf.
[392] *Id.* at 12.
[393] *Id.* at 12, 67; *see also* FINAL REPORT, *supra, at* 20.
[394] *Centers*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/centers (last visited Aug. 6, 2026).
[395] FINAL REPORT, *supra,* at 10.
[396] *Id.*
[397] FINAL REPORT, *supra*, at 10.
[398] DEP'T OF HOMELAND SEC., OFF. OF THE INSPECTOR GEN., DHS ACTIONS RELATED TO AN I&A INTELLIGENCE PRODUCT DEVIATED FROM STANDARD PROCEDURES 2 (2022), https://www.oig.dhs.gov/sites/default/files/assets/2022-05/OIG-22-41-Apr22-Redacted.pdf; DHS NEEDS A UNIFIED STRATEGY, *supra,* at 6.
[399] DHS NEEDS A UNIFIED STRATEGY *supra,* at 6.
[400] *Centers*, *supra*; DHS ACTIONS RELATED TO AN I&A INTELLIGENCE PRODUCT, *supra,* at 67.
[401] DHS ACTIONS RELATED TO AN I&A INTELLIGENCE PRODUCT, *supra,* at 67. The other three branches are: Trade & Supply Chain Resiliency, Technology Transfer, and Foreign Investment. *Id.*
[402] Bridget Johnson, *DHS Standing Up Disinformation Governance Board Led by Information Warfare Expert,* HOMELAND SECURITY TODAY (Apr. 27, 2022), https://www.hstoday.us/federal-pages/dhs/dhs-standing-up-disinformation-governance-board-led-by-information-warfare-expert/.

address mis-, dis-, and mal-information that threatens homeland security ('MDM')."[403] The DGB's role was to "focus on the following four cross-functional lines of effort to counter MDM, many of which are already underway ('lines of effort',): (1) identifying MDM ('Identification'); (2) assessing and analyzing the risk that such MDM poses to homeland security ('Risk Assessment'); (3) responding to these MOM threats ('Response'); and (4) building resilience to MDM ('Building Resilience')."[404] In a May 2022 fact sheet, DHS said that the DGB was "an internal working group that was established with the explicit goal of ensuring [Americans' freedom of speech, civil rights, civil liberties, and privacy] protections are appropriately incorporated across DHS's disinformation-related work and that rigorous safeguards are in place."[405] Two months later, in July 2022, the HSAC's Disinformation Best Practices and Safeguards Subcommittee released a final interim recommendation concluding "that there is no need for a Disinformation Governance Board," without detailing why or explaining whether DHS's disinformation-related work had also ceased.[406] In August 2022, DHS terminated the DGB based on HSAC's recommendation.[407]

Department of Justice

National Security Division

DOJ's National Security Division (NSD)'s public-facing disinformation work focused on countering foreign malign influence (FMI) threats to elections, according to a now-deleted February 2024 fact sheet.[408] A July 2024 DOJ OIG report outlined NSD's role in coordinating information sharing about FMI threats to U.S. elections, explaining that NSD's Counterintelligence and Export Control Section "assists [U.S. Attorney's Offices] in the prosecution of foreign malign influence and interference cases,…while the Office of Law and

[403] SENS. CHARLES GRASSLEY & JOSH HAWLEY, LETTER TO DHS SEC. ALEJANDRO MAYORKAS (June 7, 2022), https://www.grassley.senate.gov/imo/media/doc/grassley_hawley_to_deptofhomelandsecuritydisinformationgovernanceboard.pdf.
[404] *Id.* at 14.
[405] *Fact Sheet: DHS Internal Working Group Protects Free Speech and Other Fundamental Rights When Addressing Disinformation That Threatens the Security of the United States,* DEP'T OF HOMELAND SEC. (May 2, 2022), https://www.dhs.gov/archive/news/2022/05/02/fact-sheet-dhs-internal-working-group-protects-free-speech-other-fundamental-rights.
[406] HOMELAND SEC. ADVISORY COUNCIL, DISINFORMATION BEST PRAC. & SAFEGUARDS SUBCOMM., FINAL INTERIM RECOMMENDATION 2 (July 18, 2022), https://www.dhs.gov/sites/default/files/2022-07/22_0718_ope_final-interim-recommendation-disinformation-best-practices-safeguards-subcommittee_0.pdf.
[407] *Following HSAC Recommendation, DHS terminates Disinformation Governance Board,* DEP'T OF HOMELAND SEC. (Aug. 24, 2022), https://www.dhs.gov/archive/news/2022/08/24/following-hsac-recommendation-dhs-terminates-disinformation-governance-board.
[408] DEP'T OF HOMELAND SEC., FEDERAL EXECUTIVE BRANCH AGENCIES ROLES AND RESPONSIBILITIES IN UNITED STATES ELECTIONS 3-4, https://web.archive.org/web/20250204111012/https://www.dhs.gov/sites/default/files/2024-02/24_1215_opa_interagency-election-security-fact-sheet-final-508-revised.pdf (last visited Aug. 6, 2026) ("DOJ's NSD oversees matters involving a range of malign influence activities that foreign governments may attempt, including computer hacking of election or campaign infrastructure; covert information operations (e.g., to promulgate disinformation through social media); covert efforts to support or denigrate political candidates or organizations; and other covert influence operations that might violate various criminal statutes.").

Policy serves as the primary nexus for the development of DOJ policy on countering foreign malign influence."[409] In addition, NSD's National Security Cyber Section is "primarily responsible for investigating and prosecuting foreign influence and interference cases that are 'cyber-enabled.'"[410]

Office of Justice Programs

DOJ's Office of Justice Programs (OJP) funded a wide range of programs related to criminal justice, including violence prevention research that addresses disinformation and domestic terrorism.[411] For example, in 2022, the National Institute of Justice (NIJ)— an agency within OJP—solicited proposals for "projects targeted toward developing a better understanding of the domestic radicalization phenomenon," including "research on countering mis-, dis-, and mal-information" in relation to "radicalization to violent extremism," though the rewarded proposals do not appear to cover disinformation.[412]

[409] U.S. DEP'T OF JUST., OFF. OF THE INSPECTOR GENERAL, EVALUATION OF THE U.S. DEPARTMENT OF JUSTICE'S EFFORTS TO COORDINATE INFORMATION SHARING ABOUT FOREIGN MALIGN INFLUENCE THREATS TO U.S. ELECTIONS 4 (2024), https://oig.justice.gov/sites/default/files/reports/24-080.pdf [hereinafter DOJ OIG REPORT ON FMI]. In fact, the report states "NSD's [Counterintelligence and Export Control Section] is the lead NSD office for responding to foreign malign influence threats." *Id.* at 23.

[410] *Id.* at 4. In press releases in 2024, DOJ credited the Counterintelligence and Export Control Section and the National Security Cyber Section with work around investigating and prosecuting Russian government-operated social media operations directing disinformation to U.S. audiences and elsewhere, as well as the indictment of two RT employees for "a $10 million scheme to create and distribute content to U.S. audiences with hidden Russian government messaging." *Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm,* DEP'T OF JUST. (July 9, 2024), https://www.justice.gov/opa/pr/justice-department-leads-efforts-among-federal-international-and-private-sector-partners; *Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere,* DEP'T OF JUST. (Sept. 4, 2024), https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence; *Two RT Employees Indicted for Covertly Funding and Directing U.S. Company that Published Thousands of Videos in Furtherance of Russian Interests*, DEP'T OF JUST. (Sept. 4, 2024), https://www.justice.gov/opa/pr/two-rt-employees-indicted-covertly-funding-and-directing-us-company-published-thousands.

[411] *See About Us,* OFF. OF JUST. PROGRAMS, https://www.ojp.gov/about (last visited Aug. 6, 2026).

[412] *NY FY22 Research and Evaluation on Domestic Radicalization and Violent Extremism,* NAT'L INST. OF JUST., https://nij.ojp.gov/funding/opportunities/o-nij-2022-171193 (last visited Aug. 6, 2026) (NIJ rewarded two awards for 2022: *Understanding and Responding to Domestic Extremism Financing* and *Understanding the Complete Spectrum of the Left-Wing and Environmental Movement: A Data Driven Approach* – the proposals can be read at the above link.).

In 2023, NIJ solicited proposals on the same topic of radicalization to violent extremism pipeline, with a passing reference to disinformation in the full solicitation.[413] Two proposals awarded by NIJ specifically reference disinformation: $449,897 award to Youngstown State University to further develop their "existing big-data project, the Frames of Misinformation, Extremism, and Conspiracism" in order "to measure and examine the content of violent extremist and accelerationist discourse" on social media; and a $953,203 award to Clemson University examining how high-profile events trigger disinformation.[414]

In April 2025, DOJ terminated 373 grants from OJP, including grants under the 2022 solicitation on domestic radicalization and violent extremism.

Federal Bureau of Investigation

As part of the FBI's National Security Branch (NSB), the Foreign Influence Task Force (FITF) was housed within the Counterintelligence Division "and composed agents, analysts, and professional staff from the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative Divisions."[415] As of July 2024, the FITF was "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 was "specifically charged with identifying and combating foreign influence operations targeting democratic institutions and values inside the United States."[416]

[413] *NIJ FY23 Research and Evaluation on Domestic Radicalization and Violent Extremism*, NAT'L INST. OF JUST., https://nij.ojp.gov/funding/opportunities/o-nij-2023-171569 (last visited Aug. 6, 2026); *NIJ FY23 Research and Evaluation on Domestic Radicalization and Violent Extremism*, NAT'L INST. OF JUST., https://nij.ojp.gov/funding/opportunities/o-nij-2023-171569 (last visited Aug. 6, 2026). Indeed, in a NIJ webinar on the funding solicitation, NIJ said that they "went beyond just mis-, dis-, and mal- information this year and showed interest in research that proposes strategies for effective technologies and tools for identification, moderation, and/or removal of extremist content with the end goal of informing effective messaging and counter-narrative campaigns." *Transcript: Fiscal Year 2023 Research and Evaluation on Domestic Radicalization and Violent Extremism*, NAT'L INST. OF JUST. https://web.archive.org/web/20240706114950/https://nij.ojp.gov/funding/transcript-fiscal-year-2023-research-and-evaluation-domestic-radicalization-and-violent-extremism (last visited Aug. 6, 2026).

[414] *A Frame Analysis of Violence and Acceleration in Cognitive Radicalization*, NAT'L INST. OF JUST., https://nij.ojp.gov/funding/awards/15pnij-23-gg-01382-domr (last visited July 14, 2026); *Networks and Pathways of Violent Extremism: Effectiveness of Dis/Misinformation Campaigns*, NAT'L INST. OF JUST., https://nij.ojp.gov/funding/awards/15pnij-23-gg-01381-domr (last visited July 14, 2026).

[415] Nikki Floris, *Securing America's Elections: Oversight of Government Agencies,* FED. BUREAU OF INVESTIGATION (Oct. 22, 2019), https://www.fbi.gov/news/speeches-and-testimony/securing-americas-elections-oversight-of-government-agencies-102219.

[416] DOJ OIG REPORT ON FMI, *supra,* at 31; *Oversight of Government Agencies, supra*; *Combating Foreign Influence*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/investigate/counterintelligence/foreign-influence [https://web.archive.org/web/20240719084414/https://www.fbi.gov/investigate/counterintelligence/foreign-influence] (last visited July 29, 2026).

According to the FBI's website in 2024, one way the FITF supported its mission was "by providing foreign malign influence (FMI) threat information to companies hosting social media (Social Media Platforms) so that they may, based on their independent judgment, initiative, and decision-making process, take steps to mitigate such threats."[417] The FITF has claimed it "does not perform narrative or content-based analysis,"[418] although there are documented instances in which the FBI shared specific posts or content with a social media platform after determining it had foreign origin.[419] The FITF was disbanded in February 2025.[420]

[417] *Combating Foreign Influence*, *supra*.
[418] THE WEAPONIZATION OF CISA, *supra,* at 17.
[419] DOJ OIG REPORT ON FMI, *supra,* at 17, fn. 32.
[420] DEP'T OF JUST., OFF. OF THE ATT'Y GEN., GENERAL POLICY REGARDING CHARGING, PLEA NEGOTIATIONS, AND SENTENCING 4 (Feb. 5, 2025), https://www.justice.gov/ag/media/1388541/dl.

Counter-Disinformation Funding

PCLOB sought information on counter-disinformation programming, grants, and research funding efforts since 2020. The FBI reported no such funding. DOJ provided specific funding examples that were responsive to PCLOB's request (see Table 1 below and brief descriptions thereafter). DHS did not respond to PCLOB's requests regarding funding.[421]

Table 1. DOJ OJP Disinformation-Related Funding

Number	Type	Fiscal Year	Award ID	Awarding/Funding Agency	Recipient	Amount
01	Grant	2022	15PBJA22 GG01559 HATE	DOJ	Multnomah County	$800,000
02	Grant	2023	15PNIJ23 GG01382 DOMR	DOJ	Youngstown State University	$449,897
03	Grant	2023	15PNIJ23 GG01381 DOMR	DOJ	Clemson University	$953,203
04	Grant	2023	15PNIJ23 GG01385 DOMR	DOJ	University of Illinois	$751,254
05	Grant	2022	15PBJA22 GG04859 ADVA	DOJ	Committee of 100, Inc.	$ 400,000
06	Grant	2024	15PBJA24 GG02835 ADVA	DOJ	Institute for Strategic Dialogue-U.S.	$ 2,000,000
07	Grant	2023	15PBJA23 GG05356 HATE	DOJ	City of Chicago	$ 399,976

Grant 01

- Funding Program Name: Matthew Shepard and James Byrd, Jr. Hate Crimes Education, Investigation, and Prosecution Program[422]
- Recipient Program Name: The Hate Crime Reporting and Response Initiative (HCRRI)

[421] CISA informed PCLOB that they had no responsive funding obligations to report during the period in question. PCLOB Correspondence with CISA (Mar. 12, 2025).
[422] *Grant to Multnomah County,* USASPENDING.GOV https://www.usaspending.gov/award/ASST_NON_15PBJA22GG01559HATE_1550 (last visited Aug. 7, 2026).

- Description of Recipient Programs: "Focuses on outreach, education, and investigation and prosecution of hate crimes. The Multnomah County District Attorney's Office (MCDA) will detail a specialized bias [data-driven approach] to create an interwoven network of knowledge and relationships that ensures victims are heard and supported in reporting hate incidents and crimes, and that these crimes are consistently referred to MCDA for investigation and prosecution."[423]

Grant 02

- Funding Program Name: National Institute of Justice Research, Evaluation, and Development Project Grants[424]
- Recipient Program Name: A Frame Analysis of Violence and Accelerationism in Cognitive Radicalization[425]
- Description of Recipient Programs: "Measure and examine the content of violent extremist and accelerationist discourse using social-media posts from a group of platforms known to host concentrations of extremist material."[426]

Grant 03

- Funding Program Name: National Institute of Justice Research, Evaluation, and Development Project Grants[427]
- Recipient Program Name: Networks and Pathways of Violent Extremism: Effectiveness of Dis/Misinformation Campaigns[428]
- Description of Recipient Programs: "This project seeks to answer the following overarching questions: (1) what characteristics of high-profile events are more likely to trigger online MDM campaigns? (2) what network patterns are associated with online MDM clusters, and dissemination pathways, and what are the technical characteristics of more vulnerable platforms? (3) what are the common characteristics of organizations and

[423] *Id. See Bias Crimes Dashboard*, MULTNOMAH CNTY. DIST. ATT'Y https://www.mcda.us/index.php/bias-crimes-dashboard (last visited Aug. 7, 2026).
[424] *Grant to Youngstown University*, USASPENDING.GOV https://www.usaspending.gov/award/ASST_NON_15PNIJ23GG01382DOMR_1550 (last visited Aug. 7, 2026).
[425] *A Frame Analysis of Violence and Accelerationism in Cognitive Radicalization,* NAT'L INST. OF JUST. https://nij.ojp.gov/funding/awards/15pnij-23-gg-01382-domr (last visited Aug. 7, 2026).
[426] *Grant to Youngstown University*, *supra. See* Richard Rogers, *Frames of Misinformation, Extremism, and Conspiracism: A Purposive Sample of Social-Media Channels, Discussion Forums, and Web Pages*, RESEARCHGATE, https://www.researchgate.net/publication/378336450_Frames_of_Misinformation_Extremism_and_Conspiracism_December_2023 (Feb. 2024).
[427] *Grant to Clemson University*, USASPENDING.GOV https://www.usaspending.gov/award/ASST_NON_15PNIJ23GG01381DOMR_1550 (last visited Aug. 7, 2026).
[428] *Networks and Pathways of Violent Extremism: Effectiveness of Dis/Misinformation Campaigns*, NAT'L INST. OF JUST. https://nij.ojp.gov/funding/awards/15pnij-23-gg-01381-domr (last visited Aug. 7, 2026).

- other actors engaged in MDM campaigns? (4) what are the key themes and linguistic features of MDM campaigns, and how do they vary across disseminators and adopters?"

Grant 04

- Funding Program Name: National Institute of Justice Research, Evaluation, and Development Project Grants[429]
- Recipient Program Name: Domestic Terrorism Targeting America's Political Elites[430]
- Description of Recipient Programs: "The purpose is to investigate the prevalence and political consequences of exposure to diffused domestic terrorism (DDT) among state legislators, mayors and staff nationwide."[431]

Grant 05

- Funding Program Name: Community-Based Approaches to Advancing Justice[432]
- Recipient Program Name: A Comprehensive and Coordinated Response to Anti-Asian Hate Crimes in NYC[433]
- Description of Recipient Programs: "Grant funds will be used to accomplish three goals: (1) the standardization of community-based anti-Asian hate crime data; (2) the development and implementation of an anti-Asian hate crime awareness campaign; and (3) the development and implementation of an [Asian American and Pacific Islander] curriculum for K-12 students focused on Asian American history and culture as an anti-Asian hate crime prevention measure."[434]

Grant 06

- Funding Program Name: Community-Based Approaches to Advancing Justice[435]
- Recipient Program Name: Strengthening Sustainable Community-Based Efforts to Prevent and Respond to Hate[436]
- Description of Recipient Programs: "The purpose is to work with community-based organizations (CBOS) and local governments in five cities across the US to enhance

[429] *Grant to University of Illinois*, USASPENDING.GOV https://www.usaspending.gov/award/ASST_NON_15PNIJ23GG01385DOMR_1550 (last visited Aug. 7, 2026).
[430] *Domestic Terrorism Targeting America's Political Elites*, NAT'L INST. OF JUST. https://nij.ojp.gov/funding/awards/15pnij-23-gg-01385-domr (last visited Aug. 7, 2026).
[431] *Grant to University of Illinois*, *supra.*
[432] *Grant to Committee of 100, Inc.,* USASPENDING.GOV https://www.usaspending.gov/award/ASST_NON_15PBJA22GG04859ADVA_1550 (last visited Aug. 7, 2026).
[433] *Id.*
[434] *Id.*
[435] *Grant to Institute for Strategic Dialogue-U.S.,* USASPENDING.GOV https://www.usaspending.gov/award/ASST_NON_15PBJA24GG02835ADVA_1550 (last visited Aug. 7, 2026).
[436] *Id.*

community-based prevention of, responses to and reporting of hate crimes and incidents."[437]

Grant 07

- Funding Program Name: Matthew Shepard and James Byrd, Jr. Hate Crimes Education, Investigation, and Prosecution Program[438]
- Recipient Program Name: Hate Crime Reporting Community Pilot Program[439]
- Description of Recipient Programs: "The purpose of the program is to encourage the reporting of hate crimes, hate incidents, and community tensions that may lead to hate crimes in communities of the city of Chicago that experience higher levels of hate crimes."[440]

[437] *Id.*
[438] *Grant to City of Chicago,* USASPENDING.GOV https://www.usaspending.gov/award/ASST_NON_15PBJA23GG05356HATE_1550 (last visited Aug. 7, 2026).
[439] *Id.*
[440] *Id.*

APPENDIX C: DISINFORMATION COUNTERMEASURES

Table C, 1: *Disinformation Countermeasures*[441]

Countermeasures	Definition	Impact[442]
Bans & Deplatforming	Removing an account or preventing an individual from creating an account	Speaker-based intervention Impacts user, platform, and marketplace
Shadow Bans & Demotion	Tagging an account for de-prioritization by the platform's algorithm, so the account's posts appear less frequently or to fewer people, if at all	Speaker- or speech-based intervention Impacts user, platform, and marketplace
Post Takedowns	Removing individual posts and re-posts based on their content or source of re-post	Speech-based intervention Impacts user, platform, and marketplace
Labeling	Insertion of relevant context or advisories to inform or influence how content is viewed, does not always include fact-checking[443]	Speech-based intervention Impacts user, platform, marketplace
Debunking/ Fact-checking	Issuance of corrective information to disprove a false or misleading claim[444]	Speech-based intervention Impacts platform and marketplace, possibly impacts user
Prebunking	Anticipating a specific disinformation narrative or technique and proactively confronting it before it spreads[445]	Speech-based intervention May impact marketplace
Counter-narratives	Truthful communication campaigns designed to compete with disinformation at a narrative and psychological level instead of relying solely on the presentation of facts[446]	Speech-based intervention May impact marketplace

[441] This appendix is intended to include only countermeasures occurring online; other countermeasures, such as prosecution under FARA, exist. For a public example of a foreign malign influence indictment, *see*, *United States v. Kalashnikov*, No. 1:24-cr-00519 (S.D.N.Y. Sept. 3, 2024).
[442] Specific countermeasures can impact the speaker (or author) or speech (or content). Specific countermeasures, such as deplatforming a user or demoting his speech, may impact free speech more than other interventions, such as labeling or media literacy programs.
[443] Jon Bateman and Dean Jackson, *Countering Disinformation Effectively: An Evidence-Based Policy Guide*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE 35 (2024), https://assets.carnegieendowment.org/static/files/Carnegie_Countering_Disinformation_Effectively.pdf.
[444] *Id.* at 29.
[445] *Id.* at 55.
[446] *Id.* at 43.

Monitoring & Analysis	Tracking the origin, spread, and other patterns associated with disinformation to facilitate future countermeasures, analytic work, or investigations	Speaker- or speech-based non-intervention May impact user and marketplace through chilling effects
Media Literacy/ Media Rating	Encouraging development of critical thinking skills to better assess the value, accuracy, and trustworthiness of content and providers of content	Speech-based intervention May impact marketplace
Criminal Prosecution or Civil Liability Actions	Imposing public disclosure obligations when acting in the United States as an agent of a foreign government. Publicly trying FARA violators and stopping foreign governments from using undisclosed agents "to illegally influence public debate or suborn sedition"[447]	Speaker-based intervention Impacts user

[447] *Press Release: Liability for Unregistered Foreign Agents*, DEP'T OF JUST. (Sept. 16, 2026), https://www.justice.gov/opa/pr/liability-unregistered-foreign-agents.

APPENDIX D: PCLOB CORRESPONDENCE WITH DHS

[THIS PAGE INTENTIONALLY LEFT BLANK]

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
WASHINGTON, D.C. 20002

August 4, 2022

VIA E-MAIL AND U.S. MAIL

The Honorable Alejandro Mayorkas
Secretary of Homeland Security
Washington, DC 20528

Dear Secretary Mayorkas:

As Chair and Member of the Privacy and Civil Liberties Oversight Board ("PCLOB"), we are writing to request information about activities conducted by the Department of Homeland Security ("DHS") to counter disinformation. Counter-disinformation activities may have serious impacts on privacy and civil liberties, and the PCLOB has the authority to review and assess these activities and those impacts.

The mission of the PCLOB is to: "(1) analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and (2) ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism."[1]

Consistent with those authorities, the PCLOB is currently considering an oversight review of the government's efforts to combat domestic terrorism. As you are aware, the PCLOB held an online public forum on May 26, 2022, to examine privacy and civil liberties issues related to these efforts, and one central area of inquiry involved examining the steps federal agencies are taking to ensure that they are protecting Americans' First Amendment rights, including free speech online. The rules under which the government may lawfully monitor communications, including efforts to combat disinformation, must be transparent and include safeguards for privacy and civil liberties.

We are aware that DHS has suspended its Disinformation Governance Board ("DGB"),[2] but the controversy over DHS's creation of the DGB has highlighted that, as a DHS fact sheet about the DGB stated, "For nearly 10 years, different agencies across DHS have worked to address

[1] 42 U.S.C. 2000ee(c).
[2] Nomaan Merchant and Amanda Seitz, "New 'Disinformation Board' Paused Amid Free Speech Questions," Associated Press, May 18, 2022, *available at* https://apnews.com/article/government-and-politics-national-security-83c67505703c02b0de154b21abd5c569.

disinformation that threatens our homeland security."[3] In addition, the National Strategy to Combat Domestic Terrorism ("National Strategy") states:

> A number of departments and agencies are already pursuing efforts to enhance community-level and individual-level resilience to violence, many of which help to advance the prevention of domestic terrorism. For example, the Department of Homeland Security and others are either currently funding and implementing or planning evidence- based digital programming, including enhancing media literacy and critical thinking skills, as a mechanism for strengthening user resilience to disinformation and misinformation online for domestic audiences.[4]

The National Strategy further links efforts to combat terrorism to the examination of disinformation, stating, "[T]he intelligence and law enforcement communities will enhance the government's understanding of how foreign malign influence operations and the dissemination of disinformation, including by foreign governments, relate to the domestic terrorism threat we face."[5]

Internal DHS documents provided to Senators Charles E. Grassley and Josh Hawley, and released by the Senators on June 7, 2022, confirm that these DHS activities predated the creation of the DGB and were premised, at least in part, on counterterrorism.[6] For example, a memorandum entitled, "Organizing DHS Efforts to Counter Disinformation" states, "DHS components are already engaged in countering disinformation," and goes on to list five functional areas in which they do so.[7]

DHS's efforts to monitor online speech and counter disinformation raise many questions about the impact of DHS activities on Americans' rights. As the PCLOB assesses the scope and nature of its oversight of the government's efforts to combat domestic terrorism, we seek to

[3] Fact Sheet: DHS Internal Working Group Protects Free Speech and Other Fundamental Rights When Addressing Disinformation That Threatens the Security of the United States, May 2, 2022, *available at* https://www.dhs.gov/news/2022/05/02/fact-sheet-dhs-internal-working-group-protects-free-speech-other-fundamental-rights. The fact sheet provided three examples of such work, by the U.S. Customs and Border Protection ("CBP"), the Federal Emergency Management Agency ("FEMA"), and the Cybersecurity and Infrastructure Security Agency ("CISA"). *Id.* We note CISA has a public website that describes its work, which refers to, and defines, three terms— "misinformation," "disinformation," and "malinformation" (collectively labeled "MDM"). See, https://www.cisa.gov/mdm.

[4] *National Strategy for Countering Domestic Terrorism*, p. 18, https://www.whitehouse.gov/wp-content/uploads/2021/06/National-Strategy-for-Countering-Domestic-Terrorism.pdf.

[5] *Id.*, p. 20.

[6] Sen. Charles E. Grassley and Sen. Josh Hawley, Letter to Secretary Alejandro Mayorkas, June 7, 2022, https://www.grassley.senate.gov/imo/media/doc/grassley_hawley_to_deptofhomelandsecuritydisinformationgovernanceboard.pdf

[7] Robert Silvers and Samantha Vinograd, Memorandum for the Secretary: Organizing DHS Efforts to Counter Disinformation, Sept. 13, 2021, p. 2. The memorandum notes three functions—identification, analysis, and information sharing—in which DHS's Office of Intelligence and Analysis (I&A) is engaged, including a "Homeland Influence Task Force" that I&A operates that "collects information on possible disinformation from publicly available sources as well as other intelligence sources." *Id.*

examine whether DHS's activities have been limited to issuing statements to counter alleged disinformation, or whether DHS has taken efforts to suppress or in any way limit speech that it labels "disinformation"; whether any DHS efforts were taken to distinguish the speech of foreign actors from that of U.S. persons; and whether DHS has worked with or asked private companies to suppress or limit U.S. persons' speech.[8]

To enable the PCLOB to begin to assess the privacy and civil liberties impacts of DHS's monitoring of American's speech, and its efforts to combat disinformation/mis-,dis-, and mal-information ("MDM") activities, we request the following information:[9]

1. Is there a uniform definition of "disinformation" employed by all DHS components? If so, please state it. If not, why not?
2. Please explain (a) how DHS determines that a particular source of disinformation is foreign or domestic; (b) how DHS determines that a foreign source is influencing a domestic audience and what metrics are applied to this determination; (c) how DHS assesses the effectiveness of its efforts to combat disinformation; and (d) any minimization procedures used to remove consideration of U.S. person information.
3. What is the process by which DHS makes determinations of the truth or falsehood of statements? Who are the officials making these determinations, and what review process, if any, exists?
4. What is the process by which DHS determines whether to "counter" disinformation? Who are the officials making the determination whether to counter disinformation, and what review process, if any, exists for those determinations?
5. What are the means and methods by which DHS has countered disinformation? Which methods are ongoing, and which have ceased? What other methods has DHS contemplated or considered to counter disinformation?
6. What steps has DHS asked or suggested that private companies take or consider taking to counter disinformation? Has DHS established any formal or informal public-private partnerships to support counter-disinformation efforts, including but not limited to, contracts, memoranda of agreement/memoranda of understanding, cooperative research and development agreements, or any other formal or informal agreements?
7. What actions have been taken by DHS, or at the behest of or in cooperation with DHS, to influence U.S. persons' opinions or beliefs on topics about which DHS believes disinformation has been disseminated? What actions have been taken by DHS, or at the behest of or cooperation with DHS, to limit speech that DHS has deemed disinformation?

[8] For example, among the documents released by Senators Grassley and Hawley is a briefing memo for a meeting between Undersecretary Silvers and executives at Twitter described as "an opportunity to discuss operationalizing public-private partnerships between DHS and Twitter," including "that Twitter become involved in Disinformation Governance Board Analytic Exchanges on Domestic Violent Extemism [sic] (DVE) and Irregular Migration." *See*, Letter to Secretary Mayorkas, p.18.

[9] While we acknowledge the review being conducted by the Homeland Security Advisory Council, *see,* Rebecca Beitsch, "DHS to Pause Work of Disinformation Board," The Hill, May 18, 2022, *available at* https://thehill.com/news/state-watch/3493070-dhs-to-pause-work-of-disinformation-board/, the PCLOB provides a Congressionally-established independent check on the sufficiency of privacy and civil liberties protections.

We request this information in our individual capacities. As such, this request does not yet currently constitute a formal oversight project of the PCLOB.

To provide your responses, or should you or your staff have any questions about this letter, please contact Tatjana Naquin (tatjana.naquin@pclob.gov) or John Tran (john.tran@pclob.gov). Thank you for your attention to our request for information.

Sincerely,

Sharon Bradford Franklin

Sharon Bradford Franklin
Chair, Privacy and Civil Liberties Oversight Board

Beth A. Williams

Beth A. Williams
Member, Privacy and Civil Liberties Oversight Board

cc: Lynn Parker Dupree, Chief Privacy Officer
Katherine Culliton-González, Officer for Civil Rights and Civil Liberties

Executive Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

July 20, 2023

Sharon Bradford Franklin
Chair, Privacy and Civil Liberties Oversight Board
Washington, DC 20002

Edward W. Felten
Member, Privacy and Civil Liberties Oversight Board
Washington, DC 20002

Travis LeBlanc
Member, Privacy and Civil Liberties Oversight Board
Washington, DC 20002

Beth A. Williams
Member, Privacy and Civil Liberties Oversight Board
Washington, DC 20002

Richard E. DiZinno
Member, Privacy and Civil Liberties Oversight Board
Washington, DC 20002

Dear Privacy and Civil Liberties Oversight Board Members:

Thank you for your August 4, 2022 letter to the Department of Homeland Security (DHS), in which you inquired about the Department's efforts to address disinformation that threatens homeland security missions. I am responding on behalf of the Department, and I apologize for the delayed response.

I understand that the Privacy and Civil Liberties Oversight Board (PCLOB) is pursuing an oversight project on countering domestic terrorism,[1] and that there was an introductory meeting with DHS offices and agencies and PCLOB staff to discuss a path forward for this review.

In recent years, many threats to the homeland have been exacerbated by disinformation. While there is no Department-wide definition for this term, the Cybersecurity and Infrastructure Security Agency (CISA) defines disinformation as information "deliberately created to mislead,

[1] As provided in a February 9, 2023 email to the then-Acting Chief Privacy Officer, it is the Department's understanding that the August 4, 2022 request for information from Chair Bradford Franklin and Member Williams is now a full Board request pursuant to the Board's oversight project on domestic terrorism.

harm, or manipulate a person, social group, organization, or country."[2] DHS offices and agencies work to mitigate the harms of disinformation and misinformation in their respective mission areas.

For example, CISA works with critical infrastructure owners and operators to ensure they are aware of the risks of influence operations leveraging social media and online platforms for disinformation. In February 2022, in light of increased risk after Russia's invasion of Ukraine, CISA published a guide intended to assist with preparing for and mitigating foreign influence operations targeting critical infrastructure.[3] CISA found that recently observed foreign influence operations abroad demonstrate that foreign governments and related actors have the capability to quickly employ sophisticated influence techniques to target U.S. audiences with the goal to disrupt U.S. critical infrastructure and undermine U.S. interests and authorities. The guide outlines insights and proactive steps organizations can take to assess their risk from information manipulation, increase resilience, and mitigate the impact of potential foreign influence operations on U.S. critical infrastructure. Additional products on this topic are available on the CISA website.[4]

The Department's Office of Intelligence and Analysis (I&A) shared information with state and local law enforcement and private sector critical infrastructure owners and operators on foreign efforts to amplify misinformation about 5G telecommunications spreading the COVID-19 virus. Through 2020 and into 2021, I&A noted in intelligence assessments that such misinformation was likely responsible for an increase in criminal vandalism and destruction of a range of 5G communications infrastructure in the United States. I&A's efforts involve all-source intelligence, including open-source information.

With respect to your specific inquiry regarding the Department's efforts to counter disinformation with a nexus to domestic terrorism, on May 18, 2022, Secretary Mayorkas tasked the nonpartisan Homeland Security Advisory Council (HSAC) to stand up a subcommittee to conduct a thorough review and assessment of those efforts. The Disinformation Best Practices and Safeguards Subcommittee (the "Subcommittee"), which was led by Former Secretary of Homeland Security Michael Chertoff and former Deputy Attorney General Jamie Gorelick, completed its work in late August 2022. On August 24, 2022, the HSAC deliberated and approved the HSAC Subcommittee's Final Report in a public meeting. The Subcommittee concluded that disinformation threatens the homeland and that it is critical that the Department take steps to address this threat.[1] In accordance with the HSAC's recommendation, Secretary Mayorkas terminated the Disinformation Governance Board and rescinded its charter effective, August 24, 2022. [5]

As noted by the HSAC in its final report on the issue, "The Department's Office of General Counsel, the Department's Privacy Office, and the Department's Office for Civil Rights and Civil Liberties (CRCL) support the Department's mission to secure the nation while

[2] https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation.
[3] https://www.cisa.gov/resources-tools/resources/cisa-insights-preparing-and-mitigating-foreign-influence-operations
[4] cisa.gov/mdm.
[5] dhs.gov/news/2022/08/24/following-hsac-recommendation-dhs-terminates-disinformation-govemance-board

preserving individual liberty, fairness, and equality under the law, to include setting policies for each Component, especially with respect to the requirements and constraints mandated by legal, privacy, and civil rights and civil liberties responsibilities. These policies are properly assembled by the relevant legal, privacy, and civil rights officers and conveyed to the relevant Components and among Department senior leadership."[6]

The Department used the HSAC recommendations as a guide to address threat streams that undermine the security of our country, while promoting transparency in our work. DHS does not seek to compel, pressure, or influence social media companies to take actions with respect to specific posts or actors on social media, nor does it seek to obtain or exercise any new authorities concerning disinformation. DHS remains committed to conducting all its activities, including those pertaining to disinformation, in a manner that complies with the law and protects individuals' privacy, civil rights, and civil liberties.

We are committed to continue working with you to answer any outstanding questions on DHS'swork.

Sincerely,



Kimberly O'Connor
Executive Secretary

[6] https://www.dhs.gov/publication/homeland-security-advisory-council-disinformation-subcommittee-final-report