



**THE WEAPONIZATION OF CISA:  
HOW A “CYBERSECURITY” AGENCY COLLUDED WITH BIG TECH  
AND “DISINFORMATION” PARTNERS TO CENSOR AMERICANS**

Interim Staff Report of the  
Committee on the Judiciary  
and the  
Select Subcommittee on the Weaponization of the Federal Government

U.S. House of Representatives



June 26, 2023

---

## EXECUTIVE SUMMARY

---

“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.”

– CISA Director Jen Easterly, November 10, 2021.<sup>1</sup>

The First Amendment recognizes that no person or entity has a monopoly on the truth, and that the “truth” of today can quickly become the “misinformation” of tomorrow. Labeling speech “misinformation” or “disinformation” does not strip it of its First Amendment protection. As such, under the Constitution, the federal government is strictly prohibited from censoring Americans’ political speech. The government also may not use third parties to bypass the First Amendment and conduct censorship by proxy.<sup>2</sup>

The Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government have been conducting an investigation into government-induced censorship on social media. Although the investigation is ongoing, information obtained to date has revealed that the Cybersecurity and Infrastructure Security Agency (CISA)—an upstart agency within the Department of Homeland Security (DHS)—has facilitated the censorship of Americans directly and through third-party intermediaries.

Founded in 2018, CISA was originally intended to be an ancillary agency designed to protect “critical infrastructure” and guard against cybersecurity threats.<sup>3</sup> In the years since its creation, however, CISA metastasized into the nerve center of the federal government’s domestic surveillance and censorship operations on social media.<sup>4</sup> By 2020, CISA routinely reported social media posts that allegedly spread “disinformation” to social media platforms.<sup>5</sup> By 2021, CISA had a formal “Mis-, Dis-, and Malinformation” (MDM) team.<sup>6</sup> In 2022 and 2023, in response to growing public and private criticism of CISA’s unconstitutional behavior, CISA attempted to camouflage its activities, duplicitously claiming it serves a purely “informational” role.<sup>7</sup>

This interim staff report details, among other things, that:

---

<sup>1</sup> Maggie Miller, *Cyber agency beefing up disinformation, misinformation team*, THE HILL (Nov. 10, 2021).

<sup>2</sup> See *Norwood v. Harrison*, 413 U.S. 455, 465 (1973) (“It is also axiomatic that a state may not induce, encourage or promote private persons to accomplish what it is constitutionally forbidden to accomplish.”).

<sup>3</sup> See 6 U.S. Code § 652; *Federal Government*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, <https://www.cisa.gov/audiences/federal-government> (last visited Jun. 23, 2023).

<sup>4</sup> See Ken Klippenstein and Lee Fang, *Truth Cops: Leaked Documents Outline DHS’s Plans to Police Disinformation*, THE INTERCEPT (Oct. 31, 2022).

<sup>5</sup> Scully Dep. 16:16–17:8, *Missouri v. Biden*, No. 3:22-cv-01213 (W.D. La. 2022), ECF No. 209.

<sup>6</sup> *DHS Needs a Unified Strategy to Counter Disinformation Campaigns*, DEP’T OF HOMELAND SEC. OFFICE OF INSPECTOR GEN., at 7 (Aug. 10, 2022), <https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-58-Aug22.pdf>.

<sup>7</sup> See, e.g., Scully Dep. 17:9–14, *supra* note 5.

- CISA is “working with federal partners to mature a whole-of-government approach” to curbing alleged misinformation and disinformation.<sup>8</sup>
- CISA considered the creation of an anti-misinformation “rapid response team” capable of physically deploying across the United States.<sup>9</sup>
- CISA moved its censorship operation to a CISA-funded non-profit after CISA and the Biden Administration were sued in federal court, implicitly admitting that its censorship activities are unconstitutional.<sup>10</sup>
- CISA wanted to use the same CISA-funded non-profit as its mouthpiece to “avoid the appearance of government propaganda.”<sup>11</sup>
- Members of CISA’s advisory committee agonized that it was “only a matter of time before someone realizes we exist and starts asking about our work.”<sup>12</sup>

The Committee and the Select Subcommittee are responsible for investigating “violation[s] of the civil liberties of citizens of the United States.”<sup>13</sup> In accordance with this mandate, this interim staff report on CISA’s violations of the First Amendment and other unconstitutional activities fulfills the obligation to identify and report on the weaponization of the federal government against American citizens. The work, however, is not done. CISA still has not adequately complied with a subpoena for relevant documents, and much more fact-finding is necessary. In order to better inform the Committee’s legislative efforts, the Committee and Select Subcommittee will continue to investigate CISA’s and other Executive Branch agencies’ entanglement with social media platforms.

---

<sup>8</sup> CISA CYBERSECURITY ADVISORY COMM., SUBCOMMITTEE OVERVIEW & UPDATE: PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION, at 1 (2022) (on file with the Comm.).

<sup>9</sup> CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING JUNE 14, 2022, at 2 (on file with the Comm.).

<sup>10</sup> CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING JULY 26, 2022, at 1 (on file with the Comm.).

<sup>11</sup> CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING APRIL 12, 2022, at 2 (on file with the Comm.).

<sup>12</sup> E-mail from Suzanne Spaulding to Kate Starbird (May 20, 2022, 7:27 AM) (on file with the Comm.).

<sup>13</sup> H. Res. 12 § 1(b)(E).

---

**TABLE OF CONTENTS**

---

**Executive Summary** ..... 1

**Table of Contents** ..... 3

**Background** ..... 4

**CISA’s Mission Creep into Surveillance, Censorship, and Cover-ups** ..... 9

    I. CISA has transformed into a domestic intelligence and speech-police agency, far exceeding its statutory authority ..... 9

        A. Switchboarding: CISA’s coordination with Big Tech to censor Americans ..... 12

        B. CISA’s MDM consultants rejected constitutional “limitations” on the surveillance and censorship of domestic speech ..... 12

        C. CISA considered creating an anti-MDM “rapid response team” to physically deploy across the United States. .... 14

        D. MDM “experts” wanted CISA to crack down on *factual* information ..... 15

        E. CISA is only one part of a “whole-of-government approach” to MDM ..... 16

        F. State election officials warned CISA to “remain within [its] operational and mission limits,” lest it should earn the public’s “distrust.” ..... 17

        G. DHS was eager to cement CISA as a domestic intelligence agency ..... 18

        H. Social media companies mocked CISA’s MDM team and DHS’s Disinformation Governance Board ..... 19

        I. CSAC members were concerned about the MDM Subcommittee ..... 20

    II. CISA colludes with third parties to circumvent the First Amendment and conduct censorship by proxy ..... 21

        A. CISA’s external censorship arm: the EI-ISAC ..... 22

        B. State and local election officials used the EI-ISAC in an effort to silence critics and political opponents ..... 23

        C. CISA admitted to outsourcing its surveillance operation to third parties ..... 26

    III. CISA has attempted to conceal its unconstitutional activities and remove evidence of wrongdoing ..... 28

        A. Fearing public pressure and legal risks, CISA outsourced its censorship operation to the EI-ISAC ..... 28

        B. The MDM Subcommittee tried to disguise its recommendations by removing references to surveillance and censorship ..... 29

        C. CISA’s MDM advisors fretted that it was “only a matter of time before someone realizes we exist and starts asking about our work.” ..... 30

        D. CISA purged its website of references to domestic MDM and its First Amendment violations in response to public pressure ..... 32

        E. The Biden Justice Department interfered with records requests in order to shield CISA from public scrutiny of its unconstitutional practices ..... 34

**Conclusion** ..... 36

---

## BACKGROUND

---

The Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government have been conducting oversight of the federal government’s work with non-government entities to censor speech online. The Select Subcommittee has also convened two hearings on the subject of social media censorship<sup>14</sup> and published an interim staff report exposing the Federal Trade Commission’s (FTC) politically motivated harassment campaign against Elon Musk’s Twitter.<sup>15</sup>

The First Amendment to the United States Constitution rests on the principle that no person or institution, including the government, has a monopoly on the truth, and that viewpoint-based suppression of speech by the government is dangerous and may even spell the death of a constitutional republic.<sup>16</sup> Under the First Amendment, the “government has no power to restrict expression because of its message, its ideas, its subject matter, or its content.”<sup>17</sup> As the Supreme Court has explained: “If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion.”<sup>18</sup>

Labeling speech “misinformation” does not strip it of First Amendment protection. That is so even if the speech is untrue, as “[s]ome false statements are inevitable if there is to be an open and vigorous expression of views in public and private conversation.”<sup>19</sup> In refusing to carve out a First Amendment exception for “false” speech, the Framers of our Constitution recognized the significant danger in making the government the ultimate arbiter of truth.<sup>20</sup> The First Amendment also protects the right to receive information, “an inherent corollary of the rights to free speech and press that are explicitly guaranteed by the Constitution” because “the right to receive ideas follows ineluctably from the *sender’s* First Amendment right to send them.”<sup>21</sup>

It is “axiomatic,” in the words of the Supreme Court, that the government may not “induce, encourage, or promote private persons to accomplish what it is constitutionally forbidden to accomplish.”<sup>22</sup> Moreover, the First Amendment prohibits the government from

---

<sup>14</sup> *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Federal Government of the H. Comm. on the Judiciary*, 118th Cong. (Mar. 9, 2023); *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Federal Government of the H. Comm. on the Judiciary*, 118th Cong. (Mar. 30, 2023).

<sup>15</sup> STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., *THE WEAPONIZATION OF THE FEDERAL TRADE COMMISSION: AN AGENCY’S OVERREACH TO HARASS ELON MUSK’S TWITTER* (Comm. Print 2023).

<sup>16</sup> *See* *Wood v. Georgia*, 370 U.S. 375, 388 (1962) (“Those who won our independence had confidence in the power of free and fearless reasoning and communication of ideas to discover and spread political truth.”).

<sup>17</sup> *Ashcroft v. ACLU*, 535 U.S. 564, 573 (2002).

<sup>18</sup> *W.Va. State Bd. of Educ. v. Barnette*, 319 U.S. 624, 642 (1943).

<sup>19</sup> *United States v. Alvarez*, 567 U.S. 709, 718 (2012) (plurality opinion).

<sup>20</sup> *See id.* at 752 (Alito, J., dissenting) (“Even where there is a wide scholarly consensus concerning a particular matter, the truth is served by allowing that consensus to be challenged without fear of reprisal. Today’s accepted wisdom sometimes turns out to be mistaken.”).

<sup>21</sup> *Bd. of Educ., Island Trees Union Free Sch. Dist. No. 26 v. Pico*, 457 U.S. 853, 867 (1982).

<sup>22</sup> *Norwood v. Harrison*, 413 U.S. 455, 465 (1973).

“abridging the freedom of speech”<sup>23</sup>—not “negating” or “abrogating,” but merely “abridging.” Thus, any law or administrative policy that impedes the ability of users to speak freely on privately owned social media platforms violates the First Amendment.<sup>24</sup>

This interim report focuses primarily on the censorship efforts of the Cybersecurity and Infrastructure Security Agency (CISA), a component of the Department of Homeland Security (DHS), and its role in what one journalist and commentator has called the “censorship industrial complex.”<sup>25</sup>

## The Cybersecurity and Infrastructure Security Agency

Congress established CISA in 2018, redesignating the National Protection and Programs Directorate (NPPD) within DHS as CISA.<sup>26</sup> CISA’s statutory mission included “lead[ing] cybersecurity and critical infrastructure security programs, operations, and associated policy,” and “carry[ing] out the requirements of the Chemical Facility Anti-Terrorism Standards Program.”<sup>27</sup> In April 2019, Daniel Sutherland, CISA’s Chief Counsel, claimed: “We are a non-regulatory, non-law enforcement, non-intelligence community” agency.<sup>28</sup>



As defined in 2003 by Homeland Security Presidential Directive 7, the term “critical infrastructure” was formerly used to describe “information technology; telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping.”<sup>29</sup> It was not until 2017, shortly after the 2016 election, that President Obama’s DHS Secretary Jeh Johnson designated “election infrastructure” as a “critical infrastructure subsector.”<sup>30</sup>

Ostensibly created to protect the electrical grid and other “critical infrastructure” sectors from cybersecurity threats,<sup>31</sup> CISA, a little-known agency buried in the depths of DHS, soon expanded its mission to combat “foreign disinformation.”<sup>32</sup> Not long thereafter, under the pretext of protecting “election infrastructure,” CISA began surveilling and censoring American citizens online, directly and by proxy.

---

<sup>23</sup> U.S. CONST. amend. I (emphasis added).

<sup>24</sup> See Philip Hamburger, *How the Government Justifies Its Social-Media Censorship*, WALL STREET JOURNAL (Jun. 9, 2023).

<sup>25</sup> *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Federal Government of the H. Comm. on the Judiciary*, 118th Cong. at 6 (Mar. 9, 2023) (statement of Michael Shellenberger).

<sup>26</sup> 6 U.S. Code § 652.

<sup>27</sup> *Id.*

<sup>28</sup> *CISA and Cyber Threats: How Government and Private Sector Secure Our Networks and Infrastructure*, THE FEDERALIST SOCIETY (Jun. 11, 2019).

<sup>29</sup> Homeland Sec. Presidential Directive 7, 2. Pub. Papers 1739 (Dec. 17, 2003).

<sup>30</sup> Press Release, Dep’t of Homeland Sec., Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017).

<sup>31</sup> 6 U.S. Code § 652.

<sup>32</sup> See, e.g., CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, #PROTECT2020 STRATEGIC PLAN, at 20 (2020), [https://www.cisa.gov/sites/default/files/publications/ESI\\_Strategic\\_Plan\\_FINAL\\_2-7-20\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/ESI_Strategic_Plan_FINAL_2-7-20_508.pdf).

## CISA's Cybersecurity Advisory Committee (CSAC)

DHS created the CISA Cybersecurity Advisory Committee (CSAC) in June 2021 “to advance CISA’s cybersecurity mission and strengthen the cybersecurity of the United States.”<sup>33</sup> CSAC in turn established a “Protecting Critical Infrastructure from Misinformation & Disinformation” Subcommittee,<sup>34</sup> commonly known as the “MDM Subcommittee.”<sup>35</sup>



The MDM Subcommittee, which has since disbanded,<sup>36</sup> brought together government, Big Tech, and academic misinformation “experts,” including:

- **Dr. Kate Starbird**, Associate Professor and Co-Founder of the University of Washington’s Center for an Informed Public (CIP).<sup>37</sup> CIP was a member of both the Election Integrity Partnership (EIP)<sup>38</sup> and the Virality Project (VP).<sup>39</sup> Starbird served as the Chair of the MDM Subcommittee.<sup>40</sup>
- **Vijaya Gadde**, the former Chief Legal Officer of Twitter, who was “involved in censoring [the *New York Post*’s Hunter Biden laptop” story.<sup>41</sup> Gadde was also “behind the decision to permanently ban former President Trump from Twitter.”<sup>42</sup> Shortly after Elon Musk completed his purchase of Twitter, Gadde was fired from the company in October 2022.<sup>43</sup>
- **Suzanne Spaulding**, a former assistant general counsel and legal adviser for the Central Intelligence Agency (CIA), who also served as the Under Secretary for the NPPD,

---

<sup>33</sup> *CISA Cybersecurity Advisory Committee*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, <https://www.cisa.gov/resources-tools/groups/cisa-cybersecurity-advisory-committee> (last visited Jun. 23, 2023).

<sup>34</sup> CISA CYBERSECURITY ADVISORY COMM., 2022 ANNUAL REPORT, at 2 (2022), [https://www.cisa.gov/sites/default/files/2023-01/csac\\_annual\\_report\\_2023-01-18\\_508\\_0.pdf](https://www.cisa.gov/sites/default/files/2023-01/csac_annual_report_2023-01-18_508_0.pdf).

<sup>35</sup> *See, e.g.*, CISA CYBERSECURITY ADVISORY COMM., DECEMBER 6, 2022 MEETING SUMMARY CLOSED SESSION, at 3 (On file with the Comm.).

<sup>36</sup> CISA CYBERSECURITY ADVISORY COMM., DECEMBER 6, 2022 MEETING SUMMARY OPEN SESSION, at 1, [https://www.cisa.gov/sites/default/files/publications/CSAC\\_December-Quarterly-Meeting-Summary\\_508\\_01062023\\_0.pdf](https://www.cisa.gov/sites/default/files/publications/CSAC_December-Quarterly-Meeting-Summary_508_01062023_0.pdf).

<sup>37</sup> *Kate Starbird*, UNIVERSITY OF WASHINGTON, <https://www.hcde.washington.edu/starbird> (last visited Jun. 12, 2023).

<sup>38</sup> ELECTION INTEGRITY P’SHIP, *THE LONG FUSE: MISINFORMATION AND THE 2020 ELECTION*, at vi (Eden Beck ed., 2021).

<sup>39</sup> VIRALITY PROJECT, *MEMES, MAGNETS, AND MICROCHIPS: NARRATIVE DYNAMICS AROUND COVID-19 VACCINES*, at 1 (Eden Beck ed., 2022).

<sup>40</sup> CISA CYBERSECURITY ADVISORY COMM., SUBCOMMITTEE FACTSHEET (2022), [https://www.cisa.gov/sites/default/files/publications/CSAC\\_Subcommittee\\_Fact\\_Sheet\\_05192022\\_508c.pdf](https://www.cisa.gov/sites/default/files/publications/CSAC_Subcommittee_Fact_Sheet_05192022_508c.pdf).

<sup>41</sup> Victor Nava, *Who is Vijaya Gadde, the Twitter exec involved in censoring Post’s Hunter Biden laptop bombshell?*, NEW YORK POST (Dec. 3, 2022).

<sup>42</sup> *The Twitter executives fired after Elon Musk’s takeover*, AXIOS (Oct. 28, 2022).

<sup>43</sup> *Id.*

CISA’s predecessor within DHS.<sup>44</sup> Spaulding is now the “director of the Defending Democratic Institutions project at the Center for Strategic International Studies (CSIS).”<sup>45</sup>

MDM Subcommittee meetings also featured government participants, including Geoff Hale, who leads CISA’s “Election Security Initiative,”<sup>46</sup> and Kim Wyman, the former Washington Secretary of State, who now serves as CISA’s Senior Election Security Advisor.<sup>47</sup>

During its existence, the MDM Subcommittee issued two sets of formal recommendations: one set in June 2022,<sup>48</sup> and another in September 2022.<sup>49</sup> The Subcommittee’s June 2022 recommendations included, among other things, recommendations that “CISA should approach the [misinformation and disinformation] problem with the entire information ecosystem in view. This includes social media platforms of all sizes, mainstream media, cable news, hyper partisan media, talk radio, and other online resources.”<sup>50</sup>

### The Center for Internet Security (CIS)

The Center for Internet Security (CIS) is a nonprofit organization that operates the Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).<sup>51</sup> According to a postmortem report covering social media activity related to the 2020 election cycle, “the EI-ISAC served as a singular conduit for election officials to report false or misleading information to platforms.”<sup>52</sup> Put plainly, election officials around the country sent CIS purportedly false or misleading content, which CIS forwarded to the relevant social media platforms.<sup>53</sup>



---

<sup>44</sup> *Suzanne Spaulding*, CENTER FOR STRATEGIC & INT’L STUDIES, <https://www.csis.org/people/suzanne-spaulding> (last visited Jun. 23, 2023).

<sup>45</sup> *Id.*

<sup>46</sup> *Geoff Hale*, RSA CONF., <https://www.rsaconference.com/experts/geoff-hale> (last visited Jun. 23, 2023).

<sup>47</sup> *Kim Wyman*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, <https://www.cisa.gov/about/leadership/kim-wyman> (last visited Jun. 23, 2023).

<sup>48</sup> CISA CYBERSECURITY ADVISORY COMM., JUNE 22, 2022 MEETING SUMMARY OPEN SESSION, [https://www.cisa.gov/sites/default/files/publications/CSAC\\_June\\_Quarterly\\_Meeting\\_Summary.pdf](https://www.cisa.gov/sites/default/files/publications/CSAC_June_Quarterly_Meeting_Summary.pdf).

<sup>49</sup> CISA CYBERSECURITY ADVISORY COMM., DECEMBER 6, 2022 MEETING SUMMARY OPEN SESSION, [https://www.cisa.gov/sites/default/files/publications/CSAC\\_December-Quarterly-Meeting-Summary\\_508\\_01062023\\_0.pdf](https://www.cisa.gov/sites/default/files/publications/CSAC_December-Quarterly-Meeting-Summary_508_01062023_0.pdf).

<sup>50</sup> CISA CYBERSECURITY ADVISORY COMM., REPORT TO THE CISA DIRECTOR PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION AND DISINFORMATION JUNE 22, 2022, at 2, [https://www.cisa.gov/sites/default/files/publications/June%202022%20CSAC%20Recommendations%20%E2%80%93%20MDM\\_0.pdf](https://www.cisa.gov/sites/default/files/publications/June%202022%20CSAC%20Recommendations%20%E2%80%93%20MDM_0.pdf).

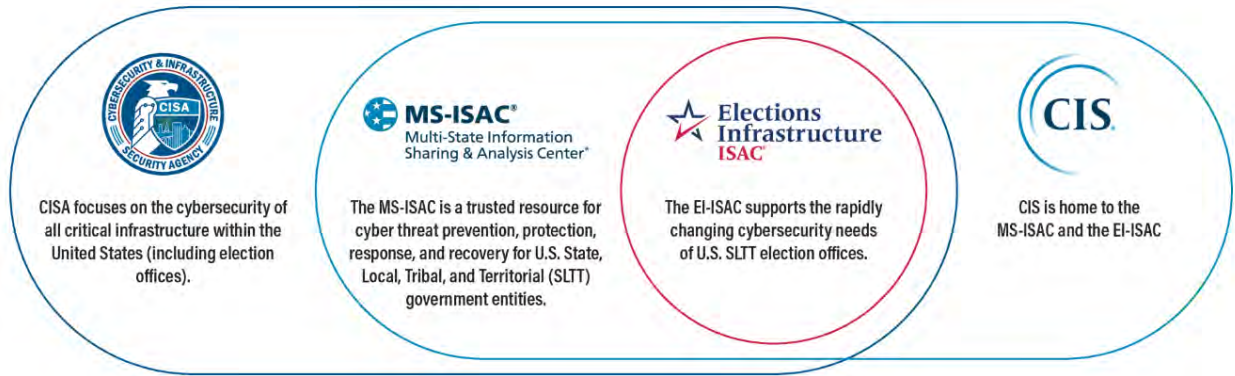
<sup>51</sup> *EI-ISAC*, CENTER FOR INTERNET SEC., <https://www.cisecurity.org/ei-isac> (last visited Jun. 23, 2023).

<sup>52</sup> ELECTION INTEGRITY P’SHIP, *supra* note 38, at 13.

<sup>53</sup> *See id.*



CISA funds CIS, including spending \$27 million in FY 2024 on operating the EI-ISAC and the MS-ISAC.<sup>54</sup> As illustrated by the diagram below from CIS’s website, the “EI-ISAC is federally funded by CISA and a division of the Center for Internet Security.”<sup>55</sup>



<sup>54</sup> DEP’T OF HOMELAND SEC., DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY BUDGET OVERVIEW FISCAL YEAR 2024 CONGRESSIONAL JUSTIFICATION, at 37 (2023).

<sup>55</sup> *EI-ISAC*, *supra* note 51.

---

## CISA'S MISSION CREEP INTO SURVEILLANCE, CENSORSHIP, AND COVER-UPS

---

The Committee and Select Subcommittee have obtained previously undisclosed, non-public documents that reveal CISA expanded its mission to surveil Americans' speech on social media, colluded with Big Tech and government-funded third parties to censor by proxy, and tried to hide its plainly unconstitutional activities from the public.

**Surveillance.** CISA expanded its mission from “cybersecurity” to monitor foreign “disinformation” to eventually monitor all “disinformation,” including Americans' speech. In one e-mail exchange obtained by the Committee and Select Subcommittee, the agency's rapid mission creep surprised even a non-profit focused on foreign “disinformation.”

**Censorship.** CISA exploited its connections with Big Tech and government-funded non-profits to censor by proxy, in order to circumvent the First Amendment's prohibition against government-induced censorship. This included the creation of reporting “portals” which funneled “misinformation” reports from the government directly to social media platforms. Newly uncovered meeting minutes show that CISA was advised by a group Big Tech executives and academics who encouraged CISA's unconstitutional behavior.

**Cover-ups.** As CISA's operational scope expanded further into unconstitutional territory, the agency and its advisors tried to cover their tracks and cover up CISA's censorship of domestic speech and surveillance of American citizens' social media activity. This included scrubbing CISA's website of references to domestic “misinformation” and “disinformation.”

### I. CISA has transformed into a domestic intelligence and speech-police agency, far exceeding its statutory authority

CISA's focus on “cybersecurity” quickly expanded into social media surveillance of real and perceived foreign actors. Shortly after CISA became its own agency, then-DHS Secretary Kristjen Nielsen created the “Countering Foreign Influence Task Force” (CFITF) within CISA “to focus on election infrastructure disinformation.”<sup>56</sup> Following the unfounded claims by Democrats that foreign—particularly Russian—influence changed the outcome of the 2016 election,<sup>57</sup> CISA expanded its “cybersecurity” role to include countering foreign malign influence operations. In its public materials, CISA emphasized at the time that it was primarily concerned with addressing foreign, rather than domestic, disinformation.<sup>58</sup> Starting in January 2019, Brian Scully served first as the head of the CFITF and later as the head of the MDM team at CISA.<sup>59</sup>

---

<sup>56</sup> *DHS Needs a Unified Strategy to Counter Disinformation Campaigns*, *supra* note 6 at 5.

<sup>57</sup> See 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*, 14:62 *NATURE COMMUNICATIONS* 1, at 8-9 (2023).

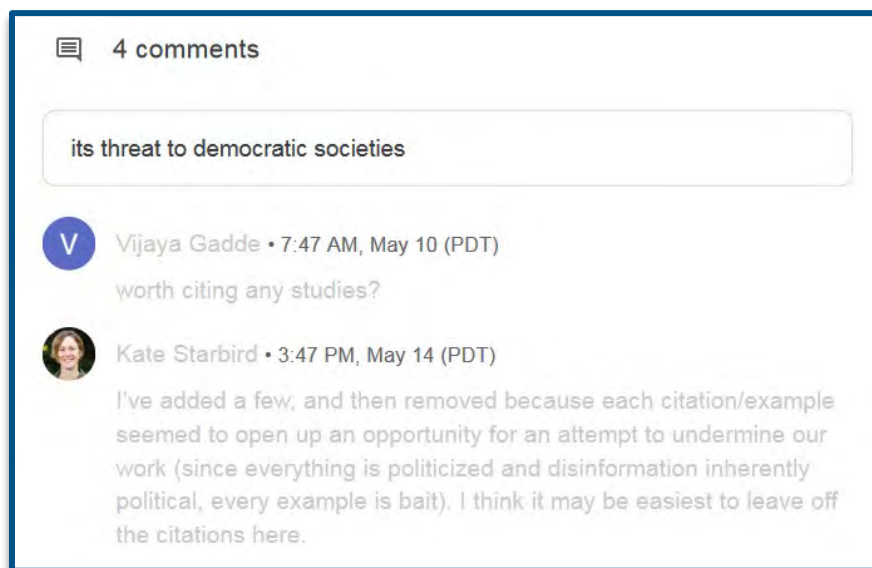
<sup>58</sup> See, e.g., *Resilience Series Graphic Novels*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, <https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation/resilience-series-graphic-novels> (last visited Jun. 23, 2023).

<sup>59</sup> See Scully Dep. 11:24–12:2, *supra* note 5.

In January 2021, after President Biden took office, “CISA transitioned its [CFITF] to promote more flexibility to focus on general MDM,” or so-called “Mis-, Dis-, and Malinformation.”<sup>60</sup> In so doing, CISA admitted that its focus was no longer exclusively on “countering foreign influence,” but was also targeting MDM originating from domestic sources. For example, according to a 2022 CISA pamphlet titled “Planning and Incident Response Guide for Election Officials,” “MDM also may originate from domestic sources aiming to sow divisions and reduce national cohesion.”<sup>61</sup>

Although CISA’s efforts to police speech are highly troubling overall, one particularly problematic aspect is CISA’s focus on “malinformation.” According to CISA’s own definition, “[m]alinformation is based on fact, but used out of context to mislead, harm, or manipulate.”<sup>62</sup> In other words, malinformation is *factual* information that is objectionable not because it is false or untruthful, but because it is provided without adequate “context”—context as determined by the government.

In addition, what constitutes “misinformation” or “disinformation” is determined by government actors, whose evaluations of truth and falsity are necessarily subjective, and “inherently political,” as explained in the comments of a Google Doc by Starbird below.<sup>63</sup>



CISA’s involvement in policing alleged mis- and disinformation, as well as malinformation—truthful information without “sufficient” context—is a direct and serious threat to First Amendment principles.

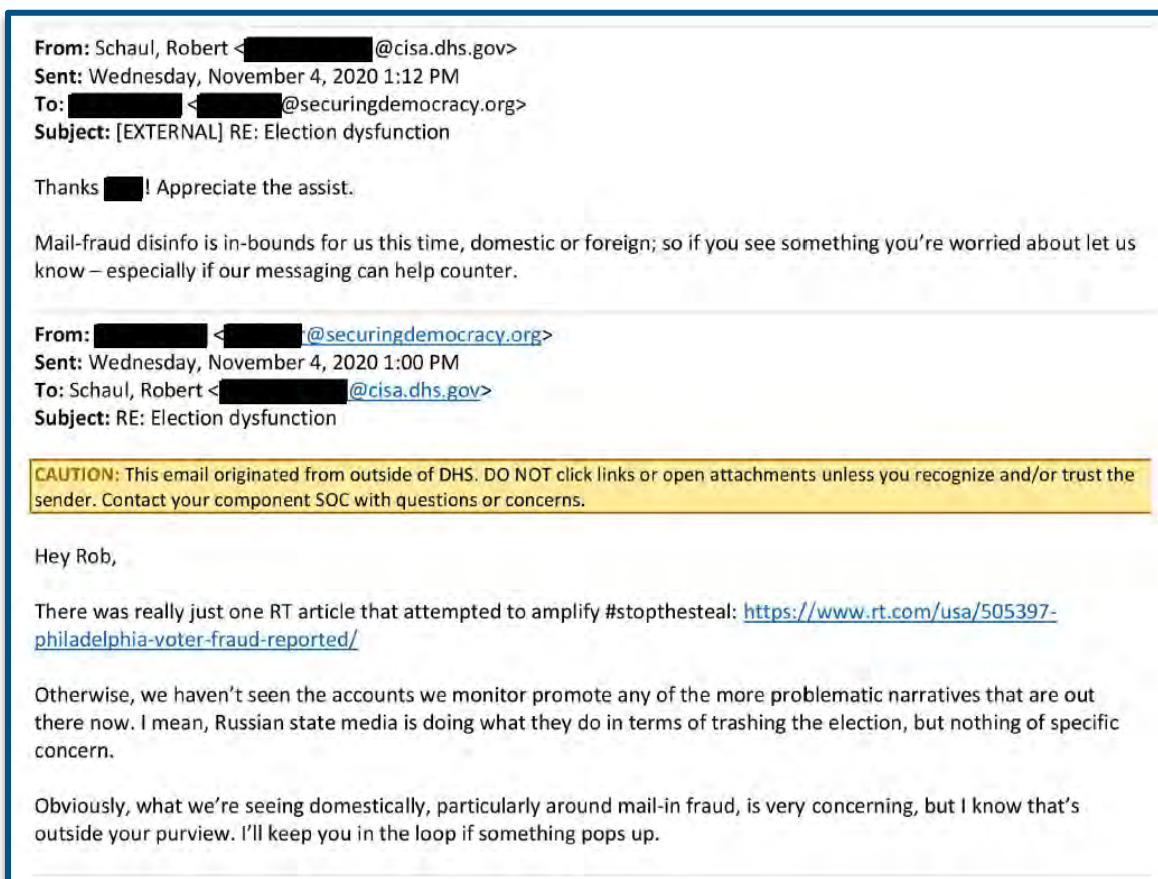
<sup>60</sup> *DHS Needs a Unified Strategy to Counter Disinformation Campaigns*, *supra* note 6 at 7.

<sup>61</sup> CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, MIS-, DIS-, AND MALINFORMATION PLANNING AND INCIDENT RESPONSE GUIDE FOR ELECTION OFFICIALS, at 1 (2022), [https://www.cisa.gov/sites/default/files/2022-11/mdm-incident-response-guide\\_508.pdf](https://www.cisa.gov/sites/default/files/2022-11/mdm-incident-response-guide_508.pdf).

<sup>62</sup> *Id.*

<sup>63</sup> E-mail from Suzanne Spaulding (Google Docs) to Kate Starbird (May 16, 2022, 6:27 PM) (on file with the Comm.).

Although the CFITF did not formally shed “foreign” from its name until January 2021, CISA’s efforts to curb domestic MDM had been ongoing for months, ramping up in advance of the 2020 election. An e-mail exchange on November 4, 2020 demonstrates that even non-profits focused on “disinformation,” such as the German Marshall Fund’s Alliance for Securing Democracy (ASD), were caught off guard by CISA’s expansion into the surveillance of domestic speech. In the exchange, an ASD employee emailed Robert Schaul, the Analysis and Resilience Policy Lead at CISA,<sup>64</sup> writing: “Obviously, what we’re seeing domestically, particularly around mail-in fraud, is very concerning, but I know that’s outside your purview.”<sup>65</sup> Schaul corrected the ASD employee: “Mail-fraud disinfo[rmination] is in-bounds for us this time, domestic or foreign; so if you see something you’re worried about let us know.”<sup>66</sup>



Despite constituting a clear departure from its statutory mandate, CISA’s MDM team has, at its peak, been comprised of “a total of 15 dedicated part- and full-time staff,” who focus on “disinformation activities targeting elections and critical infrastructure.”<sup>67</sup> Jen Easterly, the

<sup>64</sup> *U.S.-Paris Tech Challenge*, ATLANTIC COUNCIL, <https://www.atlanticcouncil.org/event/u-s-paris-tech-challenge/> (last visited Jun. 23, 2023).

<sup>65</sup> E-mail from German Marshall Fund employee to Robert Schaul (Nov. 4, 2020, 1:00 PM) (on file with the Comm.).

<sup>66</sup> E-mail from Robert Schaul to German Marshall Fund employee (Nov. 4, 2020, 1:12 PM) (on file with the Comm.).

<sup>67</sup> *DHS Needs a Unified Strategy to Counter Disinformation Campaigns*, *supra* note 6 at 7.

current Director of CISA, justified CISA’s MDM-related activities by saying: “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.”<sup>68</sup>

### **A. Switchboarding: CISA’s coordination with Big Tech to censor Americans**

CISA’s Director, Jen Easterly, claimed in her March 28, 2023 testimony before Congress that “we don’t flag anything to social media organizations at all. We are focused on building resilience to foreign influence and disinformation.”<sup>69</sup> Despite Easterly’s assurances, however, the DHS Office of Inspector General (OIG) has reported that CISA began “notifying social media platforms or appropriate law enforcement official when voting-related disinformation appeared in social media” as early as 2018.<sup>70</sup>

When deposed as part of ongoing litigation in federal court, Brian Scully, the head of CISA’s MDM team, confirmed that CISA has historically flagged disinformation to social media platforms, in a process known as “switchboarding.”<sup>71</sup> Scully further described switchboarding as a “resource intensive”<sup>72</sup> process whereby CISA officials received alleged “misinformation” reports from election officials and forwarded those reports to social media companies so that they could take enforcement measures against the reported content.<sup>73</sup>

CISA has sought to disclaim any responsibility in affecting social media companies’ decisions on content moderation. In reporting content to social media platforms, CISA officials, including Scully, often appended a disclaimer to their e-mails, claiming, “CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms.”<sup>74</sup> However, when deposed as part of ongoing federal litigation, Scully admitted that CISA was aware that its outreach to social media companies about alleged disinformation would trigger content moderation.<sup>75</sup>

### **B. CISA’s MDM consultants rejected constitutional “limitations” on the surveillance and censorship of domestic speech**

Originally created to protect critical infrastructure such as dams and pipelines from foreign malign actors, CISA has ventured well beyond its founding mandate and began targeting constitutionally protected domestic speech for censorship on social media platforms. By 2020,

---

<sup>68</sup> Miller, *supra* note 1.

<sup>69</sup> H. COMM. ON APPROPRIATIONS, *Budget Hearing – Fiscal Year 2024 Request for the Cybersecurity and Infrastructure Security Agency*, YOUTUBE (Mar. 28, 2023).

<sup>70</sup> *DHS Needs a Unified Strategy to Counter Disinformation Campaigns*, *supra* note 6 at 5.

<sup>71</sup> Scully Dep. 23:16–24:2, *supra* note 5.

<sup>72</sup> Scully Dep. 62:15–22, *supra* note 5.


<sup>73</sup> Scully Dep. 17:1–18:1, *supra* note 5.

<sup>74</sup> *See, e.g.*, e-mail from Brian Scully to Facebook employees (Oct. 28, 2020, 2:09 PM) (on file with the Comm.); e-mail from Brian Scully to Google employee (Oct. 1, 2020 9:01 PM) (on file with the Comm.).

<sup>75</sup> Scully Dep. 17:15–18:1, *supra* note 5. *See also* *Hearing on the Weaponization of the Federal Government: Hearing Before the Select Subcomm. on the Weaponization of the Federal Government of the H. Comm. on the Judiciary*, 118th Cong. (Mar. 30, 2023).

just two years after its creation, CISA had unilaterally expanded its authorities from countering foreign influence operations to curtailing domestic speech. In 2021, CISA created an advisory committee, including the MDM Subcommittee, in order to receive input from Big Tech and “disinformation” experts. According to documents produced to the Committee and Select Subcommittee,<sup>76</sup> members of the MDM Subcommittee, while serving in this advisory role, pushed aside legitimate criticism and urged CISA to continue on its unconstitutional trajectory.

On August 30, 2022, MDM Subcommittee members discussed the propriety of DHS “identifying domestic actors” spreading alleged disinformation.<sup>77</sup> According to notes of the meeting that day, Suzanne Spaulding, a former CIA legal advisor, “urged Dr. Starbird not to solely focus on addressing foreign threats.”<sup>78</sup> Spaulding also “encouraged Dr. Starbird to emphasize that domestic threats remain and while attribution is sometimes unclear, CISA should be sensitive to domestic distinctions, but cannot focus too heavily on such limitations.”<sup>79</sup> In the same meeting, the director of CISA’s Election Security Initiative “[Geoff] Hale reflected that these discussions of scoping authority relate to the Subcommittee’s initial deliberations urging CISA to be actor-agnostic in their work combating mis- and dis-information.”<sup>80</sup> In other words, Hale, a federal government employee, observed that the Subcommittee’s work addressing alleged mis- and dis-information should not distinguish between foreign and domestic sources.



**August 30, 2022**

- Ms. Spaulding urged Dr. Starbird not to solely focus on addressing foreign threats during the CSAC September Quarterly Meeting. Ms. Spaulding observed a shift in narrative to combatting foreign threats. She encouraged Dr. Starbird to emphasize that domestic threats remain and while attribution is sometimes unclear, CISA should be sensitive to domestic distinctions, but cannot focus too heavily on such limitations.

Other documents produced to the Committee and Select Subcommittee suggest that Hale and the MDM Subcommittee urged action in the domestic space, even in the face of opposition from state and local election administration officials. In particular, during the MDM Subcommittee’s August 8, 2022 meeting, Twitter’s Chief Legal Officer Vijaya Gadde “reflected on the group’s previous meeting with the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED) and noted in their feedback that CISA should not be involved in this mission space, except when a foreign adversary is at play.”<sup>81</sup> Gadde doubted that this distinction could serve as a meaningful limit for CISA because “it is difficult to determine whether a foreign adversary is involved.”<sup>82</sup> Later in the same

<sup>76</sup> These documents include meeting minutes from the MDM Subcommittee. As Chair of the MDM Subcommittee, Dr. Kate Starbird reviewed and approved these meeting minutes before they were circulated. Transcribed Interview of Kate Starbird at 39 (on file with the Comm.).

<sup>77</sup> CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING AUGUST 30, 2022, at 1 (on file with the Comm.).

<sup>78</sup> *Id.* at 2.


<sup>79</sup> *Id.*

<sup>80</sup> *Id.* at 1.

<sup>81</sup> CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING AUGUST 8, 2022, at 1 (on file with the Comm.).


<sup>82</sup> *Id.*

meeting, Starbird “noted that because mis- and disinformation is universal, CISA must play a role on the national level.”<sup>83</sup>

 <b>CISA CYBERSECURITY ADVISORY COMMITTEE</b>	<b>August 8, 2022</b>
<ul style="list-style-type: none"><li>• Subcommittee members discussed CISA’s role in the elections space. Dr. Starbird addressed the doubt and manufactured doubt into whether CISA should play a role. She stressed one of the goals of the recommendations is to share why CISA should act in the elections space to combat mis- and dis-information.<ul style="list-style-type: none"><li>○ Ms. Gadde reflected on the group’s previous meeting with the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED) and noted in their feedback that CISA should not be involved in this mission space, except when a foreign adversary is at play. She cautioned that it is difficult to determine whether a foreign adversary is involved.</li></ul></li></ul>	

### **C. CISA considered creating an anti-MDM “rapid response team” to physically deploy across the United States**

In one particularly notable departure from its legal authority, during the MDM Subcommittee’s June 14, 2022 meeting, participants “explore[d] the idea of how CISA could develop a rapid response team to deploy . . . in-person to local election officials’ jurisdictions struggling with specific informational threats.”<sup>84</sup> The CISA officials present at the meeting seemed receptive to the idea, with Geoff Hale, the director of CISA’s Election Security Initiative, commenting that “this is a fascinating idea that takes CISA’s existing operational responsibilities to consider MDM as part of its core mission set.”<sup>85</sup>

 <b>CISA CYBERSECURITY ADVISORY COMMITTEE</b>	<b>June 14, 2022</b>
<ul style="list-style-type: none"><li>• Dr. Starbird added that Mr. Richer’s colleague, Mr. Scott Jarred, suggested that the subcommittee explore the idea of how CISA could develop a rapid response team to deploy virtually or in-person to local election officials’ jurisdictions struggling with specific informational threats. The support would include checking equipment to verify if a breach is present or not, determining how to communicate the existence of a breach, and determining how to target certain kinds of communication.<ul style="list-style-type: none"><li>○ Ms. Tate-Nadeau clarified if this rapid response team would only act in the context of MDM threats. Dr. Starbird noted that the response team would require a broader range of expertise, as they first must be able to verify whether a real threat exists, then be able to communicate the existence of an MDM threat.</li><li>○ Mr. Geoff Hale, CISA, commented that this is a fascinating idea that takes CISA’s existing operational responsibilities to consider MDM as part of its core mission set. He noted that this would be an evolution of CISA’s current defensive posture. Ms. Gadde agreed with this framing of the question.</li><li>○ Dr. Starbird commented that the rapid response team would need to surge for short periods of time around elections. She suggested the subcommittee consider the requirements for the team’s expandability, ability to conduct media analysis, and the level of understanding on MDM in a communications context.</li></ul></li></ul>	

<sup>83</sup> *Id.* at 2.

<sup>84</sup> CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING JUNE 14, 2022, at 2 (on file with the Comm.).

<sup>85</sup> *Id.*

Starbird, the chair of the MDM Subcommittee, also “commented that the rapid response team would need to surge for short periods of time around elections.”<sup>86</sup> Hale then “noted the possibility to stand up this team in the short term by encouraging the communications team to consider MDM equities.”<sup>87</sup>

Subcommittee members then abandoned any pretext of operating within CISA’s legal authority, with Twitter’s Vijaya Gadde noting “that the idea of a rapid response team must include the ability to engage whether or not a cyber component is present.”<sup>88</sup> “Dr. Starbird agreed with Ms. Gadde’s point that threats to critical infrastructure are not limited to cyber threats.”<sup>89</sup>

- Ms. Gadde noted that physical and MDM-related threats are often interrelated, so the group cannot address the physical threats against elections officials without addressing the root cause of MDM-related threats. She continued by stressing that MDM threat exist with or without a cyber component. She noted that the idea of a rapid response team must include the ability to engage whether or not a cyber component is present.
- Dr. Starbird agreed with Ms. Gadde’s point that threats to critical infrastructure are not limited to cyber threats.

#### D. MDM “experts” wanted CISA to crack down on *factual* information

Even so-called “malinformation”—truthful information that, according to the government, may carry the potential to mislead—could not escape the scrutiny of CISA’s MDM “experts.”<sup>90</sup> In an e-mail exchange between MDM Subcommittee members Starbird and Spaulding, Spaulding wrote: “As I’ve read more about malinformation, I think you’re right that it could fit the kinds of risks we are concerned about. The challenge may be that because it is not false, per se . . . it is much trickier from a policy perspective.”<sup>91</sup> Spaulding proposed a “compromise”: “that [malinformation] is part of CISA’s current scope but that our recommendations, at least at this stage, are focused primarily on countering false information.”<sup>92</sup>

On May 16, 2022, at 6:02 PM, Suzanne Spaulding <[REDACTED]> wrote:

Kate,  
thanks for continuing to think about this issue. As I've read more about malinformation, I think you're right that it could fit the kinds of risks we are concerned about. The challenge may be that because it is not false, per se (though presented in a misleading, manipulative way to cause harm), it is much trickier from a policy perspective. I think we could compromise by noting that it is part of CISA's current scope but that our recommendations, at least at this stage, are focused primarily on countering false information. Would that work? I'll try suggesting line-in line-out changes to the text.  
best,  
Suzanne

<sup>86</sup> *Id.*

<sup>87</sup> *Id.*

<sup>88</sup> *Id.*

<sup>89</sup> *Id.*

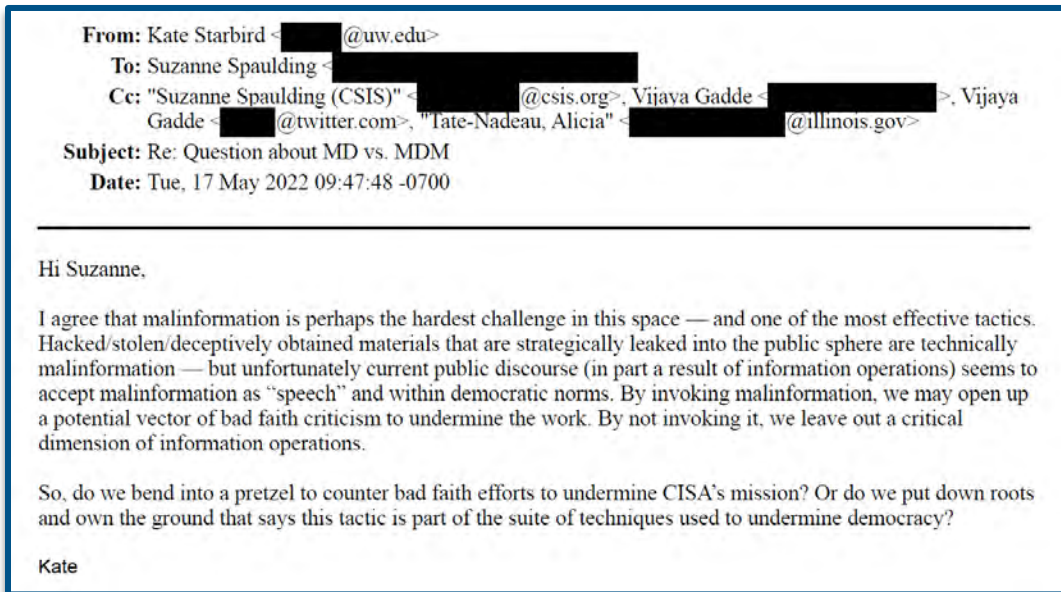
<sup>90</sup> The First Amendment protects domestic speech, regardless of whether government actors consider it mis-, dis-, or malinformation. *See United States v. Alvarez*, 567 U.S. 709, 718 (2012) (plurality opinion).

<sup>91</sup> E-mail from Suzanne Spaulding to Kate Starbird (May 16, 2022, 6:02 PM) (on file with the Comm.).

<sup>92</sup> *Id.*

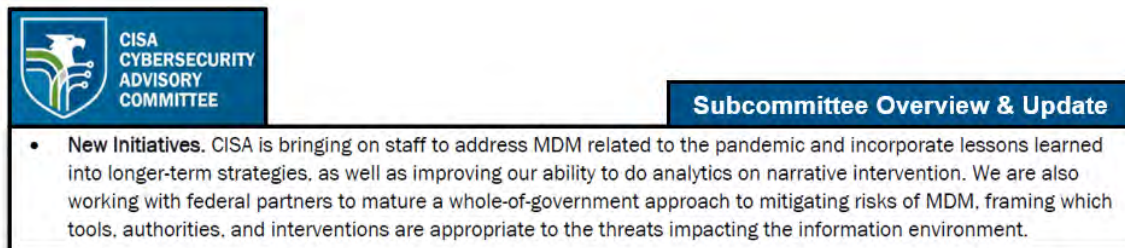


Starbird responded that “malinformation is perhaps the hardest challenge in this space.”<sup>93</sup> Starbird then lamented that “unfortunately current public discourse (in part a result of information operations) seems to accept malinformation as ‘speech’ and within democratic norms” and that CISA may face “bad faith criticism” for censoring content that is true.<sup>94</sup>



### E. CISA is only one part of a “whole-of-government” approach to MDM

Documents obtained by the Committee and Select Subcommittee establish that CISA and the MDM Subcommittee considered CISA to be only one part of a grander, “whole-of-government” approach to tackling disfavored speech. For example, according to the MDM Subcommittee’s “Subcommittee Overview & Update,” “CISA is bringing on staff to address MDM related to the pandemic . . . as well as improving our ability to do analytics on narrative intervention. We are also working with federal partners to mature a whole-of-government approach to mitigating risks of MDM, framing which . . . interventions are appropriate to the threats impacting the information environment.”<sup>95</sup>

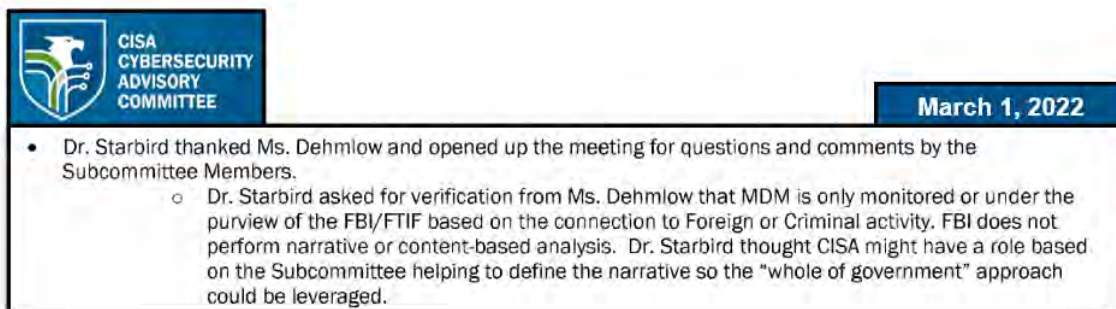


<sup>93</sup> E-mail from Kate Starbird to Suzanne Spaulding (May 17, 2022, 9:47 AM) (on file with the Comm.).

<sup>94</sup> *Id.*

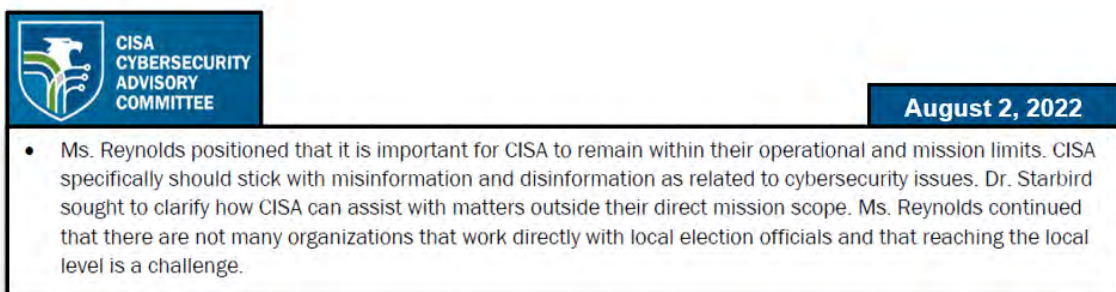
<sup>95</sup> CISA CYBERSECURITY ADVISORY COMM., SUBCOMMITTEE OVERVIEW & UPDATE: PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION, at 1 (2022) (on file with the Comm.).

As another example, during a March 1, 2022 meeting of the MDM Subcommittee, Laura Dehmlow of the FBI’s Foreign Influence Task Force (FITF), who had been invited to brief the MDM Subcommittee, claimed that the “FBI does not perform narrative or content-based analysis.”<sup>96</sup> According to the meeting notes, Starbird, the chair of the MDM Subcommittee, then offered CISA to fill this perceived gap in the government’s censorship efforts, suggesting that “CISA might have a role based on the Subcommittee helping to define the narrative so the ‘whole of government’ approach could be leveraged.”<sup>97</sup>



**F. State election officials warned CISA to “remain within [its] operational and mission limits,” lest it should earn the public’s “distrust.”**

MDM Subcommittee meeting notes and other documents obtained by the Committee and Select Subcommittee reveal that those engaging with CISA, and even election officials, were critical of CISA’s efforts to crack down on domestic speech related to elections. On August 2, 2022, Leslie Reynolds of the National Association of Secretaries of State (NASS) cautioned the MDM Subcommittee “that it is important for CISA to remain within their operational and mission limits. CISA specifically should stick with misinformation and disinformation as related to cybersecurity issues.”<sup>98</sup> Unfazed by the admonishment, Starbird promptly “sought to clarify how CISA can assist with matters outside their direct mission scope.”<sup>99</sup>



<sup>96</sup> CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING MARCH 1, 2022, at 1 (on file with the Comm.).

<sup>97</sup> *Id.*

<sup>98</sup> CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING AUGUST 2, 2022, at 2 (on file with the Comm.).

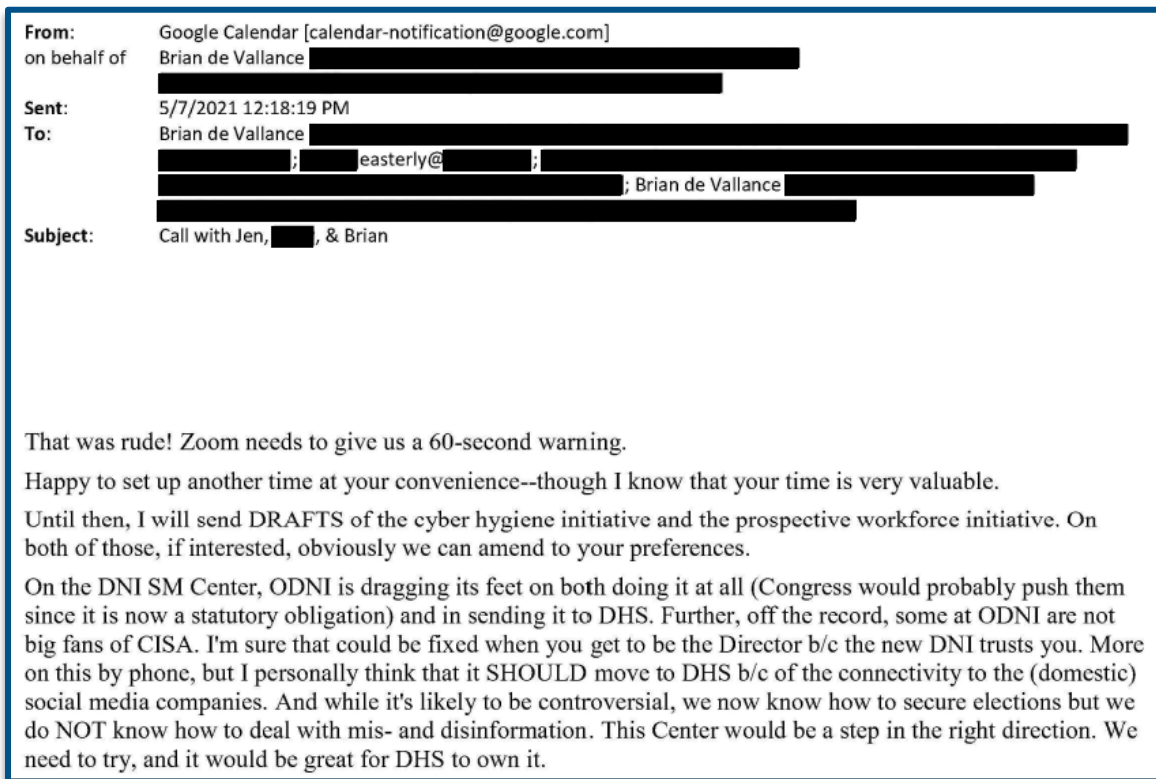
<sup>99</sup> *Id.*

Lindsey Forson, also affiliated with NASS, similarly “cautioned that the public could grow to distrust government agencies if they are not careful in the ways they interact with election related issues.”<sup>100</sup>

- Ms. Lindsey Forson, NASS, added that political sensibilities cannot be stressed enough. She cautioned that the public could grow to distrust government agencies if they are not careful in the ways they interact with election related issues. She expressed interest in hearing what subcommittee members think CISA’s support should look

### G. DHS was eager to cement CISA as a domestic intelligence agency

In May 2021, Brian de Vallance, a former DHS Assistant Secretary for Legislative Affairs,<sup>101</sup> sent an e-mail to Jen Easterly—who would later become CISA’s director—among others, about the National Defense Authorization Act (NDAA) provision establishing a Social Media Data and Threat Analysis Center to address disinformation within the Office of the Director of National Intelligence (ODNI). He relayed to Easterly, “off the record, some at ODNI are not big fans of CISA . . . More on this by phone, but I personally think that [the Social Media Data and Threat Analysis Center] SHOULD move to DHS [because] of the connectivity to the (domestic) social media companies.”<sup>102</sup>



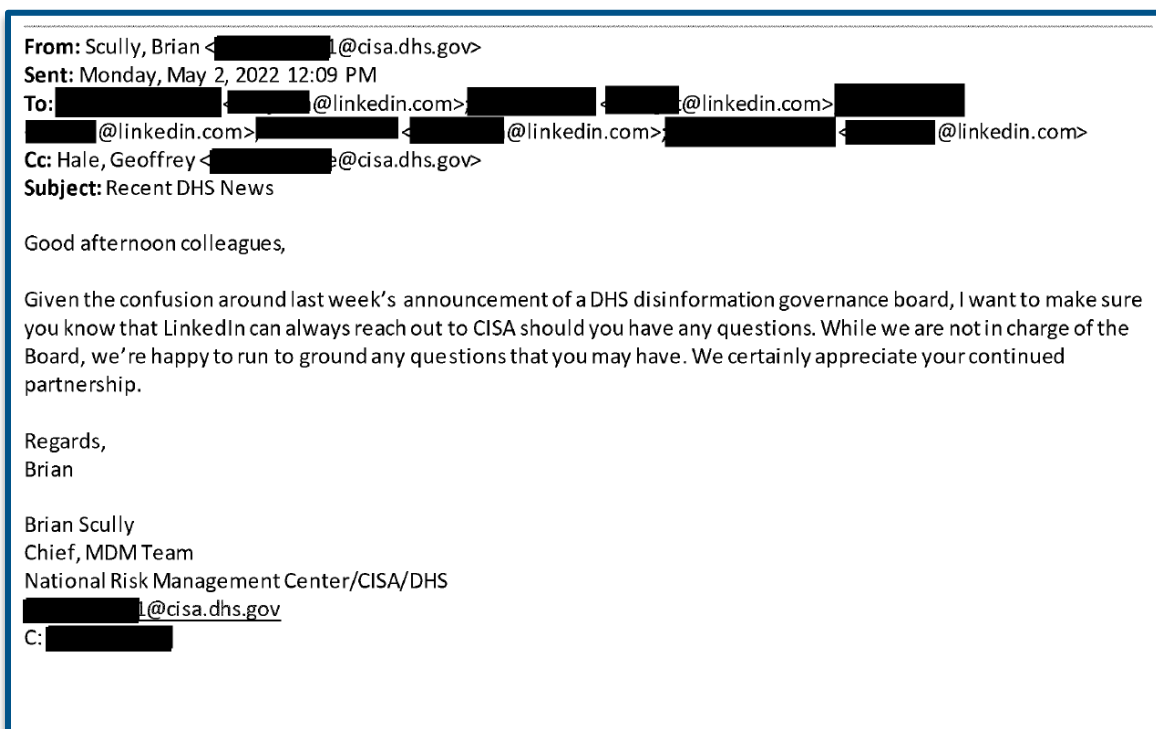
<sup>100</sup> *Id.* at 1.

<sup>101</sup> Brian de Vallance, DEP’T OF HOMELAND SEC., <https://www.dhs.gov/archive/person/brian-de-vallance> (last visited Jun. 23, 2023).

<sup>102</sup> E-mail from Google Calendar on behalf of Brian de Vallance to Jen Easterly (May 7, 2021, 12:18 PM) (on file with the Comm.).

## H. Social media companies mocked CISA’s MDM team and DHS’s Disinformation Governance Board

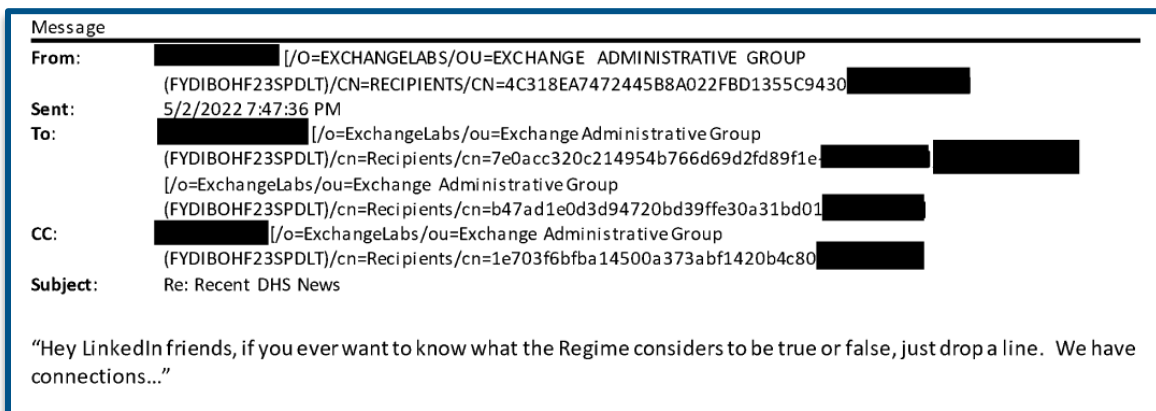
CISA’s “connectivity to the (domestic) social media companies” did not, however, prevent it from being criticized by these social media companies. In May 2022, following public backlash concerning DHS’s Orwellian Disinformation Governance Board,<sup>103</sup> Brian Scully, the head of CISA’s MDM team, e-mailed several LinkedIn employees, writing, “[g]iven the confusion around last week’s announcement of a DHS disinformation governance board, I want to make sure you know that LinkedIn can always reach out to CISA should you have any questions.”<sup>104</sup>



<sup>103</sup> The Disinformation Governance Board was an organ of DHS intended to “coordinate countering misinformation related to homeland security,” which was first announced on April 27, 2022. Eugene Daniels, Rachel Bade, and Ryan Lizza, *POLITICO Playbook: Fauci pulls out of WHCD. Is Biden next?*, POLITICO (Apr. 27, 2022). The Board’s inaugural (in fact, only) director was Nina Jankowicz. Prior to assuming the helm of the Board, Jankowicz falsely described the Hunter Biden laptop as a “Trump campaign product.” Roger Koppl and Abigail Devereaux, *Biden Establishes a Ministry of Truth*, WALL STREET JOURNAL (May 1, 2022). The Board was “met with an overwhelmingly negative response” and “[e]ven Democratic lawmakers were skeptical” of the initiative. Nicole Sganga, *What is DHS’ Disinformation Governance Board and why is everyone so mad about it?*, CBS NEWS (May 6, 2022). After significant public backlash, the Board was paused on May 18, 2022, with Jankowicz announcing her resignation. Rebecca Beitsch, *DHS to pause work of disinformation board*, THE HILL (May 18, 2022). The Board was formally terminated on August 24, 2022. Press Release, Dep’t of Homeland Sec., *Following HSAC Recommendation, DHS terminates Disinformation Governance Board* (Aug. 24, 2022), <https://www.dhs.gov/news/2022/08/24/following-hsac-recommendation-dhs-terminates-disinformation-governance-board>.

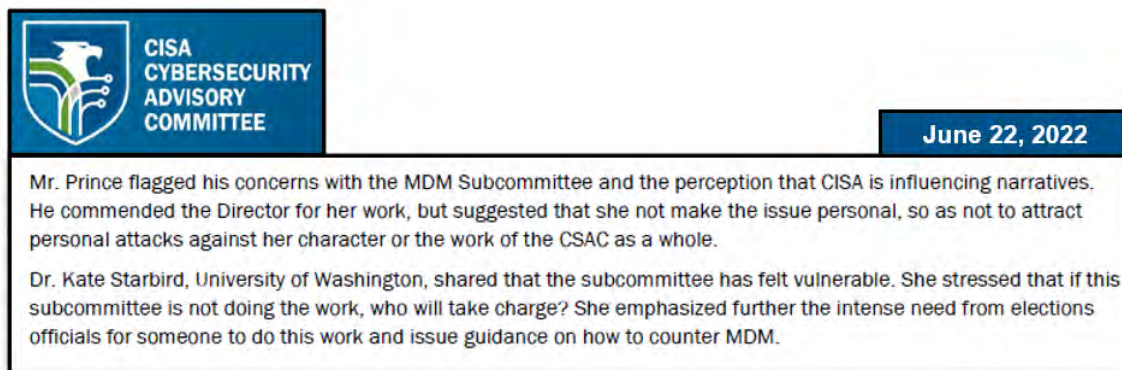
<sup>104</sup> E-mail from Brian Scully to LinkedIn employees (May 2, 2022, 12:09 PM) (on file with the Comm.).

A LinkedIn employee then forwarded Scully’s e-mail to another LinkedIn employee, who responded internally, mocking Scully: “Hey LinkedIn friends, if you ever want to know what the Regime considers to be true or false, just drop a line. We have connections...”<sup>105</sup>



### I. CSAC members were concerned about the MDM Subcommittee

Other members of the broader CSAC also exhibited discomfort at CISA’s and the MDM Subcommittee’s efforts related to MDM. During a closed session of the CSAC at its June 2022 Quarterly meeting, Cloudflare CEO Matthew Prince “flagged his concerns with the MDM Subcommittee and the perception that CISA is influencing narratives.”<sup>106</sup>



Nicole Perloth, another CSAC member, also “recommended that CISA establish an independent equivalent of a Facebook oversight board with people who are not vocal on Twitter, nor are they politically active, to give honest feedback. She expressed concern that since Director Easterly is serving under a political administration, this will put the recommendations at a higher risk.”<sup>107</sup>

<sup>105</sup> E-mail from LinkedIn employee to LinkedIn employees (May 2, 2022, 7:47 PM) (on file with the Comm.).

<sup>106</sup> CISA CYBERSECURITY ADVISORY COMM., JUNE 22, 2022 MEETING SUMMARY CLOSED SESSION, at 5 (on file with the Comm.).

<sup>107</sup> *Id.* at 6.

## II. CISA colludes with third parties to circumvent the First Amendment and conduct censorship by proxy

For the same reasons that the federal government may not censor Americans' speech, the federal government is also prohibited from using third parties to censor speech on its behalf. Under the First Amendment, the government may not "abridg[e] the freedom of speech."<sup>108</sup> The Constitution thus forbids the government from engaging in conduct that prevents or hampers speech on private social media platforms because of its content or the viewpoint that it expresses.<sup>109</sup>

Challenges to government involvement in the suppression of speech on social media are all relatively recent. As such, courts have had little opportunity to address the matter. However, a federal court recently found that this type of conduct gave rise to a plausible First Amendment claim: "Plaintiffs have clearly and plausibly alleged that [the government] engaged in viewpoint discrimination and prior restraints,"<sup>110</sup> the court declared, citing the plaintiffs' allegations of "extensive and highly effective efforts of government officials to silence or muffle the expression of disfavored viewpoints."<sup>111</sup> The court concluded that the plaintiffs had "plausibly alleged state action under the theories of joint participation, entwinement, and the combining of factors such as subsidization, authorization, and encouragement."<sup>112</sup>

In a draft of its June 2022 recommendations, the MDM Subcommittee refers to this pattern of unconstitutional outsourcing, writing, "CISA should also engage in content- and narrative-specific mitigation efforts . . . CISA should support these efforts . . . through funding outside organizations to assist in this work."<sup>113</sup>

- **#2: CISA should also engage in content- and narrative-specific mitigation efforts.** Proactive work should also include identifying and supporting trusted, authoritative sources in specific communities, e.g. in the elections context, local media and election officials. These efforts should also include building knowledge and experience that can empower individuals to be more resilient against divisive and despair-inducing MDM. CISA should support these efforts by creating and sharing materials; by providing education and frameworks for others to produce their own materials; and through funding to outside organizations to assist in this work

<sup>108</sup> U.S. CONST. amend. I.

<sup>109</sup> *Ashcroft v. ACLU*, 535 U.S. 564, 573 (2002). *See also* Hamburger, *supra* note 24.

<sup>110</sup> Mem. Ruling re 128 Mot. to Dismiss at 70, *Missouri v. Biden*, No. 3:22-cv-01213 (W.D. La. 2022), ECF No. 224.

<sup>111</sup> *Id.* at 63

<sup>112</sup> *Id.* at 68.

<sup>113</sup> E-mail from Kate Starbird to James Nash (May 10, 2022, 9:38 PM) (on file with the Comm.).

## A. CISA's external censorship arm: the EI-ISAC

The CISA-funded EI-ISAC was used by CIS during the 2020 election cycle as “a single point of reporting and tracking for misinformation across all channels and platforms.”<sup>114</sup> As described in a slide from a CIS presentation titled, “2020 CIS Election Infrastructure Misinformation Reporting Summary,” the EI-ISAC was intended to “[s]treamline and simplify misinformation reporting for election officials by eliminating multiple interactions to submit and follow up on reports.”<sup>115</sup> In so doing, CIS boasted that it “leverage[d] DHS CISA’s relationship with social media organizations to ensure priority treatment of misinformation reports.”<sup>116</sup>

**CIS** **The CIS Approach**

- Streamline and simplify misinformation reporting for election officials by eliminating multiple interactions to submit and follow up on reports
- Established a single EI-ISAC email account and database to serve as a single point of reporting and tracking for misinformation across all channels and platforms
- Leverage DHS CISA’s relationship with social media organizations to ensure priority treatment of misinformation reports
- Facilitate information sharing between election officials about reported misinformation
- Provide timely and meaningful feedback to election officials on the status of their reports
- Partner with outside analysis efforts, the Election Integrity Partnership\*, to augment identification and analysis of elections-related misinformation

\* The Election Integrity Partnership (EIP) was comprised of the [Stanford Internet Observatory](#) and [Program on Democracy and the Internet](#), [Graphika](#), the [Atlantic Council’s Digital Forensic Research Lab](#), and the [University of Washington’s Center for an Informed Public](#).

3

CISA also became involved with the Election Integrity Partnership (EIP). CIS and the EI-ISAC, as well as CISA itself, all served as “external stakeholders” of the project.<sup>117</sup> During the 2020 election cycle, the CISA-funded entities could—and did—send in reports of alleged misinformation to the EIP. Members of EIP, such as Alex Stamos, the director of the Stanford Internet Observatory, would send purportedly problematic content directly to social media platforms with recommendations on what content moderation steps the platforms should take.

Brian Scully, CISA’s MDM lead, confirmed in his deposition, that CISA did not directly engage in switchboarding for the 2022 election cycle, unlike in the 2020 election cycle.<sup>118</sup> Rather, CISA transferred the “switchboard function” to the EI-ISAC.<sup>119</sup>

<sup>114</sup> Aaron Wilson, 2020 CIS Election Infrastructure Misinformation Reporting Summary, at 3 (presentation materials) (on file with the Comm.).

<sup>115</sup> *Id.*

<sup>116</sup> *Id.*

<sup>117</sup> ELECTION INTEGRITY P’SHP, *supra* note 38, at 12.

<sup>118</sup> Scully Dep. 21:19–25, *supra* note 5.

<sup>119</sup> CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING JULY 26, 2022, at 1 (on file with the Comm.).

**B. State and local election officials used the EI-ISAC in an effort to silence critics and political opponents**

CIS had previously claimed that “Election Infrastructure Misinformation and Disinformation does NOT include: “content that is polarizing, biased, partisan or contains viewpoints expressed about elections or politics”; “inaccurate statements about an elected or appointed official, candidate, or political party”; or “broad, non-specific statements about the integrity of elections or civic processes that do not reference a specific current election administration activity.”<sup>120</sup>

But, in practice, state and local election officials used the CISA-funded EI-ISAC in an effort to silence criticism and political dissent of the nature allegedly “NOT include[d]” in CIS’s definition of “Election Infrastructure Misinformation and Disinformation.” For example, in August 2022, a Loudoun County, Virginia, government official reported a Tweet featuring an unedited video of a county official “because it was posted as part of a larger campaign to discredit the word of” that official.<sup>121</sup> The Loudon County official’s remark that the account she flagged “is connected to Parents Against Critical Race Theory” reveals that her “misinformation report” was nothing more than a politically motivated censorship attempt.<sup>122</sup>

**From:** [REDACTED] <[REDACTED]@loudoun.gov>  
**Sent:** Thursday, August 4, 2022 4:57 PM  
**To:** Misinformation Reports <misinformation@cisecurity.org>  
**Cc:** [REDACTED] <[REDACTED]@loudoun.gov>; [REDACTED] <[REDACTED]@loudoun.gov>; [REDACTED]@elections.virginia.gov  
**Subject:** [External] Voter Misinformation

Hello,

My name is [REDACTED], and I am the Outreach Coordinator for the Office of Elections in Loudoun County. I am reaching out because our office has recently been the focus of a misinformation campaign on the website VA Overwatch. This website is connected to Parents Against Critical Theory and the information is being shared on both sites.

a. In this video a person is asking [REDACTED] if there were any laws broken in the 2020/2021 election and about List Maintenance. [REDACTED] states that no laws were broken and explains the process of how list maintenance works in accordance with the State Law. This video is misinformation because it was posted as a part of a larger campaign to discredit the word of [REDACTED] and give the impression to voters that she is being negligent and breaking laws.

<sup>120</sup> CENTER FOR INTERNET SEC., TERMS OF USE ELECTION INFRASTRUCTURE MISINFORMATION PORTAL, at 1–2 (2020) (on file with the Comm.).

<sup>121</sup> E-mail from Loudoun County government official to misinformation@cisecurity.org (Aug. 4, 2022, 4:57 PM) (on file with the Comm.).

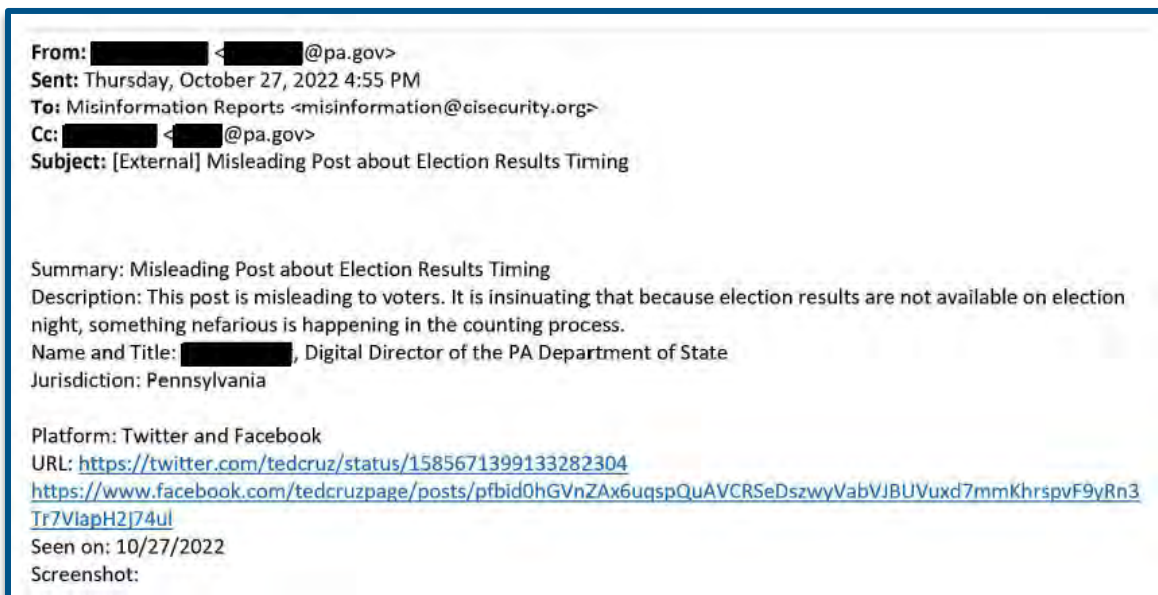
<sup>122</sup> *Id.*



The EI-ISAC then forwarded the report from the Loudoun County government to Twitter.<sup>123</sup>



The CISA-funded EI-ISAC also facilitated a Democratic state government official’s attempt to censor core political speech by a sitting Republican U.S. Senator. As demonstrated below, a state government official working for Pennsylvania’s Secretary of State reported to the EI-ISAC posts on Twitter and Facebook from Senator Ted Cruz’s accounts,<sup>124</sup> in which Senator Cruz asked: “Why is it only Democrat blue cities that take ‘days’ to count their votes? The rest of the country manages to get it done on election night.”<sup>125</sup>



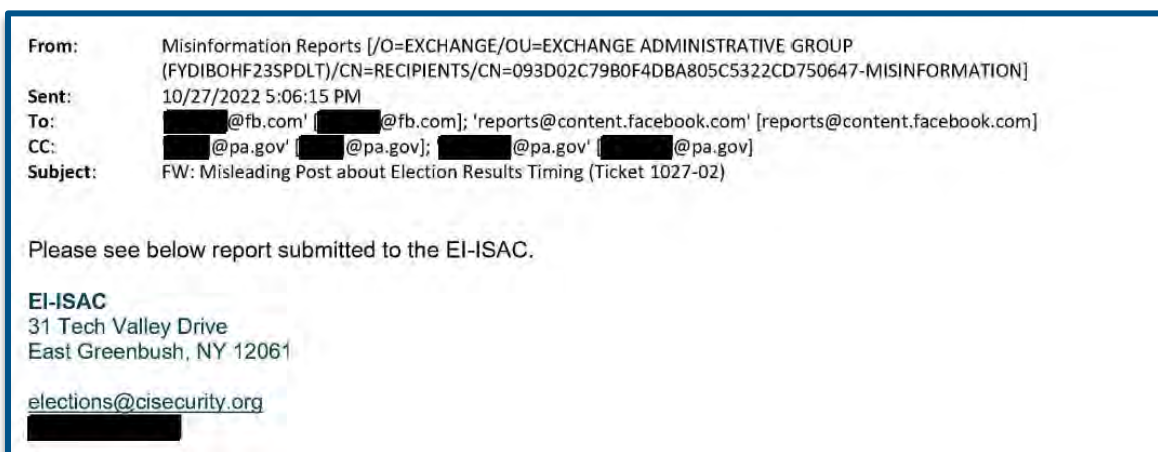
<sup>123</sup> E-mail from misinformation@cisecurity.org to Twitter employees (Aug. 18, 2022, 8:15 AM) (on file with the Comm.).

<sup>124</sup> E-mail from Pennsylvania state government official to misinformation@cisecurity.org (Oct. 27, 2022, 4:55 PM) (on file with the Comm.).

<sup>125</sup> Ted Cruz (@tedcruz), TWITTER (Oct. 27, 2022, 12:34 PM), <https://twitter.com/tedcruz/status/1585671399133282304>.



The EI-ISAC dutifully forwarded the report to Facebook.<sup>126</sup>

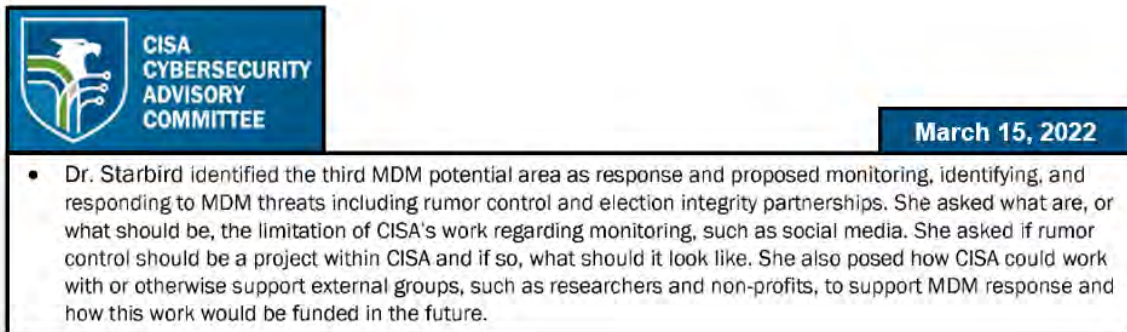


<sup>126</sup> E-mail from misinformation@cisecurity.org to Meta employees (Oct. 27, 2022, 5:06 PM) (on file with the Comm.).

### C. CISA admitted to outsourcing its surveillance operation to third parties

On numerous occasions, CISA officials and MDM Subcommittee members acknowledged, both implicitly and explicitly, that CISA was not authorized to conduct the kind of surveillance and censorship it was conducting. Instead of calling for an end to CISA’s unconstitutional activity, however, those involved routinely attempted to conceive methods by which CISA could surreptitiously outsource its surveillance and censorship to non-governmental third parties.

For example, during a March 15, 2022 meeting of the MDM Subcommittee, Starbird “asked what are, or what should be, the limitation of CISA’s work regarding monitoring, such as social media.”<sup>127</sup> Starbird then “addressed the highly limited scope for government in terms of social media monitoring . . . She also posed how CISA could work with or otherwise support external groups, such as researchers and non-profits, to support MDM response and how this work would be funded in the future.”<sup>128</sup> According to Starbird later in the meeting, “[t]hese limitations provide an opportunity for this subcommittee to inform gaps in this information.”<sup>129</sup>

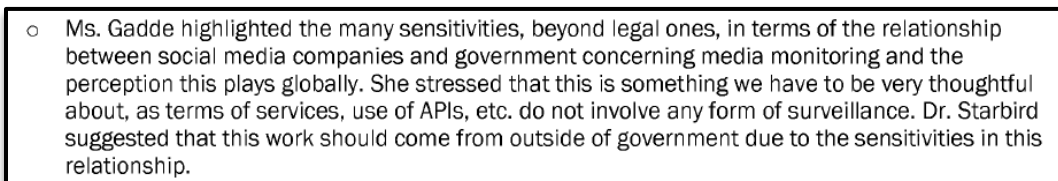


**CISA CYBERSECURITY ADVISORY COMMITTEE**

**March 15, 2022**

- Dr. Starbird identified the third MDM potential area as response and proposed monitoring, identifying, and responding to MDM threats including rumor control and election integrity partnerships. She asked what are, or what should be, the limitation of CISA's work regarding monitoring, such as social media. She asked if rumor control should be a project within CISA and if so, what should it look like. She also posed how CISA could work with or otherwise support external groups, such as researchers and non-profits, to support MDM response and how this work would be funded in the future.

Twitter’s Chief Legal Officer, Vijaya Gadde, then “highlighted the many sensitivities, beyond legal ones, in terms of the relationship between social media companies and government concerning media monitoring and the perception this plays globally,” as well as the need to ensure that this government-social media relationship did not result in “any form of surveillance.”<sup>130</sup> Starbird responded that “this work should come from outside of government due to the sensitivities in this relationship.”<sup>131</sup>



- Ms. Gadde highlighted the many sensitivities, beyond legal ones, in terms of the relationship between social media companies and government concerning media monitoring and the perception this plays globally. She stressed that this is something we have to be very thoughtful about, as terms of services, use of APIs, etc. do not involve any form of surveillance. Dr. Starbird suggested that this work should come from outside of government due to the sensitivities in this relationship.

<sup>127</sup> CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING MARCH 15, 2022, at 2 (on file with the Comm.).

<sup>128</sup> *Id.*

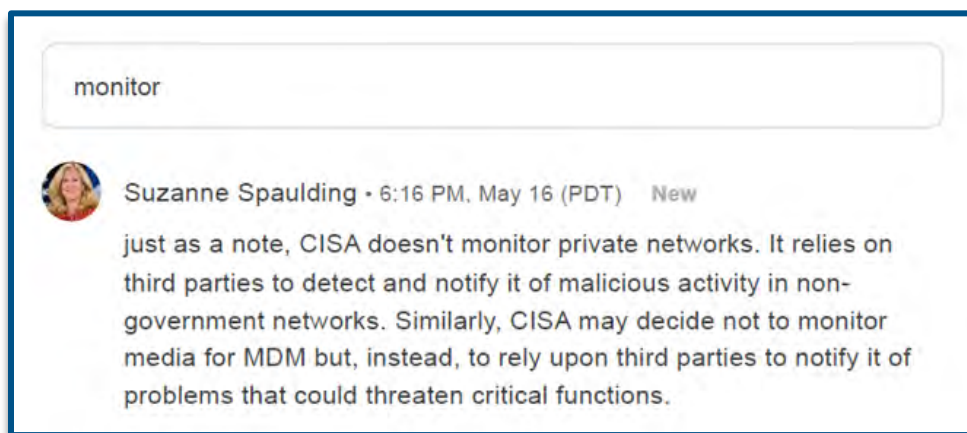
<sup>129</sup> *Id.*

<sup>130</sup> *Id.*

<sup>131</sup> *Id.*

Rather than abandon the consideration of surveilling Americans, Starbird and Gadde attempted to find ways to circumvent the First Amendment’s strictures by outsourcing the “monitoring” activity from the government to private entities.

In the same March meeting, Spaulding warned that “the government cannot ask an outside party to do something the Intelligence Community cannot do.”<sup>132</sup> But a few months later, MDM Subcommittee members were still considering how CISA could “rely upon third parties” rather than “monitor media for MDM” itself.<sup>133</sup> In the comments of an outline for the MDM Subcommittee’s June 2022 recommendations, Spaulding wrote, “[CISA] relies on third parties to detect and notify it of malicious activity in non-government networks. Similarly, CISA may decide not to monitor media for MDM but, instead, to rely upon third parties to notify it of problems.”<sup>134</sup>



---

<sup>132</sup> *Id.*

<sup>133</sup> E-mail from Suzanne Spaulding (Google Docs) to Kate Starbird (May 16, 2022, 6:27 PM) (on file with the Comm.).

<sup>134</sup> *Id.*

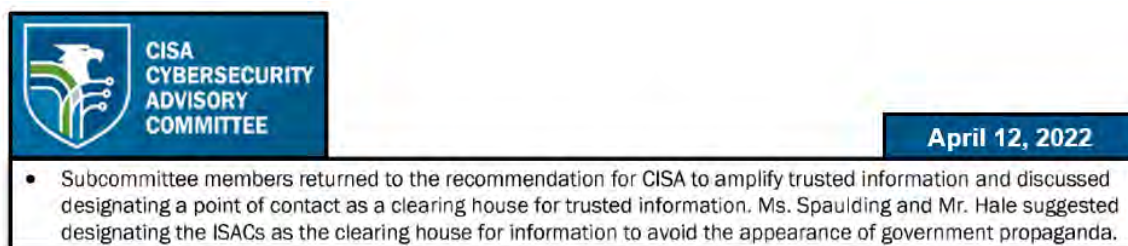
### III. CISA has attempted to conceal its unconstitutional activities and remove evidence of wrongdoing

April and May 2022 were difficult months for the censorship regime. President Biden’s DHS announced the formation of the Disinformation Governance Board on April 27, 2022, but had to pause its work on May 18,<sup>135</sup> and subsequently disband it,<sup>136</sup> following severe public outcry.<sup>137</sup> On May 5, the Attorneys General of Missouri and Louisiana filed a federal lawsuit against the Biden Administration, including CISA, alleging government-induced viewpoint-based censorship.<sup>138</sup> This lawsuit would soon reveal, among other things, direct pressure from the Biden White House to social media companies to censor vaccine-skeptical content.<sup>139</sup>

Meeting notes of the MDM Subcommittee from this period demonstrate that its members and CISA were fully aware of these developments and discussed how CISA could outsource its MDM-related activities to third parties so as to bypass the First Amendment and “avoid the appearance of government propaganda.”<sup>140</sup>

#### A. Fearing public pressure and legal risks, CISA outsourced its censorship operation to the EI-ISAC

In addition to outsourcing its censorship operation to the EI-ISAC, an MDM Subcommittee member and CISA official also suggested laundering its messaging through the EI-ISAC, thereby making the EI-ISAC the mouthpiece for “trusted information.”<sup>141</sup> During the April 12, 2022 MDM Subcommittee meeting, “Subcommittee members . . . discussed designating a point of contact as a clearing house for trusted information. Ms. Spaulding and Mr. Hale suggested designating the ISACs as the clearing house for information to avoid the appearance of government propaganda.”<sup>142</sup>



On July 26, 2022, CISA’s Kim Wyman made a particularly forthright admission about CISA’s attempts to launder its censorship operation to outside parties. According to the meeting notes, Wyman was discussing CISA’s “switchboard function to alert a media platform if a mis-

<sup>135</sup> Beitsch, *supra* note 103.

<sup>136</sup> Dep’t of Homeland Sec., *supra* note 103.

<sup>137</sup> Sganga, *supra* note 103.

<sup>138</sup> Missouri v. Biden, No. 3:22-cv-01213 (W.D. La. 2022), ECF No. 1 (Complaint).


<sup>139</sup> See Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Robert Flaherty (Jun. 23, 2023).

<sup>140</sup> CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING APRIL 12, 2022, at 2 (on file with the Comm.).

<sup>141</sup> *Id.*


<sup>142</sup> *Id.*

or dis-information post is identified by another user.”<sup>143</sup> In that discussion, Wyman indicated that “CISA is currently transferring this work to the Information and Sharing and Analysis Centers (ISACs). She noted the concern over CISA operating this function given the current lawsuit filed by Louisiana and Missouri against CISA over perceived suppression of free speech.”<sup>144</sup>

	<b>July 26, 2022</b>
<ul style="list-style-type: none"><li>• Ms. Wyman shared concerns expressed by the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED) since they were not consulted when the Subcommittee was drafting recommendations. She reviewed a sample of CISA’s work to deliver products to the elections community to include operating a switchboard function to alert a media platform if a mis- or dis-information post is identified by another user. CISA is currently transferring this work to the Information Sharing and Analysis Centers (ISACs). She noted the concern over CISA operating this function given the current lawsuit filed by Louisiana and Missouri against CISA over perceived suppression of free speech.</li></ul>	

### **B. The MDM Subcommittee tried to disguise its recommendations by removing references to surveillance and censorship**

Both CISA and its advisory subcommittee were keenly aware of and concerned about the political environment and legal risks that accompanied its surveillance and censorship activities. During the May 10, 2022 meeting of the MDM Subcommittee, “Dr. Starbird suggested refining the name of the subcommittee to ‘Informational Threats to Critical Infrastructure’ or ‘Informational Threats to Election Security’ so as not to conflate the group’s efforts with the work of the DHS Disinformation Governance Board.”<sup>145</sup> Twitter’s Gadde then “affirmed this [suggestion] and cautioned the group against pursuing any social listening recommendations for the CSAC June Quarterly Meeting.”<sup>146</sup>

	<b>May 10, 2022</b>
<ul style="list-style-type: none"><li>• Dr. Kate Starbird, Associate Professor, Human Centered Design &amp; Engineering, University of Washington, MDM Subcommittee Chair, began the meeting by asking subcommittee members to discuss the announcement of the new DHS Disinformation Governance Board and the broader implications for this subcommittee.<ul style="list-style-type: none"><li>○ Ms. Kim Wyman, Senior Election Security Lead, CISA, stressed that misinformation and disinformation are elevated to national awareness due to this board. Dr. Starbird suggested refining the name of the subcommittee to “Informational Threats to Critical Infrastructure” or “Informational Threats to Election Security” so as not to conflate the group’s efforts with the work of the DHS Disinformation Governance Board. Ms. Vijaya Gadde, Legal, Public Policy, and Trust and Safety Lead, Twitter, affirmed this and cautioned the group against pursuing any social listening recommendations for the CSAC June Quarterly Meeting.</li></ul></li></ul>	

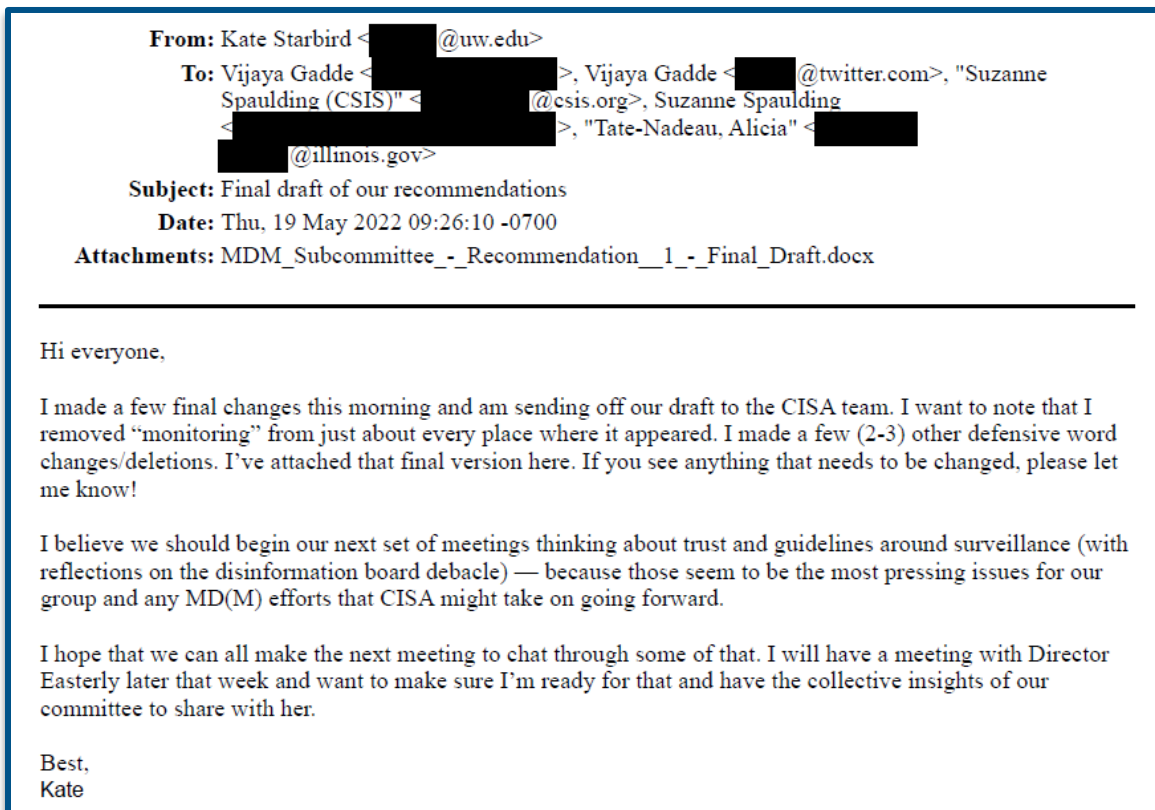
<sup>143</sup> CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING JULY 26, 2022, at 1 (on file with the Comm.).

<sup>144</sup> *Id.*

<sup>145</sup> CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING MAY 10, 2022, at 1 (on file with the Comm.).

<sup>146</sup> *Id.*

A little over a week later, on May 19, Starbird sent an e-mail to the other members of the MDM Subcommittee, writing: “I made a few final changes this morning and am sending off our draft [of the MDM Subcommittee’s June 2022 recommendations] to the CISA team. I want to note that I removed ‘monitoring’ from just about every place where it appeared.”<sup>147</sup>



These attempts to disguise the true nature of counter-MDM work are emblematic of the tactics employed by academics “studying” disinformation. According to recent reporting by the *Washington Post*, in response to the Committee’s request for documents from Stanford University, “lawyers at the institution warned researchers to be more thoughtful about what they said in emails. ‘It makes me more careful in my communications with colleagues and collaborators,’ said professor Jeff Hancock, the faculty director of the Stanford Internet Observatory.”<sup>148</sup>

**C. CISA’s MDM advisors fretted that it was “only a matter of time before someone realizes we exist and starts asking about our work.”**

On May 20, Spaulding sent an e-mail to Starbird expressing her concerns about growing public attention. In an e-mail, Spaulding wrote: “It’s only a matter of time before someone

<sup>147</sup> E-mail from Kate Starbird to Vijaya Gadde, Suzanne Spaulding, and Alicia Tate-Nadeau (May 19, 2022, 9:26 AM) (on file with the Comm.).

<sup>148</sup> Naomi Nix and Joseph Menn, *These academics studied falsehoods spread by Trump. Now the GOP wants answers*, WASHINGTON POST (Jun. 6, 2023).

realizes we exist and starts asking about our work. . . . I'm not sure this keeps until our public meeting in June."<sup>149</sup>

On May 20, 2022, at 7:27 AM, Suzanne Spaulding <[REDACTED]> wrote:

Kate,  
It's only a matter of time before someone realizes we exist and starts asking about our work. You may have already discussed this with Jen, but I'm wondering if we should try to find time to talk with CISA's comms and legislative folks about how we socialize what we're doing. It would be good to be proactive in telling our story rather than reacting to how someone else decides to portray it, right? And I'm not sure this keeps until our public meeting in June. I know neither of us has time for this, but I am telling myself that it might save us time in the long run!

best,  
Suzanne

Starbird responded to Spaulding, writing, "Yes. I agree. We have a couple of pretty obvious vulnerabilities."<sup>150</sup>

**From:** Kate Starbird [REDACTED]@uw.edu  
**Subject:** Re: CSAC MDM Subcommittee Meeting  
**Date:** May 20, 2022 at 7:37 AM  
**To:** Suzanne Spaulding suzannespaulding10@gmail.com

KS

Yes. I agree. We have a couple of pretty obvious vulnerabilities. Do we want to meet prior to our Tues meeting or use that to start this conversation and make a plan? This is currently our singular topic for Tues. I'm supposed to meet with Jen later next week, but we haven't touched base on this yet.

Kate

During a May 24 meeting of the MDM Subcommittee, Starbird "restated the Subcommittee's commitment to transparency but expressed concern for the Subcommittee's efforts and cautioned the group on how to communicate their ongoing work."<sup>151</sup>



May 24, 2022

- Dr. Kate Starbird, Associate Professor, Human Centered Design & Engineering, University of Washington, MDM Subcommittee Chair, discussed the Subcommittee's recommendations to present during the CSAC June Quarterly Meeting and the path forward to strategically approach MDM in the government during the current discourse. Dr. Starbird restated the Subcommittee's commitment to transparency but expressed concern for the Subcommittee's efforts and cautioned the group on how to communicate their ongoing work.

<sup>149</sup> E-mail from Suzanne Spaulding to Kate Starbird (May 20, 2022, 7:27 AM) (on file with the Comm.).

<sup>150</sup> E-mail from Kate Starbird to Suzanne Spaulding (May 20, 2022, 7:37 AM) (on file with the Comm.).

<sup>151</sup> CISA CYBERSECURITY ADVISORY COMM., PROTECTING CRITICAL INFRASTRUCTURE FROM MISINFORMATION & DISINFORMATION SUBCOMMITTEE MEETING MAY 24, 2022, at 1 (on file with the Comm.).



In an apparent effort to conceal the full scope of CISA’s MDM-related efforts, Spaulding then “stressed that CISA should examine MDM beyond elections but suggested including in the recommendations that the Subcommittee is scoping their work around elections given the approaching election cycle.”<sup>152</sup>

o Ms. Suzanne Spaulding, Senior Advisor for Homeland Security and Director of the Defending Democratic Institutions Center for Strategic and International Studies (CSIS), suggested that the group recruit subject matter experts (SMEs) to support the Subcommittee’s efforts, solicit different perspectives, and apply credibility to the Subcommittee’s work with a broader audience. Ms. Spaulding offered an additional suggestion of asking Director Easterly for her perspective of socializing this Subcommittee’s work with Congress to prevent outside parties from being blindsided by their efforts. She further suggested the Subcommittee re-read and refine the recommendations and stressed that the safest ground in election is the recommendation for CISA to 1) point individuals to an authoritative source and 2) utilize their convening power. She stressed that CISA should examine MDM beyond elections, but suggested including in the recommendations that the Subcommittee is scoping their work around elections given the approaching election cycle. Ms. Spaulding offered an additional recommendation for CISA to scope their mission space to MDM that poses significant risk to national critical functions (NCFs).

Spaulding’s and others’ proposal to “socialize” the MDM Subcommittee’s work was met with resistance from CISA’s Megan Tsuyi, who told Starbird that “[t]he Subcommittee should not be socializing its work with outside parties . . . as it’s pre-deliberative at this time. We also shouldn’t be soliciting feedback on the recommendations from outside parties.”<sup>153</sup>

**From:** Tsuyi, Megan [REDACTED]@cisa.dhs.gov  
**Subject:** RE: Minutes/Meeting Summary 5 - 24- 2022.  
**Date:** May 26, 2022 at 3:49 AM  
**To:** Nash, James [REDACTED]@cisa.dhs.gov, Kate Starbird [REDACTED]@uw.edu  
**Cc:** EVANS, MARIEFRED (CTR) [REDACTED]@associates.cisa.dhs.gov, Heidelberg, Kirsten [REDACTED]@cisa.dhs.gov, Tsuyi, Megan [REDACTED]@cisa.dhs.gov

Thanks to all of you for the quick turn on the minutes.

Kate – we can discuss this more on tomorrow’s planning call, but wanted to send a quick email in case you were planning to take any additional action between now and that time...The Subcommittee should not be socializing its work with outside parties (work = deliverables/recommendations), as it’s pre-deliberative at this time. We also shouldn’t be soliciting feedback on the recommendations from outside parties. If the subcommittee would like to bring in [REDACTED] to be a part of a discussion on the validation of their findings and recommendations, that is fine.

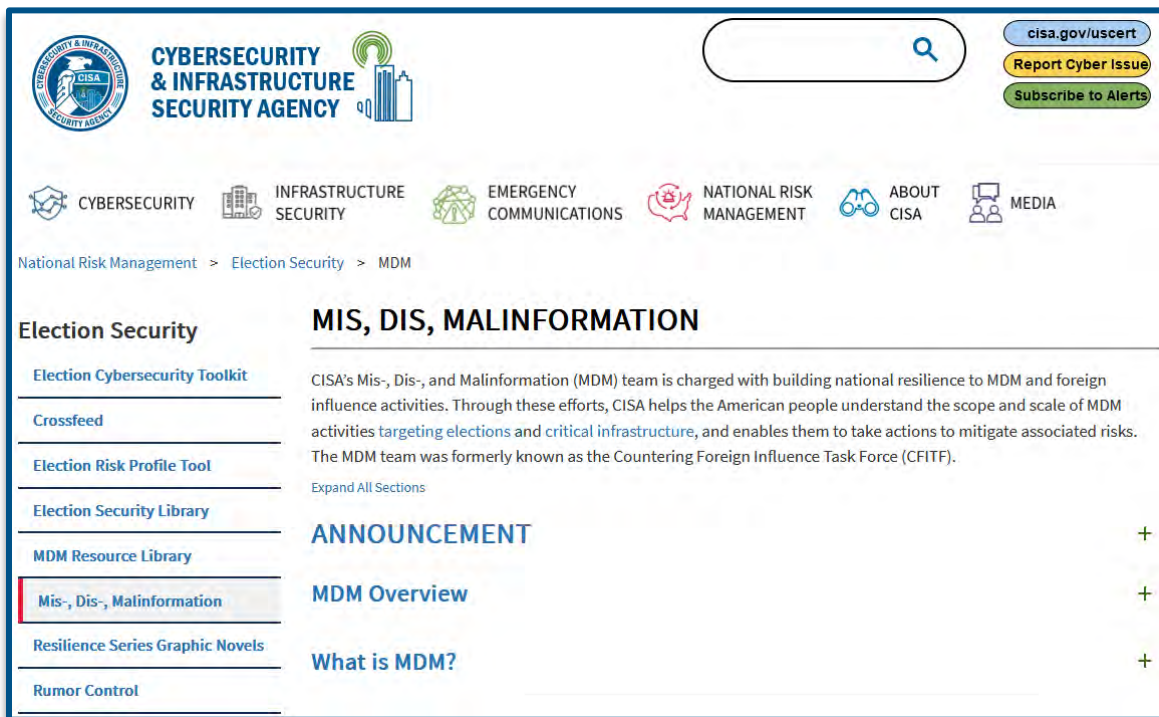
#### **D. CISA purged its website of references to domestic MDM and its First Amendment violations in response to public pressure**

Following increased public awareness of CISA’s role in government-induced censorship and the Committee’s issuance of subpoenas to Alphabet, Amazon, Apple, Microsoft, and Meta in February 2023, CISA scrubbed its website of references to domestic MDM. Prior to the cleansing, the domain “CISA.gov/mdm” was associated with a webpage titled “Mis, Dis,

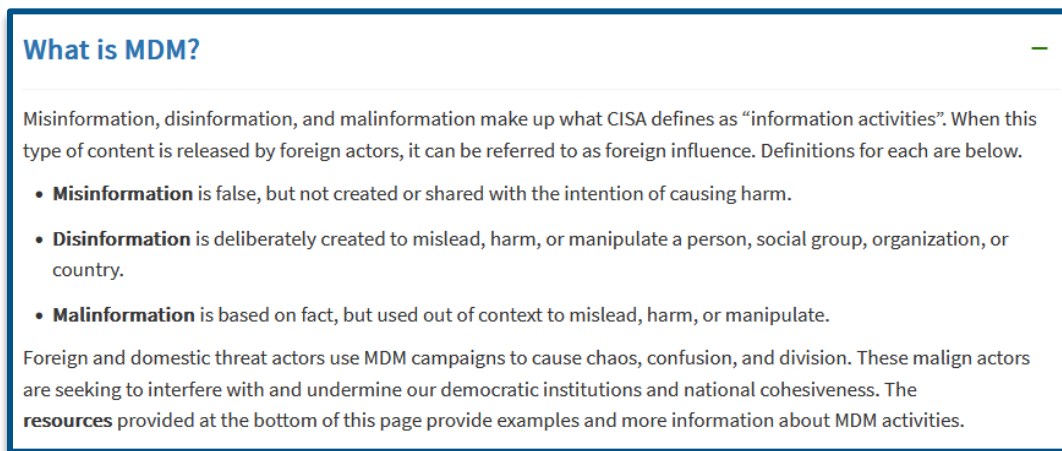
<sup>152</sup> *Id.*

<sup>153</sup> E-mail from Megan Tsuyi to Kate Starbird and James Nash (May 26, 2022, 3:49 AM) (on file with the Comm.).

Malinformation,” as seen in the screenshot below, which shows the website as it appeared on February 12, 2023.<sup>154</sup>



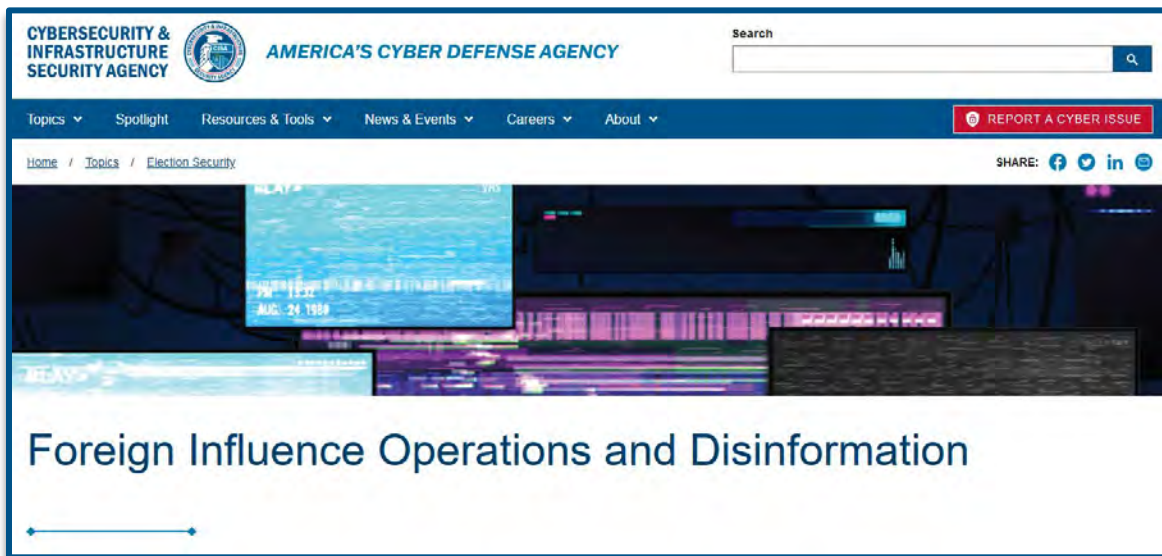
The website previously described the threats posed by both foreign and domestic MDM. For example, the section titled “What is MDM?” read, “Foreign *and domestic* threat actors use MDM campaigns to cause chaos, confusion, and division. These malign actors are seeking to interfere with and undermine our democratic institutions and national cohesiveness.”<sup>155</sup>



<sup>154</sup> *Mis, Dis, Malinformation*, Cybersecurity and Infrastructure Sec. Agency, <https://cisa.gov/mdm> [<https://web.archive.org/web/20230215235115/https://www.cisa.gov/mdm>].

<sup>155</sup> *Id.* (emphasis added).

Now, the same URL redirects to a different page titled “Foreign Influence Operations and Disinformation,” which omits any reference to “domestic” MDM.<sup>156</sup>



As reported by the Foundation for Freedom Online, “between Friday, Feb. 24 at 4:37 p.m. and Sunday, Feb. 26 at 5:55 am., CISA’s once loud-and-proud declaration of long-arm jurisdiction over domestic opinions online seems to have been walked back.”<sup>157</sup>

#### **E. The Biden Justice Department interfered with public records requests in order to shield CISA from public scrutiny of its unconstitutional practices**

The effort to cover up CISA’s malfeasance appears to be a joint effort across the Biden Administration, according to recent reporting by journalist Lee Fang. In the fall of 2022, several non-profits and journalists, including Fang, individually submitted record requests to the University of Washington for material about Starbird’s work with CISA.<sup>158</sup> On September 26, 2022, Annalisa Cravens, an Assistant United States Attorney with the Department of Justice (DOJ), sent an e-mail to Starbird, writing, “Could we please see a copy of any relevant CISA documents that you may plan to produce? We’re also not sure when you received the records request, but we would ask to have an extension of time to review them and assess whether we’ll have to file suit to protect them from disclosure.”<sup>159</sup>

<sup>156</sup> *Foreign Influence Operations and Disinformation*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, <https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation> (last visited Jun. 23, 2023).

<sup>157</sup> Mike Benz, *DHS Quietly Purges CISA “Mis, Dis and Malinformation” Website To Remove Domestic Censorship References*, FOUNDATION FOR FREEDOM ONLINE (Mar. 16, 2023), <https://foundationforfreedomonline.com/wp-content/uploads/2023/03/FFO-FLASH-REPORT.pdf>.

<sup>158</sup> Lee Fang, *Biden Justice Dept. Intervened to Block Release of Social Media Censorship Docs*, SUBSTACK (Jun. 6, 2023), <https://www.leefang.com/p/biden-justice-dept-intervened-to>.

<sup>159</sup> *Id.*

On Sep 26, 2022, at 1:58 PM, Cravens, Annalisa (USAWAW)  
<[REDACTED]@usdoj.gov> wrote:

Dr. Starbird and Mr. Fleming:

I hope this finds you well. We've heard from the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security that the Daily Caller News Foundation has requested documents from the University, which may include documents that belong to CISA.

Could we please see a copy of any relevant CISA documents that you may plan to produce? We're also not sure when you received the records request, but we would ask to have an extension of time before the records are produced so that we can have time to review them and assess whether we'll have to file suit to protect them from disclosure.

Coincidentally, Dr. Starbird, I was at your talk this afternoon, and I found it very interesting. I was disappointed when Nick cut off the Q&A at 1 o'clock! Thanks for coming to speak to us.

Best regards,

**Annalisa Cravens**  
Assistant United States Attorney  
U.S. Attorney's Office | Western District of Washington  
[REDACTED] | [REDACTED] (cell)  
[REDACTED]@usdoj.gov

As Fang subsequently explained, “[t]he stalling effort highlights not only the broad authority that the federal government has to shape the political content available to the public, but also the toolkit that it relies upon to limit scrutiny of its involvement in the regulation of speech.”<sup>160</sup>

---

<sup>160</sup> *Id.*

---

## CONCLUSION

---

“Silencing those who disagree with us is a sign of weakness, not strength, and it won’t lead to progress.”  
– former President Barack Obama, April 6, 2023.<sup>161</sup>

In 2019, CISA’s Chief Counsel claimed: “We are not law enforcement and we’re not the intelligence community.”<sup>162</sup> In theory, the statement is accurate. CISA is not a law enforcement agency and is not authorized to act as an intelligence agency. But, in practice, that is how CISA has behaved, arrogating to itself the authority to conduct surveillance of Americans on social media. CISA expanded its unconstitutional practice by developing an elaborate social media censorship apparatus spanning multiple organizations, in order to facilitate the censorship of Americans’ political speech both directly and by proxy. There is no constitutionally viable legal authority that allows CISA to engage in this or any other kind of censorship. Thus, not only does CISA’s conduct violate the First Amendment, it also disregards the basic principle of the separation of powers, which prohibits agencies from acting outside of their congressionally delegated sphere.<sup>163</sup>

As Suzanne Spaulding, the former CIA legal advisor and MDM Subcommittee member, presaged, it was “only a matter of time before someone realizes we exist and starts asking about”<sup>164</sup> CISA’s repeated violations of the First Amendment. CISA’s attempts to cover up its surveillance and censorship operations will not rectify the damage inflicted on the American people by government-induced censorship. Neither CISA’s scrubbing of its website, nor the Biden Administration’s stalling of records requests can conceal the true nature of CISA’s work in “combating MDM.”

CISA must be reined in, as must the Biden Administration’s “whole-of-government” approach to social media censorship. Every American has the right to express his or her opinion online, and to receive information from others. Government classifications of opinions as “misinformation” or “disinformation” do not nullify the First Amendment’s guarantees. A free and democratic society is impossible under a government that acts as the ultimate arbiter of truth in political discourse. To better inform legislative efforts to end government censorship on the Internet and protect Americans’ rights guaranteed by the First Amendment, the Committee and Select Subcommittee will continue to investigate the extent of CISA’s and other Executive Branch agencies’ interactions with social media platforms.

---

<sup>161</sup> Barack Obama (@BarackObama), TWITTER (Apr. 6, 2023, 10:20 PM), <https://twitter.com/BarackObama/status/1644163255189774337>.

<sup>162</sup> *CISA and Cyber Threats: How Government and Private Sector Secure Our Networks and Infrastructure*, *supra* note 28.

<sup>163</sup> *Am. Hosp. Ass’n v. Azar*, 410 F. Supp. 3d 142, 151 (D.D.C. 2019) (“[A]gency actions beyond delegated authority are *ultra vires* and should be invalidated.”).

<sup>164</sup> E-mail from Suzanne Spaulding to Kate Starbird (May 20, 2022, 7:27 AM) (on file with the Comm.).