The Mechanics of Government Censorship

How the Biden Administration Converted the Cybersecurity and Infrastructure Security Agency into the Thought Police

U.S. SENATE COMMITTEE ON
COMMERCE, SCIENCE, & TRANSPORTATION
CHAIRMAN TED CRUZ

EXECUTIVE SUMMARY

Under the leadership of Senator Ted Cruz, the United States Senate Committee on Commerce, Science, and Transportation (the Committee) led an investigation into how the Biden administration transformed the Cybersecurity and Infrastructure Security Agency (CISA) from an agency focused on cyber and foreign threats to critical infrastructure into an agency focused on policing the speech of Americans. The Committee determined that CISA (1) acted outside both the First Amendment and its own authority by pressuring social media companies to take action against constitutionally protected speech, (2) developed internal programs to monitor and flag content before essentially outsourcing its operation to third parties, (3) expanded these activities without challenge from either industry or the DHS Office of Inspector General (OIG), enabling the agency to operate with impunity, and (4) provided evasive responses when DHS OIG attempted to examine its censoring activities, further obstructing accountability.

While CISA focused its censorship efforts on social media, anti-free speech bureaucrats are now setting their sights on the next major technological advancement: artificial intelligence (AI). As members of Congress consider legislation to establish new AI regulations and AI-focused government agencies, they should keep in mind the Biden administration's transformation of CISA—which Congress created with widespread bipartisan support to protect national security—into an unaccountable censorship agency.

Congress must continue to take an active role in the operations and policies of federal agencies because, regardless of who occupies the White House, unelected bureaucrats have outsized power to direct agencies' activities. The Committee recommends that Congress pass legislation to:

- Create transparency around federal agency communication with private entities on issues that may affect American speech.
- Produce guidelines that clearly restrict government officials from influencing social media platforms' content moderation decisions of constitutionally protected speech.
- Establish a reporting mechanism to allow platforms to report when they may be subjected to government jawboning efforts around censorship or content moderation.
- Before contemplating any new federal AI regulation, enact guardrails to prevent federal AI programs, such as the NAIRR and the Center for AI Standards and Innovation (CAISI) (formerly known as the AI Safety Institute), from curtailing speech in the name of addressing so-called harms.

TABLE OF CONTENTS

REPORT

I. *Background*

When President Trump won the 2016 presidential election, Democrats grew obsessed with the idea that his election was only made possible by Russian interference—namely collusion between the Trump campaign and faux-supporters spreading "fake news" on social media.[1] For instance, House Democrat Minority Leader Hakeem Jeffries claimed that Russia "interfered with our election" by "artificially plac[ing] Donald Trump at 1600 Pennsylvania Avenue"[2] and failed presidential candidate Hillary Clinton referred to President Trump as an "illegitimate president."[3] We now know these claims were false. There is no evidence that the Trump campaign colluded with Russia.[4] A 2023 New York University study demonstrated that Russian operations on Twitter played no meaningful role in President Trump's 2016 victory.[5]

Since 2016, the Left has decried "fake news" on social media. They typically have defined "fake news" to be anything that does not fit the Democrat Party's narrative, such as the COVID-19 lab leak theory, which is now acknowledged by the Federal Bureau of Investigation, Department of Energy, and Central Intelligence Agency (CIA) as the pandemic's "likely" cause.[6] Other examples of supposedly "fake" news included the authenticity of the contents of Hunter Biden's laptop—which the Department of Justice later presented in federal court as authentic[7]—and even the fact that biological sex makes a difference in sports competition.[8] At the same time, Democrats increased political pressure on social media companies to scrub supposedly fake news from their websites.[9]

Realizing that the term "fake news" could only do so much to prevent people from talking about these topics, the Left coined a new term for objectionable content on social media: "MDM"— "misinformation," "disinformation," and "malinformation."[10]

- Misinformation is information that is "false, but not created or shared with the intention of causing harm."[11]
- Disinformation is information that is "deliberately created to mislead, harm, or manipulate a person, social group, organization, or country."[12]
- Malinformation is "information that is factual, but used out of context to mislead, harm, or manipulate."[13]

Claiming that MDM was a threat to the country and that social media platforms were "killing people," President Biden ramped

---

1 Eric Tucker & Nomaan Merchant, *Durham Report Takeaways: A 'Seriously Flawed' Russia Investigation and Its Lasting Impact on the FBI*, Associated Press (May 16, 2023), https://apnews.com/article/durham-report-fbi-trump-clinton-2016-campaign-f3039e651eeb35a09091c363419e6766.

2 Judy Woodruff, *On Mueller Report, Trump Is 'Completely Clueless,' Says Jeffries*, PBS NewsHour (Apr. 18, 2019), https://www.pbs.org/newshour/show/on-mueller-report-trump-is-completely-clueless-says-jeffries.

3 Jane Pauley, *Hillary Clinton: "Trump Knows He's An Illegitimate President*," CBS Sunday Morning (Sept. 29, 2019), https://www.youtube.com/watch?v=XQesfLIycJw.

4 Minority Staff of S. Select Comm. on Intel., 116th Cong., Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 5: Counterintelligence Threats and Vulnerabilities, S. Rep. No. 116-290, at 941 (2020).

5 Gregory Eady et al., *Exposure to the Russian Internet Research Agency Foreign Influence Campaign on Twitter in the 2016 US election and Its Relationship to Attitudes and Voting Behavior*, 14 Nature Commc'ns 62 (2023).

6 Hannah Rabinowitz, *Director Wray Acknowledges Bureau Assessment that Covid-19 Likely Resulted from Lab Incident,* CNN (Mar. 1, 2023), https://www.cnn.com/2023/02/28/politics/wray-fbi-covid-origins-lab-china/index.html; Julian E. Barnes, *C.I.A. Now Favors Lab Leak Theory to Explain COVID's Origins*, N.Y. Times (Jan. 27, 2025), https://www.nytimes.com/2025/01/25/us/politics/cia-covid-lab-leak.html.

7 *See* United States v. Biden, No. 1:23cr00061-MN, Pl.'s Opp'n to Def.'s Mot. to Dismiss at 7, ECF No. 68 (D. Del. Jan. 16, 2024).

8 Elizabeth Troutman Mitchell, *Democrats Flip-Flop on Unpopular Positions on Transgenderism*, Daily Signal (Oct. 28, 2024), https://www.dailysignal.com/2024/10/28/why-do-democrats-flip-flop-men-womens-sports-transgender-procedures/.

9 Nicholas Confessore & Matthew Rosenberg, *Facebook Fallout Ruptures Democrats' Longtime Alliance With Silicon Valley,* N.Y. Times (Nov. 17, 2018), https://www.nytimes.com/2018/11/17/technology/facebook-democrats-congress.html.

10 CISA, *Mis-, Dis-, and Malinformation: Planning and Incident Response Guide for Election Officials*, 1 (2023), https://web.archive.org/web/20250203215736/https://www.cisa.gov/sites/default/files/publications/mdm-incident-response-guide_508.pdf.

11 *Id.*

12 *Id.*

13 *Id.*

up government efforts to censor Americans' speech online.[14] But the government's claim that MDM was a "crisis"[15] and national security threat[16] was just an attempt to accomplish what the Biden administration had long tried to do: shut down the speech of Americans with whom it disagreed.

A. The Federal Government's History of Censoring "Disinformation"

The First Amendment prohibits the federal government from censoring Americans' speech. In full, it provides that:

> "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or **abridging the freedom of speech**, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."[17]

Despite this prohibition, throughout American history the federal government has, at times, suppressed speech under the guise of national security. For instance, in 1798, Congress passed the Sedition Act, which prohibited publishing or saying anything "false, scandalous, and malicious" against the government for fear that disloyal people within the United States would side with France during the Quasi War.[18] Before it expired in 1801, ten people—including a member of Congress who declared President John Adams fit for "a madhouse" and a man who drunkenly shouted that he did not mind if a cannon shot President Adams in the rear—were convicted under the act.[19] Over a century later, during World War I, President Woodrow Wilson signed into law the Sedition Act of 1918, which imposed heavy penalties for criticizing the war effort, including saying or publishing "any disloyal, profane, scurrilous, or abusive language about the form of government of the United States, or the Constitution of the United States, or the military or naval forces of the United States."[20] Thousands were convicted under this law for putting the nation in peril by speaking out against the war.[21]

Since these laws expired, however, the Supreme Court has repeatedly held that government efforts to censor speech, including false speech, are unconstitutional.[22] For instance, in *Bond v. Floyd*, the Court considered whether the Georgia House of Representatives could constitutionally exclude a member for criticizing the Vietnam War.[23] In holding that the member's disqualification violated his First Amendment rights, the Court noted that even statements considered erroneous "must be protected to give freedom of expression the breathing space it needs to survive."[24] Almost fifty years later, in *United States v. Alvarez*, the Court struck down the Stolen Valor Act, which prohibited false claims of military commendations.[25] The Court rejected the government's argument that there was a "general exception" to First Amendment protection "for false statements."[26] The Court reasoned that if "the interest in truth discourse alone [were] sufficient to sustain a ban on speech,

---

[14] *See, e.g.*, Zeke Miller, *Watch: Biden Says Virus Disinformation Is 'Killing People,'* Associated Press (July 16, 2021), https://www.pbs.org/newshour/politics/watch-biden-says-virus-disinformation-is-killing-people.

[15] Nat'l Sec. Council, Nat'l Strategy for Countering Domestic Terrorism, 29 (June 2021), https://int.nyt.com/data/documenttools/biden-s-strategy-for-combating-domestic-extremism/22ddf1f2f328e688/full.pdf.

[16] Press Release, The White House, Fact Sheet: The Biden-Harris Administration is Taking Action to Restore and Strengthen American Democracy (Dec. 8, 2021) ("The Biden-Harris Administration is working to mitigate threats that mis- and disinformation pose to public safety and national security..."); Info. Integrity Rsch. Devel. Interagency Working Grp., Networking & Info. Tech. Rsch & Dev. Subcomm. of the Nat'l Sci. Tech. Council, Roadmap Researchers on Priorities Related to Information Integrity Research and Development, 1, 14 (Dec. 2022), https://www.nitrd.gov/pubs/Roadmap-Information-Integrity-RD-2022.pdf.

[17] U.S. Const. Amend. I (emphasis added).

[18] Sedition Act of 1798, ch. 74, 1 Stat. 596 (July 14, 1798).

[19] Stuart Leibiger, *The Alien and Sedition Acts*, https://billofrightsinstitute.org/essays/the-alien-and-sedition-acts, (last visited Sept. 25, 2025).

[20] Sedition Act of 1918, Pub. L. No. 65-150, § 3, 40 Stat. 553.

[21] Acacia Reed, et al., *Perilous Times; Free Speech in Wartime from the Sedition Act of 1798 to the War on Terrorism*, Wilson Center (Feb. 27, 2005), https://www.wilsoncenter.org/event/perilous-times-free-speech-wartime-the-sedition-act-1798-to-the-war-terrorism.

[22] *See* Valerie C. Brannon, Cong. Rsch. Serv. IF12180, False Speech and the First Amendment: Constitutional Limits on Regulating Misinformation (2022), https://crsreports.congress.gov/product/pdf/IF/IF12180.

[23] 385 U.S. 116, 132–35 (1966).

[24] *Id*. at 136.

[25] 567 U.S. 709, 730 (2012).

[26] *Id.* at 718.

absent any evidence that the speech was used to gain a material advantage, it would give government a broad censorial power unprecedented in [the] Court's cases or in our constitutional tradition."[27] As the Court concluded, the First Amendment "protects the speech we detest as well as the speech we embrace."[28]

The Supreme Court has repeatedly emphasized "that speech on public issues occupies the 'highest rung of the hierarchy of First Amendment values,' and is entitled to special protection."[29] The First Amendment gives such speech the "broadest protection" in order "'to assure (the) unfettered interchange of ideas for the bringing about of political and social changes desired by the people.'"[30] Moreover, the First Amendment "protects an individual's right to speak his mind regardless of whether the government considers his speech sensible and well intentioned or deeply 'misguided,' and likely to cause 'anguish' or 'incalculable grief.'"[31] The import of this protection is illustrated in *Matal v. Tam*, a 2017 case in which the Court held that the Lanham Act's broad prohibition on registering trademarks that may "'disparage….or bring…into contemp[t] or disrepute'…any person, group, or institution" violates the First Amendment.[32] In striking down the Act's disparagement clause, the Court reaffirmed that under the First Amendment, "'the public expression of ideas cannot be prohibited merely because the ideas are themselves offensive to some of their hearers.'"[33]

B. The Creation of CISA

The Cybersecurity and Infrastructure Security Agency Act of 2018 established CISA as a standalone agency within the Department of Homeland Security. [34] Both the Senate and the House passed the legislation unanimously, and President Trump signed it into law on November 16, 2018.[35] Congress created CISA to protect federal government networks and help protect the nation's critical infrastructure—like power grids, chemical and nuclear facilities, financial networks, and transportation systems—from physical and cyber threats. Its legal role is to formalize public-private threat sharing, coordinate incident response, and serve as a clearinghouse for technical expertise and assistance.[36] The Act's explicit purpose was to rebrand and strengthen the preexisting National Protection and Programs Directorate (NPPD) within DHS.[37]

Before CISA's creation, NPPD spearheaded the federal government's efforts to coordinate with "public sector, private sector, and government partners" to secure the country's cyber and physical infrastructure.[38] These efforts included actions aimed at protecting election infrastructure, which the Obama administration designated as critical infrastructure immediately following the 2016 election.[39] Of note, NPPD established an Election Task Force to "ensure a coordinated approach from the federal government" regarding cyber threats to election infrastructure."[40] Yet NPPD insisted its work was limited to election

[27] *Id.* at 723.

[28] *Id*. at 729.

[29] Connick v. Myers, 461 U.S. 138, 145 (1983) (quoting NAACP v. Claiborne Hardware Co., 458 U.S. 886, 913 (1982); Carey v. Brown, 447 U.S. 455, 467 (1980)).

[30] Buckley v. Valeo, 424 U.S. 1, 14 (1976) (quoting Roth v. U.S., 354 U.S. 476, 484 (1957)).

[31] 303 Creative LLC v. Elenis, 600 U.S. 570, 586 (2023) (quoting Hurley v. Irish-Am. Gay, Lesbian and Bisexual Grp. of Boston, 515 U.S. 557, 574 (1995); Snyder v. Phelps, 562 U.S. 443, 456 (2011)).

[32] 582 U.S. 218, 246 (2017) (quoting 15 U.S.C. § 1052(a)).

[33] *Id.* at 244 (quoting Street v. New York, 394 U.S. 576, 592 (1969)).

[34] 6 U.S.C. § 652.

[35] *Remarks by President Trump at the Signing of H.R. 3359, Cybersecurity and Infrastructure Security Agency Act*, White House (Nov. 16, 2018), https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-signing-h-r-3359-cybersecurity-infrastructure-security-agency-act/.

[36] Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, § 2202(c)(1)–(2), (4)–(5), 132 Stat. 4168 (2018), codified at 6 U.S.C. § 652.

[37] H. Comm. on Homeland Sec., 115th Cong., Cybersecurity and Infrastructure Security Agency Act of 2017, H. Rep. No. 115-454, at 2 (2017), https://www.congress.gov/congressional-report/115th-congress/house-report/454/1?outputFormat=pdf.

[38] Interagency Cyber Cooperation: Roles, Responsibilities and Authorities of the Dept. of Defense and Homeland Sec, Hearing Before the H. Comm. on Homeland Sec. and H. Comm. on Armed Servs. S. Comm. on Emerging Threats and Capabilities (2018) (testimony of NPPD Office of Cybersecurity and Communication Asst. Sec'y Jeanette Manfra), https://www.dhs.gov/news/2018/11/14/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity.

[39] U.S. Dep't of Homeland Sec., *Written Testimony of DHS for a Senate Select Committee on Intelligence Hearing Titled "Election Security"* (Mar. 21, 2018), https://www.dhs.gov/news/2018/03/21/written-testimony-dhs-senate-select-committee-intelligence-hearing-titled-election.

[40] *Id.*

infrastructure—not online communications regarding elections. As Matthew Masterson, a senior cybersecurity advisor at DHS, explained in his 2018 testimony to the Senate Judiciary Committee, NPPD worked with state, local, and private sector partners to identify "malicious cyber activity targeting ***election infrastructure***," and the Election Task Force, in particular, "serv[ed] to provide actionable information and offer assistance to assist election officials with strengthening their election infrastructure ***by reducing and mitigating cyber risk.***"[41] Throughout his testimony, Masterson focused on how NPPD provided "voluntary cybersecurity assistance for election infrastructure" and never addressed the possibility that NPPD could have any role in policing speech.[42] According to DHS's FY 2019 budget request to Congress, NPPD did not plan to conduct any operations related to MDM or foreign influence on elections.[43]

Those responsible for and involved in creating CISA generally understood that CISA's role would be limited to "lead[ing] the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure," just as they understood NPPD to have been doing.[44] Politico described the CISA Act as a "bill renaming the main DHS cybersecurity wing."[45] Both DHS leaders and members of Congress who championed the bill thought that in creating CISA, Congress was merely codifying and renaming NPPD:

- **DHS Secretary Kirstjen Nielsen:** "The cyber threat landscape is constantly evolving, and we need to ensure we're properly positioned to defend America's infrastructure from threats digital and physical. It was time to reorganize and operationalize NPPD into the Cybersecurity and Infrastructure Security Agency."[46]
- **NPPD Under Secretary, and future CISA Director, Christopher Krebs:** "Elevating the cybersecurity mission within the Department of Homeland Security, streamlining our operations, and giving NPPD a name that reflects what it actually does will help better secure the nation's critical infrastructure and cyber platforms."[47]
- **Senator Ron Johnson, Chairman of the U.S. Senate Committee on Homeland Security and Governmental Affairs:** "It is ridiculous that DHS needs an act of Congress to rename and reorganize an agency wholly within its jurisdiction. Nevertheless, I am glad the Senate passed the CISA bill to help the agency recruit talent and focus its efforts on protecting the homeland from cyber-attacks."[48]
- **Representative John Ratcliffe, Chairman of the Subcommittee on Cybersecurity and Infrastructure Protection of the U.S. House Committee on Homeland Security:** "CISA will define our nation's leading cybersecurity agency as a standalone operational organization clearly tasked with deploying DHS' cybersecurity and infrastructure security missions. By delineating CISA into three divisions, we can ensure that Undersecretary Krebs will have ongoing and enhanced success in carrying out the existing authorities provided in law."[49]

We know now, however, that agency leadership expanded CISA's mission into something far beyond what Congress intended.

---

41 *Election Security: Hearing Before the S. Comm. on the Judiciary*, 115th Cong., (2018) (statement of Matthew Masterson, National Protection and Programs Directorate, U.S. Dep't of Homeland Sec.), https://www.judiciary.senate.gov/imo/media/doc/06-12-18%20Masterson%20Testimony.pdf (emphasis added).

42 *Id.* at 1–2.

43 U.S. Dep't of Homeland Sec., Nat'l Protection and Programs Directorate, Budget Overview: Fiscal Year 2019 (2019), https://www.dhs.gov/sites/default/files/publications/National%20Protection%20and%20Programs%20Directorate.pdf.

44 *Cybersecurity and Infrastructure Security Agency*, CISA (Nov. 20, 2018), https://www.cisa.gov/news-events/alerts/2018/11/19/cybersecurity-and-infrastructure-security-agency.

45 Tim Starks, *CISA Almost Done After Senate Passage*, Politico, (Oct. 4, 2018), https://www.politico.com/newsletters/morning-cybersecurity/2018/10/04/cisa-almost-done-after-senate-passage-361984.

46 Press Release, U.S. Dep't of Homeland Sec., Congress Passes Legislation Standing Up Cybersecurity Agency in DHS (Nov. 13, 2018), https://www.dhs.gov/archive/news/2018/11/13/congress-passes-legislation-standing-cybersecurity-agency-dhs.

47 *Id.*

48 Press Release, S. Comm. on Homeland Sec. and Governmental Affs., Johnson-Backed Legislation to Establish DHS Cybersecurity Agency Passes Senate (Oct. 3, 2018), https://www.hsgac.senate.gov/media/reps/johnson-backed-legislation-to-establish-dhs-cybersecurity-agency-passes-senate/.

49 Starks, *supra* note 45.

II. *CISA's Censorship Efforts in the 2020 and 2022 Elections*

A. The Countering Foreign Influence Task Force and the 2020 Elections

While lawmakers were considering legislation to establish CISA, DHS began "internal and external coordination efforts . . . to counter disinformation appearing in social media."[50] In March 2018, DHS created the Countering Foreign Influence Task Force to "focus on the 2018 midterm elections" and election infrastructure disinformation.[51] Through this task force, DHS began working with social media platforms, third party organizations, and law enforcement officials to stop election-related disinformation in social media.[52] Soon after CISA's establishment at the end of 2018, the Countering Foreign Influence Task Force was "institutionalized as the Election Security Initiative (ESI) within CISA."[53] Efforts to regulate misinformation, disinformation, and malinformation had already begun despite no such authority being included or even discussed as a possibility in CISA's just-concluded authorization.[54]

In promoting "election security" and other initiatives, the Countering Foreign Influence Task Force—later the MDM team—censored American speech on the internet.[55] It did so in numerous ways, including by (1) ignoring the important distinction between foreign and domestic sources of speech,[56] (2) holding meetings with industry in which they discussed foreign and domestic misinformation about the election,[57] (3) "switchboarding,"[58] (4) attempting to create monitoring and reporting portals,[59] and (5) helping to create and partnering with nonprofits dedicated to censorship.[60]

1. *CISA Disregarded the Critical Distinction Between Foreign and Domestic Sources of Speech.*

Despite its name—the Countering ***Foreign Influence*** Task Force—the task force, and what would become the MDM team, targeted ***Americans*** in addition to foreign speech.[61] CISA officials who worked on the Countering Foreign Influence Task Force told the Committee that when reviewing posts, they did not differentiate domestic content from foreign content.[62] Similarly, the outside academics and researchers who helped CISA censor information during the 2020 presidential election (through the actions described below) acknowledged that most of the alleged MDM regarding the 2020 presidential election came from domestic actors. Alex Stamos, who worked with CISA as the director of the Stanford Internet Observatory, said in

---

50 U.S. Dep't of Homeland Sec., Office of Inspector General, OIG-22-58, DHS Needs a Unified Strategy to Counter Disinformation Campaigns 1 (2022) [hereinafter DHS OIG Disinformation Report], https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-58-Aug22.pdf.

51 Melissa Dalton et al., *2 The Information Game, in* By Other Means: Part II: Adapting to Compete in the Gray Zone, at 5, 6 (2019), https://www.jstor.org/stable/resrep22608.6?seq=2.

52 *Id.*

53 CISA, #Protect2020 Strategic Plan, at 1, 4 (2020), https://www.cisa.gov/sites/default/files/publications/ESI_Strategic_Plan_FINAL_2-7-20_508.pdf.

54 *Id.* at 20.

55 *See* Press Release, CISA, CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure (Feb. 18, 2022), https://www.cisa.gov/news-events/alerts/2022/02/18/cisa-insights-foreign-influence-operations-targeting-critical-infrastructure; Aaron Kliegman, *DHS Agency Appears to Be 'Burying' Evidence of Involvement with 'Domestic Censorship Activities': Expert*, Fox News (Mar. 7, 2023), https://www.foxnews.com/politics/dhs-agency-appears-burying-evidence-involvement-domestic-censorship-activities-expert.

56 *Id.*

57 Brianna Herlihy, *FBI Met Weekly with Big Tech Ahead of the 2020 Election, Agent Testifies*, Fox News (Dec. 2, 2022), https://www.fxnews.com/politics/fbi-weekly-big-tech-ahead-2020-election-agent-testifies.

58 *Louisiana v. Biden*¸ No. 3:22cv1213-TAD-KDM, B. Scully Dep., ECF No. 209, at 17:1-8, 23:24–24:2 (W.D. La. March 4, 2023) [hereinafter Scully Dep.].

59 Josh Christenson, *New Emails Show DHS Created Stanford 'Disinfo' Group that Censored Speech Before 2020 Election*, N.Y. Post (Nov. 6, 2023), https://nypost.com/2023/11/06/news/new-emails-show-dhs-created-stanford-disinfo-group-that-censored-speech-before-2020-election/.

60 Interim Staff of H. Comm. on the Judiciary Select Subcomm. on the Weaponization of the Fed. Gov't, 118th Cong, Rep. on The Weaponization of CISA: How a "Cybersecurity" Agency Colluded with Big Tech and "Disinformation" Partners to Censor Americans, 1-2, 7 (2023) [hereinafter House CISA Weaponization Report], https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/cisa-staff-report6-26-23.pdf.

61 *Id.* at 1–2, 7; Brooke Singman, *House Weaponization Committee: Biden Admin 'Colluded' with Big Tech, 'Facilitated the Censorship of Americans'*, Fox News (June 26, 2023), https://www.foxnews.com/politics/house-weaponization-committee-biden-admin-colluded-big-tech-facilitated-censorship-americans.

62 DHS OIG Comm. Briefing (Jan. 4, 2024) (notes on file with Comm. staff)

November 2020 that "almost all" of the election-related MDM "is domestic."[63] He further clarified that "[t]here's been some foreign action . . . but nothing that is that interesting."[64] Stamos's colleague, Renée DiResta also said the "vast majority of voting related misinformation in the 2020 election was domestic."[65] Similarly, Kate Starbird, a professor in the Department Human Centered Design and Engineering at the University of Washington and a member of the MDM Subcommittee at CISA, said that while in the aftermath of the 2016 election they "concentrated on . . . coordinated behavior from inauthentic actors that were foreign," ahead of the 2020 election the focus became "authentic actors [with] verified accounts" who "were not coordinating behind the scenes . . . to spread mis- and dis-information" and who were "mostly domestic."[66]

2. *CISA Held Meetings with Social Media Companies Regarding Alleged Misinformation on Their Platforms.*

Beginning in 2018, CISA organized and attended regular meetings with industry and government officials to push its censorship agenda.[67] Government participants included CISA representatives—Chris Keast, Lauren Protentis (Partnerships and Engagements Lead, Countering Foreign Influence Task Force), Robert Schaul (Analysis and Resilience Policy Lead, Countering Foreign Influence Task Force), Kim Wyman (Senior Advisor, Election Security), Allison Snell, Matthew Masterson (Senior Cybersecurity Advisor at CISA), Geoffrey Hale (Director, Election Security Initiative), and Brian Scully (Head of CISA's Countering Foreign Influence Task Force)—as well as representatives from DOJ, FBI, ODNI, and DHS.[68] CISA also invited representatives from social media companies—Twitter, Google, WikiMedia, Yahoo, Reddit, Facebook/Meta, Pinterest, and Microsoft/LinkedIn—to attend these meetings.[69] CISA told Committee staff these meetings were on a wide variety of topics, including the election, foreign and domestic threats to the election, and election security.[70]

Government and industry representatives specifically discussed concerns about MDM on social media platforms.[71] One frequent attendee of these meetings, Yoel Roth of Twitter, testified that potential hack and leak operations—cyberattacks aimed at obtaining and releasing information that could influence public opinion, particularly on political issues—were discussed.[72] Other topics of discussion included the processes for reporting misinformation, resiliency efforts to counter misinformation,[73] election day coordination,[74] election security,[75] intelligence reporting from social media companies,[76] and notable content social media platforms had observed.[77] For a detailed account of these discussions, see the Interim Staff Report of the Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government: "The Weaponization Of CISA: How A 'Cybersecurity' Agency Colluded With Big Tech And 'Disinformation' Partners To Censor Americans."[78]

Moreover, social media companies reported changes to their

[63] Election Integrity P'ship, *What Happened: Disinformation in the 2020 Elections*, YouTube (Nov. 10, 2020), https://www.youtube.com/watch?v=QWO0Y_0GhWA&t=1s.

[64] *Id*.

[65] Joe Bak-Coleman & Renée DiResta, *Foreign vs. Domestic: An Examination of Amplification in a Ballot Misinformation Story*, Election Integrity P'ship (Oct. 7, 2020), https://www.eipartnership.net/2020/vast-majority-of-discarded-ballot-amplification-isnt-from-foreign-sources.

[66] Election Integrity P'ship, supra note 63.

[67] DHS OIG Disinformation Report, *supra* note 50 at 1, 5; CISA Comm. Briefing (Feb. 23, 2023) (notes on file with Comm. staff).

[68] E-mail from Emily Triffin to Lauren Protentis et al. (Oct. 5, 2022) (on file with Comm. staff); E-mail from Allison Snell to Stacia Cardille et al. (Mar. 4, 2020) (on file with Comm. staff); Scully Dep. 25:23–26:6.

[69] E-mail from Emily Triffin to Lauren Protentis et al. (Oct. 25, 2022) (on file with Comm. staff).

[70] CISA Comm. Briefing (Feb. 23, 2023) (notes on file with Comm. staff).

[71] Scully Dep. 39:7–23.

[72] *Id*. at 245:23–246:11; Ex. 13 at 2 (Decl. of Yoel Roth).

[73] *Id*. at 117:25–118-5.

[74] *Id*. at 262:9–18.

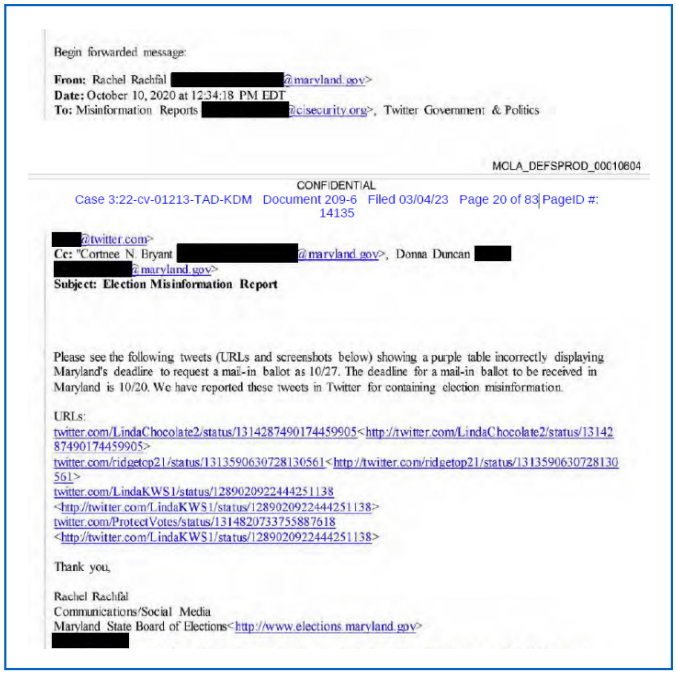
[75] *Id*. at 234:22–24

[76] *Id*. at 36:6–8; 235:1–4.

[77] *Id*. at 235:5–10.

[78] House CISA Weaponization Report, *supra* note 60.

content moderation policies at these government-led meetings.[79] Brian Scully testified that CISA "would often get a briefing" on updates to social media content platforms at their regular government-industry sync meetings.[80] In addition to these regular updates, Scully also asked social media companies to "provide a one-page summary of their content moderation rules that [CISA] could share with election officials."[81]



Begin forwarded message:

From: Rachel Rachfal [redacted]@maryland.gov>
Date: October 10, 2020 at 12:34:18 PM EDT
To: Misinformation Reports [redacted]@cisecurity.org>, Twitter Government & Politics [redacted]@twitter.com>
Cc: "Cortnee N. Bryant [redacted]@maryland.gov>, Donna Duncan [redacted]@maryland.gov>
Subject: Election Misinformation Report

MCLA_DEFSPROD_00010804

CONFIDENTIAL

Case 3:22-cv-01213-TAD-KDM Document 209-6 Filed 03/04/23 Page 20 of 83 PageID #: 14135

Please see the following tweets (URLs and screenshots below) showing a purple table incorrectly displaying Maryland's deadline to request a mail-in ballot as 10/27. The deadline for a mail-in ballot to be received in Maryland is 10/20. We have reported these tweets in Twitter for containing election misinformation.

URLs:
twitter.com/LindaChocolate2/status/1314287490174459905<http://twitter.com/LindaChocolate2/status/1314287490174459905>
twitter.com/ridgetop21/status/1313590630728130561<http://twitter.com/ridgetop21/status/1313590630728130561>
twitter.com/LindaKWS1/status/1289020922444251138
<http://twitter.com/LindaKWS1/status/1289020922444251138>
twitter.com/ProtectVotes/status/1314820733755887618
<http://twitter.com/LindaKWS1/status/1289020922444251138>

Thank you,

Rachel Rachfal
Communications/Social Media
Maryland State Board of Elections<http://www.elections.maryland.gov>
[redacted]

3. *CISA Facilitated Censorship through "Switchboarding."*

During the 2020 election, CISA directed state and local election officials to report supposed election-related MDM to CISA. [82] CISA would then review the reports and forward them to social media companies so they could remove the content.[83] This process is referred to as "switchboarding."[84] As Mr. Scully, who led the CISA team performing this work, explained, switchboarding "was essentially an [election] official…identify[ing] something on social media they deemed to be disinformation aimed at their jurisdiction. They could forward that to CISA, and CISA would share that with the appropriate social media companies."[85]

The emails below between Scully, the Maryland State Board of Electors, and Twitter illustrate how the switchboarding process worked.[86] Step One: the Maryland Official emailed Scully a few tweets regarding mail-in ballots. Step Two: Scully forwarded that email to Twitter. Step Three: Twitter immediately responded that it would "escalate" the tweets and later confirmed that the "[t]weets have been actioned for violations of our policies."

---

79 Scully Dep. at 127:4–129:6.

80 *Id.* at 21, 127.

81 *Id.* at 260:2–261:11

82 DHS OIG Disinformation Report, *supra* note 50, at 4–5; *see also Election Integrity Partnership*, Univ. of Washington, Center for an Informed Pub., https://ischool.uw.edu/research/research-fair/election-integrity-partnership.

83 *Id.* at 9.

84 House CISA Weaponization Report, *supra* note 60, at 12.

85 Scully Dep. 17:1-8, 23:24–24:2.

86 *See* Scully Dep., Ex. 9 at 18–20.

To: [redacted]@twitter.com>, [redacted]@twitter.com>, [redacted]@twitter.com>

Hello Team Twitter,

We received the below report from Maryland. It appears they have already reported to you all, but wanted to make sure you had for awareness.

Regards,
Brian

The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.

CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

From: Misinformation Reports [redacted]@cisecurity.org>
Sent: Saturday, October 10, 2020 12:42 PM
To: [redacted]@2020partnership.atlassian.net; Misinformation Reports [redacted]@cisecurity.org>; CISA Central [redacted]@cisa.dhs.gov>; CFITF [redacted]@hq.dhs.gov>; Scully, Brian [redacted]@cisa.dhs.gov>
Subject: Case #CIS-MIS000036: Misinformation regarding voter registration deadline in Maryland

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Misinformation tweet regarding voter registration deadline in Maryland

Begin forwarded message:

From: Rachel Rachfal [redacted]@maryland.gov>
Date: October 10, 2020 at 12:34:18 PM EDT
To: Misinformation Reports [redacted]@cisecurity.org>, Twitter Government & Politics

[redacted]@twitter.com>
Cc: "Cortnee N. Bryant [redacted]@maryland.gov>, Donna Duncan [redacted]@maryland.gov>
Subject: Election Misinformation Report

Please see the following tweets (URLs and screenshots below) showing a purple table incorrectly displaying Maryland's deadline to request a mail-in ballot as 10/27. The deadline for a mail-in ballot to be received in Maryland is 10/20. We have reported these tweets in Twitter for containing election misinformation.

URLs:
twitter.com/LindaChocolate2/status/1314287490174459905<http://twitter.com/LindaChocolate2/status/1314287490174459905>
twitter.com/ridgetop21/status/1313590630728130561<http://twitter.com/ridgetop21/status/1313590630728130561>
twitter.com/LindaKWS1/status/1289020922444251138
<http://twitter.com/LindaKWS1/status/1289020922444251138>
twitter.com/ProtectVotes/status/1314820733755887618
<http://twitter.com/LindaKWS1/status/1289020922444251138>

Thank you,

Rachel Rachfal
Communications/Social Media
Maryland State Board of Elections<http://www.elections.maryland.gov>

From: [redacted]@twitter.com>
Sent: Saturday, October 10, 2020 6:33:10 PM
To: Scully, Brian [redacted]@cisa.dhs.gov>
Cc: [redacted]@twitter.com>; [redacted]@twitter.com>
Subject: Re: FW: Case #CIS-MIS000036: Misinformation regarding voter registration deadline in Maryland

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

These Tweets have been actioned for violations of our policies.

Thanks, Brian!

On Sat, Oct 10, 2020 at 1:21 PM Scully, Brian [redacted]@cisa.dhs.gov> wrote:
Thanks [redacted]

Brian Scully
DHS Countering Foreign Interference Task Force
National Risk Management Center
[redacted]
[redacted]@cisa.dhs.gov

From: [redacted]@twitter.com>
Sent: Saturday, October 10, 2020 1:12:43 PM
To: Scully, Brian [redacted]@cisa.dhs.gov>
Cc: [redacted]@twitter.com>; [redacted]@twitter.com>
Subject: Re: FW: Case #CIS-MIS000036: Misinformation regarding voter registration deadline in Maryland

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thanks, Brian. We will escalate.

---------- Forwarded message ---------
From: **Scully, Brian** [redacted]@cisa.dhs.gov>
Date: Sat, Oct 10, 2020 at 12:52 PM
Subject: FW: Case #CIS-MIS000036: Misinformation regarding voter registration deadline in Maryland

[87]

[87] *Id.*

Begin forwarded message:

From: "Zabel, Kylee" [redacted]@sos.wa.gov>
Date: October 7, 2020 at 7:48:49 PM EDT
To: Misinformation Reports [redacted]@cisecurity.org>
Cc: Lori Augino [redacted]@sos.wa.gov>, "Boyal, Kiran" [redacted]@sos.wa.gov>
Subject: Possible misinformation on Twitter

Hello,

I wanted to flag this tweet the Washington Office of the Secretary of State's official Twitter account was tagged in. I've attached a screenshot of the post itself, and it can be found here: https://twitter.com/JeffKis88392967/status/1313926786804113408

The reason I am flagging this as potential misinformation is it's not clear if this tweet is a simple statement or recommendation to "conservatives," or if this is a directive. If it's the latter, that would not be true. In Washington state, voters may return their ballots by mail, by placing their ballot in an official ballot drop box, or by visiting a county voting center.

My name is Kylee Zabel, and I'm the Communications Director for the Washington Office of the Secretary of State. I can be reached via this email or the two numbers listed in my signature block below. My cell phone is monitored after hours if I need to be reached urgently. I am also copying Washington State Elections Director Lori Augino and our Web and Social Media Coordinator Kiran Boyal.

Please let me know if you have any questions or need additional information.

Thank you.
-Kylee

Kylee Zabel
Communications Director
[redacted]
Secretary of State

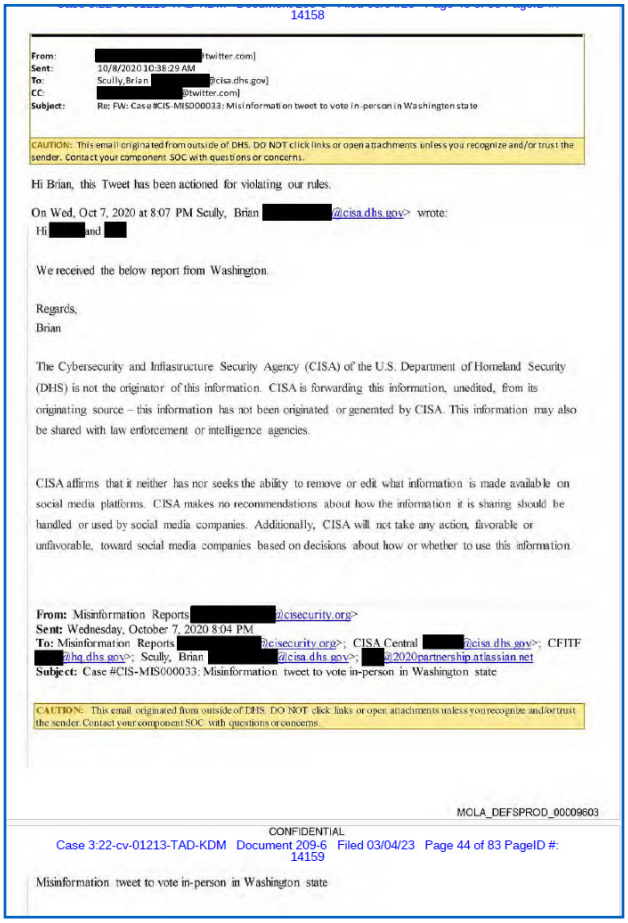
.....

nodrog danarb
@JeffKis88392967

@secstatewa All conservatives vote in person. Don't trust the mail

12:38 PM · Oct 7, 2020 · Twitter for iPhone

. . . . .



14158

From: [redacted]twitter.com]
Sent: 10/8/2020 10:38:29 AM
To: Scully, Brian [redacted]@cisa.dhs.gov]
CC: [redacted]@twitter.com]
Subject: Re: FW: Case #CIS-MIS000033: Misinformation tweet to vote in-person in Washington state

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi Brian, this Tweet has been actioned for violating our rules.

On Wed, Oct 7, 2020 at 8:07 PM Scully, Brian [redacted]@cisa.dhs.gov> wrote:
Hi [redacted] and [redacted]

We received the below report from Washington.

Regards,
Brian

The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.

CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

From: Misinformation Reports [redacted]@cisecurity.org>
Sent: Wednesday, October 7, 2020 8:04 PM
To: Misinformation Reports [redacted]@cisecurity.org>; CISA Central [redacted]@cisa.dhs.gov>; CFITF [redacted]@hq.dhs.gov>; Scully, Brian [redacted]@cisa.dhs.gov>; [redacted]@2020partnership.atlassian.net
Subject: Case #CIS-MIS000033: Misinformation tweet to vote in-person in Washington state

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

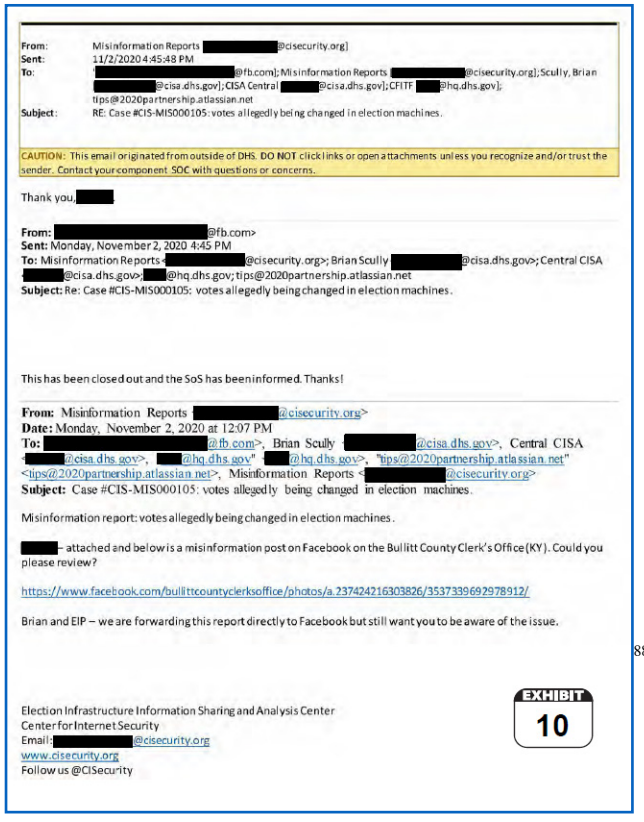
MCLA_DEFSPROD_00009603

CONFIDENTIAL

Case 3:22-cv-01213-TAD-KDM Document 209-6 Filed 03/04/23 Page 44 of 83 PageID #: 14159

Misinformation tweet to vote in-person in Washington state

The screenshot below illustrates a similar scenario for election-related content shared on Facebook.



From: Misinformation Reports [redacted]@cisecurity.org]
Sent: 11/2/2020 4:45:48 PM
To: [redacted]@fb.com]; Misinformation Reports [redacted]@cisecurity.org]; Scully, Brian [redacted]@cisa.dhs.gov]; CISA Central [redacted]@cisa.dhs.gov]; CFITF [redacted]@hq.dhs.gov]; tips@2020partnership.atlassian.net
Subject: RE: Case #CIS-MIS000105: votes allegedly being changed in election machines.

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thank you, [redacted]

From: [redacted]@fb.com>
Sent: Monday, November 2, 2020 4:45 PM
To: Misinformation Reports <[redacted]@cisecurity.org>; Brian Scully [redacted]@cisa.dhs.gov>; Central CISA <[redacted]@cisa.dhs.gov>; [redacted]@hq.dhs.gov; tips@2020partnership.atlassian.net
Subject: Re: Case #CIS-MIS000105: votes allegedly being changed in election machines.

This has been closed out and the SoS has been informed. Thanks!

From: Misinformation Reports [redacted]@cisecurity.org>
Date: Monday, November 2, 2020 at 12:07 PM
To: [redacted]@fb.com>, Brian Scully [redacted]@cisa.dhs.gov>, Central CISA <[redacted]@cisa.dhs.gov>, [redacted]@hq.dhs.gov" [redacted]@hq.dhs.gov>, "tips@2020partnership.atlassian.net" <tips@2020partnership.atlassian.net>, Misinformation Reports <[redacted]@cisecurity.org>
Subject: Case #CIS-MIS000105: votes allegedly being changed in election machines.

Misinformation report: votes allegedly being changed in election machines.

[redacted] – attached and below is a misinformation post on Facebook on the Bullitt County Clerk's Office (KY). Could you please review?

https://www.facebook.com/bullittcountyclerksoffice/photos/a.237424216303826/3537339692978912/

Brian and EIP – we are forwarding this report directly to Facebook but still want you to be aware of the issue.

EXHIBIT 10

Election Infrastructure Information Sharing and Analysis Center
Center for Internet Security
Email: [redacted]@cisecurity.org
www.cisecurity.org
Follow us @CISecurity

[88]

[88] Scully Dep. Ex. 10 at 1.

According to Scully, CISA knew social media companies would apply their content moderation policies to "disinformation" if CISA alerted them to it.[89] "The idea was," he explained, that social media companies "would make [a] decision on the content that [CISA] forward[ed] to them based on their policies."[90] He acknowledged that if the content had not been brought to social media companies' attention, the platforms would not have otherwise moderated it.[91]

CISA tracked its switchboarding efforts but has not shared its tracker with the Committee.[92]

4. *CISA Tried to Create Monitoring Systems and an Industry Reporting Portal.*

CISA continued to push for the censorship of alleged MDM on social media by contracting with third parties to further monitor social media content. CISA hired Limbik—a private company that identifies and attempts to respond to misinformation online to mitigate information threats or unfavorable ideas online[93]—and another company to build pilot portals for monitoring online narratives and tracking misinformation.[94]

Additionally, DHS funds the Center for Internet Security (CIS), which attempted to build another portal to integrate MDM reporting by election officials to social media companies.[95] CIS is a government-funded, non-profit organization that purports to focus on "cybersecurity" issues related to election infrastructure.[96] According to a 2020 email from Twitter recapping a call with the National Association of Secretaries of State, National Association of State Election Directors (NASED), CISA, and DHS, CISA received "a grant to build a web portal for state and local election officials to report incidents of election-related misinformation."[97] In other words, DHS funded multiple portals and programs in an attempt to facilitate election officials monitoring and reporting on Americans' speech and directed social media companies to censor Americans' posts. The platforms were never operationalized outside of beta form, at least in part because the social media companies claimed they could not be operational across different platforms.[98]

5. *CISA Encouraged the Formation of, and Partnered with, Nonprofits to Assist Its Work.*

In 2020, during the first Trump administration, the Stanford University Internet Observatory (SIO)—"in consultation with" CISA—formed the Election Integrity Partnership (EIP) to counter election misinformation on social media.[99] CISA's objective in helping to create EIP was to fill "the gap" for "state and local election officials" that "don't have the bandwidth or capacity to monitor mis and disinformation [on] social media that may affect their jurisdictions."[100]

The idea to establish what would become EIP originated with the government from personnel at CISA.[101] As Scully testified in *Missouri v. Biden*, "a couple of our interns" at CISA, who were then students at Stanford University, "came up with the idea" to create EIP.[102] These interns had lamented that most election offices did not have capacity or capability to monitor social media for disinformation within their jurisdictions.[103] The interns discussed this issue with Scully and other CISA officials, who then

---

89 *Id*. at 17:15–21.

90 *Id*. at 17:15–21.

91 *Id*. at 17:22–18:1.

92 *Id*. at 165:21–166:6.

93 *See* Limbik, https://www.limbik.com/ (last visited Sept. 26, 2025).

94 Scully Dep. 153:13–155:14.

95 *Center for Internet Security*, USASpending.gov, https://www.usaspending.gov/recipient/3fe5cc66-9042-5e94-dd7b-53e58329f4bf-C/latest (last visited Sept. 26, 2025).

96 *About Us*, Center for Internet Security, https://www.cisecurity.org/about-us (last visited Sept. 20, 20245).

97 E-mail from Lisa Roman to Bridget Coyne et al. (May 11, 2020) (on file with Comm. staff).

98 E-mail from Stacia Cardille to Bridget Coyne et al. (Apr. 27, 2020) (on file with Comm. staff).

99 Scully Dep. 97:4–10, 98:2–8; *see also A Statement from the Election Integrity Partnership,* Election Integrity P'ship (Oct. 5, 2024), https://www.eipartnership.net/blog/a-statement-from-the-election-integrity-partnership.

100 Scully Dep. 57:18–22.

101 *Id*. at 49:5–10 and 51:4–24.

102 *Id.*

103 *Id*. at 56:22–58:14.

"had a conversation with the Stanford Internet Observatory folks about the gap."[104] Stanford's documents confirm this version of events. According to SIO's "Operational Timeline," on July 9, 2020, SIO had a "[m]eeting with CISA to present [the] EIP concept."[105] Shortly after that meeting, Stanford, together with the University of Washington, formally stood up EIP and the CISA interns who first proposed what would become EIP "ended up working on it."[106] While the EIP was originally pushed by unelected bureaucrats in 2020, in 2021 the Biden administration actively began supporting the organization to become quasi-state censors.

During the late summer and early fall of 2020, EIP successfully pressured social media platforms to adopt restrictive speech policies.[107] For instance, on August 18, 2020, EIP published a document "evaluating platform election-related speech policies."[108] The document summarizes EIP's review of the policies on numerous social media platforms—including Facebook, Twitter, YouTube, Pinterest, Nextdoor, TikTok, and Snapchat—and issues each platform a subjective rating based on how comprehensive EIP deemed its content moderation.[109] After EIP published its findings, multiple social media platforms changed their community guidelines to secure better EIP ratings.[110] EIP then updated its findings, rewarding the companies that succumbed to the pressure, and prompting other social media companies to update their community guidelines.[111] The back and forth indicates that the EIP rankings directly affected the type of content that social media companies permitted on their sites. In addition, over the two months preceding the 2020 election, EIP sent over 600 "tickets" to social media companies, *i.e.* requests to remove content from platforms.[112]

After EIP had worked diligently during the 2020 election to suppress speech favorable to President Trump, the Biden administration gave EIP funding to turn into a true extension of the state. In summer 2021, the National Science Foundation issued a $3 million collaborative grant to the University of Washington and Stanford University to support EIP.[113] EIP would partner with both schools, Graphika (a social media analytics company), and the Atlantic Council to investigate misinformation and pressure social media platforms to censor American online content.[114]

B. The MDM Team and the 2022 Elections

In January 2021, the Biden administration made it official: CISA's censorship efforts were not limited to foreign actors spreading election-related disinformation. As was detailed in a 2022 DHS OIG audit on DHS's efforts to counter MDM, CISA transitioned what was originally the Countering Foreign Influence Task Force into the "MDM Team" "to promote more

---

[104] *Id*. at 52:3–6.

[105] Election Integrity P'ship, Center for an Informed Pub., Digital Forensic Rsch. Lab, Graphika, & Stanford Internet Observatory, The Long Fuse: Misinformation and the 2020 Election, 3 (June 21, 2021) [hereinafter EIP Report], https://stacks.stanford.edu/file/druid:tr171zs0069/EIP-Final-Report.pdf.

[106] Scully Dep. 49:14–16.

[107] Election Integrity P'ship, Evaluating Platform Election-Related Speech Policies Platform Policy Details (Oct. 28, 2020), https://web.archive.org/web/20250123223743/https://static1.squarespace.com/static/5f19d72fae0908591b9fec-cb/t/5f99b20b9261b014f0dac468/1603908112824/3_EIP_Platform_Policy_Comparison.docx+-+Google+Docs.pdf.

[108] *Id.*

[109] *Id.*

[110] *Id.* (EIP initially published this PDF in Aug. 2020. Companies' policy changes made since August 2020 are reflected in red text); *see also* Election Integrity P'ship, Evaluating Platform Election-Related Speech Policies (Sept. 10, 2020), https://web.archive.org/web/20201106144345/https://static1.squarespace.com/static/5f19d72fae0908591b9feccb/t/5f874565c462df71f95cc65d/1602700646999/%28PDF%29+Evaluating+Platform+Election-Related+Speech+Policies+%281%29.pdf (outlining Facebook's, Pinterest's and Twitter's policy changes to "...show the evolution that has occurred during this short period of time").

[111] *Id.*

[112] EIP Report, *supra* note 105, at 27.

[113] Press Release, Center for an Informed Pub., Univ. of Washington, $2.25 Million in National Science Foundation Funding Will Support Center for an Informed Public's Rapid-Response Research of Mis- and Disinformation (Aug. 15, 2021), https://www.cip.uw.edu/2021/08/15/national-science-foundation-uw-cip-misinformation-rapid-response-research/; *A Statement from the Election Integrity Partnership,* Election Integrity P'ship (Oct. 5, 2022), https://www.eipartnership.net/blog/a-statement-from-the-election-integrity-partnership; *Award Abstract # 2120496:Collaborative Research: SaTC: CORE: Large: Rapid-Response Frameworks for Mitigating Online Disinformation,* Nat'l Sci. Found. (initial amendment dated July 24, 2021), https://www.nsf.gov/awardsearch/showAward?AWD_ID=2120496&HistoricalAwards=false.

[114] Scully Dep. 48:16–49:4.

flexibility to focus on general MDM" in January 2021.[115] Brian Scully, who led the Countering Foreign Influence Task Force and then the MDM Team, claimed that the MDM Team's purpose was to "build national resilience to MDM, targeting critical infrastructure."[116] According to unnamed CISA officials, the MDM team had "a total of 15 dedicated part- and full-time staff" who would "counter all types of disinformation, to be responsive to current events," such as the COVID-19 pandemic.[117]

1. *CISA Ignored the Distinction between Foreign and Domestic Sources.*

In establishing the MDM Team, CISA abandoned the pretense that its MDM efforts would be limited to foreign actors. As Bob Kolasky, who ran CISA's National Risk Management Center, explained:

> At the start of the new administration, we disbanded the department's Countering Foreign Influence Task Force because we recognized that there needed to be a new approach to addressing mis-, dis- and mal-information (MDM)—one that acknowledged that false information arising from ***both foreign and domestic bad actors*** presented security risk to the nation.[118]

Similarly, Scully acknowledged that when taking action to remove MDM from social media, CISA would not attempt to determine whether the information came from a foreign or domestic source:

> Q: So you would receive reports and you would forward them onto social media platforms, you know, for consideration under their content moderation policies, without assessing whether they were originated from foreign or domestic sources?
>
> Scully: That's correct.
>
> Q: In other words, a report would come in, and you, like, didn't take steps to see whether this came from a foreign or domestic source?
>
> Scully: Correct.[119]

Furthermore, in a September 2022 report to the CISA Director on foreign threats, CISA's Cybersecurity Advisory Committee acknowledged the censorship mission creep, stating that "[i]n more recent years, attention has shifted to domestic sources of disinformation."[120]

As a result of CISA's drifting into domestic censorship, the National Association of Secretaries of State and the National Association of State Election Directors recommended CISA leave the MDM space because of its domestic nature.[121] These organizations understood the Department of Homeland Security and CISA's focus was supposed to be on foreign actors and recognized that, for much of CISA's MDM work, it was "difficult to determine whether a foreign adversary is involved."[122] This is further evidence that CISA understood, or should have understood, that its MDM work was not only exceeding the scope of its authority but also going beyond whatever level of government jawboning is permissible under the First Amendment.

2. *CISA Continued Meetings with Social Media Companies Regarding MDM.*

In the months leading up to the 2022 election, CISA coordinated weekly meetings between Biden administration officials and industry representatives, including representatives from Twitter, Meta, Microsoft, LinkedIn, Reddit, Yahoo, Wikimedia, Google,

---

[115] DHS OIG Disinformation Report, *supra* note 50, at 7.

[116] Scully Dep. 16:1–6

[117] DHS OIG Disinformation Report, *supra* note 50, at 7.

[118] Bob Kolasky, *Column: The Country Can't Afford a 'Pause' on Combating Disinformation and Violence*, GTSC Homeland Security Today.US (July 15, 2022), https://www.hstoday.us/featured/column-the-country-cant-afford-a-pause-on-combating-disinformation-and-violence/ (emphasis added).

[119] Scully Dep. 123:4–15.

[120] CISA Cybersecurity Advisory Comm., Report to the CISA Director: Protecting Critical Infrastructure from Misinformation and Disinformation, Information Sharing Around Foreign Adversary Threats to Elections, 1, 2 (Sept. 13, 2022), https://www.cisa.gov/sites/default/files/publications/CSAC_MDM_September_2022_Final_Recommendations_09132022-508.pdf.

[121] House CISA Weaponization Report, *supra* note 60, at 13.

[122] *Id.*

and Pinterest.[123] During these meetings, government officials highlighted trends in the intelligence space they claimed could affect online misinformation, and the social media company representatives presented misinformation they saw on their platforms.[124]

The Committee found evidence indicating that CISA directly instructed social media companies to moderate specific content. For instance, in one document the Committee reviewed, a lawyer hired by Twitter reviewed Twitter's communications with government entities and summarized the instances in which CISA had either raised its "direct concerns" with Twitter or forwarded an email from an election official about "inaccurate" information on the platform, and Twitter "took action."[125] Documents like these reinforced the Committee's suspicion that CISA was hiding the true extent of its relationship with social media companies and its content moderation pressure campaign.

Although the regular sync meetings between CISA and industry continued, and social media companies continued to brief CISA on their content moderation policies and activities throughout 2022,[126] at some point CISA ultimately stopped switchboarding because of the "heavy burden on [its] resources."[127]

3. *CISA Handed Off Its Switchboarding Work to its Nonprofit Partners.*

CISA told the Committee that it stopped switchboarding in 2022.[128] Brian Scully testified that former CISA Director Jen Easterly apparently made the decision to forgo this work.[129] CISA, however, did not stop because it recognized the constitutional concerns with a government agency limiting domestic speech.[130] Rather, as Scully explained, switchboarding "was not a role [CISA] necessarily wanted to play" any longer "because it is very resource intensive."[131]

Moreover, before CISA stopped switchboarding, it groomed third parties—EIP and CIS's Elections Infrastructure Information Sharing and Analysis Center (EI-SAC)—to continue monitoring speech for potential censorship. As discussed above, EIP is the Election Integrity Partnership, which assisted CISA in switchboarding during the 2020 election. CIS operates EI-SAC, a public-private partnership that provides election officials with information concerning cybersecurity and supply chain risks related to election infrastructure.[132] EI-SAC also reports election-related content that it deems "misinformation" to CISA and social media companies.[133] The U.S. government, primarily DHS, provides EI-SAC's parent organization, CIS, tens of millions of dollars a year, including $38.1 million in 2022 and $43 million in 2023.[134]

CISA connected CIS with EIP because, according to Scully, "EIP was working on the same mission [switchboarding]" and "we wanted to make sure that they were all connected."[135]

While CISA formally ended its switchboarding work in early 2022, CIS and EIP continued switchboarding throughout the 2022 election cycle.[136] Scully testified that CIS's switchboarding operation was "up and running" in time for the 2022 election cycle.[137] Moreover, as Scully explained, CISA coordinated with CIS and EIP on their efforts to report misinformation to social

---

123 E-mail from Emily Triffin to Lauren Protentis et al. (Oct. 25, 2022) (on file with Comm. staff).

124 CISA Comm. Briefing (Feb. 23, 2023) (notes on file with Comm. staff).

125 E-mail on file with Comm. Staff (Dec. 12, 2021).

126 Scully Dep. 21:1–18.

127 *Id.* at 367:12–13.

128 CISA Comm. Briefing (Feb. 23, 2023) (notes on file with Comm. staff).

129 *Id.*; Scully Dep. 22:11–14.

130 Election Integrity P'ship, *supra* note 105, at 41; *see also* Scully Dep. 62:11–22.

131 Scully Dep. 62:16–19.

132 *EI-ISAC Overview*, Center for Internet Security, https://www.cisecurity.org/ei-isac (last visited Sept. 26, 2025).

133 Scully Dep. 112: 9–19.

134 *Center for Internet Security*, *supra* note 95.

135 Scully Dep. 62:24–63:1.

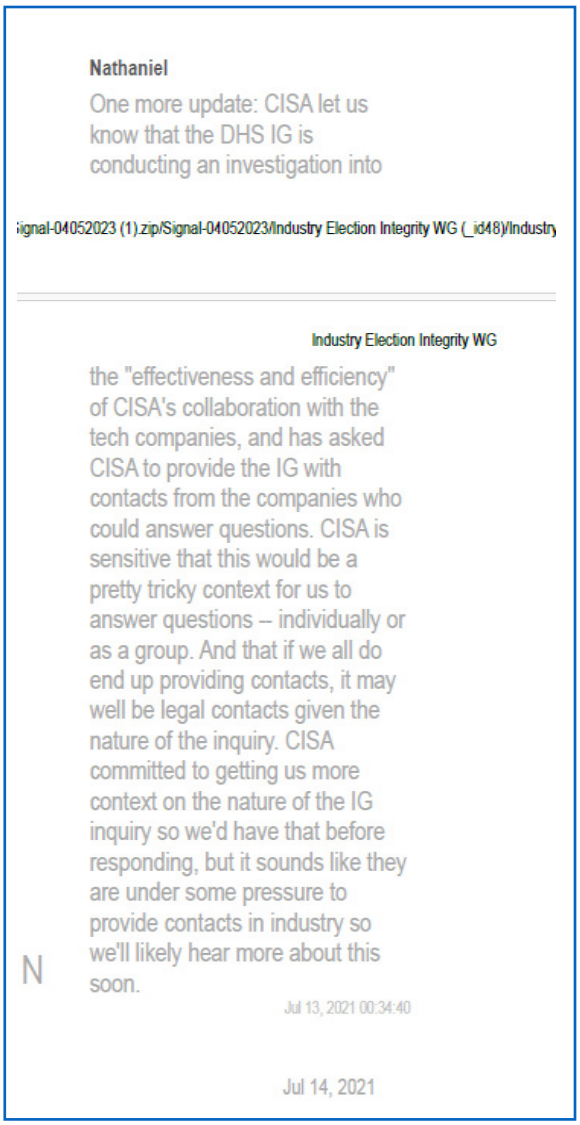
136 *Id.* at 266:20–22; 265:23–266:4.

137 *Id.* at 266:2–3.

media companies: "There was a point where one of the platforms was concerned about too much kind of duplicate reporting coming in, and so we did have some conversations with EIP and CIS on how to kind of better manage that activity to make sure we weren't overwhelming the platforms."[138] Scully further testified that CISA "facilitated some meetings between Stanford folks, the Center for Internet Security, and election officials, where they had discussions about how they would work together."[139]

4. *CISA Created the MDM Subcommittee to Recommend How the Government Should Best Target Americans' Speech.*

CISA also engaged with so-called experts on how it could censor misinformation moving forward. In June 2021, CISA created the Cybersecurity Advisory Committee (CSAC), made up of academics and leaders in various industries, to "facilitate subcommittees" to study specific cybersecurity topics, including "information exchange; critical infrastructure; risk management; and public and private partnerships."[140] One of the subcommittees CISA established in May 2022 was the Protecting Critical Infrastructure for Misinformation and Disinformation Subcommittee, commonly referred to as the "MDM Subcommittee."[141] Its purpose was to "evaluate and provide recommendations on potentially effective critical infrastructure related counter-MDM efforts."[142] It consisted of various "experts" on misinformation, including Kate Starbird, a professor of Human Centered Design and Engineering at the University of Washington who also led the Election Integrity Partnership (and led the subcommittee); Vijaya Gadde, head of Twitter's Public Policy & Trust and Safety; Suzanne Spaulding, Senior Advisor for Homeland Security at CSIS; and Alicia Tate-Nadeau, Director of the Illinois Emergency Management Agency.[143]


Nathaniel

One more update: CISA let us know that the DHS IG is conducting an investigation into

ignal-04052023 (1).zip/Signal-04052023/Industry Election Integrity WG (_id48)/Industry

Industry Election Integrity WG

the "effectiveness and efficiency" of CISA's collaboration with the tech companies, and has asked CISA to provide the IG with contacts from the companies who could answer questions. CISA is sensitive that this would be a pretty tricky context for us to answer questions -- individually or as a group. And that if we all do end up providing contacts, it may well be legal contacts given the nature of the inquiry. CISA committed to getting us more context on the nature of the IG inquiry so we'd have that before responding, but it sounds like they are under some pressure to provide contacts in industry so we'll likely hear more about this soon.

Jul 13, 2021 00:34:40

Jul 14, 2021

Before joining the MDM Subcommittee, several of these individuals expressed biased, left-wing views concerning national elections and online speech. For instance, in 2021, Starbird called the U.S. flag and Constitution "propaganda"[144] and urged people to vote against Trump because Trump and "current GOP congresspeople" are a "wholly different kind of threat" to "our country, our values, and even our freedom."[145] At Twitter, Gadde was involved in a litany of anti-speech decisions, including Twitter's decision to censor press coverage of the Hunter Biden laptop story and remove content that questioned official COVID-19 dogma.[146]

---

[138] *Id.* at. 64:21–65:1.

[139] *Id.* at 52:10–13.

[140] *Cybersecurity Advisory Comm. Bylaws*, CISA, 1 (Nov. 27, 2023), https://www.cisa.gov/sites/default/files/2023-11/CSAC_Bylaws_20231011_Clean_Signed_508.pdf; Samantha Schwartz, *CISA Names 23 Industry Leaders to Advisory Board*, Cybersecurity Dive (Dec. 2, 2021), https://www.cybersecuritydive.com/news/cisa-cybersecurity-advisory-committee-private-public-partnership/610844/.

[141] *CISA Cybersecurity Advisory Committee: Subcommittee Factsheet*, CISA (Feb. 2023), https://www.cisa.gov/sites/default/files/2023-02/csac_subcommittee_fact_sheet_05192022_508c.pdf; Report to the CISA Director, *supra* note 120, at 3.

[142] *CISA Cybersecurity Advisory Committee: Subcommittee Factsheet*, *supra* note 141.

[143] *CISA Cybersecurity Advisory Committee Factsheet*, CISA (May 19, 2022), https://www.cisa.gov/sites/default/files/publications/CSAC_Factsheet_5-19-22_508c.pdf.

[144] Kate Starbird (@katestarbird), Twitter (June 20, 2021), https://twitter.com/katestarbird/status/1406722804280565761?ref_src=twsrc%5Etfw (post on file with Comm. staff).

[145] Kate Starbird, Facebook (Oct. 31, 2018), https://www.facebook.com/story.php?story_fbid=10217622714864121&id=1366111779&mibextid=wwXIfr&rdid=VLtniEEnuqS5hA2P#.

[146] *Protecting Speech from Government Interference and Social Media Bias, Part I: Twitter's Role in Suppressing the Biden Laptop Story: Hearing Before the H.*

In the end, CSAC unanimously approved the MDM Subcommittee's recommendations and recommended that CISA take the following actions to address MDM:

- "[F]ocus on [MDM] that risks undermining critical functions of American society including [MDM] that suppresses election participation or falsely undermines confidence in elections . . . undermines critical functions carried out by other key democratic institutions, such as the court, or by other sectors such as . . . public health measures.[147]
- "[R]apidly respond—through transparency and communication—to emergent informational threats to critical infrastructure. . . . These response efforts can be actor-agnostic, but special attention should be paid to countering foreign threats."[148]
- "[P]roactively participate—in collaboration with outside researchers and those with first-hand authoritative information—in correcting [MDM] that poses a significant threat to critical functions. If possible, CISA should also support external organizations doing [MDM] response work in their own communities."[149]

The MDM Subcommittee disbanded in 2023 after it "successfully answered their taskings and provided recommendations to CISA."[150]

III. Investigation

As the expansive scope of CISA's efforts to censor Americans' speech became increasingly clear, the Committee launched an investigation into three key questions:

1. Did CISA have the authority to monitor, evaluate, and regulate speech on social media?

2. If not, did anyone, including DHS OIG, question CISA's authority to monitor, evaluate, and regulate speech on social media?

3. Did CISA comply with DHS OIG's efforts to oversee CISA's work to monitor, evaluate, and regulate speech on social media?

The Committee's investigation revealed that CISA lacked authority to pressure social media companies to remove election-related social media posts. At times, CISA's nonprofit censorship partners questioned CISA's authority to do this work. However, the social media companies that CISA directed to moderate content never appeared to question CISA's authority. Nor did DHS OIG question CISA's authority, even as it led an audit "to determine the internal and external coordination efforts the Department has taken to counter disinformation campaigns and efforts that appear in social media."[151]

The Committee's investigation also revealed that CISA did not fully cooperate with DHS OIG's audit and oversight of CISA's work monitoring, evaluating, and regulating speech on social media. Notably, CISA did not comply with DHS OIG's request to provide the office with its contacts at social media companies.

As revealed in a Signal group chat among companies in CISA's industry working group meetings (captured in the graphic on the left), CISA was "under some pressure to provide [its] contacts in industry" to the OIG.[152] CISA nevertheless dragged its

Comm. on Oversight and Accountability, 118th Cong., 7, 9 (2023) (statements of Chairman Comer and Vijaya Gadde, Former Chief Legal Officer, Twitter); Alex Hern, *Twitter to Remove Harmful Fake News About Coronavirus*, The Guardian (Mar. 19, 2020), https://www.theguardian.com/world/2020/mar/19/twitter-to-remove-harmful-fake-news-about-coronavirus.

147 Report to the CISA Director, Protecting Critical Infrastructure from Misinformation and Disinformation, CISA Cybersecurity Advisory Comm., at 2 (June 22, 2022), https://www.cisa.gov/sites/default/files/publications/June%202022%20CSAC%20Recommendations%20%E2%80%93%20MDM_0.pdf.

148 *Id.* at 3.

149 *Id.* at 4.

150 *CISA Cybersecurity Advisory Committee Meeting Summary*, CISA Cyber Security Advisory Comm. (Dec. 6, 2022), https://www.cisa.gov/sites/default/files/publications/CSAC_December-Quarterly-Meeting-Summary_508_01062023_0.pdf; *see CISA Cybersecurity Advisory Committee March 21, 2023 Meeting Summary*, CISA Cybersecurity Advisory Comm., at 2 (Mar. 21, 2023), https://www.cisa.gov/sites/default/files/2023-04/csac_march-quarterly-meeting_open-session-summary_2023-04-06_508.pdf.

151 DHS OIG Disinformation Report, *supra* note 50, at 5.

152 Yahoo Industry Election Integrity WG Signal Chat (July 13, 2021) (messages on file with Comm. staff).

feet for months, and rather than connecting DHS OIG with the people whom CISA had worked with to remove content from platforms, CISA *asked* the social media companies to specify whom DHS OIG should contact (i.e. their government affairs teams).[153] CISA successfully delayed until DHS OIG concluded the audit stage of its report.[154] This purposeful delay impeded DHS OIG's ability to complete a comprehensive review of CISA's censorship activities.

Moreover, CISA withheld information from DHS OIG regarding the actions it took to address DHS OIG's recommendations. Following the audit, DHS OIG recommended that DHS's Office of Strategy, Policy, and Plans develop a "unified strategy to improve DHS' coordinated actions . . . to counter disinformation campaigns that appear in social media."[155] In response to that recommendation, DHS General Counsel Jonathan E. Meyer issued a memo announcing the establishment of an Emerging Technology Group.[156] The memo allowed DHS OIG to close the recommendation as fulfilled by the Department.[157] However, DHS did not actually establish the group. Nor did it notify DHS OIG that it had changed course. DHS OIG only learned that DHS had delayed establishing the group for over a year when the Committee asked about a subsequent DHS memo, which revealed DHS had paused the effort.[158]

A. CISA Does Not Have Authority to Censor Americans' Online Speech.

1. *Neither DHS Nor CISA Could Identify CISA's Statutory Authority for its Censorship Activities.*

In the past, DHS has generally asserted that CISA has authority to censor MDM because it has authority to protect against attacks on critical infrastructure. As CISA Director Jen Easterly infamously stated:

> 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. We are going to work with our partners in the private sector and throughout the rest of the government and at the department to continue to ensure that the American people have the facts that they need to help protect our critical infrastructure.[159]

To the Committee's knowledge, however, DHS has never publicly identified a statutory provision that allowed it to review and censor speech on social media.

Over a months-long period, the Committee repeatedly asked DHS to identify the statutory authority for CISA's MDM work. DHS repeatedly failed to do so. For instance, in January 2024, Committee staff asked DHS to provide "the statutory sources of DHS's authority to counter MDM."[160] DHS's response—which it sent ***four months later***—did not cite a single statutory provision.[161] Instead, DHS gave the Committee a word-salad, two-paragraph explanation:

While awaiting what would be a non-responsive written answer from DHS, Committee staff asked the same question in a briefing with CISA, which included the same officials who were actively involved in the MDM activities described in the previous section, including Geoffrey Hale, Scully's supervisor.[162] No one from CISA was able to identify the statutory provision justifying that work. Rather, Hale offered a general appeal to protecting the "security of infrastructure through threat

---

153 DHS OIG Comm. Briefing (Jan. 4, 2024) (notes on file with Comm. staff); Emails from DHS OIG Office of Audits (on file with Commerce Comm. staff).

154 *Id.*

155 DHS OIG Disinformation Report, *supra* note 50, at 12.

156 DHS OIG Comm. Briefing (Jan. 4, 2024) (notes on file with Comm. staff).

157 *Id.*

158 Memorandum from Jonathan E. Meyer, DHS Gen. Couns., to Component Chief Couns., Headquarters Assoc. Gen. Couns., Judge Advoc. General, USCG, and the Principal Legal Advisor, ICE (May 14, 2024) (on file with Comm. staff).

159 Maggie Miller, *Cyber Agency Beefing Up Disinformation, Misinformation Team*, The Hill (Nov. 10, 2021), https://thehill.com/policy/cybersecurity/580990-cyber-agency-beefing-up-disinformation-misinformation-team/.

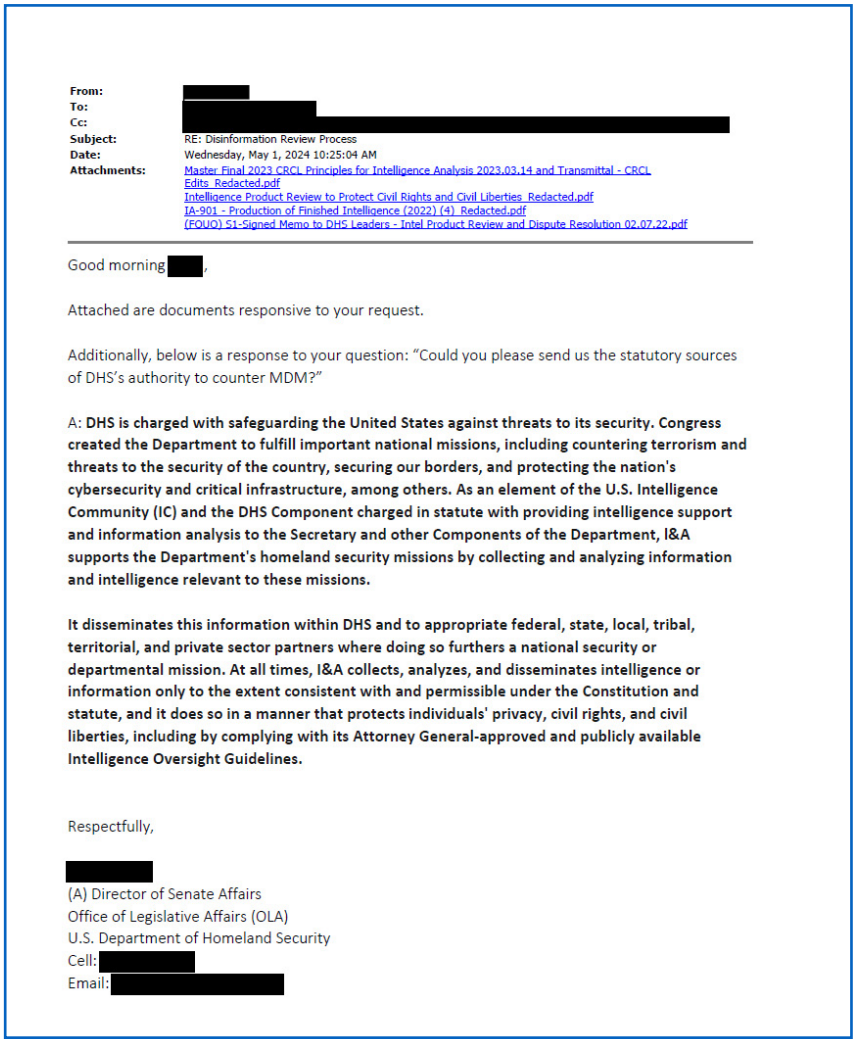
160 E-mail from Comm. Staff to Brian Gracey, Dir. of Senate Affs., DHS Office of Leg. Affs. (Jan. 31, 2024) (on file with Comm. staff).

161 E-mail from Brian Gracey, Dir. of Senate Affs., DHS Office of Leg. Affs, to Comm. Staff (May 1, 2024) (on file with Comm. staff).

162 CISA Comm. Briefing (Feb. 23, 2023) (notes on file with Comm. staff).

environments posed by foreign influence operations."[163] Hale further stated that he could "not cite specific code because [he] [was] not a lawyer," but maintained CISA's authority "has been sufficient for [its] actions."[164] He claimed that CISA has consistently stayed within its authority.[165]

The Committee's investigation, however, determined that CISA has no statutory authority to pressure social media companies to censor or take down Americans' speech.



From: [redacted]
To: [redacted]
Cc: [redacted]
Subject: RE: Disinformation Review Process
Date: Wednesday, May 1, 2024 10:25:04 AM
Attachments: Master Final 2023 CRCL Principles for Intelligence Analysis 2023.03.14 and Transmittal - CRCL Edits_Redacted.pdf
Intelligence Product Review to Protect Civil Rights and Civil Liberties_Redacted.pdf
IA-901 - Production of Finished Intelligence (2022) (4)_Redacted.pdf
(FOUO) S1-Signed Memo to DHS Leaders - Intel Product Review and Dispute Resolution 02.07.22.pdf

Good morning [redacted],

Attached are documents responsive to your request.

Additionally, below is a response to your question: "Could you please send us the statutory sources of DHS's authority to counter MDM?"

A: **DHS is charged with safeguarding the United States against threats to its security. Congress created the Department to fulfill important national missions, including countering terrorism and threats to the security of the country, securing our borders, and protecting the nation's cybersecurity and critical infrastructure, among others. As an element of the U.S. Intelligence Community (IC) and the DHS Component charged in statute with providing intelligence support and information analysis to the Secretary and other Components of the Department, I&A supports the Department's homeland security missions by collecting and analyzing information and intelligence relevant to these missions.**

It disseminates this information within DHS and to appropriate federal, state, local, tribal, territorial, and private sector partners where doing so furthers a national security or departmental mission. At all times, I&A collects, analyzes, and disseminates intelligence or information only to the extent consistent with and permissible under the Constitution and statute, and it does so in a manner that protects individuals' privacy, civil rights, and civil liberties, including by complying with its Attorney General-approved and publicly available Intelligence Oversight Guidelines.

Respectfully,

[redacted]
(A) Director of Senate Affairs
Office of Legislative Affairs (OLA)
U.S. Department of Homeland Security
Cell: [redacted]
Email: [redacted]

2. The CISA Act Does Not Provide CISA Statutory Authority to Censor Speech.

As its name suggests, Congress established the "Cybersecurity and Infrastructure Security Agency" to protect the country's cybersecurity and infrastructure.[166] Accordingly, Congress authorized CISA to perform two chief functions:

(1) Lead **cybersecurity** and **critical infrastructure** security programs, operations, and associated policy for the Agency, including national cybersecurity asset response activities; [and]
(2) Coordinate with Federal entities, including Sector-Specific Agencies, and non-Federal entities, including international entities, to carry out the **cybersecurity** and **critical infrastructure** activities of the Agency, as appropriate.[167]

Each of the activities that Congress authorized the Director of CISA to take therefore must fall within one of two categories: cybersecurity or critical infrastructure security. CISA's MDM censorship activities cannot be justified under either category.

a. CISA Did Not and Does Not Have Statutory Authority to Censor Speech Under Its "Critical Infrastructure" Function.

As recounted above, CISA Director Easterly generally referred to CISA's authority to protect "critical infrastructure" to justify its MDM work.[168] Scully similarly testified in 2023 that CISA's MDM team "build[s] resilience and reduce[s] risks to critical infrastructure."[169] But "critical infrastructure" is not a term to be defined by the CISA Director. Rather, the U.S. Code defines the term as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or

[163] *Id.*

[164] *Id.*

[165] *Id.*

[166] Cybersecurity and Infrastructure Security Act of 2018, Pub. L. No. 115-278, 132 Stat. 4169.

[167] *Id.* § 2202 (c)(1)–(2), 132 Stat. 4169, 4170 (emphasis added).

[168] Miller, *supra* note 159; Cybersecurity and Infrastructure Security Act of 2018, Pub. L. No. 115-278, § 2202 (c)(1)–(2), 132 Stat. 4169, 4170.

[169] Scully Dep. 332:1–2.

any combination of those matters."[170]

Long before the creation of CISA, presidential directives identified what sectors meet this high threshold. In 2003, President Bush issued Homeland Security Presidential Directive 7, defining critical infrastructure to include the following sectors: telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping.[171] Ten years later, President Obama updated that list through Presidential Directive 21 to include the following sectors: Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater systems.[172] Presidential Directive 21 also identifies a "Sector-Specific Agency" responsible for each critical infrastructure sector.[173] For example, the Sector-Specific Agency responsive for the Healthcare and Public Health Sector is the Department of Health and Human Services.[174] Anything related to elections is noticeably absent from the list.

Enter Obama's DHS Secretary Jeh Johnson. On January 6, 2017—just days before President Trump took office and while claims of Russian interference in the 2016 election were proliferating—Secretary Johnson unilaterally designated "election infrastructure" as a subsector of the Government Facilities' critical infrastructure sector.[175] (The designation of election infrastructure as "critical infrastructure" has never been codified or even approved at the Presidential level). Even Secretary Johnson, however, recognized that "election infrastructure" was not some all-encompassing term, but rather limited to the physical and cyber infrastructure supporting elections. Secretary Johnson thus clarified "election infrastructure" meant "storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments."[176] DHS provided a similar definition in written testimony to the U.S. Senate Select Committee on Intelligence in March 2018.[177] Brian Scully, who led much of CISA's censorship work, said "election infrastructure" referred to "the systems, physical security, things like that."[178]

Government censoring alleged misinformation related to elections—or anything else—is not protecting critical infrastructure. While misinformation may influence public thought and opinion, it does not affect "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[179] To put it another way, while misinformation related to an election may affect the way people vote, it does not jeopardize the physical voting infrastructure (like polling places and storage facilities) or the electronic infrastructure supporting elections (like internet technology and voter registration databases).

CISA tried to sidestep this obvious conclusion by claiming that misinformation could indirectly threaten critical infrastructure. For instance, in a 2023 deposition, Scully said social media posts about the 2020 Presidential Election "threaten[ed] critical infrastructure in a number of ways . . . you know, there's financial, there's reputations, there's just a multitude of ways that

---

[170] 6 U.S.C. § 101(4); 42 U.S.C. § 5195c(e).

[171] *Homeland Security Presidential Directive* 7, CISA (Dec. 17, 2003), https://www.cisa.gov/news-events/directives/homeland-security-presidential-directive-7.

[172] Press Release, Office of the Press Sec., The White House, Presidential Policy Directive – Critical Infrastructure Security and Resilience (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[173] *Id.* "The term 'Sector-Specific Agency' (SSA) means the Federal department or agency designated under this directive to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment." 15 U.S.C § 272(e)(3)(B).

[174] *Id.*

[175] Press Release, Dep't of Homeland Sec., Statement by Sec. Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

[176] *Id.*

[177] Press Release, Dep't of Homeland Sec., Written testimony of DHS for a S. Select Comm. on Intel. hearing titled 'Election Security,' https://www.dhs.gov/news/2018/03/21/written-testimony-dhs-senate-select-committee-intelligence-hearing-titled-election.

[178] Scully Dep. 270:7–15.

[179] 6 U.S.C. § 101(4); 42 U.S.C. § 5195c(e).

this disinformation could affect critical infrastructure."[180] A 2022 Homeland Security Advisory Council (HSAC) report from the "Disinformation Best Practices and Safeguards Subcommittee" asserted that countering disinformation is related to CISA's critical infrastructure mission because "disinformation undermines confidence in the security of U.S. elections."[181] Director Easterly went so far as to claim that "the most critical infrastructure is our cognitive infrastructure."[182]

Of course, neither has a statute enacted by Congress nor has a presidential directive added "cognitive infrastructure" to a list of critical infrastructure. Most importantly, this argument runs headlong into the First Amendment. As set forth in detail above, the First Amendment protects both true speech and untrue speech.[183] And speech on issues of public concern, like elections, deserves special protection from government interference.[184]

b. CISA Has No Authority to Censor American Speech Under Its "Cybersecurity" Function.

DHS has also alluded to CISA's statutory cybersecurity authority when attempting to ground its MDM work. For instance, HSAC's 2022 report from the "Disinformation Best Practices and Safeguards Subcommittee" claimed "widely believed false statements that one should never install software patches or updates on computers, or that one can always be confident that links in emails are safe to click, would impede CISA's mission to protect our cybersecurity."[185]

Unlike "critical infrastructure," the Act does not define the term "cybersecurity." The Act does, however, define similar terms, which illustrate that "cybersecurity" concerns the security of information systems. For instance, it defines:

- **"Cybersecurity purpose"** as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."[186]
- **"Cybersecurity risk"** as "threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism."[187]
- **"Cybersecurity threat"** as "an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system."[188]

The Act defines "Information Systems" as a "discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."[189]

Censoring alleged misinformation that is protected by the First Amendment, whether related to elections—or anything else—is not protecting cybersecurity. While misinformation may affect how people *view* and *react to* information, it has no direct effect on the security of information itself or information systems. Straining to expand the definition of cybersecurity to encompass protections against threats to how people understand information because it could somehow indirectly impact the security of

[180] Scully Dep. 340:10–341:1.

[181] *Disinformation Best Practices and Safeguards Subcommittee Final Report*, Dep't of Homeland Sec. (Aug. 24, 2022), https://www.dhs.gov/sites/default/files/2022-08/22_0824_ope_hsac-disinformation-subcommittee-final-report-08242022.pdf.

[182] Erin Dwinell, *Biden's Homeland Security Department Still Engaging in Censorship*, Heritage Foundation (Apr. 11, 2023), https://www.heritage.org/homeland-security/commentary/bidens-homeland-security-department-still-engaging-censorship. Even Scully would not go that far. When asked whether "critical infrastructure include[s] cognitive infrastructure," Scully responded, "not through national policy." Scully Dep. 332:6-8.

[183] Section I(A), *supra* 17.

[184] *Id.*

[185] Dep't of Homeland Sec., Disinformation Best Practices and Safeguards Subcomm. Final Report 13 (Aug. 24, 2022), https://www.dhs.gov/sites/default/files/2022-08/22_0824_ope_hsac-disinformation-subcommittee-final-report-08242022.pdf.

[186] 6 U.S.C. § 650(6).

[187] 6 U.S.C. § 650(7).

[188] 6 U.S.C. § 650(8)

[189] 44 U.S.C. § 3502(8).

an information system would expand the term cybersecurity to encompass almost any speech or action. Take HSAC's example above, in which it asserts that false statements that make people believe computer updates are unnecessary could impede cybersecurity. By that same logic, a true investigative report regarding a faulty computer update that inadvertently decreases battery life could disincline people from installing updates, putting the security of their information at risk. Should CISA insist that investigative report be retracted? Of course not.

Moreover, an election is not an "information system." Nor is public health or a company's reputation. Setting aside the fact that government censorship is barred by the First Amendment, misinformation's potential impacts on elections, public health, or corporate reputation are not threats to an "information system" and therefore actions to counter MDM do not qualify as cybersecurity.

3. *CISA Could Not Point To, and the Committee Could Not Identify, Any Other Source of Authority for CISA's Censorship Activities.*

The DHS Secretary is authorized to delegate authority to the CISA Director.[190] Therefore, although MDM authority is nowhere to be found in the CISA Act, if the DHS Secretary had authority to censor MDM online, the Secretary could have, in theory, delegated that authority to CISA.[191] Based on the Committee's review of the Homeland Security Act of 2002, however, Congress has not authorized the DHS Secretary to censor Americans.[192] Moreover, neither DHS nor CISA purported to rely upon any law other than the CISA Act in justifying CISA's actions to the Committee.[193]

B. No One—Besides CISA's Nonprofit Censorship Partners—Questioned CISA's Authority to Censor Speech.

Given CISA's representations to the Committee and the public about its claims that the CISA Act provided it with authority to censor alleged MDM, it is not surprising that the Committee found no evidence that any CISA official questioned the agency's authority to censor alleged election-related MDM. Indeed, in a 2023 deposition, Brian Scully testified that he did not believe he had ever discussed the government's authority to monitor MDM:

> Q: Do you remember any discussions of that with anyone else, suggesting that . . . there's no government agency in [the] United States with an explicit mandate to monitor and correct election mis and disinformation?
>
> A: No, not that I – not that I recall. It's possible, though.[194]

What is more shocking, however, is how CISA's partners in these activities—both nonprofits and social media companies—as well as the DHS OIG, either brushed aside or failed to question CISA's authority to engage in this work.

1. *CISA*'s *Nonprofit Censorship Partners Disregarded Their Own Concerns Regarding CISA's Authority to Censor Speech.*

Very few voiced doubts about CISA's authority to counter disinformation. And those who did were the very same people working closely with CISA in its censorship activities. Alex Stamos, the founding director of Stanford's SIO, which worked with CISA to stand up the Election Integrity Partnership (EIP), explained that CISA's disinformation capabilities "were very limited both by the kind of legal structures in place" and "the kind of people they had under their roof."[195] Similarly, Renee DiResta, SIO's Technical Research manager, remarked that "there were unclear legal authorities, including very real First Amendment questions" in reference to the federal government coordinating the removal of alleged misinformation.[196] Even EIP asserted in

---

190 6 U.S.C. § 652 (c)(14).

191 *See* 6 U.S.C. § 112(b)(1); 8 C.F.R. § 2.1 (2003).

192 Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002), https://www.dhs.gov/sites/default/files/2023-11/03_0116_hr_5005_enr.pdf.

193 E-mail from Brian Gracey, Dir. of S. Affs., DHS Office of Leg. Affs., to Comm. Staff (May 1, 2024) (on file with the Comm.).

194 Scully Dep. 95:3–9.

195 Election Integrity P'ship, supra note 63, https://www.youtube.com/watch?v=QWO0Y_0GhWA&t=353s.

196 Missouri v. Biden, F. Supp. 3d 680, 682 (W.D. La. 2023); Scully Dep. 997:1620.

a 2021 report that while CISA and other agencies play a role in the operation of elections, ***no federal agency***, including DHS, "has a focus on, or authority regarding, election misinformation originating from domestic sources within the United States."[197] Indeed, EIP doubled down on this point:

> [N]o government agency in the United States has the explicit mandate to monitor and correct election mis- and disinformation. This is especially true for election disinformation that originates from within the United States, which would likely be excluded from law enforcement action under the First Amendment and not appropriate for study by intelligence agencies restricted from operating inside the United States.[198]

Despite EIP seemingly understanding that DHS and CISA did not have the authority to censor election misinformation from domestic sources, the EIP continued to use DHS and CISA as a misinformation reporting center during the 2020 election.

2. *The Social Media Companies That Acted at CISA's Direction Did Not Question CISA's Authority.*

The Committee reached out to social media companies that were allegedly involved in CISA's efforts to censor the American public, including Meta, Google, Wikimedia, Yahoo, Reddit, Pinterest, Microsoft/LinkedIn, and Medium. As discussed in detail above, documents obtained by the Committee revealed CISA flagged reports of alleged election-related "misinformation" for Meta with the expectation that Meta would remove the content from its platform.[199]

Committee staff asked each of these companies the same question: "Prior to speaking with CISA, did anyone at your company conduct an analysis of whether CISA had statutory authority to partner with the private sector on content moderation issues?"[200]

Each of the company's complete response to this question is copied in the addendum at the end. None analyzed whether CISA had statutory authority to partner with them on content moderation issues.

Medium, Microsoft/LinkedIn, and Pinterest did not respond to the Committee.

3. *DHS OIG Did Not Question DHS's MDM Authority Even as It Audited This Work.*

From January 2021 through January 2022, DHS OIG performed the first audit of DHS related to MDM.[201] The audit focused on how the different components of DHS coordinated to counter MDM.[202] DHS OIG told the Committee that as part of this audit, it reviewed the legal authorities relevant to DHS's MDM work.[203] When the Committee asked for those authorities, however, DHS OIG could only point to Presidential Policy Directives 21 and 41, which, as discussed above, define certain sectors—not including election infrastructure—that qualify as critical infrastructure.[204] After the Committee sent multiple follow-up requests asking for the specific statutory source of authority for DHS's MDM work, DHS OIG eventually demurred and referred the Committee to DHS.[205]

---

197 EIP Report, *supra* note 105, at v.

198 *Id.* at 2.f.

199 *See supra*, Sections II.B.2, II.A.2; *Id.* at 8–10.

200 E-mail from Comm. Staff to Myriah Jordan, Public Policy, Facebook (Mar. 26, 2024) (on file with Comm. staff); E-mail from Comm. Staff to Samantha Dybas, Gov't Affs. & Pub. Pol'y, Google (Mar. 26, 2024) (on file with Comm. staff); E-mail from Comm. Staff to Stephen LaPorte, Deputy Gen. Couns., Wikimedia (Mar. 26, 2024); E-mail from Comm. Staff, to Tim Lynch, Head of U.S. Fed. Affs., Yahoo (Mar. 26, 2024) (on file with Comm. staff); E-mail from Comm. Staff, to Billy Easley II, Senior Pub. Pol'y Lead, Reddit (Mar. 26, 2024) (on file with Comm. staff); E-mail from Comm. Staff, to Greta H. Joynes, Pol'y Dir., Brownstein Hyatt Farber Schreck (Mar. 26, 2024) (on file with Comm. staff); E-mail from Comm. Staff, to Frank Cavaliere, Managing Dir. – Cong. Affs., Microsoft (Mar. 26, 2024) (on file with Comm. staff); E-mail from Comm. Staff, to Medium Legal Team (Mar. 26, 2024) (on file with Comm. staff).

201 DHS OIG Comm. Briefing (Jan. 4, 2024) (notes on file with Comm. staff).

202 DHS OIG Disinformation Report, *supra* note 50, at 1.

203 DHS OIG Comm. Briefing (Jan. 4, 2024) (notes on file with Comm. staff).

204 DHS OIG Comm. Briefing (Jan. 4, 2024) (notes on file with Comm. staff).

205 E-mail from Comm. Staff to Brian Gracey, Dir. of S. Affs., DHS Office of Leg. Affs. (Jan. 31, 2024) (on file with Comm. staff).

DHS OIG's failure to review DHS's legal authorities to "counter disinformation" resulted in a flawed report. While the final report, *DHS Needs a Unified Strategy to Counter Disinformation Campaigns*, provides some helpful insight into DHS's "internal and external coordination efforts . . . to counter disinformation appearing in social media," it does not conclude, or even consider, that DHS did not have authority to do this work.[206] Rather, it concludes that "without a more unified approach, DHS cannot effectively mitigate emerging threats or unify its work to counter disinformation campaigns that appear in social media from both foreign and domestic sources."[207] Moreover, throughout the report, the DHS OIG frequently referred to DHS's need to counter foreign ***and domestic*** sources of disinformation[208] because disinformation campaigns may affect "election ***infrastructure***."[209] To support these claims, however, the report cited only to possible harms to "public trust" in infrastructure rather than harms to the physical election infrastructure, which, as discussed above, is all CISA is authorized to address.[210]

C. CISA Did Not Comply with DHS OIG's Efforts to Oversee This Work.

1. *CISA Deliberately Delayed Responding to DHS OIG's Requests, Impeding Its Investigation.*

From January 2021 through July 2022, DHS OIG conducted an audit "to determine the internal and external coordination efforts the Department has taken to counter disinformation that appears in social media."[211] As part of that audit, from May 2021 to July 2021, DHS OIG interviewed members of various offices within DHS and intelligence agencies regarding their MDM-related work and began requesting POCs for social media companies that DHS and CISA worked with.[212] On June 23, 2021, DHS OIG asked CISA to provide "contact information for social media companies you have worked with to counter disinformation."[213] On July 7, 2021, DHS OIG followed up requesting the contacts again.[214] On July 14, 2021, DHS OIG closed its request for contacts in an email to CISA: "Per our conversation last Friday, we will not reach out to the social media POCs at this point if they do not want to talk to us."[215]

Still, CISA did not provide the contacts to DHS OIG. Instead, documents obtained by the Committee reveal that CISA notified its social media partners about DHS OIG's audit. As Nathaniel Gleicher,[216] the Director and Head of Security Policy at Meta, sent in a Signal thread on July 13, 2021, between industry including Meta, Twitter, Google, Reddit, Microsoft/LinkedIn, Yahoo, Wikipedia, Pinterest, "CISA let us know that know that DHS IG is conducting an investigation into the 'effectiveness and efficiency' of CISA's collaboration with the tech companies and has asked CISA to provide the IG with contacts from the companies who could answer questions."[217] Gleicher passed along CISA's warning "that this would be a pretty tricky context for us to answer questions"[218] and CISA's "commit[ment] to getting us more context on the nature of the IG inquiry so we'd have that before responding."[219] He further noted that "it sounds like they are under some pressure to provide contacts in industry so we'll likely hear more about this soon."[220]

Following a July 9, 2021, phone call between DHS OIG and CISA, for which no notes have been provided, DHS OIG decided

---

206 DHS OIG Disinformation Report, *supra* note 50, at 5.

207 *Id.*

208 *Id.* at 9, 11.

209 *Id.* at 1, 5 (emphasis added).

210 *Id.* at 3.

211 DHS OIG Disinformation Report, *supra* note 50, at 1.

212 DHS OIG Comm. Briefing (Jan. 4, 2024) (notes on file with Comm. staff).

213 E-mail from DHS OIG Office of Audits (June 23, 2021) (on file with Comm. staff).

214 *Id.*

215 E-mail from DHS OIG Office of Audits (July 7, 2021) (on file with Comm. staff).

216 Referred to as "Nathaniel" in the Signal chat.

217 *See* E-mail from DHS OIG Office of Audits (June 23, 2021) (on file with Comm. staff).

218 Nathaniel Gleicher, Signal group chat, "Industry Election Integrity WG" (July 13, 2021) (on file with Comm. staff).

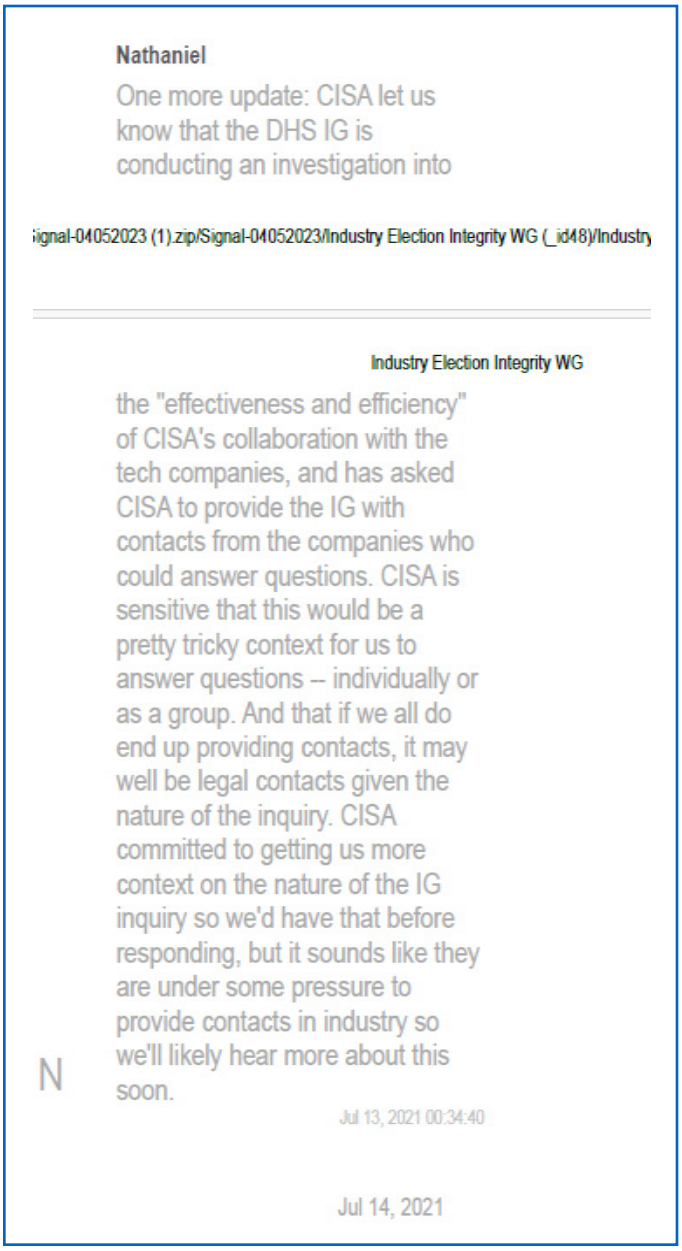
219 *Id.*

220 *Id.*

to withdraw its request for CISA's contacts at social media platforms.[221]

Ultimately, DHS OIG claimed it dropped the request because it needed to conclude the field work portion of its audit to meet the internal deadlines and CISA had moved too slowly for DHS OIG to hold interviews in time.[222]

CISA could have easily provided its contacts with social media companies. Indeed, CISA had been regularly meeting with key employees of social media companies regarding alleged MDM since before the 2020 election, and as indicted in the Signal chat, CISA knew who DHS OIG could contact.[223] But instead of providing contact information, CISA warned the social media companies about DHS OIG's audit and ran out the clock. While DHS OIG now claims that social media company perspectives were not integral to its audit, no doubt the lack of perspective limited the ability of DHS OIG from fully understanding CISA's censorship efforts.


Nathaniel

One more update: CISA let us know that the DHS IG is conducting an investigation into

ignal-04052023 (1).zip/Signal-04052023/Industry Election Integrity WG (_id48)/Industry

Industry Election Integrity WG

the "effectiveness and efficiency" of CISA's collaboration with the tech companies, and has asked CISA to provide the IG with contacts from the companies who could answer questions. CISA is sensitive that this would be a pretty tricky context for us to answer questions -- individually or as a group. And that if we all do end up providing contacts, it may well be legal contacts given the nature of the inquiry. CISA committed to getting us more context on the nature of the IG inquiry so we'd have that before responding, but it sounds like they are under some pressure to provide contacts in industry so we'll likely hear more about this soon.

N

Jul 13, 2021 00:34:40

Jul 14, 2021

2. *DHS Withdrew Policies It Told DHS OIG It Had Put in Place to Address DHS OIG's Recommendation and Hid These Actions from the Committee.*

a. DHS Hid Its Actions from the Committee and DHS OIG.

The DHS OIG's final report concluded that DHS needed a department-wide disinformation strategy, in part because a strategy would "promote consistency across the Department as components address privacy, constitutional, and other legal issues."[224] Its only recommendation was that the DHS Under Secretary for Policy "[d]evelop a unified strategy to improve DHS's coordinate actions among the Components and with other agencies to counter disinformation campaigns that appear in social media."[225]

DHS OIG told the Committee it "closed and resolved the recommendation in June 2023 when the DHS Office of General Counsel established a new Legal Practice Group on Emerging Technologies to coordinate DHS's positions and activities."[226] In doing so, DHS OIG relied on a memo from the DHS General Counsel, Jonathan Meyer, titled *Establishment of an Emerging Technology Legal Practice Group*.[227] DHS OIG told Committee staff that DHS provided it this memo on May 17, 2023.[228]

---

221 E-mail from DHS OIG Office of Audits (July 9, 2021) (on file with Comm. staff).

222 DHS OIG Comm. Briefing (Jan. 4, 2024) (notes on file with Comm. staff).

223 Scully Dep. 127:13–19.

224 DHS OIG Disinformation Report, *supra* note 50, at 10.

225 DHS OIG Disinformation Report, *supra* note 50, at 17.

226 E-mail from Debra Satkowiak, DHS OIG Executive Office/LAD, to Comm. Staff (Jan. 24, 2024) (on file with Comm. staff).

227 *Id.*; Memorandum from Jonathan E. Meyer, DHS General Counsel, to All DHS Component Chief Counsel and All OGC Headquarters Associate General Counsel (May 4, 2023) (on file with Comm. staff).

228 E-mail from Debra Satkowiak, DHS OIG Executive Office/LAD, to Comm. Staff (Aug. 16, 2024) (email on file with Comm. staff).

DHS tried to block the Committee from reviewing this memo for eight months. Committee staff first requested that DHS provide this memo, and four other relevant policy documents, on January 31, 2024.[229] DHS did not provide ***any*** of the requested documents until May 1, 2024, and omitted the *Establishment of an Emerging Technology Legal Practice Group* memo from the production.[230] Committee staff reiterated the request for this memo numerous times.[231] On July 1, 2024, DHS produced a memo from DHS General Counsel Jonathan Meyer titled the *Establishment of an Emerging Technology Legal Practice Group* (2024 DHS GC Memo), which included numerous white-out redactions (redactions that were not clearly marked by a colored box or some other method).[232] Notably, the memo was dated May 14, 2024, and referenced President Biden's November 2023 AI Executive Order and a May 21, 2024, meeting—indicating the memo somehow came out months after Committee staff requested it and almost a year after DHS provided it to the OIG.

DHS continued to obfuscate even after Committee staff pointed out this impossibility and requested all memos titled *Establishment of an Emerging Technology Legal Practice Group*.[233] Over a month passed before DHS answered Committee staff, refusing to provide any memos with that title because they would be "drafts" and therefore "considered deliberative."[234] Upon learning from DHS OIG that the memo Committee staff had been requesting since January 2024 was signed by Jonathan Meyer on May 4, 2023, Committee staff again requested DHS provide the original memo.[235] DHS again refused, stating that because the May 2023 memo was "never implemented," it was "considered deliberative," and they were therefore "unable to provide it."[236]

DHS's claim that the memo was privileged because it was deliberative was absurd. As Committee staff explained to DHS, even if FOIA exceptions applied to congressional requests (which they do not), the May 4, 2023, memo was not deliberative. To be covered by the deliberative process privilege, the memo must be "predecisional."[237] "A document is predecisional if it was 'prepared in order to assist an agency decisionmaker in arriving at his decision,' rather than to support a decision already made."[238] The May 2023 memo is not predecisional because it supported Mr. Meyer's decision to establish an "Emerging Technology Legal Practice Group." Meyer made that much clear in his May 2024 memo, in which he stated: "In early 2023 . . . ***I decided*** to establish the OGC Emerging Technology Legal Practice Group."[239] The May 2023 memo, which Meyer also signed, was issued to support that decision.[240] Therefore, the May 2023 memo was not predecisional and therefore could not have been reasonably considered subject to the deliberative process privilege.

DHS finally relented, in its words, "as an accommodation," after Committee staff pressed DHS for a call with the person who decided to hide the May 2023 memo.[241] DHS claimed the May 2023 memo "was never operationalized or shared with the workforce outside of the OGC Front Office."[242] DHS further asserted it was never operationalized because "[g]iven the

[229] E-mail from Comm. Staff to Brian Gracey, Dir. of Senate Affs., DHS Office of Leg. Affs. (July 1, 2024) (on file with Comm. staff).

[230] E-mail from Brian Gracey, Dir. of Senate Affs., DHS Office of Leg. Affs., to Comm. Staff (May 1, 2024) (on file with Comm. staff).

[231] E-mails from Comm. Staff to Brian Gracey, Dir. of Senate Affs., DHS Office of Leg. Affs. (May 14, 2024; May 20, 2024; June 4, 2024) (on file with Comm. staff).

[232] E-mails from Comm. Staff, to Brian Gracey, Dir. of Senate Affs., DHS Office of Leg. Affs. (July 1, 2024; July 19, 2024) (on file with Comm. staff).

[233] E-mail from Comm. Staff, to Brian Gracey, Dir. of S. Affs., DHS Office of Leg. Affs. (Aug. 8, 2024) (on file with Comm. staff).

[234] E-mail from Stephanie Doherty, Dep't of Homeland Sec., Deputy Asst. Sec., Leg. Affs., to Comm. Staff, to Comm. Staff (Aug. 12, 2024) (on file with Comm. staff).

[235] E-mail from Comm. Staff to Brian Gracey, Dir. of S. Affs., DHS Office of Leg. Affs. (July 1, 2024) (on file with Comm. staff); E-mail from Comm. Staff to Debra Satkowiak, DHS OIG Exec. Office/LAD (Aug. 16, 2024) (on file with Comm. staff).

[236] E-mail from Stephanie Doherty, Dep't of Homeland Sec., Deputy Asst. Sec., Leg. Affs., to Comm. Staff, to Comm. Staff (Sept. 12, 2024) (on file with Comm. staff).

[237] Citizens for Resp. & Ethics in Washington v. U.S. Gen. Servs. Admin., 358 F. Supp. 3d 50, 52 (D.D.C. 2019).

[238] *Id.* (quoting Citizens for Responsibility & Ethics in Washington v. Nat'l Archives & Records Admin., 715 F.Supp.2d 134, 139 (D.D.C. 2010)).

[239] Memorandum from Jonathan E. Meyer, DHS Gen. Couns., to All DHS Component Chief Couns. and All OGC Headquarters Assoc. Gen. Couns. (May 4, 2023) (on file with Comm. staff) (emphasis added)

[240] *Id.*

[241] E-mail from Jacob Marx, Dep't of Homeland Sec., Acting Dir. of Oversight, Office of Leg. Affairs, to Comm. Staff (Sept. 30, 2024) (on file with Comm. staff).

[242] E-mail from Jacob Marx, Dep't of Homeland Sec., Acting Dir. of Oversight, Office of Leg. Affairs, to Comm. Staff (Sept. 30, 2024) (on file with Comm. staff).

emergence of AI technologies, OGC quickly realized that the May 2023 memo had been overtaken by events."[243]

Making matters worse, DHS never informed DHS OIG that it had paused this work shortly after providing DHS OIG with the memo.[244] Again, DHS OIG relied on this memo in closing out its recommendation following its audit of CISA's censorship activities. Had DHS properly informed DHS OIG that it had put the group's establishment on pause, then it is likely that recommendation would have remained open.[245]

b. Memos Reveal DHS Learned Nothing from Its Previous Efforts to Censor Americans' Social Media Posts and Plans to Censor AI.

In the May 2023 memo to all DHS Component Chief Counsels and all OGC Headquarters Associate General Counsels, DHS General Counsel Meyer stated that he had "decided to establish the Emerging Legal Practice Group" to "provide a forum for attorneys across the Department to raise and address legal questions arising from client offices throughout DHS" and "ensure that OGC provides coordinated, consistent legal advice on issues related to the Department's use of emerging technology in furtherance of its missions," among other things.[246] While generally alluding to the group's ability to "share best practices and lessons learned from across the Department," it makes no mention of the First Amendment or abuse of authority concerns raised by CISA's online censorship work.[247] Meyer planned to schedule the group's "kickoff meeting" later that month.[248]

The May 2024 memo makes clear the Emerging Technology Legal Practice Group kickoff meeting never took place.[249] In the May 2024 memo from Meyer to Component Chief Counsel, Headquarters Associate General Counsel, the Judge Advocate General of the USCG and the Principal Legal Advisor of ICE, Meyer stated:

> Given ongoing work in both the Department and the federal government as a whole to develop policies and procedures related to emerging technology—most notably, but not exclusively, related to Artificial Intelligence (AI)—I decided to pause the official establishment of the group while those efforts remained in progress.

Meyer continued to describe how, since then, "the Department has taken on increasing and significant roles related to AI, both in ensuring DHS Components develop and use AI responsibly and in accordance with applicable law and policy and in ensuring that the homeland remains secure from any threats, or potential threats, enabled by the misuse of AI."[250] Meyer specifically noted "the establishment of the AI Safety and Security Board, which brings together governmental and non-governmental AI experts to issue recommendations and best practices to ensure AI developments are secure and resilient."[251] "In light of these developments," Meyer declared he had "decided that now is the time to officially establish the Emerging Technology Legal Practice Group."[252] He concluded by noting that "[a]lthough the practice group will not focus exclusively on AI to the exclusion of other emerging technologies . . . at least initially, the group will spend significant time and effort on legal issues related to AI."[253]

---

243 *Id.*

244 E-mail from Comm. Staff, to Debra Satkowiak, DHS OIG Executive Office/LAD (Aug. 16, 2024) (on file with Comm. staff).

245 *See Open Unresolved Recommendations Older Than Six Months as of Sept. 2023*, DHS OIG, https://www.oig.dhs.gov/sites/default/files/DHS-Open-Unresolved-Recommendations-Older-Than-Six-Months-as-of-093023.pdf ("DHS OIG typically closes recommendations once DHS completes the agreed upon corrective actions and DHS OIG verifies the actions were completed.").

246 Memorandum from Jonathan E. Meyer, DHS General Counsel, to All DHS Component Chief Counsel and All OGC Headquarters Assoc. General Couns. (May 4, 2023) (on file with Comm. staff).

247 *Id.*

248 *Id.*

249 *See* Memorandum from Jonathan E. Meyer, DHS Gen. Couns., to Component Chief Couns., Headquarters Assoc. Gen. Couns., Judge Advoc. Gen., USCG, and the Principal Legal Advisor, ICE (May 14, 2024) (on file with Comm. staff).

250 *See* Memorandum from Jonathan E. Meyer, DHS Gen. Couns., to Component Chief Couns., Headquarters Assoc. Gen. Couns., Judge Advoc. Gen., USCG, and the Principal Legal Advisor, ICE (May 14, 2024) (on file with Comm. staff).

251 *Id.*

252 *Id.*

253 *Id.*

c. A Shifting Focus Toward AI and "Emerging Technologies" to Further Government Censorship

While the Biden administration stopped short of fully implementing its agenda on AI at DHS, actions taken by the National Institute of Standards and Technology (NIST) and National Science Foundation (NSF) show the Biden administration was beginning to establish a regulatory agency apparatus capable of censoring both AI inputs and outputs.

NIST's Role in AI Censorship

Pursuant to the Biden AI Executive Order[254] and guidance from its AI Safety Institute,[255] NIST published a seminal document describing steps AI developers should take to monitor for "harmful" speech.

NIST's "AI Risk Management Framework: Generative Artificial Intelligence Profile (600-1)" advised AI developers, deployers, and "organizations identifying and managing Generative AI ('GenAI') risks" to "govern, map, measure, and mitigate" risks.[256] According to NIST's guidance, the "risks" to be managed and mitigated in generative AI included: "Dangerous, Violent, or Hateful Content," content with "harmful bias or homogenization [that supports] amplification and exacerbation of historical, societal, and systemic biases," the risk of "Information Integrity [where a] [l]owered barrier to entry to generate and support the exchange and consumption of content ...may not distinguish fact from opinion or fiction or acknowledge uncertainties, or could be leveraged for large-scale dis- and mis-information campaigns," and "Obscene, degrading, and/or abusive content."[257]

But the NIST generative AI RMF was not merely guidance.

The NIST AI Safety Institute stood up a testing apparatus (per the Biden AI EO[258]) called the "Assessing Risks and Impacts of AI (ARIA) program." This new AI testing effort was meant to red-team AI products for risks, including offensive generative AI content and speech harms.[259] In establishing ARIA, the Biden administration turned to companies that had entered into the Biden's administration's "voluntary AI pledge" and required these participants to make good on their pledges and undergo AI testing with ARIA.[260] [261] [262]

The Biden administration's definition of "red-teaming," which was used in Biden's AI EO and throughout NIST guidance to

---

[254] Exec. Order No. 14,110, 88 Fed. Reg. 75191 (Oct. 30, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[255] Press Release, U.S. Dep't. of Com., At the Direction of President Biden, Department of Commerce to Establish U.S. Artificial Intelligence Safety Institute to Lead Efforts on AI Safety (Nov. 1, 2023), https://www.commerce.gov/news/press-releases/2023/11/direction-president-biden-department-commerce-establish-us-artificial.

[256] NIST, AI Risk Management Framework, https://www.nist.gov/itl/ai-risk-management-framework (last visited Sept. 1, 2025); Nat'l. Inst. of Standards and Tech., NIST Trustworthy and Responsible AI: NIST AI 600-1, Artificial intelligence Risk management Framework: Generative Artificial Intelligence Profile 1 (2024) [hereinafter *NIST AI 600-1*], https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf.

[257] *Id*. at 4–5.

[258] *See* Exec. Order No. 14,110, §§ 4.1–4.3, §10, 88 Fed. Reg. 75191. (Oct. 30, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[259] Press Release, NIST, NIST Launches ARIA, a New Program to Advance Sociotechnical Testing and Evaluation for AI (May 28, 2024), https://www.nist.gov/news-events/news/2024/05/nist-launches-aria-new-program-advance-sociotechnical-testing-and; *see also* Press Release, NIST, Department of Commerce Announces New Actions to Implement President Biden's Executive Order on AI (Apr. 29, 2024), https://www.nist.gov/news-events/news/2024/04/department-commerce-announces-new-actions-implement-president-bidens; Press Release, NIST, U.S. Secretary of Commerce Gina Raimondo Releases Strategic Vision on AI Safety, Announces Plan for Global Cooperation Among AI Safety Institutes (May 21, 2024), https://www.nist.gov/news-events/news/2024/05/us-secretary-commerce-gina-raimondo-releases-strategic-vision-ai-safety.

[260] Press Release, NIST, U.S. AI Safety Institute Signs Agreements Regarding AI Safety Research, Testing, and Evaluation with Anthropic and OpenAI (Aug. 29, 2024), https://www.nist.gov/news-events/news/2024/08/us-ai-safety-institute-signs-agreements-regarding-ai-safety-research; *see also* Press Release, The White House, FACT SHEET: Biden-Harris Administration Announces New AI Actions and Receives Additional Major Voluntary Commitment on AI (July 26, 2024), https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/07/26/fact-sheet-biden-harris-administration-announces-new-ai-actions-and-receives-additional-major-voluntary-commitment-on-ai/; Reva Schwartz, et al, *The Draft: NIST Assessing Risks and Impacts of AI (ARIA) Pilot Evaluation Plan* 4 (May 21, 2024), https://web.archive.org/web/20240529144514/https://ai-challenges.nist.gov/uassets/7.

[261] Press Release, NIST, Updated Guidelines for Managing Misuse Risk for Dual-Use Foundation Models (Jan. 15, 2025), https://www.nist.gov/news-events/news/2025/01/updated-guidelines-managing-misuse-risk-dual-use-foundation-models.

[262] U.S. AI Safety Institute, NIST 800-1 2pd: Managing Misuse Risk for Dual-Use Foundation Models 11–12 (2025) (hereinafter *NIST 800-1 2PD*), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.800-1.ipd2.pdf.

describe how to assess AI for vulnerabilities, revealed the true nature of its AI risk-testing.[263]

Traditionally, red-teaming has referred to adversarial testing of information systems for the discovery of technical vulnerabilities that could be exploited by hackers. The Biden administration vastly expanded the definition of red-teaming to capture social harms, including discrimination, bias, and misinformation operations.[264] Specifically, the Biden administration defined red-teaming to mean testing for "flaws and vulnerabilities such as harmful or discriminatory outputs from an AI system, unforeseen or undesirable system behaviors, limitations, or potential risks associated with the misuse of the system."[265]

Collectively, NIST's generative AI guidance, its definitions of "risks" and "harms," ARIA's red-team testing, and the mandated application of this testing to companies in Biden's voluntary AI pledge illustrate how NIST and the Biden administration had begun to establish a censorship apparatus for AI.[266]

NSF's Role in AI Censorship

In addition to NIST, the Biden administration was using the National Artificial Intelligence Research Resource (NAIRR) at the National Science Foundation to further censorship in AI.

In January 2021, Congress enacted the National Defense Authorization Act of Fiscal Year 2021. The law included the Artificial Intelligence Initiative Act, which directed the National Science Foundation (NSF) to establish, in coordination with the OSTP Director, a task force to consider establishing a "National Artificial Intelligence Research Resource (NAIRR)."[267]

Before enactment, the NAIRR was marketed to members of Congress as a program to expand access and exposure to AI and computing power to students and researchers around the country, create more opportunities for innovation among those who might otherwise not have it, and improve America's future talent pool and labor force.[268]

---

263 *Id.* at 22 (defining "AI Red-Teaming" as "a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI. AI red-teaming is most often performed by dedicated 'red teams' that adopt adversarial methods to identify flaws and vulnerabilities, such as harmful or discriminatory outputs from an AI system, unforeseen or undesirable system behaviors, limitations, or potential risks associated with the misuse of the system"; *see* Exec. Order No. 14,110, § 3(d), 88 Fed. Reg. 75191. (Oct. 30, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence; *see also* Harvey Geiger and Tanvi Chopra, *AI Hacking in the White House's Executive Order*, Center for Cybersecurity and Pol'y L. (Nov. 1, 2023), https://www.centerforcybersecuritypolicy.org/insights-and-research/ai-hacking-in-the-white-houses-executive-order.

264 "Most traditional definitions of red-teaming center on emulating adversarial attacks and exploitation capabilities against an organization's security posture. See, for example, the definition by the National Institute of Standards and Technology (NIST). By contrast, the EO's definition of "AI red-teaming" is clearly not limited to security and does not necessarily require adversarial attacks. Instead, under the EO, the term means structured testing to find flaws and vulnerabilities. Under the EO, this testing often—but not necessarily—uses adversarial methods and involves working with AI developers to 'identify flaws and vulnerabilities, such as harmful or discriminatory outputs from an AI system, unforeseen or undesirable system behaviors, limitations, or potential risks associated with the misuse of the system.' [Sec. 3(d)] This definition is reflected in the Office of Management and Budget (OMB) draft memo that accompanies the EO. AI red teaming under the EO becomes testing of an AI system, which the EO also defines broadly, for both security and functionality within established guardrails." Geiger, *supra* note 256 *(*citing *Red Team*, NIST Info. Tech. Lab. Comp. Sec. Res. Center, https://csrc.nist.gov/glossary/term/red_team (last visited Sept. 26, 2025); Memorandum from Shalanda D. Young, Dir. of Office of Mgmt. and Budget, Draft for Public Review (Nov. 2023) (hereinafter *OMB AI Memo*), https://ai.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-Public-Comment.pdf.

265 Exec. Order No. 14,110, §3 (d), 88 Fed. Reg. 75191 (Oct. 30, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

266 *See* Press Release, House Judiciary Comm., Report: The Federal Government's Attempt to Control Artificial Intelligence to Suppress Free Speech (Dec. 18, 2024), https://judiciary.house.gov/media/press-releases/report-federal-governments-attempt-control-artificial-intelligence-suppress; Press Release, Senate Comm. on Com. Sci. and Transp., Sen. Cruz Sounds Alarm Over Industry Role in AI Czar Harris's Censorship Agenda (Sept. 16, 2024), https://www.commerce.senate.gov/2024/9/sen-cruz-sounds-alarm-over-industry-role-in-ai-czar-harris-s-censorship-agenda; Establishment of Reporting Requirements for the Development of Advanced Artificial Intelligence Models and Computing Clusters, 89 Fed. Reg. 73612 (proposed Sept. 11, 2024); *OMB AI Memo*, *supra* note 257, at 9–14, 19, 20–21; Chase J. Cooper, *DOJ Launches Civil-Cyber Fraud Initiative to Use False Claims Act to Enforce Federal Contractors' Cyber Security Requirements*, Winston & Strawn (Nov. 2, 2021), https://www.winston.com/en/blogs-and-podcasts/government-program-fraud-false-claims-act-and-qui-tam-litigation-playbook/doj-launches-civil-cyber-fraud-initiative-to-use-false-claims-act-to-enforce-federal-contractors-cyber-security-requirements; Press Release, The White House, FACT SHEET: OMB Issues Guidance to Advance the Responsible Acquisition of AI in Government (Oct. 3, 2024), https://bidenwhitehouse.archives.gov/omb/briefing-room/2024/10/03/fact-sheet-omb-issues-guidance-to-advance-the-responsible-acquisition-of-ai-in-government/.

267 Artificial Intelligence Initiative Act of 2020, Pub. L. No. 116–283, § 5106(1)(A), 134 Stat. 4531 (2021).

268 Brandi Vincent, *Congress Inches Closer to Creating a National Cloud for AI Research*, Next Gov (July 2, 2020), https://www.nextgov.com/artificial-intelligence/2020/07/congress-inches-closer-creating-national-cloud-ai-research/166624/; Jared Council, *Defense Bill Boosts Federal AI Research and Development*, Wall Street Journal (Jan. 8, 2021), https://www.wsj.com/articles/defense-bill-boosts-federal-ai-research-and-development-11610141733; Dave Nyczepir, *White House Seeks Input on Designing a National AI Resource Center*, Fed Scoop (July 27, 2021), https://fedscoop.com/national-ai-re-

Yet, that's not what the NAIRR became.

Under the Biden administration, the Task Force held 11 public meetings and published two Requests For Information to gather public input for a final report that was published in January 2023, titled, "Strengthening and Democratizing the U.S. AI Innovation Ecosystem."[269] In the report, the Task Force stated that the NAIRR's objective should be to "strengthen and democratize the U.S. AI innovation ecosystem in a way that protects privacy, civil rights, and civil liberties."[270] The report made clear how the Biden government would use the NAIRR to monitor for speech it found objectionable.

For example, the report recommended that "the NAIRR should set the standard for responsible AI research through the design and implementation of its governance processes... by integrating appropriate technical controls, policies, and government mechanisms... in accordance with [Biden's] Blueprint for an AI Bill of Rights."[271] The Task Force wrote that the goal of the NAIRR's operating entity should include "advancing diversity, equity, inclusion, and accessibility (DEIA) in all aspects of the NAIRR" building on the report's earlier reasoning that: "lack of diversity may also contribute to the development of biased or harmful AI systems and threaten the Nation's innovation potential and global leadership."[272] The Task Force went on to say the NAIRR had multiple functions, including that establishing the NAIRR's "cyberinfrastructure also presents a unique opportunity to 'design in' the standards responsible for AI research practices and governance," and that the "cyberinfrastructure can also help open up new opportunities for progress across all scientific fields, including...AI auditing, testing, and evaluation, trustworthy AI, bias mitigation, and AI safety."[273]

Subsequent to the Task Force's recommendations, the Biden administration formally stood up the NAIRR via an October 30, 2023, EO.[274] The NAIRR, under the control of the NSF, would have the same leadership, regulatory framework, and policy regime that made government-backed censorship projects possible elsewhere.

In February 2024, the House Judiciary Committee released a report titled "The Weaponization of the National Science Foundation: How NSF is Funding The Development Of Automated Tools to Censor Online Speech 'At Scale' and Trying To Cover Up Its Actions."[275]

In its investigative report, the House Judiciary Committee wrote:

> "In the name of combatting alleged misinformation regarding COVID-19 and the 2020 election**, NSF has been issuing multi-million-dollar grants to university and non-profit research teams. The purpose of these taxpayer-funded projects is to develop artificial intelligence (AI) powered censorship and propaganda tools** that can be used by governments and Big Tech to shape public opinion by restricting certain viewpoints or promoting others."[276]

The NAIRR at NSF, which gave taxpayer funding to censorship research and drove Big Tech's adoption of censorship (in addition to the direct kind of government coercion laid out above), was poised to mirror NSF's features:

- NSF offered grants to research institutions and academia related to combatting "misinformation" and "disinformation";
- That academic and non-profit research informing how to use AI to combat "misinformation" and "disinformation" was

search-resource-input/.

[269] National Artificial Intelligence Research Resource Task Force, Strengthening and Democratizing the U.S. Artificial intelligence Innovation Ecosystem iii (2023), https://www.ai.gov/wp-content/uploads/2023/01/NAIRR-TF-Final-Report-2023.pdf.

[270] *Id.*

[271] *Id.* at vi.

[272] *Id.* at 18, 1.

[273] *Id.* at ii, iv.

[274] Exec. Order No. 14,110, §5.2(i), 88 Fed. Reg. 75191 (Oct. 30, 2023), https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[275] Staff of Comm. on the Judiciary Select Subcomm. on the Weaponization of the Fed. Gov't, 118th Cong., Rep. on the Weaponization of the Nat'l Ci. Found.: How NSF Is Funding the Development of Automated Tools to Censor Online Speech "At Scale" and Trying to Cover Up Its Actions (2024), https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/NSF-Staff-Report_Appendix.pdf.

[276] *Id.* at 1.

used by NSF to further fund the development of censorship and propaganda tools; and
- Those tools and research were pushed to Big Tech companies to adopt and integrate to censor Americans online.

In 2023, this Committee, under the leadership of then-Ranking Member Cruz, found that NSF funded numerous projects to promote censorship of information. Staff identified over a hundred grants between 2021 and 2023—totaling over $66 million in taxpayer funding—to so-called "misinformation" research, directly funding organizations that work with online platforms to censor Americans.[277] Examples included:

- $5 million to the University of Wisconsin to create a "digital dashboard" so public officials could identify "trending misinformation" and "strategically correct" misinformation on social media;[278] and
- $5 million to George Washington University to create a therapy toolkit and digital reporting assistant for journalists who believed they were the targets of "misinformation-driven harassment campaigns."[279]

By the end of 2024, it became apparent that NSF through the NAIRR was prioritizing similar grants and projects with these perspectives and agendas. For example, the NAIRR awarded funds to AI research that included:

- Evaluating Large Language Models for the Measurement of Complex Social Phenomena at UC Berkeley: "In this pilot project, we will examine their performance at three complex measurement tasks (measuring income inequality, measuring the representation of race in narratives, and measuring the relationships between characters), while also exploring the degree to which LLMs capture information about language dialects and style."[280]

Thus, the pattern that emerged at the NAIRR began to resemble past scenarios where the government doled out grants furthering "research" based on political or social engineering goals. Given NSF's track record, it was likely a matter of time before the administration would have pushed a regulatory regime restricting speech outputs on AI models. And, in light of CISA's overreach on MDM, it is plausible that DHS would have implemented a similar regime to monitor AI system outputs

IV. *Conclusion*

CISA was created to protect the critical infrastructure of the United States. Instead, Biden administration bureaucrats acting without proper authority commandeered the agency to censor Americans. As the Committee's investigative report lays out:

- Prior to CISA's formal authorization at the end of 2018, the Department of Homeland Security had already initiated a program, the Countering Foreign Influence Task Force, that would enable it to censor Americans.
- CISA then began to use regular meetings with industry, the practice of "switchboarding," monitoring portals, and nonprofit partners to restrict Americans' speech in the 2020 election.
- During the Biden administration, CISA tasked its Countering Foreign Influence Task Force to focus on <u>all</u> types of misinformation (including by American citizens) through the MDM team.
- During the 2022 election cycle, CISA made no distinction between foreign and American speech online, pushed censorship on industry partners, handed off its switchboarding work to nonprofit partners purely because of capacity issues, and created an advisory committee on how CISA could best target American speech online through the MDM Subcommittee in the Cybersecurity Advisory Committee.
- During the Committee's investigation of CISA, the Committee discovered that CISA had no statutory authority for this work and had ignored concerns raised by nonprofit partners that CISA lacked this authority. Nevertheless, no one at the Department of Homeland Security questioned these actions, including the Office of Inspector General (OIG), which is responsible for oversight of CISA.
- When CISA chose to obstruct the OIG's audit of MDM work at the Department of Homeland Security, the OIG let them.

---

[277] Press Release, Senate Comm. on Com. Sci. and Transp., Sen. Cruz Demands Answers on Taxpayer-Funded Censorship (Oct. 31, 2023), https://www.commerce.senate.gov/2023/10/sen-cruz-demands-answers-on-taxpayer-funded-censorship.

[278] *Id.*

[279] *Id.*

[280] *See (NAIRR240114), Evaluating Large Language Models for the Measurement of Complex Social Phenomena*, NAIRR Pilot Resource Allocation, https://nairrpilot.org/awarded-projects?_requestNumber=NAIRR240114.

- After the DHS OIG recommended that DHS create a department-wide disinformation strategy, DHS falsely claimed it had implemented the recommendation.
- Based on the Biden administration's efforts to censor Americans through CISA and its initial attempts at censoring AI companies and models, it may have been only a matter of time before the Biden administration used programs established by Congress, like the NAIRR, to implement a censorship regime for AI.

Therefore, it is the Committee's recommendation that Congress pass legislation to:

- Create transparency around federal agency communication with private entities on issues that may affect American speech.
- Produce guidelines that clearly restrict government officials from influencing social media platforms' content moderation decisions of constitutionally protected speech.
- Establish a reporting mechanism to allow platforms to report if they think they may be experiencing government jawboning efforts of censorship or content moderation.
- Before contemplating new Federal regulation, enact guardrails that preclude existing Federal AI programs, such as the NAIRR and the Center for AI Standards and Innovation (CAISI) (formerly known as the AI Safety Institute) from curtailing speech in the name of addressing harms.

Free speech is a bedrock of American democracy and protected by the First Amendment. Even when speech might be considered objectionable or false, the government cannot attempt to suppress it. During the Biden administration, Big Tech companies admitted to being pressured to censor content by the administration; CISA had an active role in this effort. The launch of AI led the Biden administration to take similar anti-speech actions, underscoring a pressing need for Congressional action to adequately squash the risk of continued interference in speech by the administrative state.[281] Censorship around the world is growing, including among our allies. It is more important than ever for the United States to uphold free speech and zealously guard against government censorship.

[281] Gnaneshwar Rajan & Nandita Bose, *Zuckerberg Says Biden Administration Pressured Meta to Censor COVID-19 Content*, Reuters (Aug. 27, 2024), https://www.reuters.com/technology/zuckerberg-says-biden-administration-pressured-meta-censor-covid-19-content-2024-08-27/.

ADDENDUM

Meta[282]

The Cybersecurity and Infrastructure Security Agency ("CISA") was created by the Cybersecurity and Infrastructure Security Agency Act, which was passed with broad bipartisan support and signed by President Trump in November 2018. Since that time, individuals at Meta have had contact with CISA officials under both the Trump and Biden administrations as part of our ongoing election integrity work. For example, Meta has participated in industry-wide meetings facilitated by CISA to discuss potential threats to elections and election administration. Brian Scully was a main point of contact at CISA for those meetings, as he discussed in deposition testimony that is part of the public record.

Our interactions with the agency were intended to focus on our common goal of protecting our elections—our content moderation decisions are our own, and we are not aware of any internal analysis of CISA's statutory authority with respect to content moderation. As a general matter, when we receive a report or request to take down content, we evaluate the content against the Facebook Community Standards or Instagram Community Guidelines and, if we determine that the content goes against our policies, we take action.

Google[283]

Thank you for your questions regarding the U.S. Department of Homeland Security and its Cybersecurity and Infrastructure Security Agency.

We believe that CISA is best positioned to answer your specific questions regarding the timing and nature of their contacts. Although we do not have an exact date their outreach began, it is our understanding that regular meetings between U.S. government entities – including CISA – and the technology sector were established in advance of the 2018 U.S. midterms.

These meetings included representatives from various government agencies, federal law enforcement, and the intelligence community, as well as other technology companies, including Microsoft, Twitter, and Facebook. The purpose of these meetings was for the tech industry to hear from representatives of the U.S. Government about general trends that they were seeing related to upcoming elections. In the course of our conversations at these meetings, government officials generally did not discuss concerns with specific, individual pieces of content.

To be clear, Google has not and does not "partner" with CISA regarding content moderation. Outside parties across the political spectrum in the United States and globally – including government agencies, Members of Congress, political entities, non-governmental organizations, academics, and individual users – inform us of content that they believe may violate our terms of service and policies. When content is flagged, our teams voluntarily review the content in light of our terms and policies, and we independently evaluate whether the content violates our terms of service and policies, without regard for the source of the original inquiry or input from CISA.

Wikimedia[284]

My team has now had a chance to review. While some staff who were present several years ago have left the Wikimedia Foundation (and one staff member who worked on this topic area has unfortunately passed away), based on what current staff who were present at the time recall, we had one prior contact with CISA and then attended the industry group meetings that were reported in the media.

Sometime in 2019, Brian Scully from the DHS Countering Foreign Interference Task Force visited the Bay Area, and Foundation staff met him for coffee, although we don't have information if anyone else was present. He later emailed in October 2019 to ask about how to contact the Foundation if they learned of any influence operation incidents, and we connected him with a

[282] E-mail from Meta to S. Comm. on Com., Sci. & Transp. (May 1, 2024) (On file with Comm. staff).

[283] E-mail from Google to S. Comm. on Com., Sci. & Transp. (Apr. 18, 2024) (On file with Comm. staff).

[284] E-mail from Wikimedia to S. Comm. on Com., Sci. & Transp. (Apr. 4, 2024) (On file with Comm. staff).

member of our team who could be a point of contact (and who is now deceased). We don't have any records of receiving or acting on any CISA report.

Later in 2020, a Foundation staff member was invited to the information-sharing meetings, as reported in the media, by colleagues at another company rather than by anyone in the government. Subsequently, Foundation staff only attended such meetings for the purpose of receiving information, as a listening exercise.

The Foundation never formed any sort of partnership or similar relationship with CISA, so we never conducted any statutory analysis.

Yahoo[285]

CISA's initial outreach to Yahoo began in October 2019 when it shared with Yahoo indicators of ransomware and other cybersecurity threats that could impact Yahoo's systems. Outside of any information sharing relating to cybersecurity threats, CISA's contacts with Yahoo did not relate to content on any of Yahoo's platforms or systems. The individual from CISA who was responsible for conducting the initial outreach to Yahoo in October 2019 was as follows: Jonathan Halperin, Senior Cybersecurity Liaison, CISA.

At the outset, it is important to note that for any engagement Yahoo has with governmental agencies relating to content moderation issues and requests for user data, Yahoo has developed Global Principles for Responding to Government Requests (Global Principles). These Global Principles set forth the analytical framework by which Yahoo will review any requests from governmental agencies on content moderation issues or requests for user data. Our Global Principles that govern any outreach we receive from governmental agencies on content moderation issues and requests for user data are publicly accessible and can be found here.

It should also be noted that following Yahoo's sale of Tumblr in August 2019, Yahoo no longer had any social media-based products.

As a follow-up, Committee staff requested Yahoo confirm that CISA reached out to Yahoo in October 2019 (since DHS reported that CISA began outreach and meetings with tech companies about disinformation in 2018 so to confirm that they reached out to Yahoo later) and if anyone at Yahoo ever analyzed or questioned whether CISA had the statutory authority to partner with the private sector on content moderation issues. Yahoo provided the response below.[286]

Our Global Principles were referenced in response because for any government requests, whether it be for user data or here, on content moderation issues, our Principles set forth the analytical framework by which we review those requests. We apply these Principles to all requests and outreach from governments on content moderation and other issues, regardless of which government or agency conducts that outreach or request. This ensures we have a uniform consistent approach to reviewing any government requests on content moderation issues. Here, at the time CISA made their outreach to Yahoo in 2019, our Principles were already in effect and governed our review of any outreach they would have made to us on content moderation issues. As indicated in our prior response though, the initial outreach by CISA to Yahoo related to indicators of ransomware and other cybersecurity threats.

Reddit[287]

Our contact with CISA has been very minimal (and we haven't had any contact with them in nearly two years), but to our recollection, they first reached out around October 2019. While we're unfortunately not able to share details about any specific individuals' private correspondence, we can share at a high level that the interactions with CISA never pertained to content on Reddit. As for your third question, while we can't disclose attorney-client privileged material, we can share generally that we always consider every government interaction with regard to our (and our users') rights under the law, as well as our Privacy Policy and overall duty to our users, though this typically does not take the form of a formal written analysis. More information about how we assess interactions with government can be found in our Guidelines for Law Enforcement.

---

[285] E-mail from Yahoo to S. Comm. on Com., Sci. & Transp. (Apr. 5, 2024) (On file with Comm. staff).

[286] E-mail from Yahoo to S. Comm. on Com., Sci. & Transp. (Apr. 15, 2024) (On file with Comm. staff).

[287] E-mail from Reddit to S. Comm. on Com., Sci. & Transp. (Apr. 1, 2024) (On file with Comm. staff).

Reddit also briefed Committee staff on this topic on April 9, 2024. During that briefing, Reddit explained that while they have very strict rules they "did not have a partnership with [CISA] or were involved in any takedown requests," which is the clearest answer Reddit was able to give "without violating [its legal department] rules."[288]

[288] Reddit Comm. Briefing (Apr. 9, 2024) (notes on file with Comm. staff).