THE WEAPONIZATION OF "DISINFORMATION" PSUEDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS' POLITICAL SPEECH

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

November 6, 2023

EXECUTIVE SUMMARY

Following the 2016 presidential election, a sensationalized narrative emerged that foreign "disinformation" affected the integrity of the election. These claims, fueled by left-wing election denialism about the legitimacy of President Trump's victory, sparked a new focus on the role of social media platforms in spreading such information.[1] "Disinformation" think tanks and "experts," government task forces, and university centers were formed, all to study and combat the alleged rise in alleged mis- and disinformation. As the House Committee on the Judiciary and the Select Subcommittee on the Weaponization of the Federal Government have shown previously, these efforts to combat so-called foreign influence and misinformation quickly mutated to include domestic—that is, American—speech.[2]

The First Amendment to the Constitution rightly limits the government's role in monitoring and censoring Americans' speech, but these disinformation researchers (often funded, at least in part, by taxpayer dollars) were not strictly bound by these constitutional guardrails. What the federal government could not do directly, it effectively outsourced to the newly emerging censorship-industrial complex.

Enter the Election Integrity Partnership (EIP), a consortium of "disinformation" academics led by Stanford University's Stanford Internet Observatory (SIO) that worked directly with the Department of Homeland Security and the Global Engagement Center, a multi-agency entity housed within the State Department, to monitor and censor Americans' online speech in advance of the 2020 presidential election. Created in the summer of 2020 "at the request" of the Cybersecurity and Infrastructure Security Agency (CISA),[3] the EIP provided a way for the federal government to launder its censorship activities in hopes of bypassing both the First Amendment and public scrutiny.

In the lead-up to the 2020 election, amid the COVID-19 pandemic, the American public and lawmakers debated the merits of unprecedented, mid-election-cycle changes to election procedures.[4] These issues, like all contemporary discourse about questions of political import, were extensively discussed on the world's largest social media platforms—the modern town square. But as American citizens, including candidates in these elections, attempted to exercise their First Amendment rights on these platforms, their constitutionally protected speech was intentionally suppressed as a consequence of the federal government's direct coordination with

[1] *See, e.g.*, Tim Starks, *Russian trolls on Twitter had little influence on 2016 voters*, WASH. POST (Jan. 9, 2023) ("The study, which the New York University Center for Social Media and Politics helmed, explores the limits of what Russian disinformation and misinformation was able to achieve on one major social media platform in the 2016 elections."); *id*. ("There was no measurable impact on 'political attitudes, polarization, and vote preferences and behavior' from the Russian accounts and posts.").

[2] *See* STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A "CYBERSECURITY" AGENCY COLLUDED WITH BIG TECH AND "DISINFORMATION" PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).

[3] Email from Graham Brookie to Atlantic Council employees (July 31, 2020, 5:54 PM) (on file with the Comm.).

[4] *See, e.g.*, REPUBLICAN STAFF OF THE H. COMM. ON THE JUDICIARY AND THE COMM. ON OVERSIGHT AND REFORM, 116TH CONG., HOW DEMOCRATS ARE ATTEMPTING TO SOW UNCERTAINTY, INACCURACY, AND DELAY IN THE 2020 ELECTION (Sept. 23, 2020); *see also Changes to election dates, procedures, and administration in response to the coronavirus (COVID-19) pandemic, 2020*, BALLOTPEDIA (last visited Nov. 3, 2023).

third-party organizations, particularly universities, and social media platforms.[5] Speech concerning elections—the process by which Americans select their representatives—is of course entitled to robust First Amendment protections.[6] This bedrock principle is even more critical as it relates to speech by political candidates.[7] But as disinformation "experts" acknowledge, the labeling of any kind of speech is "inherently political"[8] and itself a form of "censorship."[9]

This interim staff report details the federal government's heavy-handed involvement in the creation and operation of the EIP, which facilitated the censorship of Americans' political speech in the weeks and months leading up to the 2020 election. This report also publicly reveals for the first time secret "misinformation" reports from the EIP's centralized reporting system, previously accessible only to select parties, including federal agencies, universities, and Big Tech. The Committee and Select Subcommittee obtained these nonpublic reports from Stanford University only under the threat of contempt of Congress. These reports of alleged mis- and disinformation were used to censor Americans engaged in core political speech in the lead up to the 2020 election.

As this new information reveals, and this report outlines, the federal government and universities pressured social media companies to censor true information, jokes, and political opinions. This pressure was largely directed in a way that benefitted one side of the political aisle: true information posted by Republicans and conservatives was labeled as "misinformation" while false information posted by Democrats and liberals was largely unreported and untouched by the censors. The pseudoscience of disinformation is now—and has always been—nothing more than a political ruse most frequently targeted at communities and individuals holding views contrary to the prevailing narratives.

The EIP's operation was straightforward: "external stakeholders," including federal agencies and organizations funded by the federal government, submitted misinformation reports

---

[5] *See* Missouri v. Biden, No. 23-30445, (5th Cir. Oct. 3, 2023), ECF No. 268-1 (affirming preliminary injunction in part); Missouri v. Biden, No. 3:22-cv-01213 (W.D. La. Jul. 4, 2023), ECF No. 293 (memorandum ruling granting preliminary injunction).

[6] *See, e.g.*, Snyder v. Phelps, 562 U.S. 443, 452 (2011) ("[S]peech on public issues occupies the highest rung of the hierarchy of First Amendment values") (quoting Connick v. Myers, 461 U.S. 138, 145 (1983)); Ariz. Free Enter. Club's Freedom Club PAC v. Bennett, 564 U.S. 721, 755 (2011) (internal quotation marks and citation omitted) (The First Amendment protects the "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open."); *see also* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 346 (1995) (cleaned up) ("There is practically universal agreement that a major purpose of the Amendment was to protect the free discussion of governmental affairs, of course including discussions of candidates.").

[7] "The First Amendment 'has its fullest and most urgent application precisely to the conduct of campaigns for political office,'" FEC v. Cruz, 142 S. Ct. 1638, 1650 (2022) (quoting Monitor Patriot Co. v. Roy, 401 U.S. 265, 272 (1971)); *see also* Buckley v. Valeo, 424 U.S. 1, 52 (1976) (A candidate "has a First Amendment right to engage in the discussion of public issues and vigorously and tirelessly to advocate his own election.").

[8] Email from Suzanne Spaulding (Google Docs) to Kate Starbird (May 16, 2022, 6:27 PM) (on file with the Comm.); *see also* Kate Starbird et al., Proposal to the National Science Foundation for "Collaborative Research: SaTC: Core: Large: Building Rapid-Response Frameworks to Support Multi-Stakeholder Collaborations for Mitigating Online Disinformation" (Jan. 29, 2021) (unpublished proposal) (on file with the Comm.) ("The study of disinformation today invariably includes elements of politics.").

[9] Team F-469 First Pitch to NSF Convergence Accelerator, UNIV. OF MICH., at 1 (presentation notes) (Oct. 27, 2021) (on file with the Comm.).

directly to the EIP. The EIP's misinformation "analysts" next scoured the internet for additional examples for censorship. If the submitted report flagged a Facebook post, for example, the EIP analysts searched for similar content on Twitter, YouTube, TikTok, Reddit, and other major social media platforms. Once all of the offending links were compiled, the EIP sent the most significant ones directly to Big Tech with *specific* recommendations on how the social media platforms should censor the posts, such as reducing the posts' "discoverability," "suspending [an account's] ability to continue tweeting for 12 hours," "monitoring if any of the tagged influencer accounts retweet" a particular user, and, of course, removing thousands of Americans' posts.[10]

Government agencies and disinformation "experts" are quick to cite the need to combat foreign actors attempting to undermine American elections as a justification for this censorship regime. While foreign states do attempt to conduct influence operations, the Committee's and Select Subcommittee's investigation has revealed that the true focus and purpose of the censors' "election integrity" work was to target the very Americans they claim to protect. Instead of targeting foreign or inauthentic accounts, the EIP targeted Americans, disproportionately candidates and commentators with conservative viewpoints. And despite its stated purpose to combat "disinformation," the EIP worked with social media companies to censor true information, jokes and satire, and political opinions.

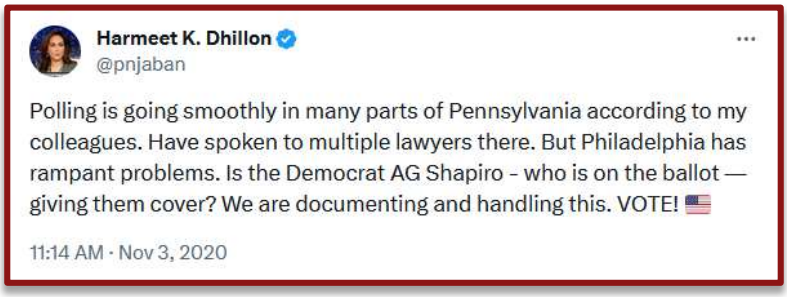
[10] *See, e.g.*, EIP-581, submitted by [REDACTED], ticket created (Nov. 2, 2020, 2:36 PM) (archived Jira ticket data produced to the Comm.); EIP-673, submitted by [REDACTED], ticket created (Nov. 3, 2020, 11:51 AM) (archived Jira ticket data produced to the Comm.) (citing Mike Coudrey, TWITTER (Nov. 3, 2020, 10:13 AM), https://twitter.com/MichaelCoudrey/status/1323644406998597633); EIP-638, submitted by [REDACTED], ticket created (Nov. 3, 2020, 9:23 AM) (archived Jira ticket data produced to the Comm.).

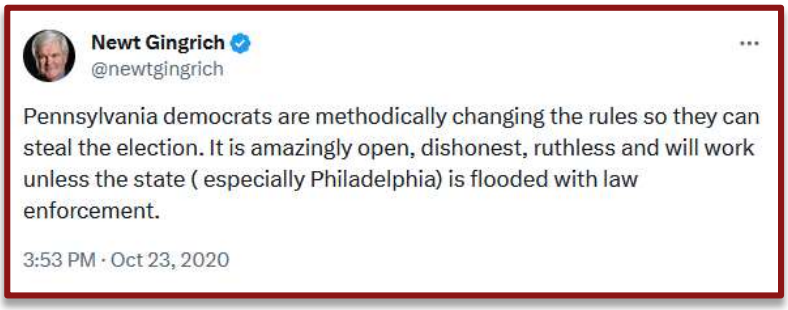
Who was being censored?

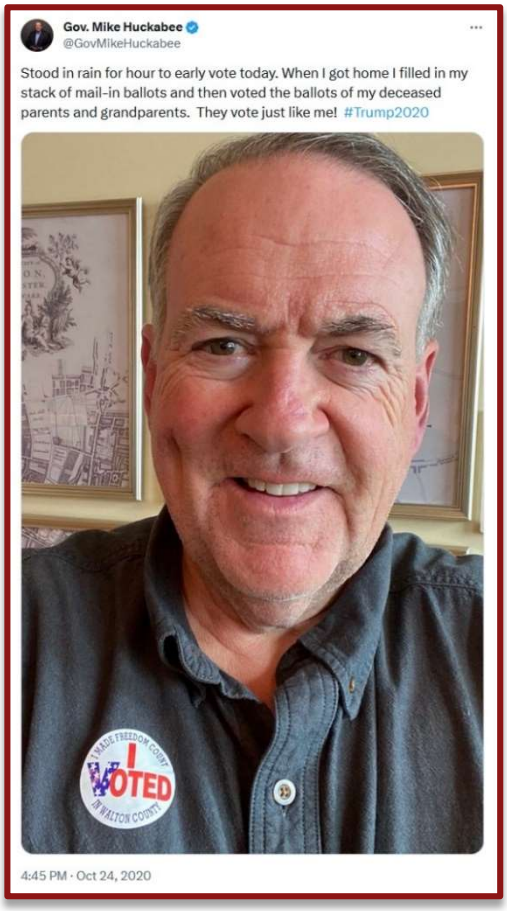
- President Donald J. Trump
- Senator Thom Tillis
- Speaker Newt Gingrich
- Governor Mike Huckabee
- Congressman Thomas Massie
- Congresswoman Marjorie Taylor Greene
- Newsmax
- The Babylon Bee
- Sean Hannity
- Mollie Hemingway
- Harmeet Dhillon
- Charlie Kirk
- Candace Owens
- Jack Posobiec
- Tom Fitton
- James O'Keefe
- Benny Johnson
- Michelle Malkin
- Sean Davis
- Dave Rubin
- Paul Sperry
- Tracy Beanz
- Chanel Rion
- An untold number of everyday Americans of all political affiliations

What was being censored?

- True information
- Jokes and satire
- Political opinions







As part of this report, the Committee and Select Subcommittee are releasing all of the previously secret, archived data the Committee has obtained pursuant to a subpoena issued to Stanford University, which Stanford produced only after the threat of contempt.[11] In the lead-up to the 2020 election, the Department of Homeland Security (DHS) had the ability to see what American speech was being censored. Today, as a result of the Committee's and Select Subcommittee's investigation, political candidates, journalists, and all Americans have the opportunity to see if they were targeted by their government and what viewpoints DHS, Stanford, and others worked to censor. While the EIP disproportionately targeted conservatives, Americans of all political affiliations were victims of censorship.

The First Amendment prohibits the government from "abridging the freedom of speech" and protects "the right of the people . . . to petition the Government."[12] The ability of Americans to criticize the government and its policies is a fundamental and sacrosanct principle of our constitutional republic. The Supreme Court has long recognized that for "core political speech" "the importance of First Amendment protections is at its zenith."[13] Moreover, as constitutional scholars have explained: "Because the First Amendment bars 'abridging' the freedom of speech,

[11] *See* App'x II.
[12] U.S. Const. amend. I.
[13] Meyer v. Grant, 486 U.S. 414, 420, 425 (1988) (internal quotation marks omitted).

any law or government policy that reduces that freedom on the [social media] platforms . . . violates the First Amendment."[14]

The government may not dictate the type or terms of the criticism to which it is subject, even when—especially when—the government disagrees with the merits of that criticism. To inform potential legislation, the Committee and the Select Subcommittee have been investigating the Executive Branch's collusion with third-party intermediaries, including universities, to censor protected speech on social media.

The Committee and the Select Subcommittee are responsible for investigating "violation[s] of the civil liberties of citizens of the United States."[15] 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 Committee's and Select Subcommittee's investigation remains ongoing. CISA still has not adequately complied with a subpoena for relevant documents, and more fact-finding is necessary. In order to better inform the Committee's legislative efforts, the Committee and Select Subcommittee will continue to investigate how the Executive Branch worked with social media platforms and other intermediaries to censor disfavored viewpoints in violation of the U.S. Constitution.

[14] Philip Hamburger, *How the Government Justifies Its Social-Media Censorship*, WALL ST. J. (June 9, 2023).
[15] H. Res. 12 § 1(b)(E).

TABLE OF CONTENTS

GLOSSARY OF KEY TERMS & NAMES

Term/Name	Organization	Description/Definition
CFITF	CISA's Countering Foreign Influence Task Force (CFITF)	Department of Homeland Security (DHS) Task Force under the Cybersecurity & Infrastructure Security Agency (CISA) which brought together DHS components, including DHS Intelligence and Analysis and others to look at the broader foreign influence and disinformation challenge based on the U.S. intelligence community's 2017 assessment of foreign influence. In 2021, the CFITF name was changed to Mis-, Dis-. and Malinformation Team ("MDM Team").
CIP	Center for an Informed Public	University of Washington's Center for an Informed Public's mission is to resist strategic misinformation, promote an informed society and strengthen democratic discourse. One of the four founding members of the EIP.
CIS	Center for Internet Security (CIS)	CIS is a CISA-funded, nonprofit that channeled reports of mis- and disinformation from state and local government officials to social media platforms.
CISA	The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency	The Cybersecurity & Infrastructure Security Agency (CISA), a component of the Department of Homeland Security, has stated that one of its goals is to build "resiliency to foreign influence operations and disinformation . . . in close partnership with the interagency, private sector, academia, and international stakeholders."
DFRLab	The Atlantic Council's Digital Forensic Research Lab	The Atlantic Council's DFRlab is dedicated to operationalizing the study of disinformation, tracking information campaigns, exposing attempts to pollute the information space, and building digital resilience. One of the four founding members of the EIP.
DHS I&A	DHS Intelligence and Analysis	DHS I&A specializes in sharing unique intelligence and analysis with operators and decision-makers to identify and mitigate threats to the homeland.
Disinformation		CISA defines disinformation as "deliberately created to mislead, harm, or manipulate a person, social group, organization, or country."

EI-ISAC	Elections Infrastructure Information Sharing & Analysis Center	The EI-ISAC operated as an intermediary between state and local election officials and the social media platforms, offering a centralized reporting mechanism.
EIP	Election Integrity Partnership ("EIP")	Originally named the "Election Disinformation Partnership," the EIP was a collaborative project to develop real-time misinformation response capabilities. The EIP worked with a number of "external stakeholders," including the federal government. The four original members at the EIP were: • Stanford Internet Observatory; • the University of Washington, Center for an Informed Public; • Graphika; and • The Atlantic Council's Digital Forensic Research Lab (DFRLab).
FITF	The FBI's Foreign Influence Task Force (FITF)	In 2017, the Federal Bureau of Investigation (FBI) established the Foreign Influence Task Force (FITF) to identify and counteract malign foreign influence operations targeting the United States.
GEC	Department of State, Global Engagement Center	The GEC is a multi-agency organization housed within the State Department tasked with identifying and combating foreign propaganda and disinformation.
Graphika	Graphika, digital intelligence company	Graphika is a social media analytics platform that specializes in monitoring online networks as well as content to provide insights on the spread of information.
Hale, Geoff	Senior CISA official	
Jira	Jira Software system	Jira is a software system used to create tickets to assist with project management. The EIP used JIRA tickets to track and share misinformation reports with large social media companies, the government, and other parties.
Krebs, Chris	Former CISA Director	
Malinformation		CISA defines malinformation as "based on fact, but used out of context to mislead, harm, or manipulate."
MDM		Misinformation, Disinformation, and Malinformation

MDM Subcommittee	CISA Cybersecurity Advisory Committee's (CSAC) Subcommittee on "Protecting Critical Infrastructure from Misinformation & Disinformation"	The MDM Subcommittee, which has since disbanded, played an advisory role, and consisted of Big Tech executives, former federal government officials, and academic misinformation "experts." The MDM Subcommittee meetings featured CISA participants.
MDM Team (CISA)	CISA's Mis-, Dis, and Malinformation Team (formerly CISA's Countering Foreign Influence Task Force (CFITF)	In January 2021, CISA transitioned its Countering Foreign Influence Task Force to promote more flexibility to focus on general MDM, or so-called "Mis-, Dis-, and Malinformation." According to CISA's website in February 2023, the MDM team was "charged with building national resilience to MDM and foreign influence activities." CISA publicly posted that "[f]oreign and domestic threat actors use MDM campaigns to cause chaos, confusion, and division."
Misinformation		CISA defines misinformation as "false, but not created or shared with the intention of causing harm."
MS-ISAC	Multi-State Information Sharing & Analysis Center	MS-ISAC is a joint-CISA supported collaboration with the Center for Internet Security (CIS) designed to serve as the central cybersecurity resource for the nation's state, local, territorial, and tribal (SLTT) governments.
Scully, Brian	Former Head of CISA's CFITF (later MDM team)	
SIO	Stanford Internet Observatory	SIO is a cross-disciplinary laboratory, within Stanford University's Cyber Policy Center, for the study of abuse in information technologies, with a focus on the misuse of social media.
Stamos, Alex	SIO Director; former Chief Security Officer at Facebook	

I. CISA'S ROLE IN THE CREATION OF THE EIP

The Election Integrity Partnership (EIP) was established in July 2020, and consisted of the nation's self-described "leading institutions focused on understanding misinformation and disinformation in the social media landscape: the Stanford Internet Observatory, the University of Washington's Center for an Informed Public (CIP), Graphika, and the Atlantic Council's Digital Forensic Research Lab."[16] According to the EIP's postmortem report about its censorship activities during the 2020 election cycle, the EIP's goals included "[i]dentify[ing] misinformation before it goes viral," and "flag[ging] policy violations to [social media] platforms."[17]

Led by Stanford, the EIP was devised and founded in close coordination with CISA, a little-known agency within the Department of Homeland Security (DHS), created less than two years earlier.[18] Stanford and others, in collaboration with the federal government, established the EIP for the express purpose of violating Americans' civil liberties: because no federal agency "has a focus on, or authority regarding, election misinformation originating from domestic sources within the United States," there is "a critical gap for non-governmental entities to fill."[19] CISA and Stanford created the EIP to bridge this "critical gap"—an unconstitutional workaround for unconstitutional censorship.

A. CISA's Precursor Censorship Efforts

The creation of EIP did not occur in a vacuum. Before EIP's origination in the summer of 2020, CISA was directly or indirectly involved with the operation or consideration of at least three other "misinformation" reporting channels: (1) switchboarding; (2) the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC); and (3) a "Misinformation Reporting Portal" to be operated by the Center for Internet Security (CIS), a non-profit funded in part by CISA.[20]

The constitutional defects with these reporting channels notwithstanding, CISA and "disinformation" experts recognized that they needed another avenue to monitor and remove Americans' speech in the lead-up to the 2020 election. The EIP served that role, functioning in the words of the head of EIP (and former Chief Security Office at Facebook) Alex Stamos as the "one-stop shop for local election officials, *DHS*, and voter protection organizations" to work

[16] ELECTION INTEGRITY P'SHIP, THE LONG FUSE: MISINFORMATION AND THE 2020 ELECTION, at 2 (Eden Beck, ed., 2021).
[17] *Id*. at 6.
[18] *Id*. at 2*; see also* STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A "CYBERSECURITY" AGENCY COLLUDED WITH BIG TECH AND "DISINFORMATION" PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).
[19] ELECTION INTEGRITY P'SHIP, *supra* note 16, at v.
[20] *See generally* STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A "CYBERSECURITY" AGENCY COLLUDED WITH BIG TECH AND "DISINFORMATION" PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).

directly with social media platforms to censor the speech of American political candidates and commentators.[21]

1. Switchboarding, Disclaimers, and the Threat of Government Retaliation

"Switchboarding" describes the federal government's practice of referring requests for the removal of content on social media from state and local election officials to the relevant platforms.[22] CISA personnel involved in the agency's switchboarding operation have described it as a "resource intensive" process.[23] Documents and information obtained by the Committee and the Select Subcommittee reveal that CISA knew serious legal and constitutional concerns were implicated by switchboarding (a process DHS Secretary Mayorkas testified that CISA no longer participates in).[24] CISA's inclusion of a lengthy—and ever-changing—legal disclaimer betrays that internally the agency understood that there were serious legal questions with the federal government's engaging in this type of direct communication with social media platforms regarding Americans' posts and content. Though the disclaimer ostensibly served as a written commitment against government retaliation, ironically, CISA's disclaimer actually spelled out how the federal government's multi-agency approach to censorship provided a number of avenues for government retaliation if the companies did not comply.

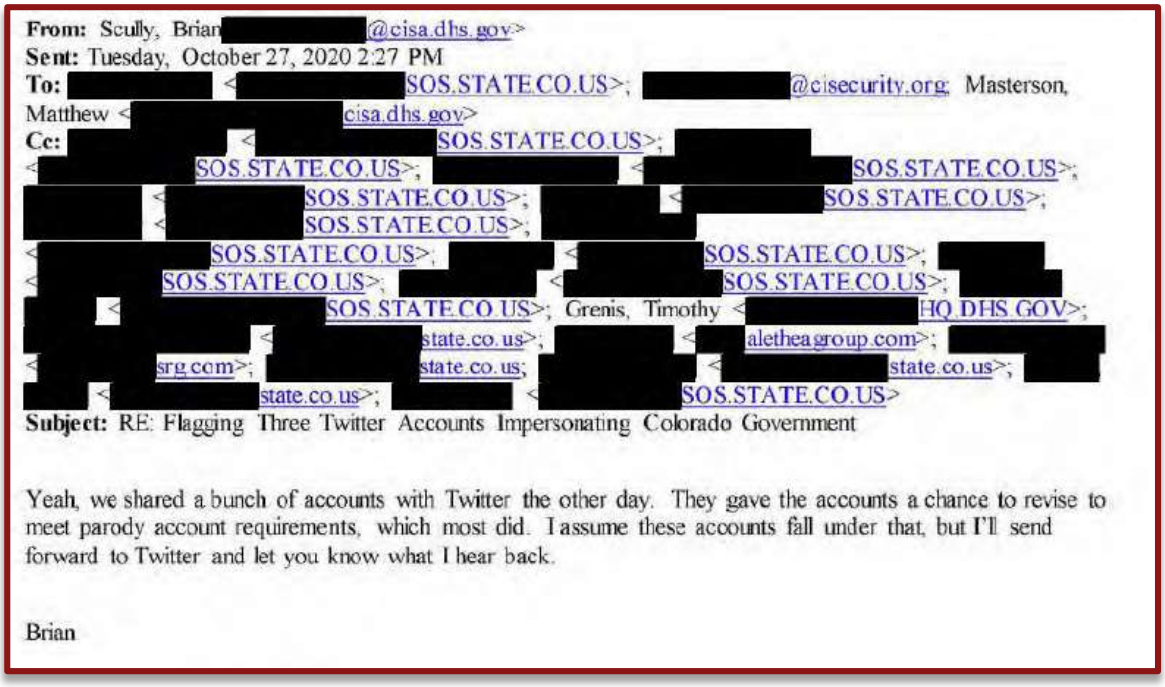
DHS's efforts to assist with the reporting of "mis- and disinformation" on social media platforms pre-date the creation of CISA. Former CISA Director Christopher Krebs testified in a transcribed interview with the Committee and Select Subcommittee that CISA's predecessor, the National Protection and Programs Directorate (NPPD), engaged in switchboarding prior to the creation of CISA.[25] After CISA's creation, switchboarding continued throughout the 2020 election cycle, but was discontinued for the 2022 election.[26]

DHS—in litigation and before the Committee—has insisted that CISA's "switchboarding" role was only that of an intermediary facilitating the sharing of reports, but not playing a substantive role in the "misinformation" reporting process. For example, DHS Secretary Mayorkas testified to the Committee in July 2023 that "what it amounted to was serving as an intermediary between election officials and social media companies; *we were not making a judgment*."[27] Head of CISA's Countering Foreign Influence Task Force, Brian Scully, testified during his deposition in *Missouri v. Biden* that switchboarding was "CISA's role in forwarding reporting received from election officials . . . to social media platforms."[28] But documents obtained by the Committee and Select Subcommittee reveal that "switchboarding"

---

[21] Email from Alex Stamos to Nextdoor employee (Aug. 4, 2020, 4:33 PM) (on file with the Comm.).
[22] Missouri v. Biden, No. 3:22-cv-01213 (W.D. La. 2022), ECF No. 209 (Deposition of Brian Scully) (hereinafter "Scully Dep.") at 17:1–8.
[23] *Id.* at 62:15–22.
[24] *Hearing on the Oversight of the U.S. Department of Homeland Security Before the H. Comm. on the Judiciary,* 118th Cong. (July 26, 2023).
[25] House Judiciary Committee's Transcribed Interview of Christopher Krebs (Oct. 11, 2023), at 7–8 (on file with the Comm.).
[26] Scully Dep., *supra* note 22, at 21:19–22:14.
[27] *Hearing on the Oversight of the U.S. Department of Homeland Security Before the H. Comm. on the Judiciary,* 118th Cong. (July 26, 2023) (emphasis added).
[28] Scully Dep., *supra* note 22, at 23:24-24:2.

could include more substantive interactions. For example, in one email chain, a senior CISA official explained to the Office of the Colorado Secretary of State how Twitter had handled flagged parody accounts previously and how Twitter is likely to handle the accounts being flagged in that chain.[29] Email exchanges such as this one contradict the descriptions of CISA's "switchboarding" as passive role, and that CISA would weigh in on the substance of the post when communicating directly with large social media platforms.



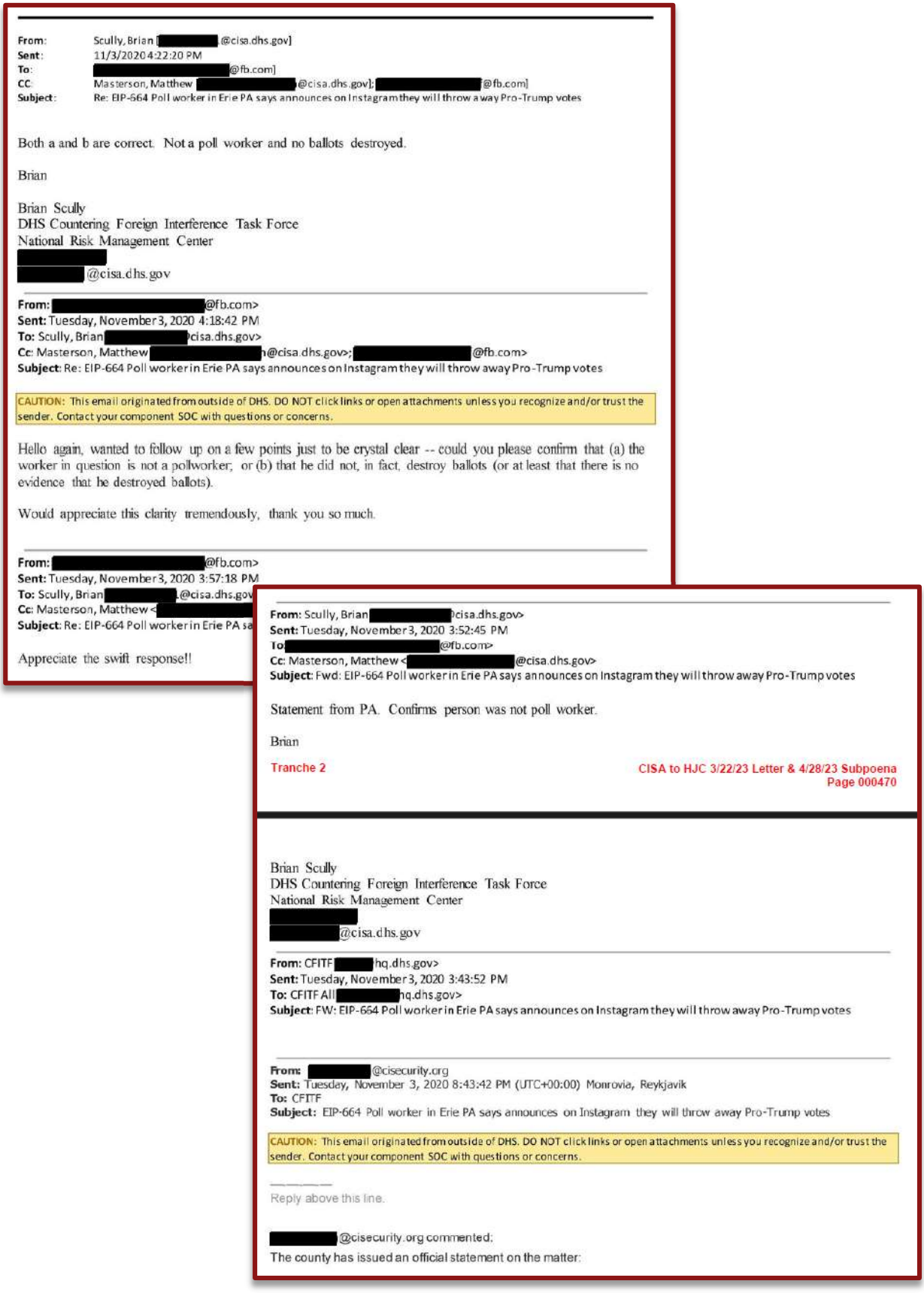
From: Scully, Brian [redacted]@cisa.dhs.gov>
Sent: Tuesday, October 27, 2020 2:27 PM
To: [redacted] <[redacted]SOS.STATE.CO.US>; [redacted]@cisecurity.org; Masterson, Matthew <[redacted]cisa.dhs.gov>
Cc: [redacted] <[redacted]SOS.STATE.CO.US>; [redacted] <[redacted]SOS.STATE.CO.US>; [redacted] <[redacted]SOS.STATE.CO.US>; [redacted] <[redacted]SOS.STATE.CO.US>; [redacted] <[redacted]SOS.STATE.CO.US>; [redacted] <[redacted]SOS.STATE.CO.US>; [redacted] <[redacted]SOS.STATE.CO.US>; [redacted] <[redacted]SOS.STATE.CO.US>; [redacted] <[redacted]SOS.STATE.CO.US>; [redacted] <[redacted]SOS.STATE.CO.US>; [redacted] <[redacted]SOS.STATE.CO.US>; [redacted] <[redacted]SOS.STATE.CO.US>; Grenis, Timothy <[redacted]HQ.DHS.GOV>; [redacted] <[redacted]state.co.us>; [redacted] <[redacted]aletheagroup.com>; [redacted] <[redacted]srg.com>; [redacted] <[redacted]state.co.us>; [redacted] <[redacted]state.co.us>; [redacted] <[redacted]state.co.us>; [redacted] <[redacted]SOS.STATE.CO.US>
Subject: RE: Flagging Three Twitter Accounts Impersonating Colorado Government

Yeah, we shared a bunch of accounts with Twitter the other day. They gave the accounts a chance to revise to meet parody account requirements, which most did. I assume these accounts fall under that, but I'll send forward to Twitter and let you know what I hear back.

Brian

In another example, CISA has an extensive exchange with Facebook in which CISA directly opined on whether a flagged post constituted "misinformation" in the eyes of CISA.[30]

[29] Email from Brian Scully to Colorado state government official, CIS employee, and Matthew Masterson (Oct. 27, 2020, 2:27 PM) (on file with the Comm.).
[30] Email from Brian Scully to Facebook employees and Matthew Masterson (Nov. 3, 2020, 4:22 PM) (on file with the Comm.).



From: Scully, Brian [redacted]@cisa.dhs.gov]
Sent: 11/3/2020 4:22:20 PM
To: [redacted]@fb.com]
CC: Masterson, Matthew [redacted]@cisa.dhs.gov]; [redacted]@fb.com]
Subject: Re: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

Both a and b are correct. Not a poll worker and no ballots destroyed.

Brian

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

From: [redacted]@fb.com>
Sent: Tuesday, November 3, 2020 4:18:42 PM
To: Scully, Brian [redacted]cisa.dhs.gov>
Cc: Masterson, Matthew [redacted]n@cisa.dhs.gov>; [redacted]@fb.com>
Subject: Re: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

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

Hello again, wanted to follow up on a few points just to be crystal clear -- could you please confirm that (a) the worker in question is not a pollworker; or (b) that he did not, in fact, destroy ballots (or at least that there is no evidence that he destroyed ballots).

Would appreciate this clarity tremendously, thank you so much.

From: [redacted]@fb.com>
Sent: Tuesday, November 3, 2020 3:57:18 PM
To: Scully, Brian [redacted].@cisa.dhs.gov
Cc: Masterson, Matthew <[redacted]
Subject: Re: EIP-664 Poll worker in Erie PA sa

Appreciate the swift response!!

From: Scully, Brian [redacted]cisa.dhs.gov>
Sent: Tuesday, November 3, 2020 3:52:45 PM
To: [redacted]@fb.com>
Cc: Masterson, Matthew <[redacted]@cisa.dhs.gov>
Subject: Fwd: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

Statement from PA. Confirms person was not poll worker.

Brian

Tranche 2

CISA to HJC 3/22/23 Letter & 4/28/23 Subpoena
Page 000470

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

From: CFITF [redacted]hq.dhs.gov>
Sent: Tuesday, November 3, 2020 3:43:52 PM
To: CFITF All [redacted]hq.dhs.gov>
Subject: FW: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

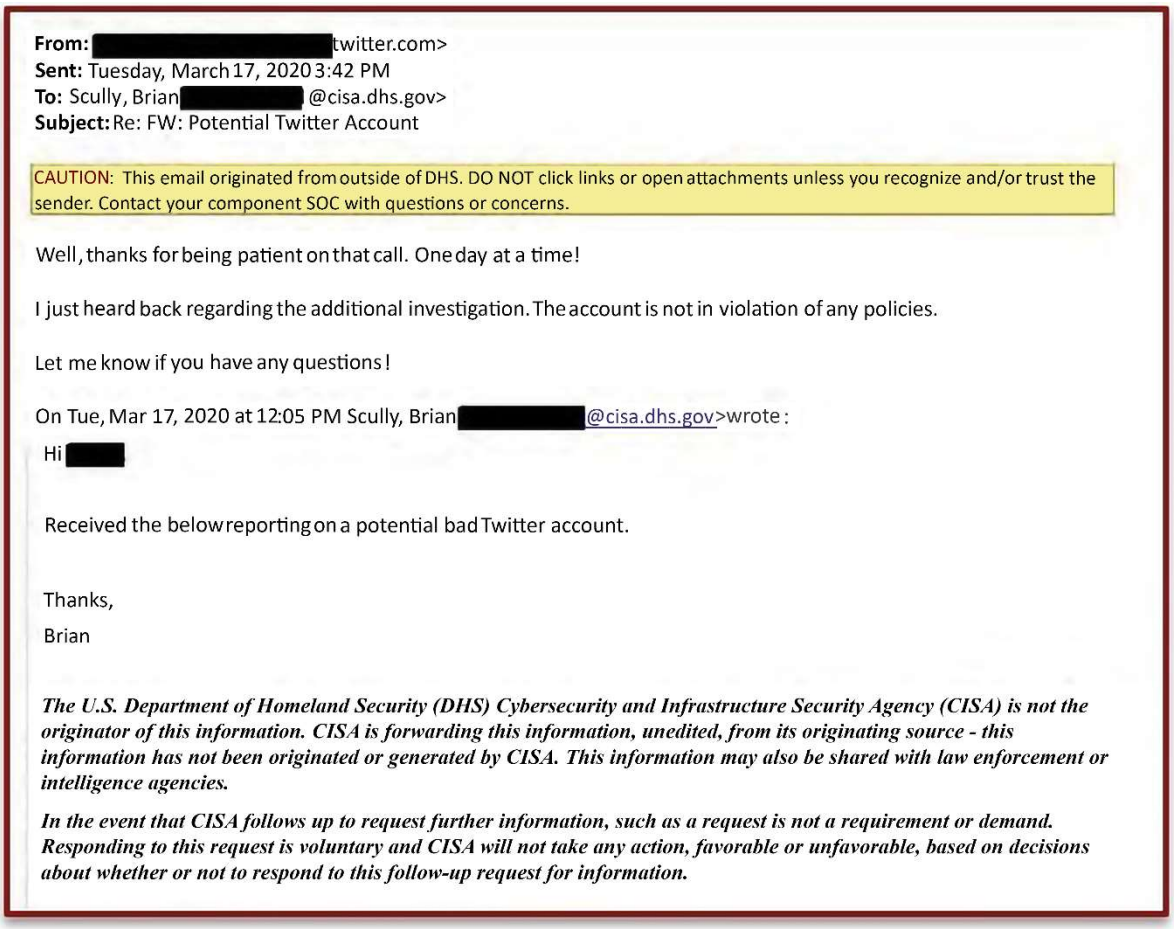
From: [redacted]@cisecurity.org
Sent: Tuesday, November 3, 2020 8:43:42 PM (UTC+00:00) Monrovia, Reykjavik
To: CFITF
Subject: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

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

Reply above this line.

[redacted]@cisecurity.org commented:
The county has issued an official statement on the matter:

In addition to CISA substantively weighing in or commenting on the misinformation reports being shared with the social media companies, CISA could also attempt to influence the social media companies' decisions by deciding whether—and how many times—to follow up. Based on documents obtained by the Committee pursuant to a subpoena to CISA, starting in or around March 2020, used a disclaimer that stated that DHS and CISA were not the "originating source" of the misinformation report, but that the report "may also be shared with law enforcement or intelligence agencies."[31] The disclaimer continued: "In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information."[32]



From: [redacted]twitter.com>
Sent: Tuesday, March 17, 2020 3:42 PM
To: Scully, Brian[redacted] @cisa.dhs.gov>
Subject: Re: FW: Potential Twitter Account

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

Well, thanks for being patient on that call. One day at a time!

I just heard back regarding the additional investigation. The account is not in violation of any policies.

Let me know if you have any questions!

On Tue, Mar 17, 2020 at 12:05 PM Scully, Brian[redacted]@cisa.dhs.gov>wrote:

Hi [redacted]

Received the below reporting on a potential bad Twitter account.

Thanks,

Brian

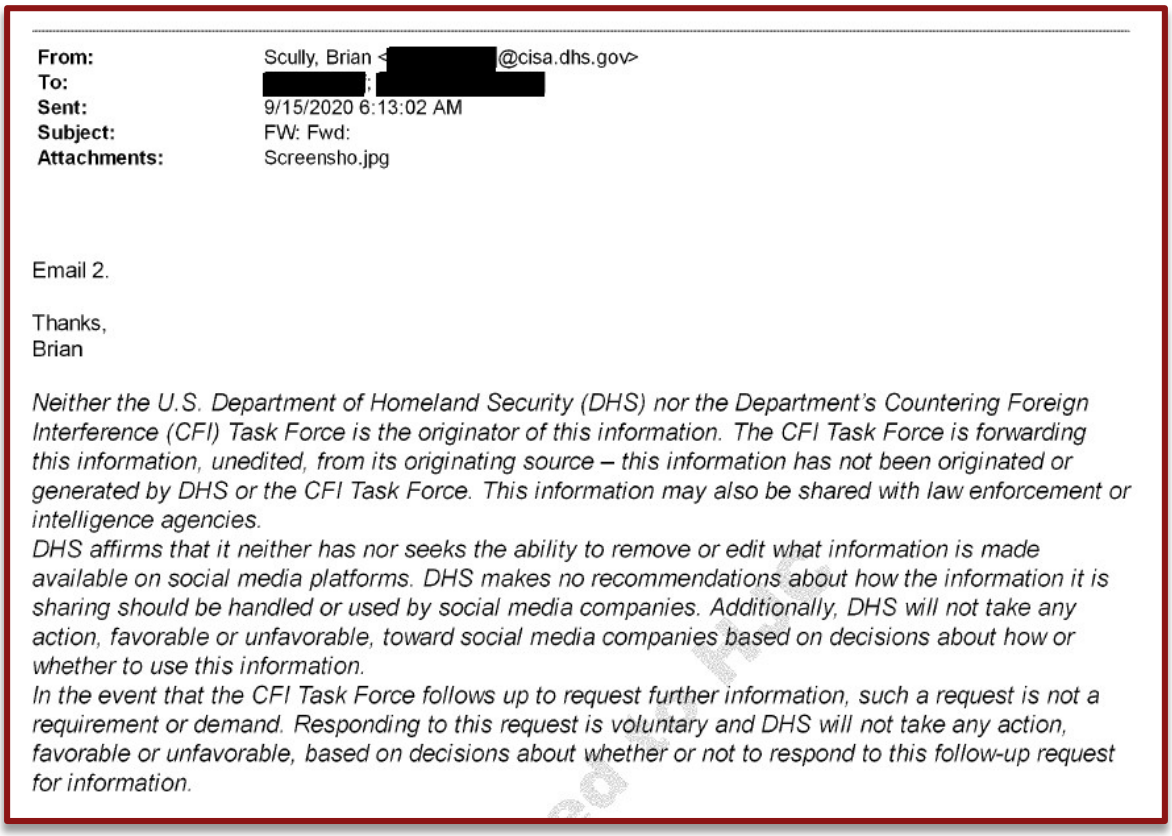
The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source - this information has not been originated or generated by CISA. This information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

In the event that CISA follows up to request further information, such as a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.

By September 2020, CISA's switchboarding emails began to include an extra paragraph declaring that "DHS affirms that it neither has nor seeks the ability to remove what information is made available on social media platforms," but it notably continued to leave open the possibility that the "information may also be shared with law enforcement or intelligence

[31] Email from Brian Scully to Twitter employee (Mar. 17, 2020, 12:05 PM) (on file with the Comm.).
[32] *Id*.

agencies."[33] Put plainly, a lawyer for one of the social media companies would see that DHS *and* law enforcement agencies (such as the FBI) may know the company received the misinformation report, but only DHS committed to not take any unfavorable action against the company based on the company's "decisions about how or whether to use this information"—i.e., the FBI or other law enforcement agencies may take action if the social media company did not censor appropriately.



From: Scully, Brian <[redacted]@cisa.dhs.gov>
To: [redacted]; [redacted]
Sent: 9/15/2020 6:13:02 AM
Subject: FW: Fwd:
Attachments: Screensho.jpg

Email 2.

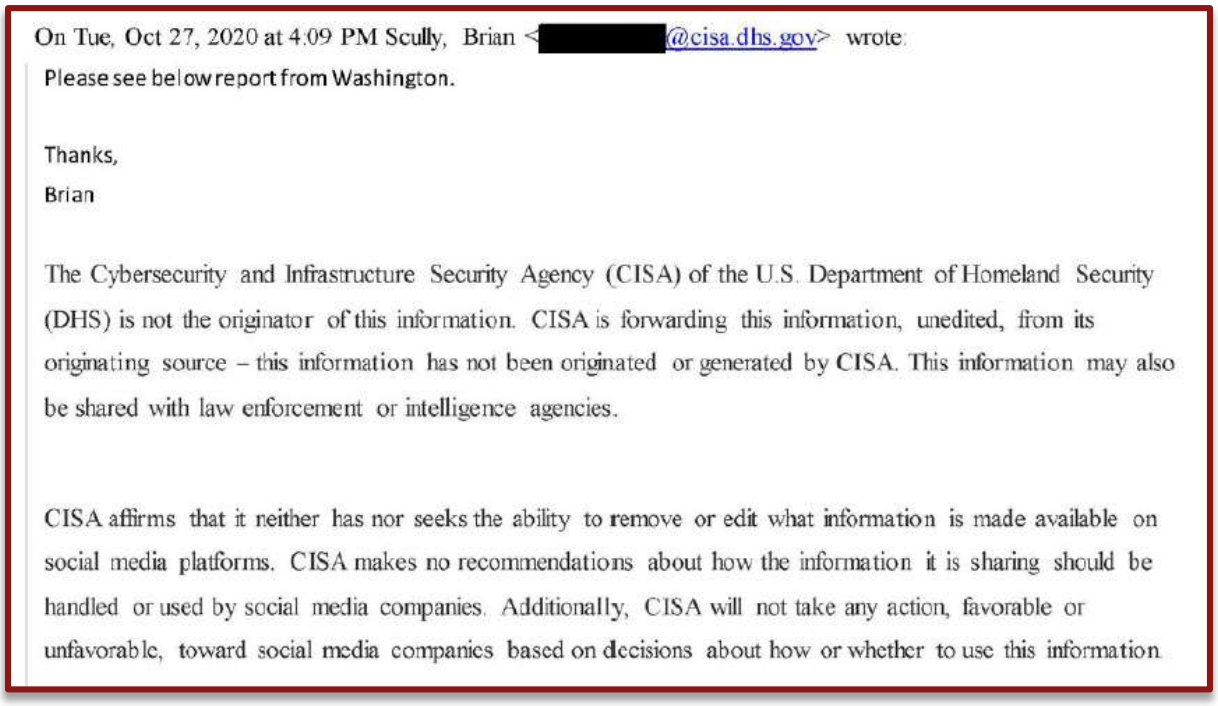
Thanks,
Brian

Neither the U.S. Department of Homeland Security (DHS) nor the Department's Countering Foreign Interference (CFI) Task Force is the originator of this information. The CFI Task Force is forwarding this information, unedited, from its originating source – this information has not been originated or generated by DHS or the CFI Task Force. This information may also be shared with law enforcement or intelligence agencies.
DHS affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. DHS makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, DHS will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.
In the event that the CFI Task Force follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and DHS will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.

The following month, CISA appeared to narrow the language of the disclaimer to state that CISA (rather than all of DHS) would not "take any action favorable or unfavorable, based on decisions about how or whether to use this information."[34] The more limited disclaimer now stated only that: "*CISA* affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. *CISA* makes no recommendations about how the information it is sharing should be handled or used by social media companies."[35] CISA also removed an entire paragraph of its disclaimer referencing follow-up communications.[36] In the ongoing federal litigation *Missouri v. Biden*, the Biden Administration cited the inclusion of this disclaimer as evidence that CIS and the EIP were not "'censorship partners' with CISA" and that the disclaimer supported companies to apply their policies

[33] Email from Brian Scully to Facebook employees (Sept. 15, 2020, 6:13 AM) (on file with the Comm.).
[34] *Cf. id.*; email from Brian Scully to Facebook employees (Oct. 1, 2020, 2:23 PM) (on file with the Comm.).
[35] *See, e.g.*, Brian Scully to Facebook employees (Oct. 1, 2020, 2:23 PM) (on file with the Comm.) (emphases added).
[36] *Id.*

"independently."[37] But as described above, rather than ensure that companies did not feel pressure, the revised disclaimer emphasized that CISA would involve law enforcement agencies and that CISA would not (or could not) commit that law enforcement agencies would not take an unfavorable action based on how the social media platforms decided to respond to the misinformation report.



On Tue, Oct 27, 2020 at 4:09 PM Scully, Brian <[redacted]@cisa.dhs.gov> wrote:

Please see below report from Washington.

Thanks,
Brian

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

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

On or around October 28, 2020, CISA reinstated the paragraph in its disclaimer concerning follow-up communications.[38] To date, CISA has produced to the Committee and Select Subcommittee over twenty email threads dated between October 1, and October 27, in which the disclaimer does not include the paragraph regarding follow-up communications.[39]

[37] *See, e.g.*, Defs.' Resp. to Pls.' Proposed Findings of Fact in Supp. of Their Mot. for Prelim. Inj. at 547–548, Missouri v. Biden, No. 3:22-cv-01213 (W.D. La. 2022), ECF No. 264-9.
[38] *Cf.* email from Brian Scully to Twitter employee (Oct. 27, 2020, 4:09 PM) (on file with the Comm.); email from Brian Scully to Twitter employee (Oct. 28, 2020, 6:29 PM) (on file with the Comm.).
[39] *See, e.g.*, email from Brian Scully to Facebook employees (Oct. 2, 2020, 7:29 PM) (on file with the Comm.); email from CFITF to Facebook employees (Oct. 20, 2020, 2:11 PM) (on file with the Comm.).

On Wed, Oct 28, 2020 at 6:29 PM Scully, Brian <[redacted]cisa.dhs.gov> wrote:

Please see below report from Washington.

Regards,

Brian

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

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

In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.

Unsurprisingly, around this time, CISA began to follow-up with social media platforms about posts the agency had flagged, as seen in the example below.[40]

From: [redacted] [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7F0C5C3963484338B25437EAAE765D72-[redacted]
Sent: 10/19/2020 6:34:53 PM
To: [redacted]@twitter.com]
CC: [redacted]twitter.com]; [redacted]@twitter.com; [redacted]twitter.com; [redacted] [redacted]hq.dhs.gov]
Subject: RE: FW: Case #CIS-MIS000041: Twitter misinformation regarding ballots dumped on highway in CT

Checking in to see if there is anything that can be shared in regards to this reported incident.
[redacted]

From: [redacted]twitter.com>
Sent: Thursday, October 15, 2020 11:42 AM
To: [redacted]@cisa.dhs.gov>
Cc: [redacted]@twitter.com>; [redacted]@twitter.com; [redacted]twitter.com; [redacted] [redacted]@hq.dhs.gov>
Subject: Re: FW: Case #CIS-MIS000041: Twitter misinformation regarding ballots dumped on highway in CT

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

Hi [redacted]
We will ask the team to review.

Best.
[redacted]

[40] Email from DHS official to Twitter employee (Oct. 19, 2020, 6:34 PM) (on file with the Comm.).

During his transcribed interview with the Committee, Matt Masterson, a former senior cybersecurity advisor at CISA, testified that there had been internal deliberations with CISA's lawyers regarding the disclaimer and whether constitutional rights and civil liberties were implicated:

> Q. Do you recall any discussions during your tenure at CISA regarding if there are any constitutional implications if CISA's work engaged with, we'll say, misinformation, disinformation, malinformation, coming from domestic actors?
>
> A. I don't recall a specific conversation around that. I recall that – obviously that CISA lawyers were involved, as I previously indicated, for instance, around the disclaimer conversation, including lawyers around constitutional and civil liberties. But I don't know or recall the specifics of any given conversation around that.[41]

CISA's inclusion of a disclaimer discussing whether CISA's frequent emails should be interpreted as a request or whether the refusal to respond could result in "unfavorable" action is evidence that, at a minimum, the lawyers within DHS felt compelled to consider whether the practice of switchboarding was legally and constitutionally sound. But rather than end the practice (as CISA apparently did by the 2022 election), in the fall of 2020, CISA decided to push forward with its censorship efforts, appending a meaningless email disclaimer as a weak and transparent attempt to satisfy the glaring First Amendment concerns.

Crucially, CISA's disclaimer included the ominous line: "This information may also be shared with law enforcement or intelligence agencies."[42] Whereas the disclaimer stated that "*CISA* will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information," the disclaimer makes no such guarantee about retaliation from the "law enforcement or intelligence agencies" with whom CISA may share the relevant social media content.[43]

The threat of law-enforcement reprisal is amplified by the fact that the FBI would inform social media companies when CISA provided the FBI a "misinformation" report. The Committee and Select Subcommittee have obtained multiple documents that show that social media companies were aware that CISA was sharing information with federal intelligence and law enforcement agencies, including the FBI.[44]

From: Elvis Chan
Date: Sunday, October 4, 2020 at 2:31 PM
To: [redacted]
Subject: Tipper & Next FITF Meeting
Facebook folks,
First, I got a tip from CISA that there is a Facebook page that is misleading voters about time, place, and manner of voting, as well as trying to elicit Facebook user information. Please review and take whatever steps you deem appropriate. We would appreciate it if you let us know whether you take any actions based on this referral.

[41] House Judiciary Committee's Transcribed Interview of Matthew Masterson (Sept. 26, 2023), at 81.
[42] *See, e.g.*, email from Brian Scully to Facebook employees (Oct 2, 2020, 7:29 PM) (on file with the Comm.).
[43] *Id*. (emphasis added).
[44] *See, e.g.*, email from Elvis Chan to Facebook employees (Oct. 4, 2020, 2:31 PM) (on file with the Comm.).

In other words, CISA's disclaimer indicated to the social media companies that CISA, law enforcement, and intelligence agencies may receive the misinformation report, but the disclaimer stated only that *CISA* would not retaliate against the social media companies if they failed to censor the flagged content. CISA made no promises with respect to what the FBI or one of the intelligence agencies may do. And the social media companies were well aware that CISA was forwarding some subset of the reports to the FBI (if not other federal law enforcement or intelligence agencies).

In his interview before the Committee and Select Subcommittee, former Facebook executive Alex Stamos testified that involvement with a law enforcement agency such as the FBI was necessarily more worrisome for companies than CISA, explaining that "you can't have a casual chat with an FBI agent when you're an executive at a company. It's not safe. You end up with a $3,000-an-hour row of people sitting next to you."[45] Mr. Stamos continued:

> Q. And what do you mean you can't have a casual conversation with the FBI? Why is that?
>
> A. I think defense attorneys would tell you that FBI agents are always looking out – you might feel like you're having a friendly conversation with them, but you never know if you're actually the target. And I think there has been a number of situations which companies have tried to engage the FBI because they were victims of, say, a cybercrime, and then they end up getting punished or their executives getting punished . . . . And so, you know, dealing with a law enforcement agency that has coercive powers is just a risky thing to do if you're part of some big organization and some other – there might be some investigation involving the organization that you don't even know about.
>
> Q. That perspective you just shared with respect to the FBI, do you think it was widely shared by the executives at Facebook when you were at the company?
>
> A. Certainly, the policy of the company was that an executive could not talk to the FBI without attorneys present . . . .
>
> Q. . . . Even if the government represents that the interests are aligned, it could be the case that, later on, the government changes its mind. Is that right?
>
> A. Yes.
>
> Q. Okay. And this fact is well known by tech executives?

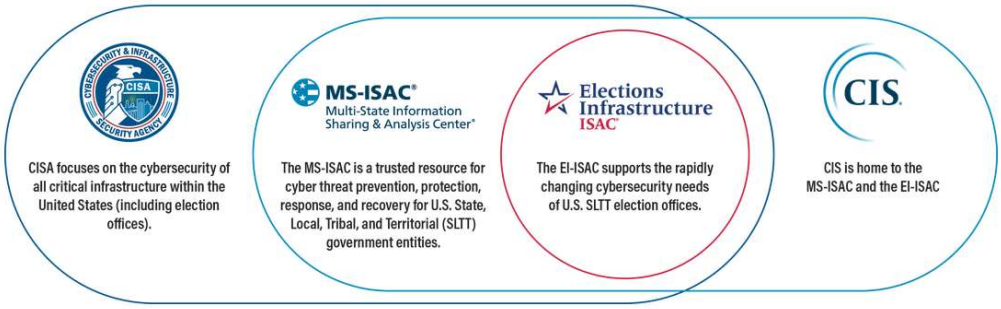
[45] House Judiciary Committee's Transcribed Interview of Alex Stamos (June 23, 2023), at 188 (on file with the Comm.).

A. Yes. And I think all executives of all public companies understand that *there's lots of parts of the government that can punish you for activity that you thought was appropriate*.[46]

So why did CISA engage in this "resource intensive" process of switchboarding, go through the trouble of writing and rewriting a disclaimer in hopes of sidestepping serious constitutional concerns, and directly involve federal law enforcement and intelligence agencies? Because CISA wanted flagged content removed, and switchboarding provided an effective means to do so. During his deposition in *Missouri v. Biden*, senior CISA official Brian Scully admitted that CISA did, in fact, have an understanding that its reporting would lead to removal by the platforms.[47]

2. EI-ISAC

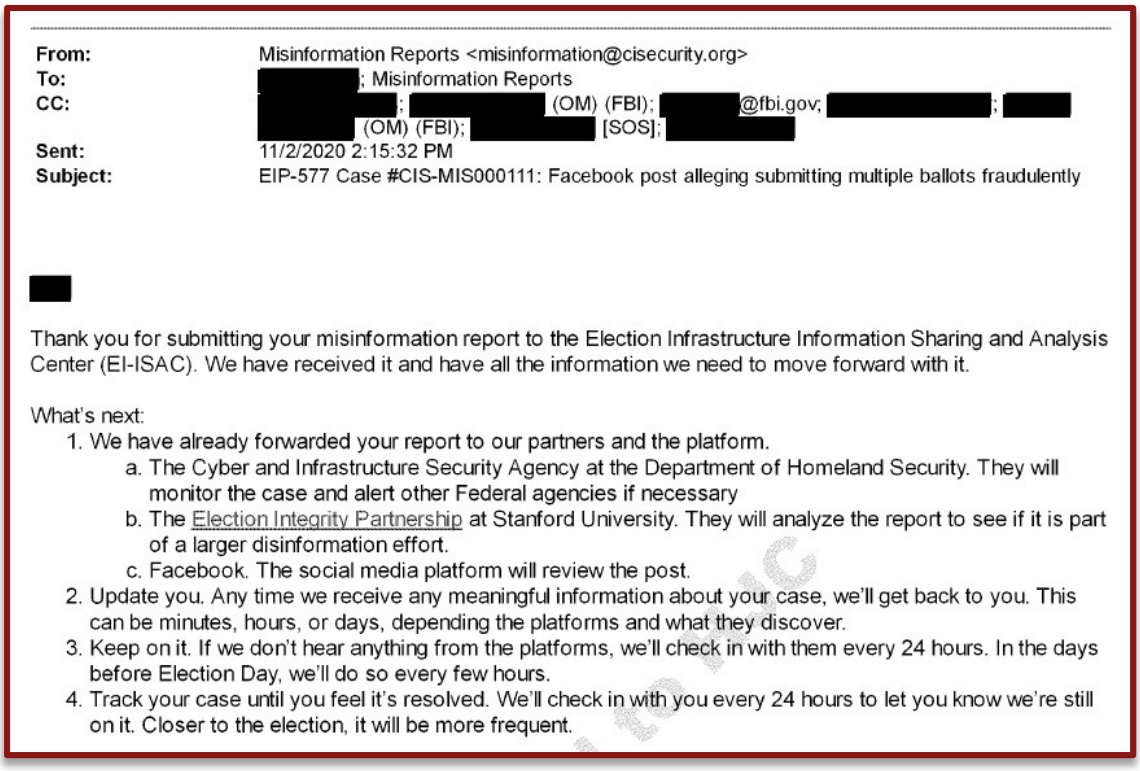
The Center for Internet Security (CIS) is a non-profit organization based in New York, which was established "in partnership with the U.S. Cybersecurity and Infrastructure Security Agency (CISA)."[48] CIS operates the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), which is funded alongside the Multi-State Information Sharing and Analysis Center (MS-ISAC) to the tune of $27 million for FY 2024 for the two ISACs.[49] The EI-ISAC is an information-sharing channel used by state and local election officials to report alleged "mis- and disinformation" to social media platforms.[50] During the 2018 midterm election cycle, all fifty states were participating in the EI-ISAC.[51] Moreover, according to witness testimony to the Committee and Select Subcommittee, EI-ISAC employees are considered CIS employees.[52]



According to the EIP's report, in the 2020 election cycle, "the EI-ISAC served as a singular conduit for election officials to report false or misleading information to platforms."[53] The report also explained EI-ISAC's function in relation to CIS: "By serving as a one-stop

[46] *Id*. at 188–190 (emphasis added).
[47] Scully Dep., *supra* note 22, at 17:15–21.
[48] *EI-ISAC Charter*, CENTER FOR INTERNET SEC., https://www.cisecurity.org/ei-isac/ei-isac-charter (last visited Nov. 3, 2023).
[49] DEP'T OF HOMELAND SEC., DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY BUDGET OVERVIEW FISCAL YEAR 2024 CONGRESSIONAL JUSTIFICATION, at 37 (2023).
[50] ELECTION INTEGRITY P'SHIP, *supra* note at 16, at 13.
[51] House Judiciary Committee's Transcribed Interview of Christopher Krebs (Oct. 11, 2023), at 34.
[52] House Judiciary Committee's Transcribed Interview of Matthew Masterson (Sept. 26, 2023), at 184.
[53] ELECTION INTEGRITY P'SHIP, *supra* note at 16, at 13.

reporting interface, the EI-ISAC allowed election officials to focus on detecting and countering election misinformation while CIS and its partners reported content to the proper social media platforms."[54] And the report described CISA's role, noting that "the Countering Foreign Influence Task Force (CFITF), a subcomponent of CISA, aided in the reporting process and in implementing resilience efforts to counter election misinformation."[55] The misinformation reports submitted to the EI-ISAC in the lead-up to the 2020 election were "also routed to the EIP ticketing system."[56]



From: Misinformation Reports <misinformation@cisecurity.org>
To: [redacted]; Misinformation Reports
CC: [redacted] (OM) (FBI); [redacted]@fbi.gov; [redacted] (OM) (FBI); [redacted] [SOS]; [redacted]
Sent: 11/2/2020 2:15:32 PM
Subject: EIP-577 Case #CIS-MIS000111: Facebook post alleging submitting multiple ballots fraudulently

[redacted]

Thank you for submitting your misinformation report to the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC). We have received it and have all the information we need to move forward with it.

What's next:

1. We have already forwarded your report to our partners and the platform.
    a. The Cyber and Infrastructure Security Agency at the Department of Homeland Security. They will monitor the case and alert other Federal agencies if necessary
    b. The Election Integrity Partnership at Stanford University. They will analyze the report to see if it is part of a larger disinformation effort.
    c. Facebook. The social media platform will review the post.
2. Update you. Any time we receive any meaningful information about your case, we'll get back to you. This can be minutes, hours, or days, depending the platforms and what they discover.
3. Keep on it. If we don't hear anything from the platforms, we'll check in with them every 24 hours. In the days before Election Day, we'll do so every few hours.
4. Track your case until you feel it's resolved. We'll check in with you every 24 hours to let you know we're still on it. Closer to the election, it will be more frequent.

Like switchboarding, the EI-ISAC operated as an intermediary between state and local election officials and the social media platforms, offering a centralized reporting mechanism in an effort to remove content from social media.[57] For example, on November 2, 2020, a state election official submitted a report of alleged misinformation to the EI-ISAC, which, in turn, forwarded the report to the relevant platform.[58] According to the EI-ISAC's response to the state official, the EI-ISAC also shared the report with both CISA and the EIP.[59]

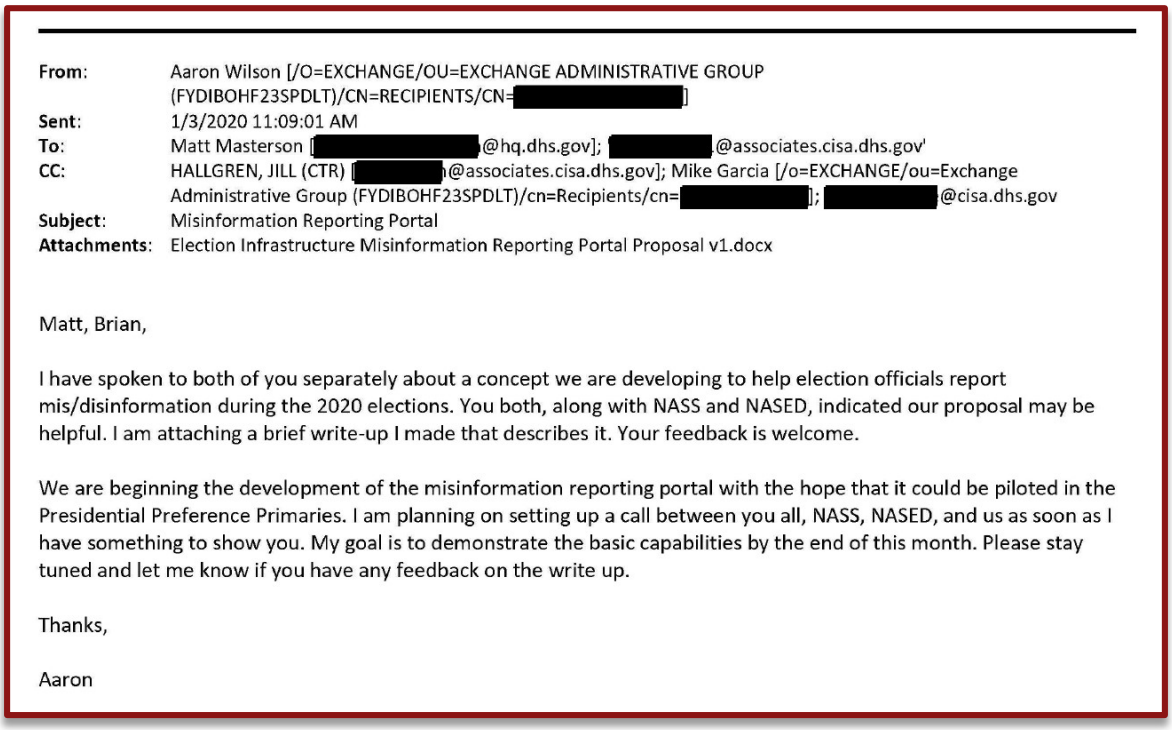
---

[54] *Id.*
[55] *Id*. In January 2021, CISA transitioned its Countering Foreign Influence Task Force to promote more flexibility to focus on general MDM, or so-called "Mis-, Dis-, and Malinformation." According to CISA's website in February 2023, the MDM team was "charged with building national resilience to MDM and foreign influence activities," and its efforts applied to "foreign and domestic" actors.
[56] *Id.*
[57] STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A "CYBERSECURITY" AGENCY COLLUDED WITH BIG TECH AND "DISINFORMATION" PARTNERS TO CENSOR AMERICANS, at 22 (Comm. Print June 26, 2023).
[58] Email from misinformation@cisecurity.org to Iowa state government official (Nov. 2, 2020, 2:15 PM) (on file with the Comm.).
[59] *Id*.

3. Misinformation Reporting Portal

Even with switchboarding and the EI-ISAC, CISA and CIS had discussions internally and with social media companies throughout the first half of 2020 on whether to create a "misinformation reporting portal." Pursuant to multiple subpoenas, the Committee and Select Subcommittee have obtained documents revealing CISA's and CIS's efforts to pursue a third avenue of "misinformation reporting."

As early as January 2020, CISA officials were in discussions with CIS to establish a "misinformation reporting portal."[60] On January 3, Aaron Wilson, the Senior Director of Election Security at CIS, sent an email to senior CISA officials Matt Masterson and Brian Scully, among others, writing: "I have spoken to both of you separately about a concept we are developing to help election officials report mis/disinformation during the 2020 elections. You both . . . indicated our proposal may be helpful."[61] Mr. Wilson indicated that his goal was "to demonstrate the basic capabilities [of the misinformation reporting portal] by the end of this month."[62]



From: Aaron Wilson [/O=EXCHANGE/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[redacted]]
Sent: 1/3/2020 11:09:01 AM
To: Matt Masterson [[redacted]@hq.dhs.gov]; [redacted].@associates.cisa.dhs.gov'
CC: HALLGREN, JILL (CTR) [[redacted]@associates.cisa.dhs.gov]; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; [redacted]@cisa.dhs.gov
Subject: Misinformation Reporting Portal
Attachments: Election Infrastructure Misinformation Reporting Portal Proposal v1.docx

Matt, Brian,

I have spoken to both of you separately about a concept we are developing to help election officials report mis/disinformation during the 2020 elections. You both, along with NASS and NASED, indicated our proposal may be helpful. I am attaching a brief write-up I made that describes it. Your feedback is welcome.

We are beginning the development of the misinformation reporting portal with the hope that it could be piloted in the Presidential Preference Primaries. I am planning on setting up a call between you all, NASS, NASED, and us as soon as I have something to show you. My goal is to demonstrate the basic capabilities by the end of this month. Please stay tuned and let me know if you have any feedback on the write up.

Thanks,

Aaron

[60] Email from Aaron Wilson to Matt Masterson, Jill Hallgren, and Mike Garcia (Jan. 3, 2020, 11:09 AM) (on file with the Comm.).
[61] *Id.*
[62] *Id.*

CIS and CISA's joint efforts were even briefed to law enforcement in January 2020 with CIS reaching out to the FBI, stating that "CIS is *working with DHS* on a misinformation reporting portal. The intent is to build a web portal to manage the reporting of election infrastructure misinformation from local and state election officials to the social media platforms. We are working with our partners at the National Association of Secretaries of States (NASS), National Association of State Election Directors (NASED), *and DHS* to vet this idea. We are currently building a prototype and will have something to show by the first week of February."[63]

From: Aaron Wilson [/O=EXCHANGE/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[redacted]]
Sent: 1/20/2020 2:09:04 PM
To: [redacted]@fbi.gov
CC: Wedekind, Kirby ([redacted]@hq.dhs.gov]; HALLGREN, JILL (CTR) [redacted]@associates.cisa.dhs.gov]; Scully, Brian [redacted]@cisa.dhs.gov]; Josiah, Chad [redacted]@cisa.dhs.gov]; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]
Subject: Misinformation Reporting Portal FBI Briefing

JC,

It was great to meet you last week. As I mentioned, CIS is working with DHS on a misinformation reporting portal. The intent is to build a web portal to manage the reporting of election infrastructure misinformation from local and state election officials to the social media platforms. We are working with our partners at the National Association of Secretaries of States (NASS), National Association of State Election Directors (NASED), and DHS to vet this idea. We are currently building a prototype and will have something to show by the first week of February.

Given the FBI's role, I'd like to bring you up to speed on our efforts and get your feedback on this effort, and hopefully your engagement. Our primary goals are to:

- Provide election officials a single place/POC to report misinformation
- Ease the burden on election officials when they go to report the misinformation
- Collect the information necessary for the FBI, DHS, and social media platforms to do their jobs
- Expedite and enhance the process by which social media companies are made aware of the misinformation
- Provide visibility about what election officials are reporting to: other election officials, DHS, NASS, NASED, FBI, etc.
- Facilitate information sharing between election officials about what they are seeing, what to look out for, etc.
- Provide meaningful feedback to election officials on the status of their misinformation reports

Are you available for a call this week to discuss more?

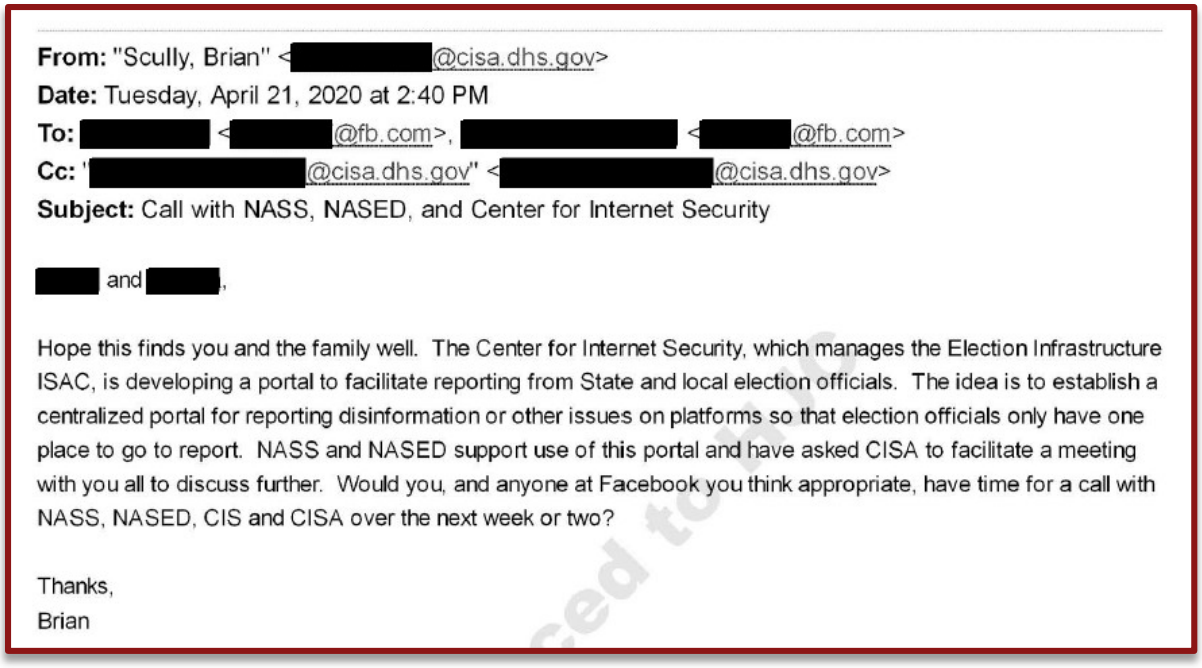
Thanks,

Aaron

CISA assumed an active role in promoting CIS's proposal for a misinformation reporting portal, facilitating meetings between the relevant third-party non-profits and social media platforms. On April 21, 2020, for example, Brian Scully sent an email to two Facebook employees, in which Scully wrote: "The idea is to establish a centralized portal for reporting dis-

[63] Email from Aaron Wilson to Kirby Wedekind, Jill Hallgren, Brian Scully, Chad Josiah, and Mike Garcia (Jan. 20, 2020, 2:09 PM) (on file with the Comm.) (emphases added).

information or other issues on platforms so that election officials only have one place to go to report."[64]



From: "Scully, Brian" <[redacted]@cisa.dhs.gov>
Date: Tuesday, April 21, 2020 at 2:40 PM
To: [redacted] <[redacted]@fb.com>, [redacted] <[redacted]@fb.com>
Cc: '[redacted]@cisa.dhs.gov" <[redacted]@cisa.dhs.gov>
Subject: Call with NASS, NASED, and Center for Internet Security

[redacted] and [redacted],

Hope this finds you and the family well. The Center for Internet Security, which manages the Election Infrastructure ISAC, is developing a portal to facilitate reporting from State and local election officials. The idea is to establish a centralized portal for reporting disinformation or other issues on platforms so that election officials only have one place to go to report. NASS and NASED support use of this portal and have asked CISA to facilitate a meeting with you all to discuss further. Would you, and anyone at Facebook you think appropriate, have time for a call with NASS, NASED, CIS and CISA over the next week or two?

Thanks,
Brian

But planning for a CIS-CISA misinformation reporting portal had hit a roadblock by May 2020. According to the internal notes of a call between Facebook employees and DHS personnel regarding a "Misinformation Reporting Portal," "*DHS cannot openly endorse the portal*, but has behind-the-scenes signaled that [the National Association of Secretaries of State]/[the National Association of State Election Directors] has told them it would be easier for many states to have 'one reporting channel' and CISA and its ISAC would like to have incoming the same time that the platforms do."[65] Less than two months later, the EIP would be established to serve that very purpose.

[64] Email from Brian Scully to Facebook employees (Apr. 21, 2020, 2:40 PM) (on file with the Comm.).
[65] Email from Facebook employee to Facebook employees (May 31, 2020, 10:44 AM) (on file with the Comm.) (emphasis added)

From: [redacted] <[redacted]@fb.com>
Sent: Sunday, May 31, 2020 10:44 AM
To: [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>
Cc: [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>
Subject: CIS & NASS/NASED & DHS Call

Team,

Wanted to share a read-out from our call late Friday with DHS, NASS & NASSED. Great job by Eva & Saleela.

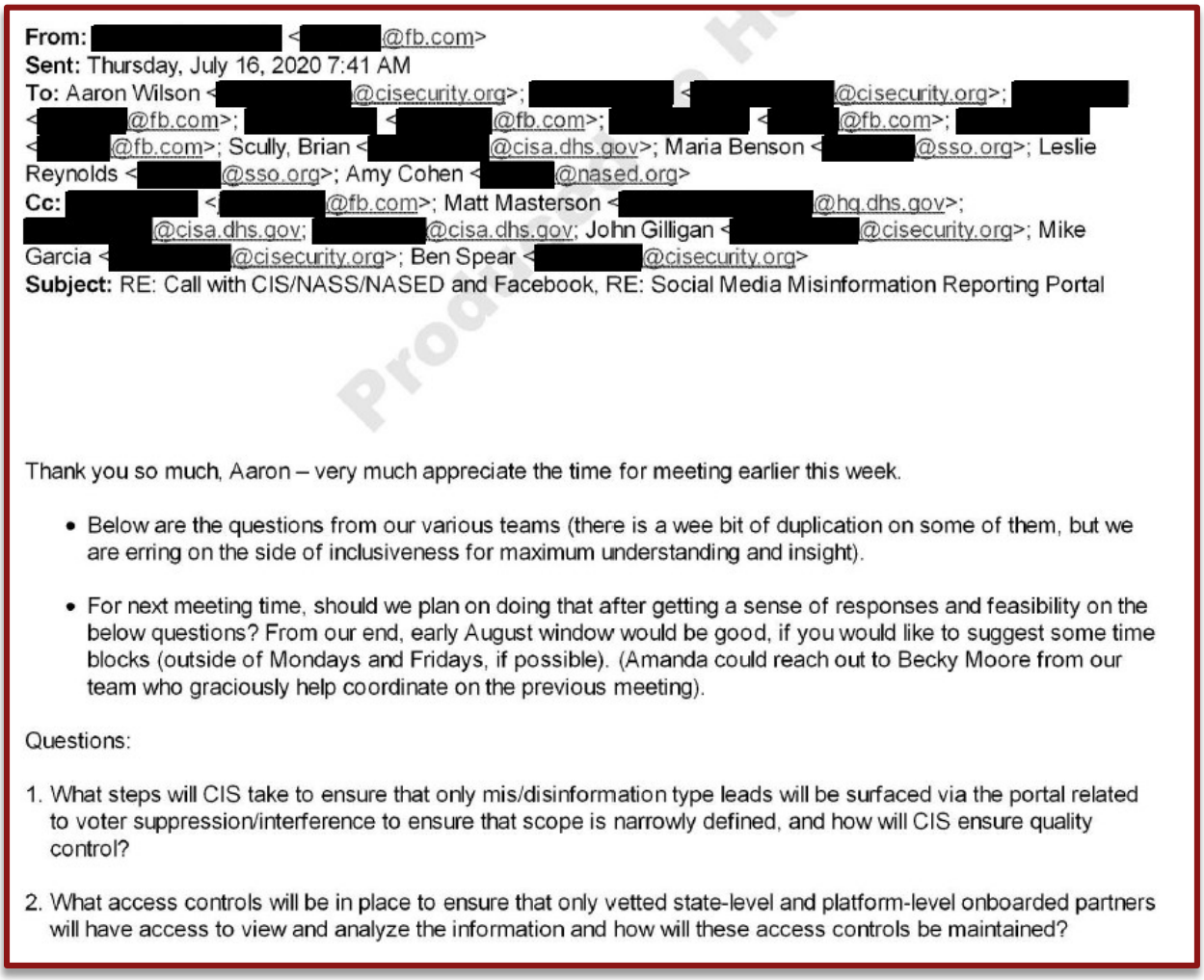
No action for us now; however, we will reconvene after a Beta test of their proposed reporting portal in the next few weeks.

Best,
Sandy

TL;DR: On May 29, U.S. Public Policy ([redacted]), P&G Outreach ([redacted]), and Security Policy ([redacted]) met with DHS, the Center for Internet Security, and NASS/NASED about a **"Misinformation Reporting Portal" that CIS is developing for state and local-level elections officials to report mis/disinformation and IO-type activity concerning election interference to the platforms**, with a focus on Facebook, Twitter, and Google. Following a beta test CIS will do in Florida, Colorado, North Carolina, and Rhode Island in early June, they would like to do a demo for Facebook. Internally, Facebook would prefer our independent reporting channel which makes us an industry leader, and was reported as successful by all parties on this call and is monitored 24/7, but we are aware that if the majority group moves towards a centralized channel, there are PR challenges for not participating.

- **Highlights:**
  - DHS cannot openly endorse the portal, but has behind-the-scenes signaled that NASS/NASED has told them it would be easier for many states to have "one reporting channel" and CISA and its ISAC would like to have incoming the same time that the platforms do.
  - CIS is in discussions with **Twitter** to gauge their interest, and it was unclear what engagement has been with **Google**.
  - CIS is talking with **Graphika**, which has said it is interested in nationwide trends that the reporting portal may reveal.
  - CIS is talking with the **Belfer Center**, which is developing an "IO Playbook & Training" that may be released in the coming months before November 2020.
  - NASS/NASED is supportive, but **not all the states are onboard** – CIS said they would like to launch with platforms supportive and engaged and bring states incrementally along.
  - **CIS would like some sort of API with Facebook –** such a set up may be impossible, and CrowdTangle, if this progresses, may be the way to go.

Social media companies, including Facebook and Twitter, engaged in months-long discussions with CIS over its proposal for a misinformation portal. After being initially briefed on the proposal in May, Facebook employees sent a list of questions to CIS about the portal on July 16, 2020.[66]



From: [redacted] <[redacted]@fb.com>
Sent: Thursday, July 16, 2020 7:41 AM
To: Aaron Wilson <[redacted]@cisecurity.org>; [redacted] <[redacted]@cisecurity.org>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; Scully, Brian <[redacted]@cisa.dhs.gov>; Maria Benson <[redacted]@sso.org>; Leslie Reynolds <[redacted]@sso.org>; Amy Cohen <[redacted]@nased.org>
Cc: [redacted] <[redacted]@fb.com>; Matt Masterson <[redacted]@hq.dhs.gov>; [redacted]@cisa.dhs.gov; [redacted]@cisa.dhs.gov; John Gilligan <[redacted]@cisecurity.org>; Mike Garcia <[redacted]@cisecurity.org>; Ben Spear <[redacted]@cisecurity.org>
Subject: RE: Call with CIS/NASS/NASED and Facebook, RE: Social Media Misinformation Reporting Portal

Thank you so much, Aaron – very much appreciate the time for meeting earlier this week.

- Below are the questions from our various teams (there is a wee bit of duplication on some of them, but we are erring on the side of inclusiveness for maximum understanding and insight).
- For next meeting time, should we plan on doing that after getting a sense of responses and feasibility on the below questions? From our end, early August window would be good, if you would like to suggest some time blocks (outside of Mondays and Fridays, if possible). (Amanda could reach out to Becky Moore from our team who graciously help coordinate on the previous meeting).

Questions:

1. What steps will CIS take to ensure that only mis/disinformation type leads will be surfaced via the portal related to voter suppression/interference to ensure that scope is narrowly defined, and how will CIS ensure quality control?

2. What access controls will be in place to ensure that only vetted state-level and platform-level onboarded partners will have access to view and analyze the information and how will these access controls be maintained?

[66] Email from Facebook employee to CIS employees, Facebook employees, CISA officials, NASS employees, and NASED employees (July 16, 2020, 7:41 AM) (on file with the Comm.).

3. To what extent can the U.S. government, other platforms, and others view back and forth with platforms and also cross-platform content or escalations, and how will this be controlled? Are you open to a version of the portal that forwards intake to a platform email, with further back and forth being handled just between the platform and the reporter (but the initial report is available to other states/platforms/portal users).

4. How will portal access be determined?

5. What is the limit on the number of people and organizations who will have access to the portal?

6. What is the data retention period for the portal?

7. Is it the expectation that the portal will be a short-term or long-term project?

8. How will the portal sort information so that it is of importance and properly sorted by various terms of service depending on the platform, so that recipients of the information will be able to triage it quickly and deconflict?

9. What quality control measures will be in place to ensure that the escalations sent to the portal are not "noise" and will be properly described and not duplicative, and also not repeats of the same already-escalated content, to avoid burdening resource, operational, and engineering bandwidth during a very high-stakes election cycle where timely response and action will be critical?

10. Is the expectation that the portal will replace the dedicated 1:1 reporting channels maintained by the platforms, either in the short or long terms?

11. How will the portal advise whether or not a particular escalation has already been reported to the platforms and avoid sending an alert when such an escalation has already been made?

12. To what extent can the portal be used to surface trends and patterns across platforms that can be shared, if of value, while maintaining direct platform-level communication from the states?

13. Which states are not yet onboarded to the portal and what is the plan for those states?

14. How will the portal be made user-friendly for the wide range of users?

15. Who will train users on the portal, trouble shoot, and provide tech support for the portal?

16. What will turn around time, both before the election, and on election day, for portal support and login issues?

17. How long does it take to approve access to the portal? Will there be expedited review closer to the election?

18. How will the portal enable platform-specific back and forth?

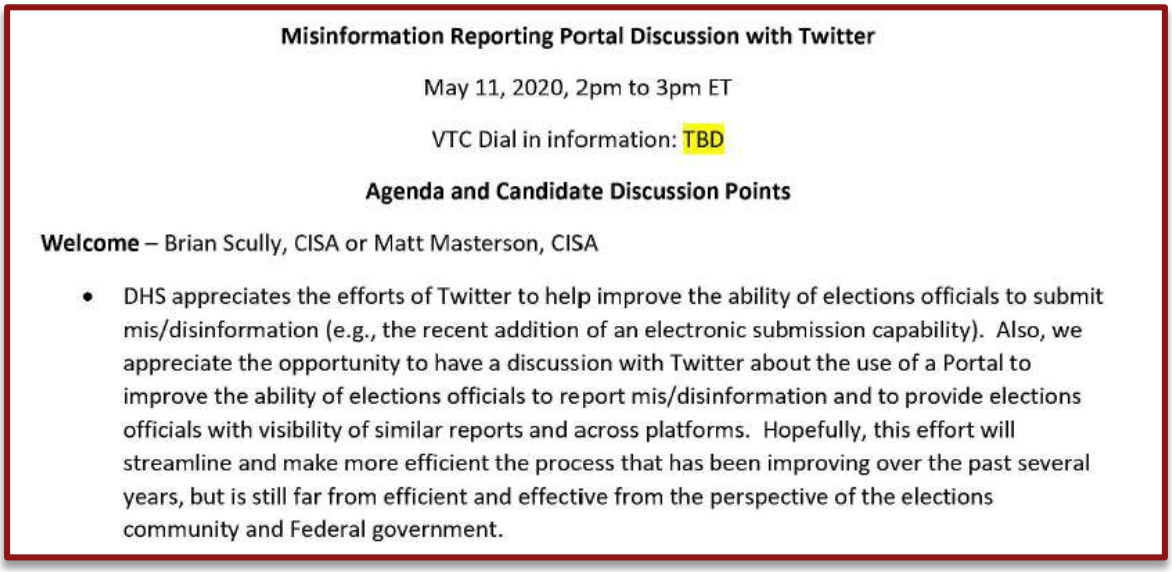
19. Will the portal provide links and not just screenshots to enable swift actioning of context?

20. How does the portal plan to surface behavior-type or pattern-type signals, as opposed to discrete pieces of content?

21. How will the portal prevent the same escalation being reported multiple times by multiple sources?

22. Aside from receiving "intake," and evaluating that, if possible, pursuant to platform-specific terms of service, what are other expectations of engagement from the platforms?

Twitter was initially briefed on the portal in May 2020, according to a meeting agenda produced to the Committee.[67] Per the agenda, "DHS appreciates the efforts of Twitter to help improve the ability of elections officials to submit mis/disinformation."[68] The agenda was also indicative of CISA's and the broader federal government's effort to enhance the censorship operation through the portal: "Hopefully, this effort will streamline and make more efficient the process that has been improving over the past several years, but is still far from efficient and effective from the perspective of the elections community and Federal government."[69] As indicated in the excerpt below, top CISA officials were scheduled to open this discussion on CIS's potential misinformation reporting portal.[70]



Misinformation Reporting Portal Discussion with Twitter

May 11, 2020, 2pm to 3pm ET

VTC Dial in information: TBD

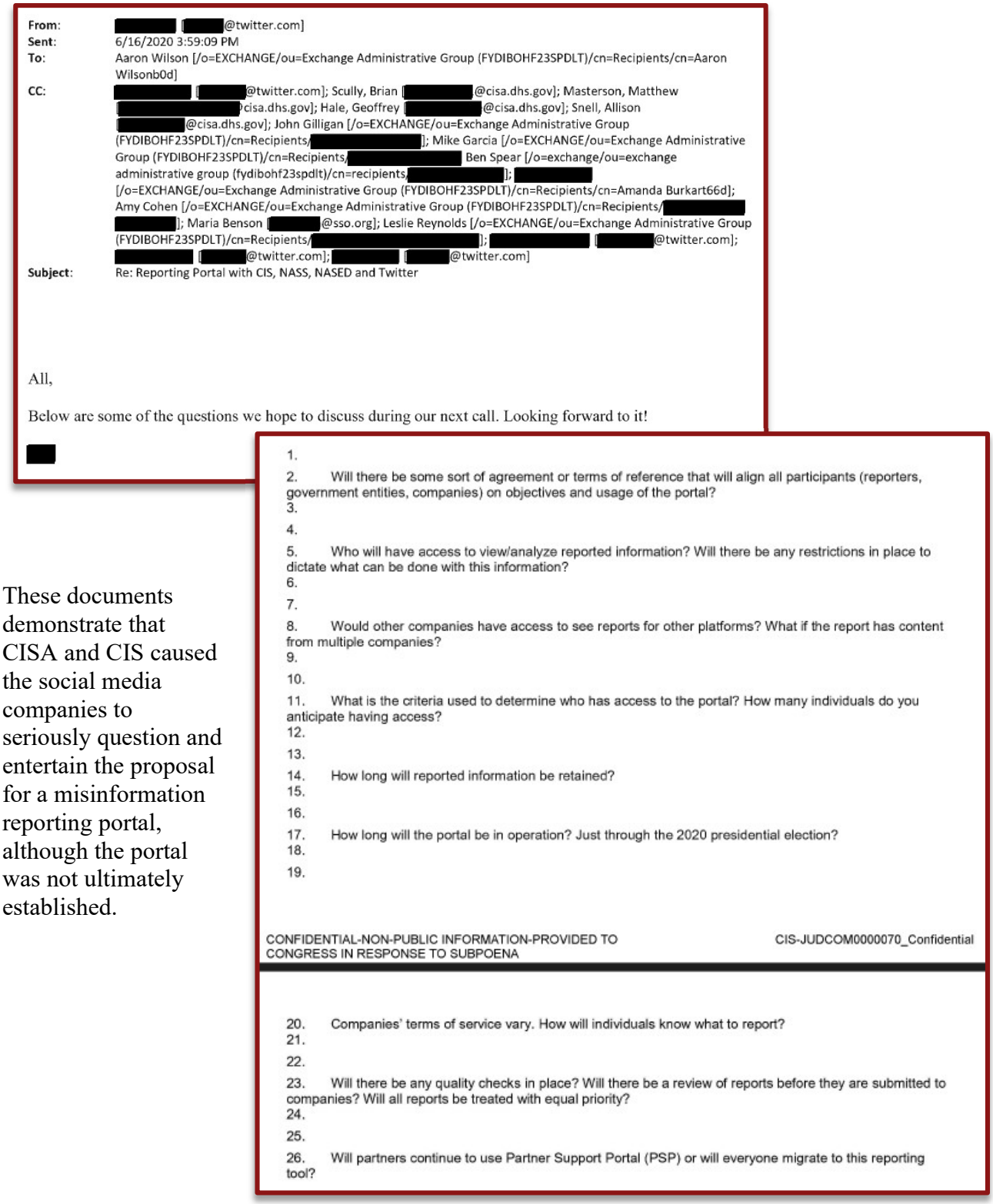
Agenda and Candidate Discussion Points

Welcome – Brian Scully, CISA or Matt Masterson, CISA

- DHS appreciates the efforts of Twitter to help improve the ability of elections officials to submit mis/disinformation (e.g., the recent addition of an electronic submission capability). Also, we appreciate the opportunity to have a discussion with Twitter about the use of a Portal to improve the ability of elections officials to report mis/disinformation and to provide elections officials with visibility of similar reports and across platforms. Hopefully, this effort will streamline and make more efficient the process that has been improving over the past several years, but is still far from efficient and effective from the perspective of the elections community and Federal government.

[67] Center for Internet Sec., Misinformation Reporting Portal Discussion with Twitter (May 11, 2020) (unpublished meeting agenda) (on file with the Comm.).
[68] *Id*.
[69] *Id*.
[70] *Id*.

Like Facebook, Twitter also submitted a list of questions to CIS regarding the portal.[71]



From: [redacted] [redacted]@twitter.com]
Sent: 6/16/2020 3:59:09 PM
To: Aaron Wilson [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Aaron Wilsonb0d]
CC: [redacted] [redacted]@twitter.com]; Scully, Brian [redacted]@cisa.dhs.gov]; Masterson, Matthew [redacted]@cisa.dhs.gov]; Hale, Geoffrey [redacted]@cisa.dhs.gov]; Snell, Allison [redacted]@cisa.dhs.gov]; John Gilligan [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[redacted]]; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[redacted] Ben Spear [/o=exchange/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/[redacted]]; [redacted] [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Amanda Burkart66d]; Amy Cohen [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[redacted]]; Maria Benson [[redacted]@sso.org]; Leslie Reynolds [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[redacted]]; [redacted] [[redacted]@twitter.com]; [redacted] [[redacted]@twitter.com]; [redacted] [[redacted]@twitter.com]
Subject: Re: Reporting Portal with CIS, NASS, NASED and Twitter

All,

Below are some of the questions we hope to discuss during our next call. Looking forward to it!

[redacted]

1.
2. Will there be some sort of agreement or terms of reference that will align all participants (reporters, government entities, companies) on objectives and usage of the portal?
3.
4.
5. Who will have access to view/analyze reported information? Will there be any restrictions in place to dictate what can be done with this information?
6.
7.
8. Would other companies have access to see reports for other platforms? What if the report has content from multiple companies?
9.
10.
11. What is the criteria used to determine who has access to the portal? How many individuals do you anticipate having access?
12.
13.
14. How long will reported information be retained?
15.
16.
17. How long will the portal be in operation? Just through the 2020 presidential election?
18.
19.

CONFIDENTIAL-NON-PUBLIC INFORMATION-PROVIDED TO CONGRESS IN RESPONSE TO SUBPOENA

CIS-JUDCOM0000070_Confidential

20. Companies' terms of service vary. How will individuals know what to report?
21.
22.
23. Will there be any quality checks in place? Will there be a review of reports before they are submitted to companies? Will all reports be treated with equal priority?
24.
25.
26. Will partners continue to use Partner Support Portal (PSP) or will everyone migrate to this reporting tool?

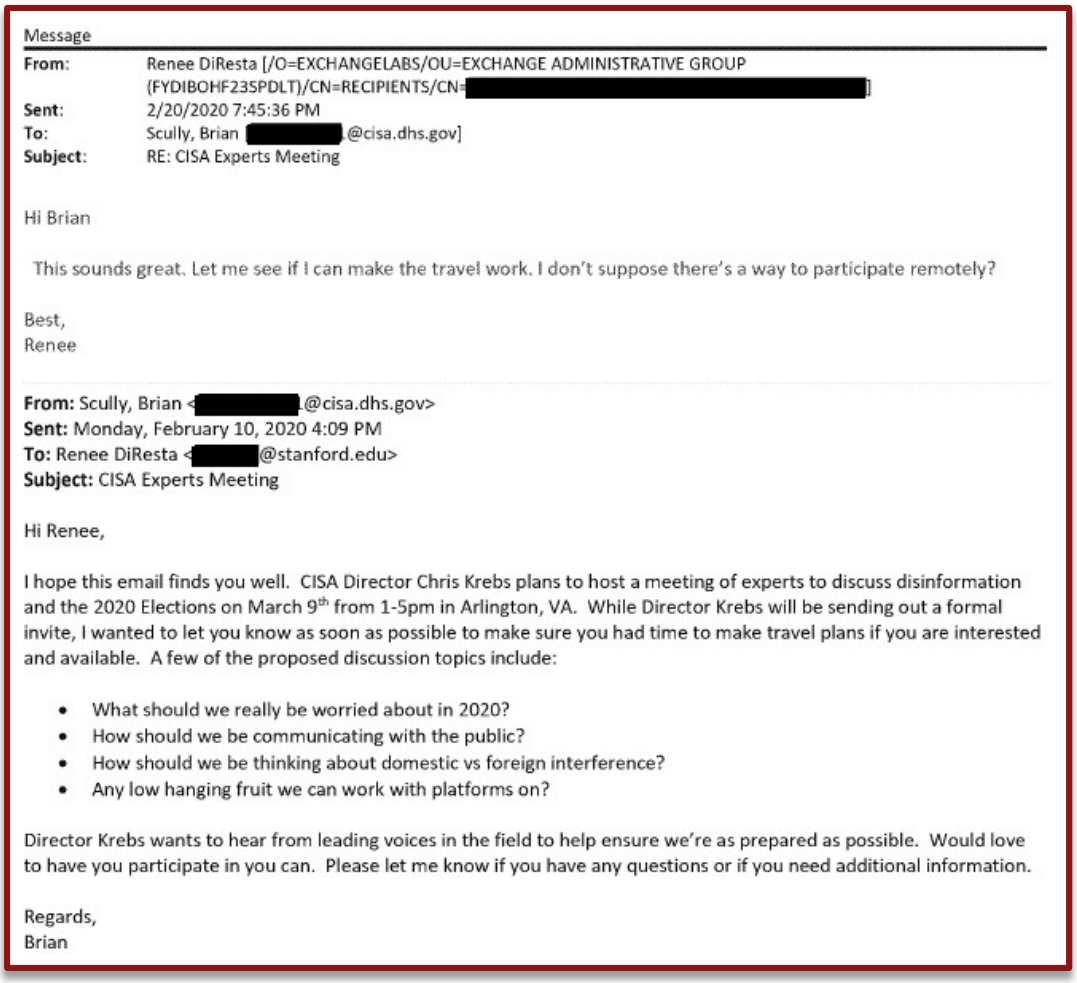
These documents demonstrate that CISA and CIS caused the social media companies to seriously question and entertain the proposal for a misinformation reporting portal, although the portal was not ultimately established.

[71] Email from Twitter employee to Aaron Wilson, Brian Scully, Matthew Masterson, and other personnel from CISA, CIS, and Twitter (June 16, 2020, 3:59 PM).

4. CISA Did Not Distinguish Foreign and Domestic Actors on Social Media

Finally, in the midst of operating or considering up to three different avenues of "misinformation reporting" (switchboarding, EI-ISAC, and the "misinformation reporting portal"), by early 2020, CISA had dropped any pretense of focusing only on foreign disinformation, openly discussing how to best monitor and censor the speech of Americans.

On February 20, 2020, Brian Scully, the head of CISA's Countering Foreign Influence Task Force (CFITF), sent an email to the SIO's Renée DiResta, inviting her to a meeting hosted by CISA Director Krebs, "to discuss disinformation and the 2020 Elections."[72] Scully provided a list of agenda items in the email, including: "How should we be thinking about domestic vs foreign interference?" and "Any low hanging fruit we can work with platforms on?"[73]



Message

From: Renee DiResta [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[redacted]]
Sent: 2/20/2020 7:45:36 PM
To: Scully, Brian [redacted]@cisa.dhs.gov]
Subject: RE: CISA Experts Meeting

Hi Brian

This sounds great. Let me see if I can make the travel work. I don't suppose there's a way to participate remotely?

Best,
Renee

From: Scully, Brian <[redacted]@cisa.dhs.gov>
Sent: Monday, February 10, 2020 4:09 PM
To: Renee DiResta <[redacted]@stanford.edu>
Subject: CISA Experts Meeting

Hi Renee,

I hope this email finds you well. CISA Director Chris Krebs plans to host a meeting of experts to discuss disinformation and the 2020 Elections on March 9th from 1-5pm in Arlington, VA. While Director Krebs will be sending out a formal invite, I wanted to let you know as soon as possible to make sure you had time to make travel plans if you are interested and available. A few of the proposed discussion topics include:

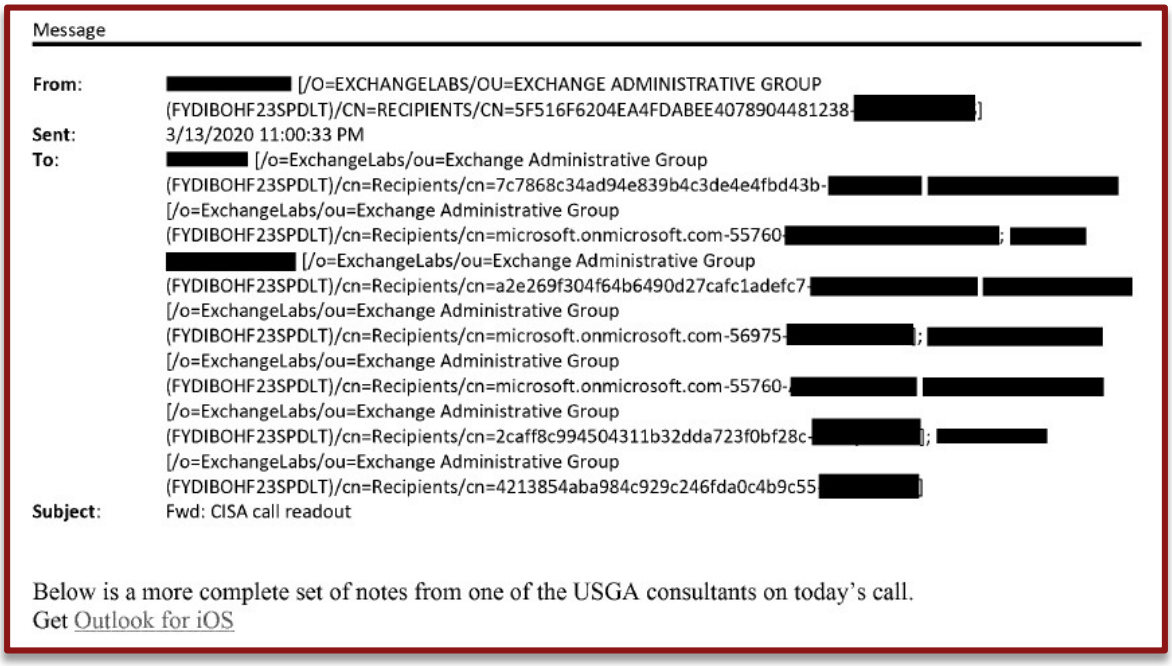
- What should we really be worried about in 2020?
- How should we be communicating with the public?
- How should we be thinking about domestic vs foreign interference?
- Any low hanging fruit we can work with platforms on?

Director Krebs wants to hear from leading voices in the field to help ensure we're as prepared as possible. Would love to have you participate in you can. Please let me know if you have any questions or if you need additional information.

Regards,
Brian

[72] Email from Brian Scully to Renée DiResta (Feb. 20, 2020, 4:09 PM) (on file with the Comm.).
[73] *Id*.

The COVID-19 pandemic reinforced CISA's desire to take a more active role in surveillance and censorship on social media. On March 13, 2020, Director Krebs participated in a "broad stakeholder conference call to provide an update regarding current activities related to" COVID-19.[74]

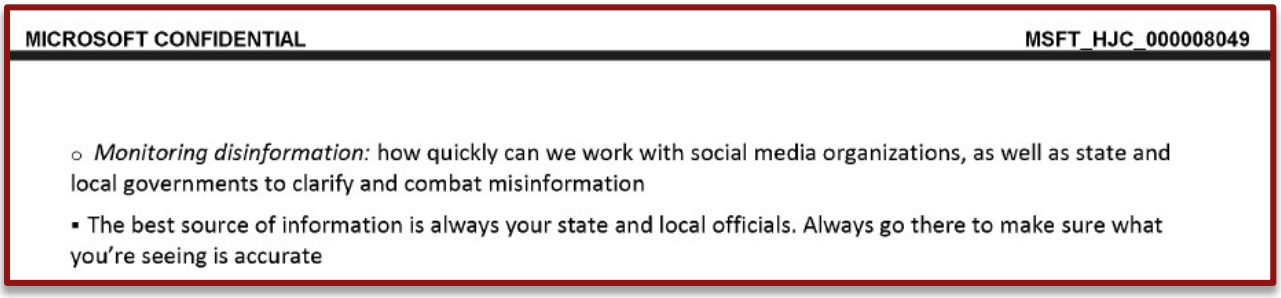


Message

From: [redacted] [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=5F516F6204EA4FDABEE4078904481238-[redacted]]
Sent: 3/13/2020 11:00:33 PM
To: [redacted] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=7c7868c34ad94e839b4c3de4e4fbd43b-[redacted]
[/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=microsoft.onmicrosoft.com-55760-[redacted]; [redacted]
[redacted] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=a2e269f304f64b6490d27cafc1adefc7-[redacted]
[/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=microsoft.onmicrosoft.com-56975-[redacted]; [redacted]
[/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=microsoft.onmicrosoft.com-55760-[redacted]
[/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=2caff8c994504311b32dda723f0bf28c-[redacted]; [redacted]
[/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=4213854aba984c929c246fda0c4b9c55[redacted]]
Subject: Fwd: CISA call readout

Below is a more complete set of notes from one of the USGA consultants on today's call.
Get Outlook for iOS

According to internal Microsoft notes from the call obtained by the Committee pursuant to a subpoena to Microsoft, Krebs identified "Monitoring disinformation" as one of four "core lines of effort," asking "how quickly can we work with social media organizations, as well as state and local governments to clarify and combat misinformation."[75]



MICROSOFT CONFIDENTIAL **MSFT_HJC_000008049**

- *Monitoring disinformation:* how quickly can we work with social media organizations, as well as state and local governments to clarify and combat misinformation
  - The best source of information is always your state and local officials. Always go there to make sure what you're seeing is accurate

[74] Email from Microsoft employee to Microsoft employees (Mar. 13, 2020, 11:00 PM) (on file with the Comm.).
[75] *Id.*

In his testimony before the Committee, Krebs stated unequivocally on multiple occasions that CISA did not treat content on social media differently based on its domestic or foreign origin.[76] At one point, Krebs even described the name of CISA's Countering Foreign Influence Task Force as "a misnomer."[77] Krebs further testified:

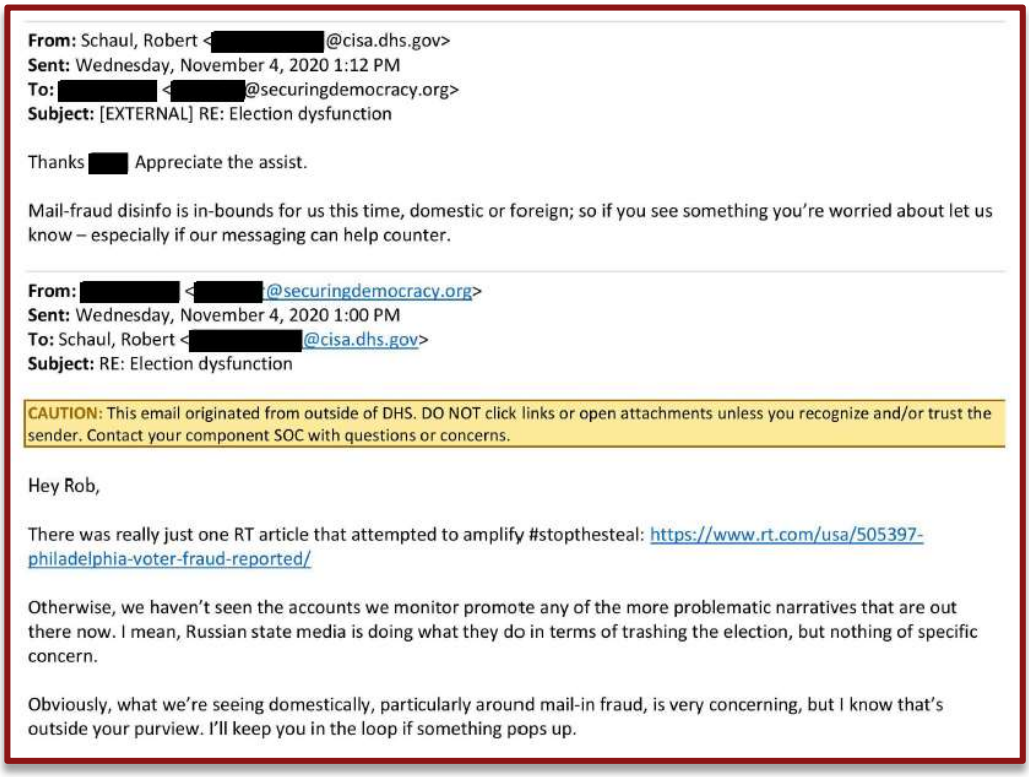
> Q. Was there an effort during this time to try to determine if the source was domestic or foreign?
>
> A. So, we certainly would look to the intelligence community if they made a determination on foreign threat actor intelligence. But, again, as these things pop up, things like "hammer and scorecard," it doesn't necessarily matter whether it's foreign or domestic. Again, our authorities are rooted in the Homeland Security Act, which enables us to act on domestic or foreign threats. And, again, they don't come waving a flag . . . .[78]

Director Krebs reiterated CISA's approach of treating foreign and domestic activity on social media in the same way in the context of CISA's "Rumor Control" initiative.[79] For example, he testified:

> Q. When did these discussions regarding domestic influence first start?
>
> A. I don't recall.
>
> Q. Okay. Were they ongoing by the beginning of 2020?
>
> A. Again, I don't recall the moment in time or the periods of time within which we were thinking about the distinction between domestic and foreign interference. Again, I think this gets to, as we ultimately saw with rumor control, narratives are narratives, and we're providing explanation on how the things actually work. So, again, it would not matter if it was foreign or domestic for the context, again, of rumor control.[80]

[76] *See e.g.*, House Judiciary Committee's Transcribed Interview of Christopher Krebs (Oct. 11, 2023), at 153–154 (on file with the Comm.).
[77] *Id*. at 154.
[78] *Id*.
[79] One telling exchange between Mr. Krebs's counsel and counsel for the Committee regarded whether any authorities limit CISA's rights to combat so-called "misinformation." Mr. Krebs's counsel appeared to dismiss what role, if any, the First Amendment played with respect to restricting CISA's ability to monitor and censor speech, demanding that the Committee cite a legal authority "other than the First Amendment" to justify its line of questioning. House Judiciary Committee's Transcribed Interview of Chris Krebs (Oct. 11, 2023), at 162 (on file with the Comm.).
[80] *Id*. at 104.

Up to and through the 2020 election, CISA considered its authority as extending to domestic speech, not just foreign disinformation.[81]



From: Schaul, Robert <[redacted]@cisa.dhs.gov>
Sent: Wednesday, November 4, 2020 1:12 PM
To: [redacted] <[redacted]@securingdemocracy.org>
Subject: [EXTERNAL] RE: Election dysfunction

Thanks [redacted] Appreciate the assist.

Mail-fraud disinfo is in-bounds for us this time, domestic or foreign; so if you see something you're worried about let us know – especially if our messaging can help counter.

From: [redacted] <[redacted]@securingdemocracy.org>
Sent: Wednesday, November 4, 2020 1:00 PM
To: Schaul, Robert <[redacted]@cisa.dhs.gov>
Subject: RE: Election dysfunction

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

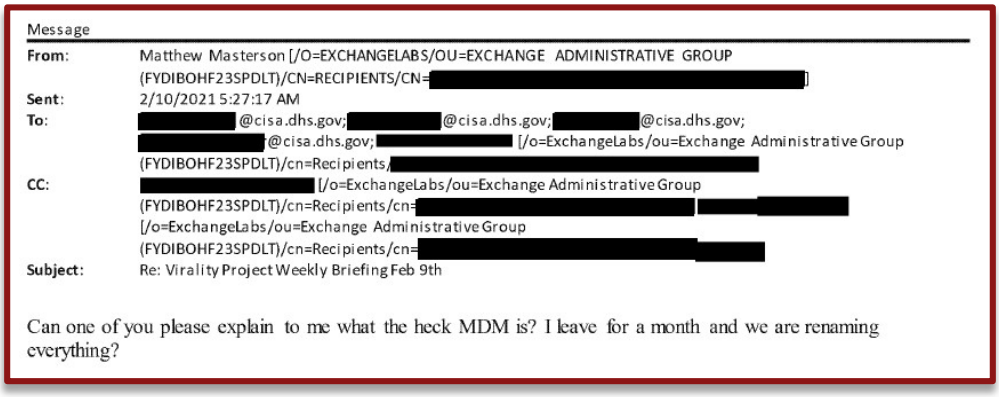
Hey Rob,

There was really just one RT article that attempted to amplify #stopthesteal: https://www.rt.com/usa/505397-philadelphia-voter-fraud-reported/

Otherwise, we haven't seen the accounts we monitor promote any of the more problematic narratives that are out there now. I mean, Russian state media is doing what they do in terms of trashing the election, but nothing of specific concern.

Obviously, what we're seeing domestically, particularly around mail-in fraud, is very concerning, but I know that's outside your purview. I'll keep you in the loop if something pops up.

In early 2021, CISA dropped the "misnomer" of the "Countering *Foreign* Influence Task Force" and became the "Mis-, Dis-, and Malinformation Team."[82] In spring 2023—following the *Missouri v. Biden* lawsuit, the Twitter Files reporting, and the Committee's investigation—CISA removed all references on its website that its MDM team was censoring domestic speech too.[83]



Message

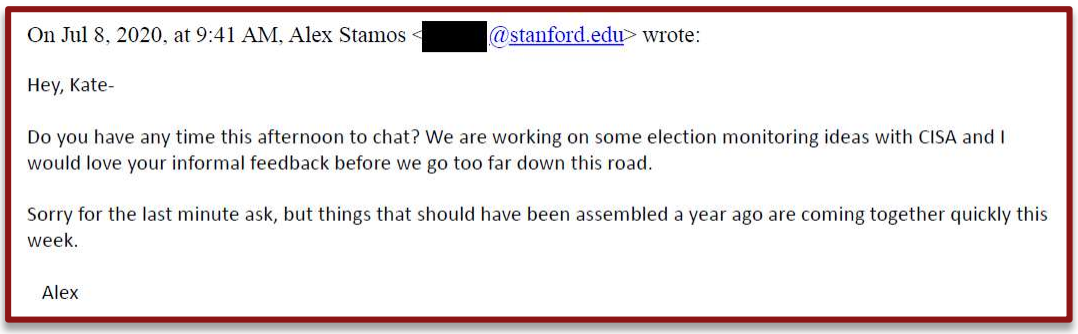
From: Matthew Masterson [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[redacted]]
Sent: 2/10/2021 5:27:17 AM
To: [redacted]@cisa.dhs.gov;[redacted]@cisa.dhs.gov;[redacted]@cisa.dhs.gov; [redacted]@cisa.dhs.gov;[redacted] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[redacted]
CC: [redacted] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]
Subject: Re: Virality Project Weekly Briefing Feb 9th

Can one of you please explain to me what the heck MDM is? I leave for a month and we are renaming everything?

[81] *See, e.g.*, Email from Robert Schaul to Alliance for Securing Democracy Employee (Nov. 4, 2020 1:12 PM) (on file with the Comm.).
[82] *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.
[83] *See* STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A "CYBERSECURITY" AGENCY COLLUDED WITH BIG TECH AND "DISINFORMATION" PARTNERS TO CENSOR AMERICANS, at 32–34 (Comm. Print June 26, 2023).

B. Creation of the EIP

Unable to proceed with its original plan, CISA enlisted Stanford to launder its censorship operation. On July 8, 2020, Stanford Internet Observatory (SIO) Director Alex Stamos sent an email to Dr. Kate Starbird at the University of Washington's Center for an Informed Public (CIP), writing: "We are working on some election monitoring ideas with CISA and I would love your informal feedback before we go too far down this road . . . . [T]hings that should have been assembled a year ago are coming together quickly this week."[84]



On Jul 8, 2020, at 9:41 AM, Alex Stamos <[redacted]@stanford.edu> wrote:

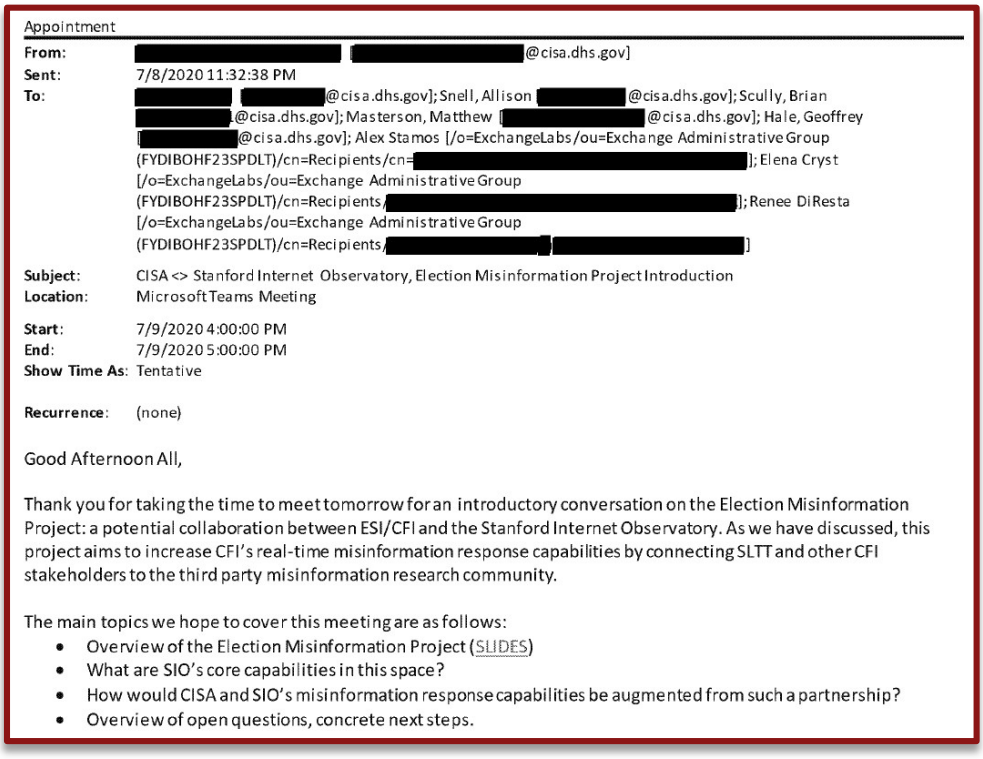
Hey, Kate-

Do you have any time this afternoon to chat? We are working on some election monitoring ideas with CISA and I would love your informal feedback before we go too far down this road.

Sorry for the last minute ask, but things that should have been assembled a year ago are coming together quickly this week.

Alex

The following day, on July 9, 2020, representatives from the SIO had a "[m]eeting with CISA to present [the] EIP concept."[85] Among those in attendance were Brian Scully, the future head of CISA's Mis-, Dis-, and Malinformation (MDM) team, Geoff Hale, the director of CISA's Election Security Initiative, and Matt Masterson, then-Senior Cybersecurity Advisor at CISA.[86]



Appointment

From: [redacted] [redacted]@cisa.dhs.gov]
Sent: 7/8/2020 11:32:38 PM
To: [redacted] [redacted]@cisa.dhs.gov]; Snell, Allison [redacted]@cisa.dhs.gov]; Scully, Brian [redacted].@cisa.dhs.gov]; Masterson, Matthew [redacted]@cisa.dhs.gov]; Hale, Geoffrey [redacted]@cisa.dhs.gov]; Alex Stamos [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; Elena Cryst [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[redacted]]; Renee DiResta [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[redacted]]
Subject: CISA <> Stanford Internet Observatory, Election Misinformation Project Introduction
Location: Microsoft Teams Meeting

Start: 7/9/2020 4:00:00 PM
End: 7/9/2020 5:00:00 PM
Show Time As: Tentative

Recurrence: (none)

Good Afternoon All,

Thank you for taking the time to meet tomorrow for an introductory conversation on the Election Misinformation Project: a potential collaboration between ESI/CFI and the Stanford Internet Observatory. As we have discussed, this project aims to increase CFI's real-time misinformation response capabilities by connecting SLTT and other CFI stakeholders to the third party misinformation research community.

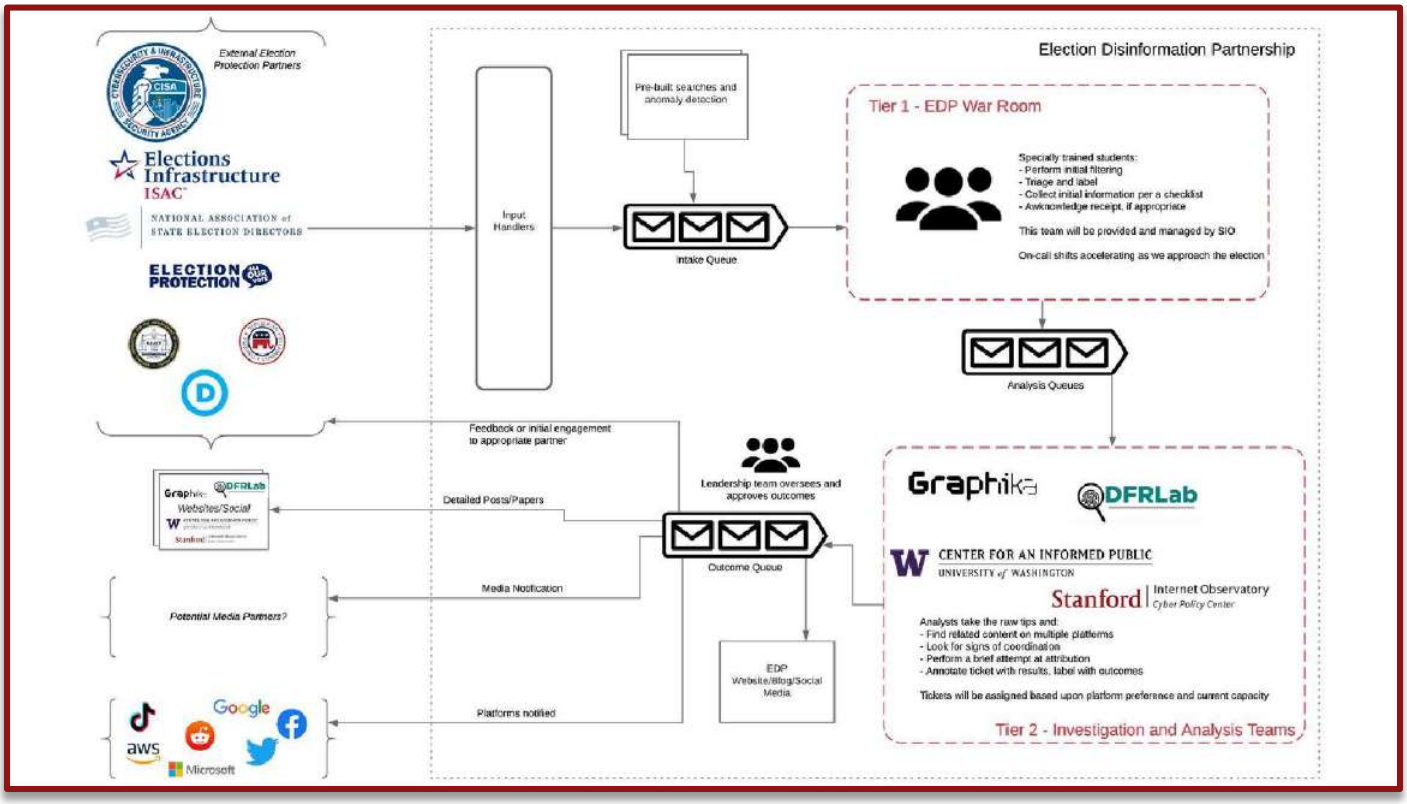
The main topics we hope to cover this meeting are as follows:

- Overview of the Election Misinformation Project (SLIDES)
- What are SIO's core capabilities in this space?
- How would CISA and SIO's misinformation response capabilities be augmented from such a partnership?
- Overview of open questions, concrete next steps.

[84] Email from Alex Stamos to Kate Starbird (July 8, 2020, 9:41 AM) (on file with the Comm.).
[85] ELECTION INTEGRITY P'SHIP, *supra* note at 16, at 3.
[86] Email from CISA official to CISA officials and SIO affiliates (July 8, 2020, 11:32 PM) (on file with the Comm.).

According to the email invitation for the meeting, the "Election Misinformation Project," which would later be rebranded as the more euphemistic "Election Integrity Partnership," "aim[ed] to increase . . . real-time misinformation response capabilities." One of the agenda items was a discussion of how "CISA and SIO's misinformation response capabilities [would] be augmented from such a partnership."[87]

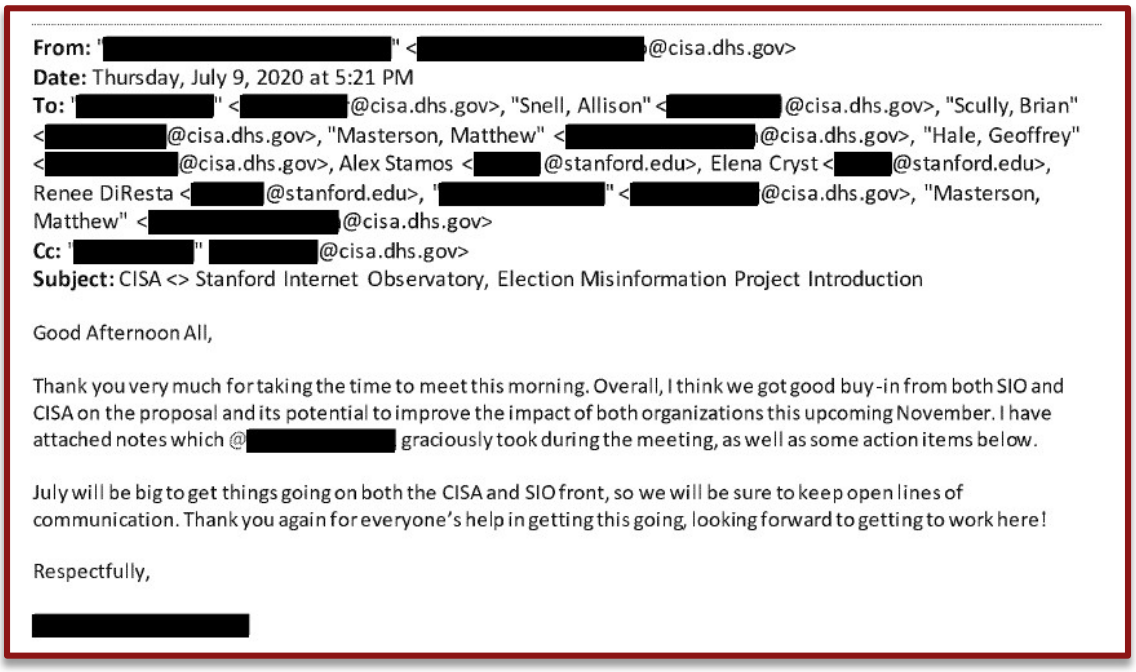
An early workflow diagram of the then-named "Election Disinformation Partnership" shows that from the beginning Stanford and CISA envisioned the partnership connecting federal agencies with social media platforms.[88]



[87] *Id*.

[88] "CISA EIP Overview Deck.pptx" attach. to email from Emerson Brooking to Atlantic Council employees (Sept. 1, 2020, 11:12 AM) (on file with the Comm.).. While the EIP invited both the DNC and RNC, the RNC declined to respond. House Judiciary Committee's Transcribed Interview of Alex Stamos (June 23, 2023), at 8 (on file with the Comm.). The DNC not only accepted the invitation, but also submitted Jira tickets. ELECTION INTEGRITY P'SHIP, *supra* note 16, at 42.

A subsequent summary of the July 9 kick-off meeting from a CISA employee stated that "I think we got good buy-in from both SIO and CISA on the proposal and its potential to improve the impact of both organizations this upcoming November . . . . July will be big to get things going on both the CISA and SIO front, so we will be sure to keep open lines of communication."[89]



From: "[redacted]" <[redacted]@cisa.dhs.gov>
Date: Thursday, July 9, 2020 at 5:21 PM
To: "[redacted]" <[redacted]@cisa.dhs.gov>, "Snell, Allison" <[redacted]@cisa.dhs.gov>, "Scully, Brian" <[redacted]@cisa.dhs.gov>, "Masterson, Matthew" <[redacted]@cisa.dhs.gov>, "Hale, Geoffrey" <[redacted]@cisa.dhs.gov>, Alex Stamos <[redacted]@stanford.edu>, Elena Cryst <[redacted]@stanford.edu>, Renee DiResta <[redacted]@stanford.edu>, "[redacted]" <[redacted]@cisa.dhs.gov>, "Masterson, Matthew" <[redacted]@cisa.dhs.gov>
Cc: "[redacted]" [redacted]@cisa.dhs.gov>
Subject: CISA <> Stanford Internet Observatory, Election Misinformation Project Introduction

Good Afternoon All,

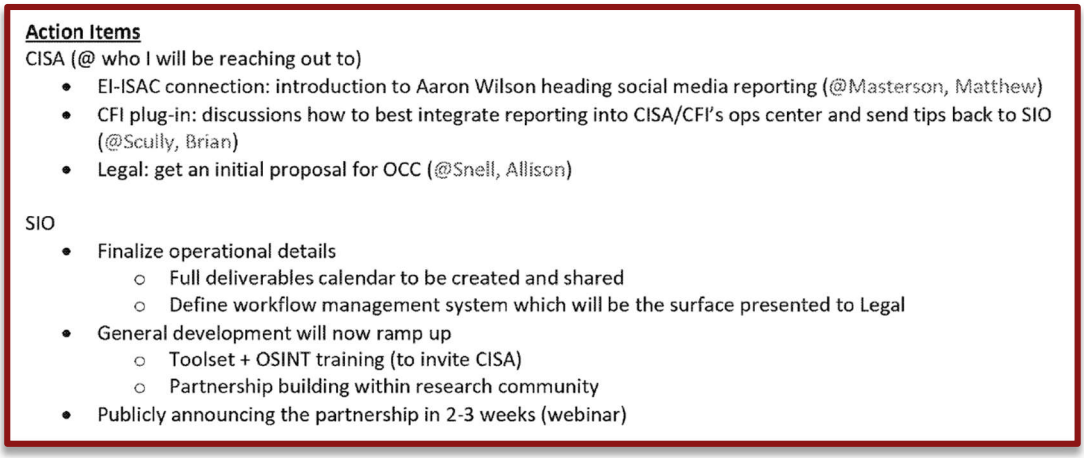
Thank you very much for taking the time to meet this morning. Overall, I think we got good buy-in from both SIO and CISA on the proposal and its potential to improve the impact of both organizations this upcoming November. I have attached notes which @[redacted] graciously took during the meeting, as well as some action items below.

July will be big to get things going on both the CISA and SIO front, so we will be sure to keep open lines of communication. Thank you again for everyone's help in getting this going, looking forward to getting to work here!

Respectfully,

[redacted]

The summary also listed a number of action items for CISA and SIO, including "discussions [about] how to best integrate reporting into CISA/[Countering Foreign Influence]'s ops center and send tips back to SIO."[90] Among the due-outs was a consultation with CISA's Office of Chief Counsel (OCC), as seen in the action item "Legal: get an initial proposal for OCC."[91]



Action Items

CISA (@ who I will be reaching out to)

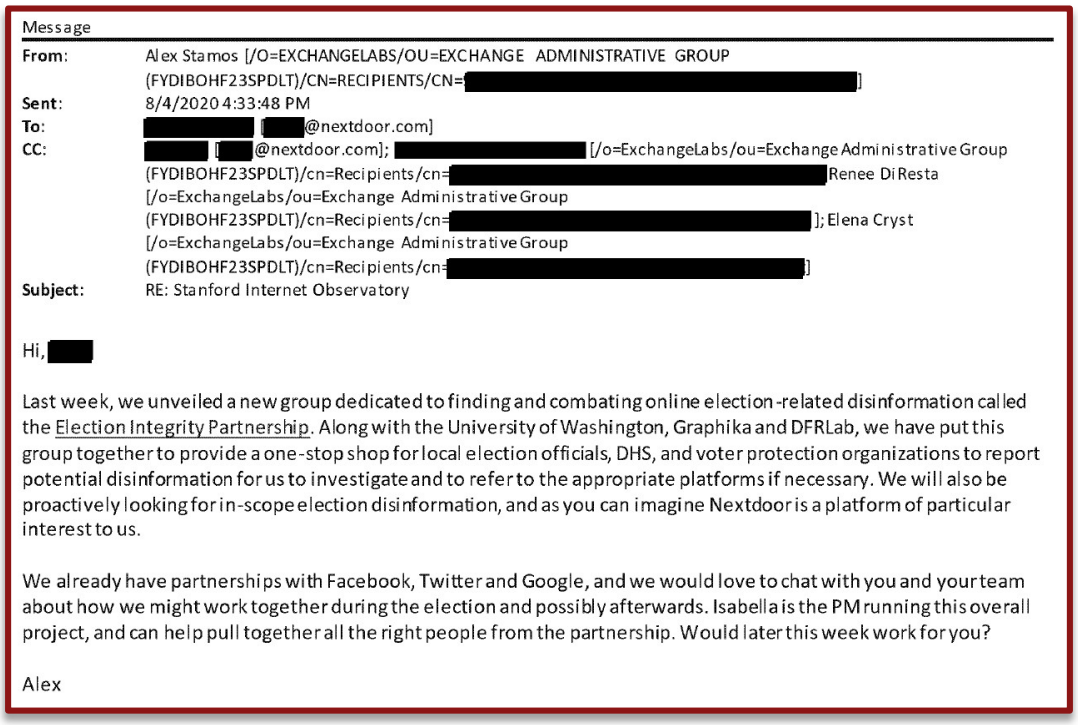
- EI-ISAC connection: introduction to Aaron Wilson heading social media reporting (@Masterson, Matthew)
- CFI plug-in: discussions how to best integrate reporting into CISA/CFI's ops center and send tips back to SIO (@Scully, Brian)
- Legal: get an initial proposal for OCC (@Snell, Allison)

SIO

- Finalize operational details
  - Full deliverables calendar to be created and shared
  - Define workflow management system which will be the surface presented to Legal
- General development will now ramp up
  - Toolset + OSINT training (to invite CISA)
  - Partnership building within research community
- Publicly announcing the partnership in 2-3 weeks (webinar)

[89] Email from CISA employee to CISA and SIO affiliates (July 9, 2020, 5:21 PM) (on file with the Comm.).
[90] *Id.*
[91] *Id.*

EIP personnel, including Alex Stamos, made clear in their outreach to social media platforms that the EIP's true purpose was to act as a censorship conduit for the federal government. For example, on August 4, 2020, Stamos wrote in an email to a Nextdoor employee that the EIP was formed "to provide a one-stop shop for local election officials, *DHS*, and voter protection organizations to report potential disinformation for [the EIP] to investigate and to refer to the appropriate platforms."[92]



Message

From: Alex Stamos [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=[redacted]]
Sent: 8/4/2020 4:33:48 PM
To: [redacted] [redacted]@nextdoor.com]
CC: [redacted] [redacted]@nextdoor.com]; [redacted] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]Renee DiResta [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; Elena Cryst [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]
Subject: RE: Stanford Internet Observatory

Hi, [redacted]

Last week, we unveiled a new group dedicated to finding and combating online election-related disinformation called the Election Integrity Partnership. Along with the University of Washington, Graphika and DFRLab, we have put this group together to provide a one-stop shop for local election officials, DHS, and voter protection organizations to report potential disinformation for us to investigate and to refer to the appropriate platforms if necessary. We will also be proactively looking for in-scope election disinformation, and as you can imagine Nextdoor is a platform of particular interest to us.

We already have partnerships with Facebook, Twitter and Google, and we would love to chat with you and your team about how we might work together during the election and possibly afterwards. Isabella is the PM running this overall project, and can help pull together all the right people from the partnership. Would later this week work for you?

Alex

In its post-election report, the EIP purports that the "initial idea for the Partnership came from four students that the Stanford Internet Observatory (SIO) funded to complete volunteer internships at [CISA]."[93] This revisionist version of events, seemingly intended to distance CISA and senior SIO leadership from the EIP's creation, is contradicted by evidence obtained by the Committee.

In June 2023, the Committee conducted a transcribed interview of Alex Stamos, the Director of the SIO. When asked about the origins of the EIP, Stamos testified that he, not the four interns, "first came up with the idea for EIP." He testified:

> Q. Do you recall who first came up with the idea for EIP?
>
> A. It was me.[94]

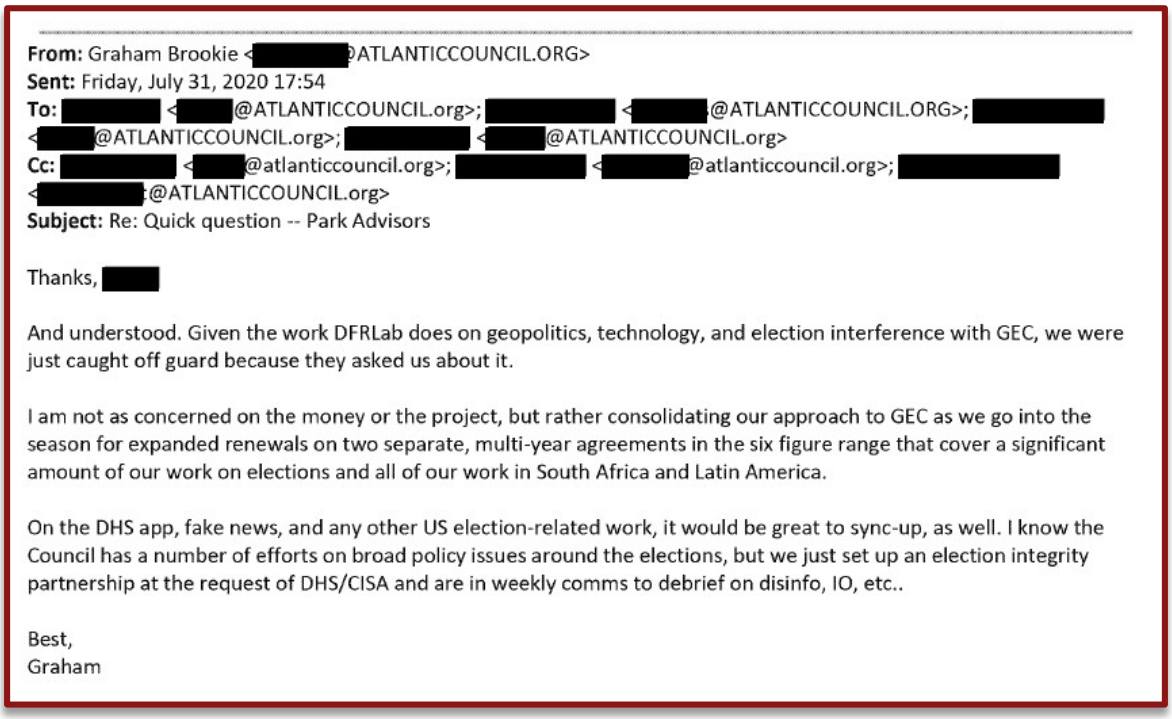
[92] Email from Alex Stamos to Nextdoor employee (Aug. 4, 2020, 4:33 PM) (on file with the Comm.) (emphasis added).
[93] ELECTION INTEGRITY P'SHIP, *supra* note at 16, at 2.
[94] House Judiciary Committee's Transcribed Interview of Alex Stamos (June 23, 2023), at 36 (on file with the Comm.).

Stamos also admitted during the interview that he had likely consulted with then-CISA Director Christopher Krebs during the summer of 2020 about the EIP. He testified:

> Q. Did you consult with Chris Krebs in the summer of 2020?
>
> A. I probably did, yes.[95]

Documents produced to the Committee and Select Subcommittee likewise cast doubt on the notion that a handful of students were responsible for the EIP's conception.[96] Regardless of what role, if any, students played in the "idea" of EIP, these documents show the direct role that high-ranking CISA, CIS, and SIO personnel played in forming an operation with nearly 100 people directly involved that worked with over a dozen partners to flag thousands of posts and narratives via hundreds of "misinformation" reports.[97]

Finally, even the founding four partners of the EIP, such as the Atlantic Council's DFRLab, understood in the summer of 2020 that the EIP was created at *CISA*'s request. As revealed in an internal Atlantic Council email obtained by the Committee pursuant to a subpoena, Graham Brookie, one of the central figures involved in the EIP, understood in July of 2020 that the EIP was "set up . . . at *the request of DHS/CISA*."[98]



From: Graham Brookie <[redacted]@ATLANTICCOUNCIL.ORG>
Sent: Friday, July 31, 2020 17:54
To: [redacted] <[redacted]@ATLANTICCOUNCIL.org>; [redacted] <[redacted]@ATLANTICCOUNCIL.ORG>; [redacted] <[redacted]@ATLANTICCOUNCIL.org>; [redacted] <[redacted]@ATLANTICCOUNCIL.org>
Cc: [redacted] <[redacted]@atlanticcouncil.org>; [redacted] <[redacted]@atlanticcouncil.org>; [redacted] <[redacted]@ATLANTICCOUNCIL.org>
Subject: Re: Quick question -- Park Advisors

Thanks, [redacted]

And understood. Given the work DFRLab does on geopolitics, technology, and election interference with GEC, we were just caught off guard because they asked us about it.

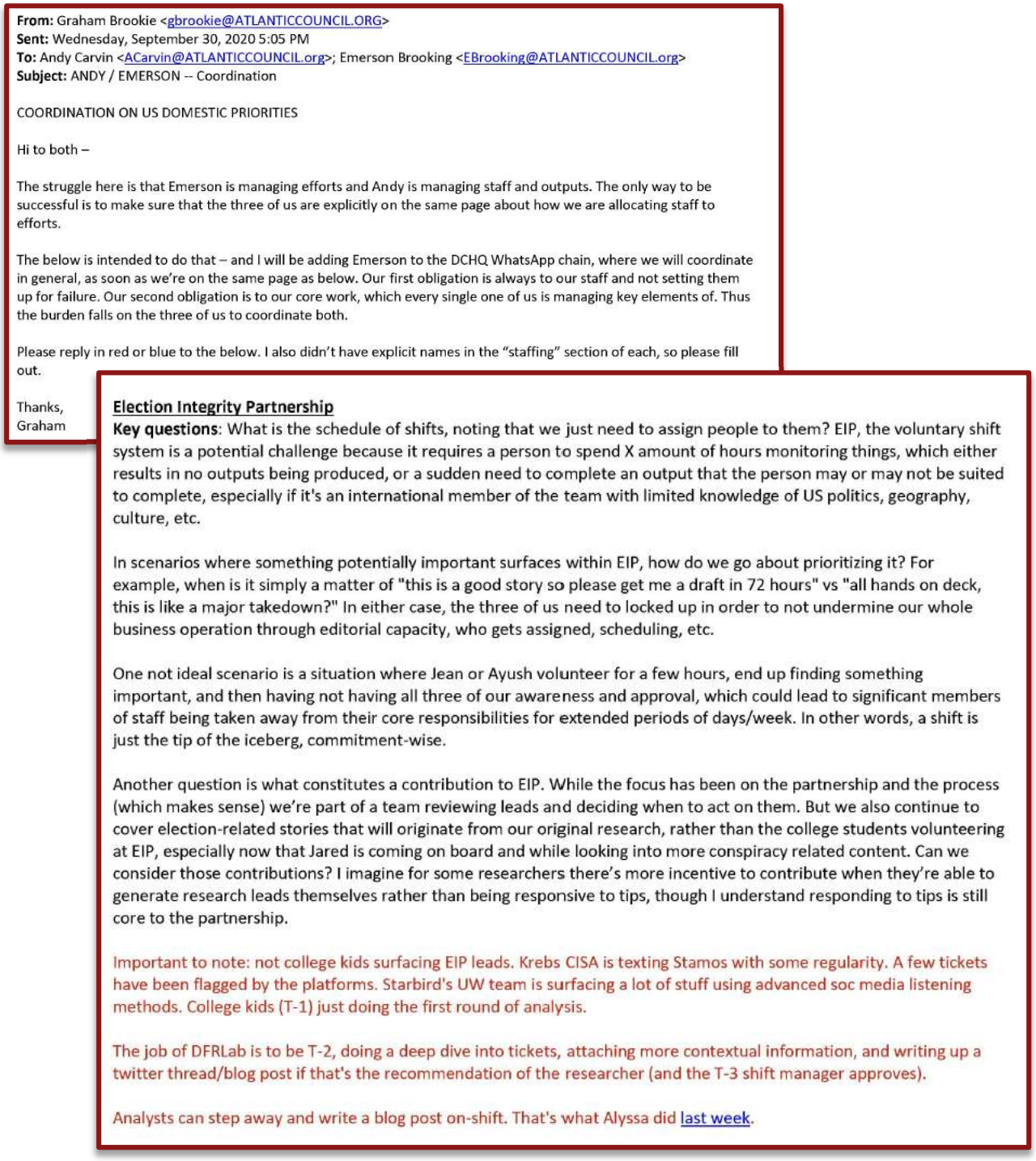
I am not as concerned on the money or the project, but rather consolidating our approach to GEC as we go into the season for expanded renewals on two separate, multi-year agreements in the six figure range that cover a significant amount of our work on elections and all of our work in South Africa and Latin America.

On the DHS app, fake news, and any other US election-related work, it would be great to sync-up, as well. I know the Council has a number of efforts on broad policy issues around the elections, but we just set up an election integrity partnership at the request of DHS/CISA and are in weekly comms to debrief on disinfo, IO, etc..

Best,
Graham

[95] *Id*. at 44. The Committee also interviewed former Director Krebs in October 2023, who claimed not to "recall any conversations with Alex [Stamos]" during the summer of 2020. House Judiciary Committee's Transcribed Interview of Christopher Krebs (Oct. 11, 2023), at 164 (on file with the Comm.).
[96] *See, e.g.*, email from Graham Brookie to Atlantic Council employees (July 31, 2020, 5:54 PM) (on file with the Comm.).
[97] ELECTION INTEGRITY P'SHIP, *supra* note at 16, at xii, 12.
[98] Email from Graham Brookie to Atlantic Council employees (July 31, 2020, 5:54 PM) (on file with the Comm.) (emphasis added).

Internal Atlantic Council documents, obtained by the Committee and Select Subcommittee pursuant to a subpoena to the Atlantic Council, also reveal that while students were involved in the EIP, the critical work, including "attaching more contextual information," preparing blog posts, and making recommendations to the social media platforms, was handled by the disinformation professionals.[99]



From: Graham Brookie <gbrookie@ATLANTICCOUNCIL.ORG>
Sent: Wednesday, September 30, 2020 5:05 PM
To: Andy Carvin <ACarvin@ATLANTICCOUNCIL.org>; Emerson Brooking <EBrooking@ATLANTICCOUNCIL.org>
Subject: ANDY / EMERSON -- Coordination

COORDINATION ON US DOMESTIC PRIORITIES

Hi to both –

The struggle here is that Emerson is managing efforts and Andy is managing staff and outputs. The only way to be successful is to make sure that the three of us are explicitly on the same page about how we are allocating staff to efforts.

The below is intended to do that – and I will be adding Emerson to the DCHQ WhatsApp chain, where we will coordinate in general, as soon as we're on the same page as below. Our first obligation is always to our staff and not setting them up for failure. Our second obligation is to our core work, which every single one of us is managing key elements of. Thus the burden falls on the three of us to coordinate both.

Please reply in red or blue to the below. I also didn't have explicit names in the "staffing" section of each, so please fill out.

Thanks,
Graham

Election Integrity Partnership

Key questions: What is the schedule of shifts, noting that we just need to assign people to them? EIP, the voluntary shift system is a potential challenge because it requires a person to spend X amount of hours monitoring things, which either results in no outputs being produced, or a sudden need to complete an output that the person may or may not be suited to complete, especially if it's an international member of the team with limited knowledge of US politics, geography, culture, etc.

In scenarios where something potentially important surfaces within EIP, how do we go about prioritizing it? For example, when is it simply a matter of "this is a good story so please get me a draft in 72 hours" vs "all hands on deck, this is like a major takedown?" In either case, the three of us need to locked up in order to not undermine our whole business operation through editorial capacity, who gets assigned, scheduling, etc.

One not ideal scenario is a situation where Jean or Ayush volunteer for a few hours, end up finding something important, and then having not having all three of our awareness and approval, which could lead to significant members of staff being taken away from their core responsibilities for extended periods of days/week. In other words, a shift is just the tip of the iceberg, commitment-wise.

Another question is what constitutes a contribution to EIP. While the focus has been on the partnership and the process (which makes sense) we're part of a team reviewing leads and deciding when to act on them. But we also continue to cover election-related stories that will originate from our original research, rather than the college students volunteering at EIP, especially now that Jared is coming on board and while looking into more conspiracy related content. Can we consider those contributions? I imagine for some researchers there's more incentive to contribute when they're able to generate research leads themselves rather than being responsive to tips, though I understand responding to tips is still core to the partnership.

Important to note: not college kids surfacing EIP leads. Krebs CISA is texting Stamos with some regularity. A few tickets have been flagged by the platforms. Starbird's UW team is surfacing a lot of stuff using advanced soc media listening methods. College kids (T-1) just doing the first round of analysis.

The job of DFRLab is to be T-2, doing a deep dive into tickets, attaching more contextual information, and writing up a twitter thread/blog post if that's the recommendation of the researcher (and the T-3 shift manager approves).

Analysts can step away and write a blog post on-shift. That's what Alyssa did last week.

[99] Email exchange between Graham Brookie, Andy Carvin and Emerson Brooking (Sept. 30, 2020 5:05 PM) (on file with the Comm.).

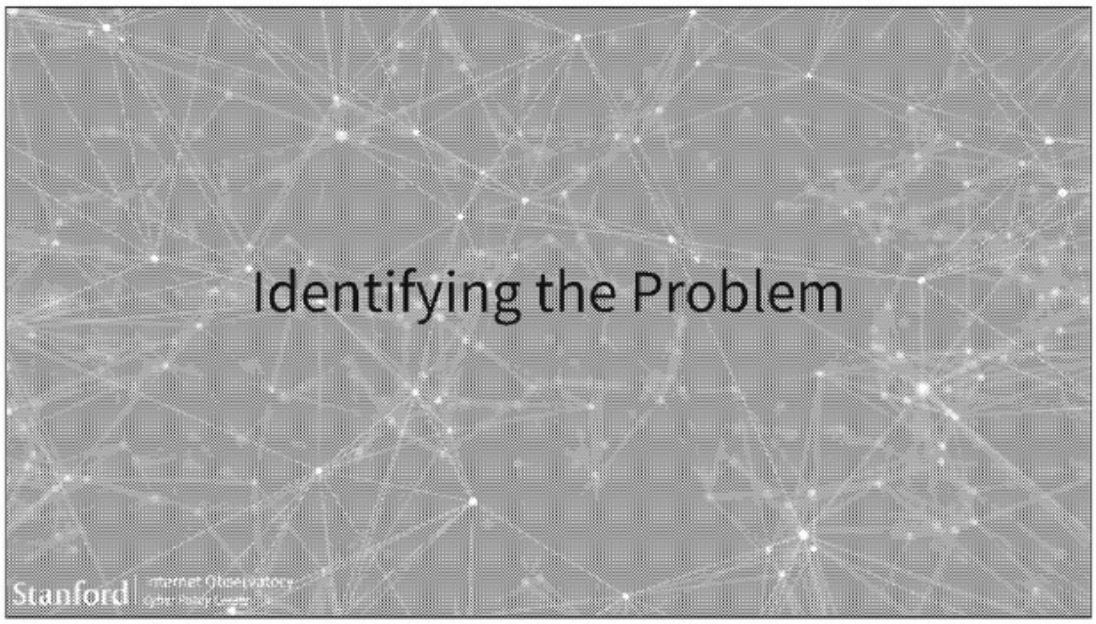
C. The EIP's Purpose: Using Proxies to Circumvent the First Amendment

By its own admission, the EIP was expressly created "in consultation with CISA"[100] to serve an unconstitutional purpose, as a mechanism for flaunting legal restrictions on illicit government activity. As stated in the EIP's post-election report:

> Yet, no government agency in the United States has the explicit mandate to monitor and correct election mis- and disinformation. This is especially true for election disinformation that originates from within the United States, which would likely be excluded from law enforcement action under the First Amendment and not appropriate for study by intelligence agencies restricted from operating inside the United States. As a result, during the 2020 election, local and state election officials, who had a strong partner on election-system and overall cybersecurity efforts in CISA, were without a clearinghouse for assessing mis- and disinformation targeting their voting operations . . . in consultation with CISA and other stakeholders, a coalition was assembled with like-minded partner institutions.[101]

In her notes for a fall 2021 presentation at the annual CISA Summit, Renée DiResta, the Research Manager at the SIO, wrote, as part of her presentation script, that the "gap" the EIP was intended to fill "had several components," one of which was "[u]nclear legal authorities including *very real 1st amendment questions*."[102]

[100] ELECTION INTEGRITY P'SHIP, *supra* note at 16, at 2.
[101] *Id*.
[102] "CISA keynote.pptx" attach. to email from Renée DiResta to Kenneth Bradley and Amanda Glenn (Oct. 6, 2021, 3:58 PM) (on file with the Comm.); *see also* email from Renée DiResta to Kenneth Bradley and Amanda Glenn (Oct. 6, 2021, 3:58 PM) (on file with the Comm.) (DiResta writes, "I was just writing out the full script into the speaker notes in case the teleprompter was the best bet.").



Our team and CISA's team have done some pioneering work in partnership thinking about how to respond to mis- and disinformation in areas in which it can have significant harm. One of those areas is elections, and I'm going to talk about some learnings from that work today.

In August 2020, students from the Stanford Internet Observatory (SIO) who were doing an internship with CISA identified a massive gap in the capability of federal, state and local governments to become aware of, analyze and rapidly respond to mis- and disinformation — both foreign and domestic — targeting the 2020 election.

That gap had several components:
- Federal gov't not prepared to identify and analyze election mis/disinfo:
- There was no clear federal lead to coordinate this work. The IC, of course, is rightly limited to a foreign-focus. The FBI also has very specific designations and limitations, and CISA had created support but had no real capability.
- Unclear legal authorities including very real 1st amendment questions
- No expertise resident within federal gov't to analyze public content across platforms to identify trends & risks
Lack of reporting mechanisms for state and local partners to surface activity that they saw building in their communities, to help them understand it.
The federal government was building relationships with platforms but there is a healthy distrust both ways for good reason

A trusted, nonpartisan partner(s) with expertise in the way that misinformation moved on public platforms, with analysts capable of understanding public conversations, and broad ability to explore publicly available data, was needed.

In order to circumvent these "very real 1st amendment questions," organizations devoted to peddling the pseudoscience of "disinformation," like the SIO and the University of Washington's CIP, were selected to serve as part of a "central organization to support elections officials or CISA in identifying and responding to misinformation."[103] According to an early EIP

[103] Election Disinformation Partnership: Overview for Partners (unpublished presentation notes) (on file with the Comm.).

presentation, "Academic/Research Institutions" were chosen to spearhead this effort specifically because they were considered to be the "'easiest' politically."[104]

Current Landscape

Who could potentially solve this problem? Why aren't they?

	CISA	Platforms	Academic/Research Institutions
Currently Offers	EI-ISAC collaboration to provide real-time monitoring tools such as the SOC as well as the classified and unclassified Situation Rooms	Direct contact with secretaries of state as well as some cross-platform communication on this front	Institutions have created their own independent groups, little coordination
Strengths	Direct communication with every election official, central node in the election infra ecosystem	Highest monitoring capacity into what is happening in the social landscape, lots of $$$ and resources	'Easiest' politically, transparent, existing institutions (SIO). Agile, lightweight teams.
Weaknesses	All efforts focused on hardware, no misinformation workstream, govt entity, can't be seen as 'monitoring' the electorate, highly political.	Political, easily seen as partisan, don't have the direct communication/rapport with all election officials.	Don't have the direct communication or rapport with all election officials, need to raise $$$

It is "axiomatic," the Supreme Court has explained, that the government "may not induce, encourage or promote private persons to accomplish what it is constitutionally forbidden to accomplish."[105] CISA's involvement in the creation of and collaboration with the EIP is the type of unconstitutional outsourcing against which the Supreme Court has long ruled.[106] Censorship-by-proxy is an especially nefarious form of state action, given that it is designed to evade detection, oversight efforts, and public records requests.[107]

---

[104] *Id*.

[105] Norwood v. Harrison, 413 U.S. 455, 465 (1973).

[106] *See also* Missouri v. Biden, No. 23-30445, slip op. (5th Cir. Oct. 3, 2023), ECF No. 271. As the Committee's investigation has revealed, CISA's practice of exploiting third-party non-profits to sidestep legal prohibitions against censorship and surveillance also extended beyond the EIP. For example, on November 4, 2020, Robert Schaul, CISA's Analysis and Resilience Policy Lead, sent an email to an individual affiliated with Alliance for Securing Democracy, a project of the German Marshall Fund and subject of several Twitter Files installments. In the email, Schaul writes that he is "checking in to see if you're seeing anything of particular concern that might be worth elevating to Director Krebs. Are you still seeing #stopthesteal popping up? We're still all hands on deck here." Email from Robert Schaul to Alliance for Securing Democracy Employee (Nov. 4, 2020 12:02 PM) (on file with the Comm.). Notably, Schaul did not distinguish between organic, domestic discussion of #stopthesteal and foreign amplification of the hashtag.

[107] *See, e.g.*, Lee Fang, *Biden Justice Dept. Intervened to Block Release of Social Media Censorship Docs,* SUBSTACK (June 6, 2023), https://www.leefang.com/p/biden-justice-dept-intervened-to; *see also* STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A "CYBERSECURITY" AGENCY COLLUDED WITH BIG TECH AND "DISINFORMATION" PARTNERS TO CENSOR AMERICANS, at 34–35 (Comm. Print June 26, 2023).

II. CISA'S COMPLETE INTERTWINEMENT WITH THE EIP

"CISA and the EIP were completely intertwined."

-*Missouri v. Biden*, Case No. 3:22-cv-1213,
ECF No. 293 (Injunction & Opinion) at 113 (July 4, 2023).

A. CISA's Collusion with the EIP

After CISA helped to create the EIP, the federal agency remained thoroughly intertwined with the EIP's operations in the months preceding the 2020 election. Throughout the fall of 2020, CISA officials coordinated extensively with the EIP and CIS.[108] Emails obtained by the Committee and Select Subcommittee pursuant to a subpoena show clearly that the EIP system was designed to operate as a unit, not as a separate entity from DHS. Moreover, while there were many students involved in the EIP (which had nearly 100 people working for it, not including external stakeholders such as the GEC and CISA), the EIP was led by well-known figures in the censorship-industrial complex, such as Stanford Internet Observatory (SIO) Director (and former Chief Security Officer at Facebook) Alex Stamos, SIO Research Manager Renee DiResta, and Vice President and Senior Director of the Atlantic Council's Digital Forensic Research Lab (DFRLab) Graham Brookie. The EIP also collaborated closely with senior CISA officials, including Brian Scully, the head of CISA's Countering Foreign Influence Task Force (CFITF).

Not only were there a number of university students involved with the EIP, at least four of the students were employed by CISA during the operation of EIP, using their government email accounts to communicate with CISA officials and other "external stakeholders" involved with the EIP. For example, by September 3, 2020, CISA had designated one of these DHS-SIO interns as the point of contact to be responsible for "taking point on a lot of the EIP <> CISA interface."[109]

[108] *See, e.g.*, email from CISA staff to CISA officials, CIS employees, and SIO affiliates (Oct. 5, 2020, 12:52 PM) (on file with the Comm.).
[109] Email from CISA staff to Aaron Wilson, Ben Spear, and Mike Garcia (Sept. 3, 2020, 1:51 PM) (on file with the Comm.).

From: [redacted]@cisa.dhs.gov]
Sent: 9/3/2020 1:51:40 PM
To: Aaron Wilson [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; Ben Spear [/o=exchange/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=[redacted]]; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; [redacted]@cisa.dhs.gov]
CC: Masterson, Matthew [[redacted]@cisa.dhs.gov]; Snell, Allison [[redacted]@cisa.dhs.gov]; Scully, Brian [[redacted]@cisa.dhs.gov]; Hale, Geoffrey [[redacted]@cisa.dhs.gov]
Subject: RE: CISA <> CSI Disinfo Reporting follow up

Hello Aaron:

Sorry for the delay here – for some reason, the @cisecurity alias keeps getting routed to my 'Other' folder, so I was about to follow up on this myself. I'll try and chat with our techdesk today about this.

On the EIP side, if you could please add tips@eipartnership.net, this alias will auto create Jira tickets for any incoming reports for visibility to the whole EiP team. I've also added [redacted] to this thread, [redacted]@cisa.dhs.gov, who will be taking point on a lot of the EIP <> CISA interface here, so he should also be added. I will let Brian and Matt note whether they also would like to be on the backend of this alias.

One note on the EIP side: we just finished getting our Jira system online to be ready for intake. For security purposes, the tips@eipartnership.net alias has a strict whitelist of emails which will be allowed through: any email not specifically designated into an organization will be silently dropped. I've created a new CIS organization on our system and added misinformation@cisecurity.org to it, as well as [redacted]'s CISA email. Any reports forwarded from these email addresses will make it into our system. However, if misinformation@cisecurity.org auto forwards anything in such a way that it is sent from a different alias (ex: bob@washington.gov), this will be dropped in our system.

There are ways around this, but I just wanted to flag this upfront and get a sense from you how this might be working on your end? I have a free calendar all day tomorrow basically, and could hop on a call with our tech lead to figure out the best way of doing this.

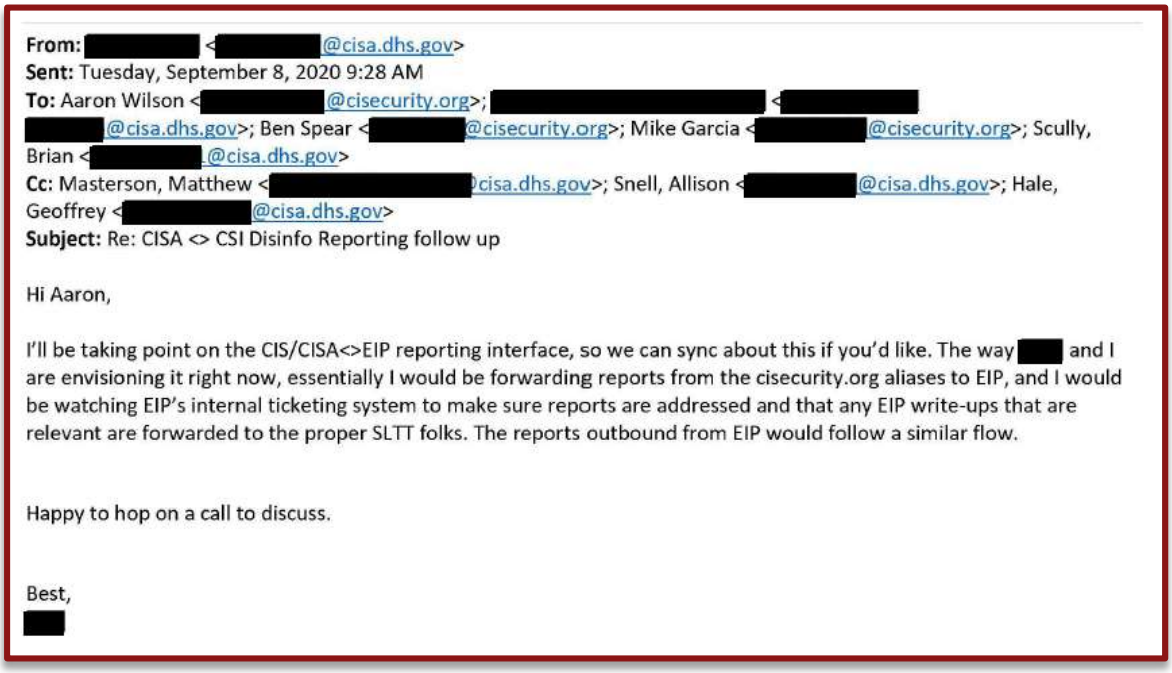
Best,

[redacted]

This Stanford student, working as a DHS intern, would be "inside the EIP network," with the responsibility of "forwarding reports from the cissecurity.org aliases to EIP," and "watching EIP's internal ticketing system to make sure reports are addressed and that any EIP write-ups that are relevant are forwarded to the proper SLTT [state, local, tribal, and territorial] folks."[110]

[110] Email from CISA official to Aaron Wilson, Ben Spear, Mike Garcia, and Brian Scully (Sept. 8, 2020, 9:28 AM) (on file with the Comm.).

In other words, DHS had a point of contact with direct access to the EIP's internal ticketing system who could (and did) share this information with the agency.[111]



From: [redacted] <[redacted]@cisa.dhs.gov>
Sent: Tuesday, September 8, 2020 9:28 AM
To: Aaron Wilson <[redacted]@cisecurity.org>; [redacted] <[redacted]@cisa.dhs.gov>; Ben Spear <[redacted]@cisecurity.org>; Mike Garcia <[redacted]@cisecurity.org>; Scully, Brian <[redacted]@cisa.dhs.gov>
Cc: Masterson, Matthew <[redacted]@cisa.dhs.gov>; Snell, Allison <[redacted]@cisa.dhs.gov>; Hale, Geoffrey <[redacted]@cisa.dhs.gov>
Subject: Re: CISA <> CSI Disinfo Reporting follow up

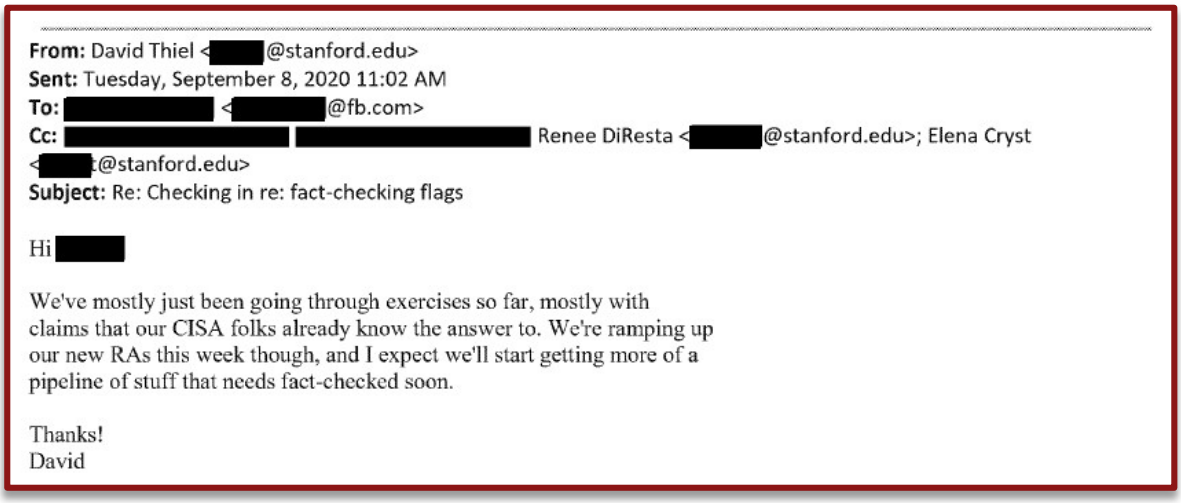
Hi Aaron,

I'll be taking point on the CIS/CISA<>EIP reporting interface, so we can sync about this if you'd like. The way [redacted] and I are envisioning it right now, essentially I would be forwarding reports from the cisecurity.org aliases to EIP, and I would be watching EIP's internal ticketing system to make sure reports are addressed and that any EIP write-ups that are relevant are forwarded to the proper SLTT folks. The reports outbound from EIP would follow a similar flow.

Happy to hop on a call to discuss.

Best,
[redacted]

As the EIP geared up for the 2020 election, it appears that the EIP coordinated with CISA to conduct censorship "exercises." A September 8, 2020, email to a Facebook employee from David Theil, the SIO's Chief Technologist, reads: "We've mostly just been going through exercises so far, mostly with claims that our CISA folks already know the answer to."[112]



From: David Thiel <[redacted]@stanford.edu>
Sent: Tuesday, September 8, 2020 11:02 AM
To: [redacted] <[redacted]@fb.com>
Cc: [redacted] [redacted] Renee DiResta <[redacted]@stanford.edu>; Elena Cryst <[redacted]@stanford.edu>
Subject: Re: Checking in re: fact-checking flags

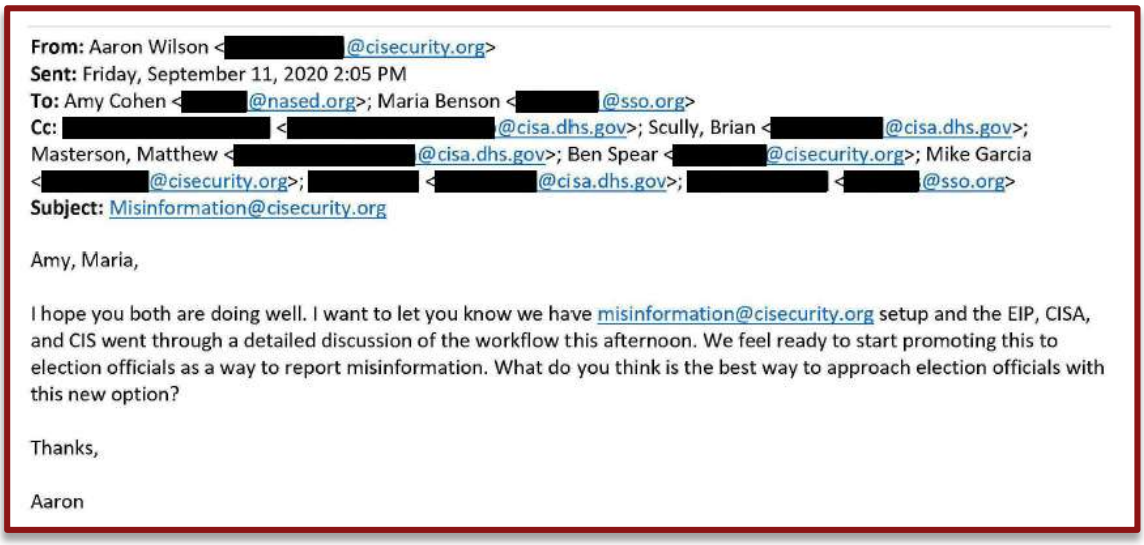
Hi [redacted]

We've mostly just been going through exercises so far, mostly with claims that our CISA folks already know the answer to. We're ramping up our new RAs this week though, and I expect we'll start getting more of a pipeline of stuff that needs fact-checked soon.

Thanks!
David

[111] Moreover, witnesses before the Committee have testified that they did not recall knowing that the individual using the "@cisa.dhs.gov" email domain was an intern. *See, e.g.*, House Judiciary Committee's Transcribed Interview of Aaron Wilson (November 2, 2023).
[112] Email from David Thiel to Facebook employee (Sept. 8, 2020, 11:02 AM) (on file with the Comm.).

On September 11, Aaron Wilson, emailed that "the EIP, CISA, and CIS went through a detailed discussion of the workflow this afternoon. We feel ready to start promoting this to election officials as a way to report misinformation."[113]



From: Aaron Wilson <[redacted]@cisecurity.org>
Sent: Friday, September 11, 2020 2:05 PM
To: Amy Cohen <[redacted]@nased.org>; Maria Benson <[redacted]@sso.org>
Cc: [redacted] <[redacted]@cisa.dhs.gov>; Scully, Brian <[redacted]@cisa.dhs.gov>; Masterson, Matthew <[redacted]@cisa.dhs.gov>; Ben Spear <[redacted]@cisecurity.org>; Mike Garcia <[redacted]@cisecurity.org>; [redacted] <[redacted]@cisa.dhs.gov>; [redacted] <[redacted]@sso.org>
Subject: Misinformation@cisecurity.org

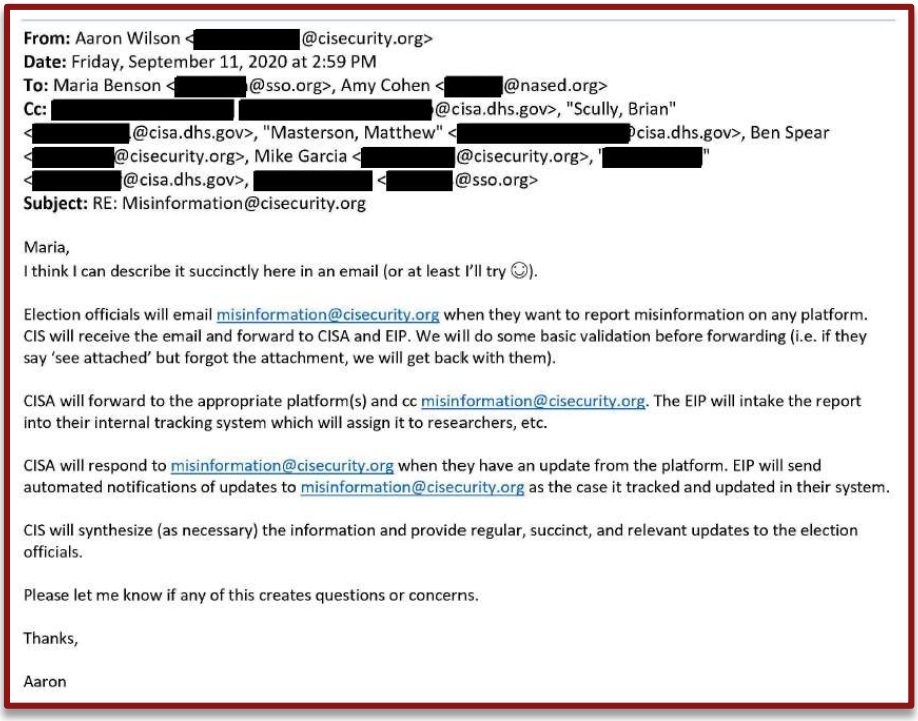
Amy, Maria,

I hope you both are doing well. I want to let you know we have misinformation@cisecurity.org setup and the EIP, CISA, and CIS went through a detailed discussion of the workflow this afternoon. We feel ready to start promoting this to election officials as a way to report misinformation. What do you think is the best way to approach election officials with this new option?

Thanks,

Aaron

The proposed workflow makes clear that neither the EIP nor CIS were acting completely independently of CISA, but instead operated cooperatively and systematically within the same censorship organ CISA helped to create. As described in the same mid-September 2020 email thread below, election officials would submit misinformation reports to CIS; CIS would then (1) forward the email to CISA, with the agency then forwarding the report to the social media platforms (i.e., the CISA track); and (2) forward the email to EIP, who would search for other similar content to be flagged before sending reports to the social media platforms (i.e., the EIP track). As a consequence, CISA had visibility on what was being submitted to the EIP. And critically, social media platforms knew that CISA had knowledge of EIP's intake.



From: Aaron Wilson <[redacted]@cisecurity.org>
Date: Friday, September 11, 2020 at 2:59 PM
To: Maria Benson <[redacted]@sso.org>, Amy Cohen <[redacted]@nased.org>
Cc: [redacted] [redacted]@cisa.dhs.gov>, "Scully, Brian" <[redacted]@cisa.dhs.gov>, "Masterson, Matthew" <[redacted]@cisa.dhs.gov>, Ben Spear <[redacted]@cisecurity.org>, Mike Garcia <[redacted]@cisecurity.org>, "[redacted]" <[redacted]@cisa.dhs.gov>, [redacted] <[redacted]@sso.org>
Subject: RE: Misinformation@cisecurity.org

Maria,
I think I can describe it succinctly here in an email (or at least I'll try ☺).

Election officials will email misinformation@cisecurity.org when they want to report misinformation on any platform. CIS will receive the email and forward to CISA and EIP. We will do some basic validation before forwarding (i.e. if they say 'see attached' but forgot the attachment, we will get back with them).

CISA will forward to the appropriate platform(s) and cc misinformation@cisecurity.org. The EIP will intake the report into their internal tracking system which will assign it to researchers, etc.

CISA will respond to misinformation@cisecurity.org when they have an update from the platform. EIP will send automated notifications of updates to misinformation@cisecurity.org as the case it tracked and updated in their system.

CIS will synthesize (as necessary) the information and provide regular, succinct, and relevant updates to the election officials.

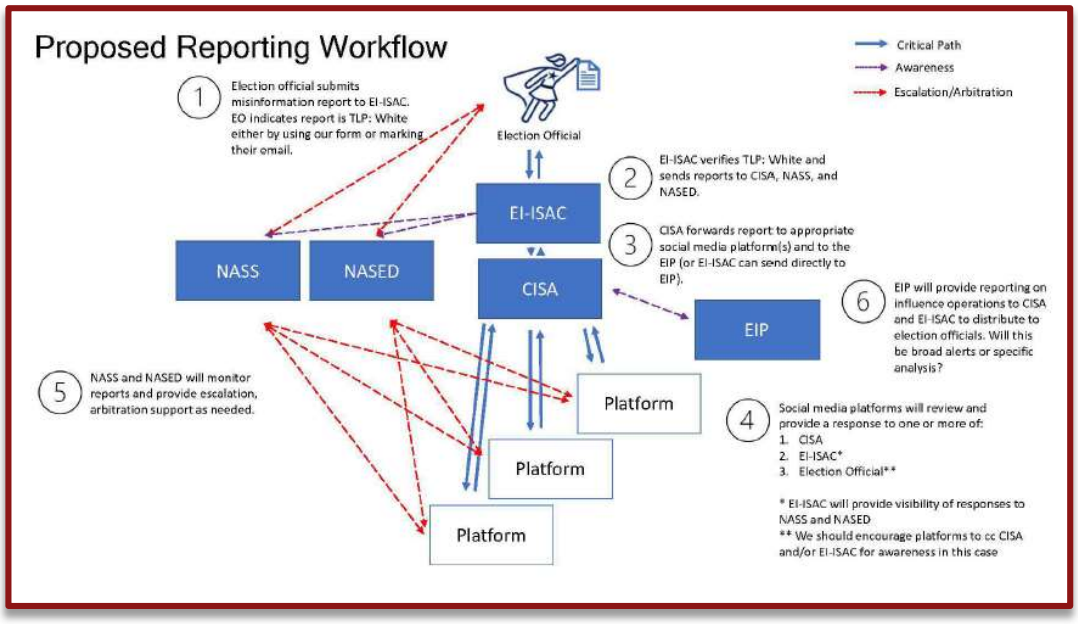
Please let me know if any of this creates questions or concerns.

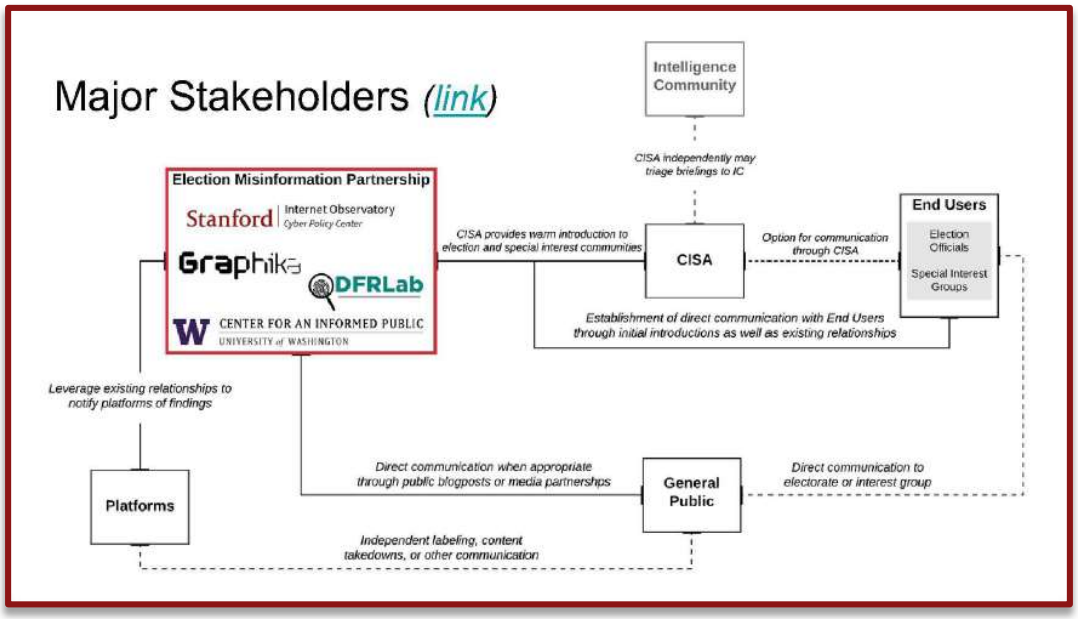
Thanks,

Aaron

[113] Email from Aaron Wilson to Amy Cohen and Maria Benson (Sept. 11, 2020, 2:05 PM) (on file with the Comm.).

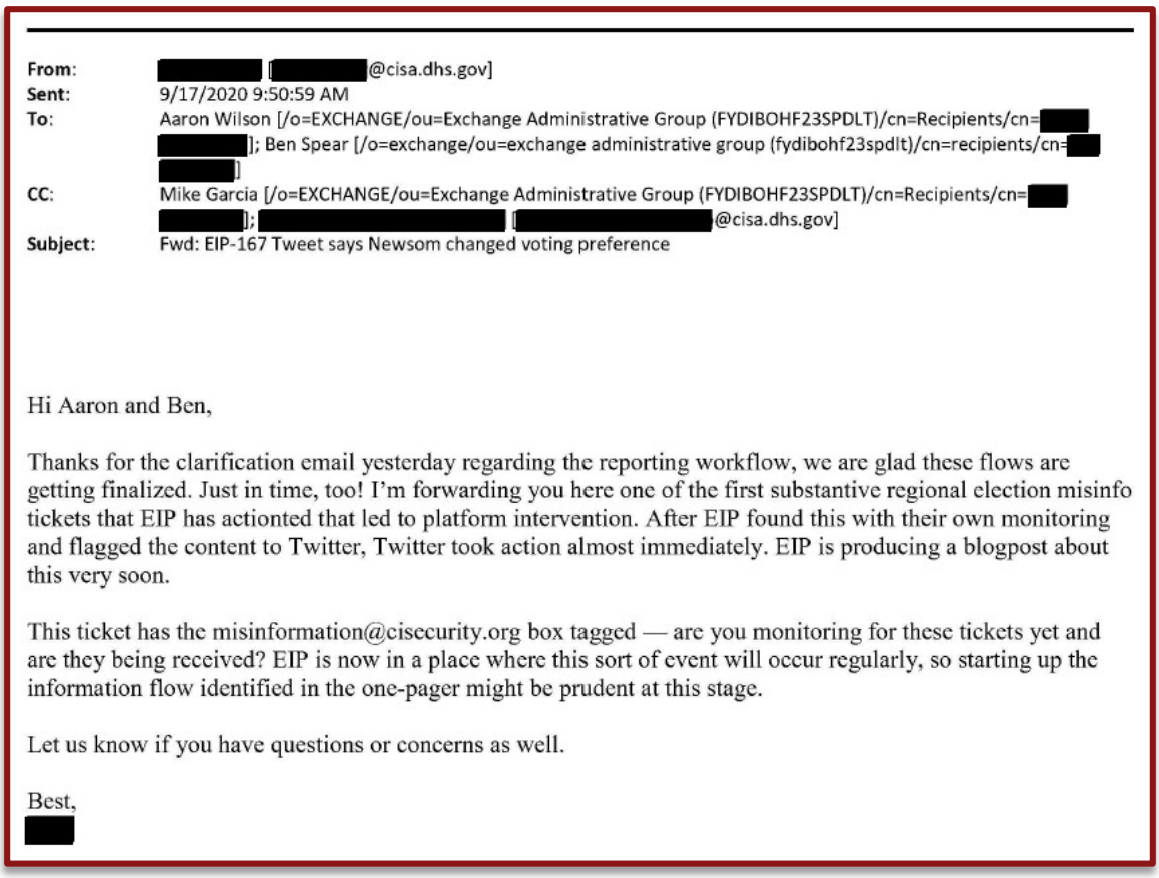
The close, direct coordination between CISA and the EIP was contemplated from the beginning, as seen in the below diagrams contained in what appear to be early EIP briefing materials. Multiple steps in the "Proposed Reporting Workflow," explicitly link CISA and the EIP. For example, one step read: "CISA forwards report to appropriate social media platform(s) and to the EIP (or EI-ISAC can send directly to EIP)."[114] Another diagram, titled "Major Stakeholders" drew a link between the EIP, CISA, and the Intelligence Community.[115]





[114] Proposed Reporting Workflow (unpublished diagram) (on file with the Comm.).
[115] Election Disinformation Partnership: Overview for Partners (unpublished presentation notes) (on file with the Comm.).

This arrangement quickly bore fruit for the federal government's censorship-laundering operation. On September 17, a CISA official emailed CIS's Aaron Wilson and Ben Spear, writing: "I'm forwarding you here one of the first substantive regional election misinfo tickets that EIP has actioned that led to platform intervention. After EIP found this with their own monitoring and flagged the content to Twitter, Twitter took action almost immediately."[116] Put plainly, the EIP reported back to the federal government that it had successfully induced Big Tech to censor Americans' political speech on behalf of CISA.



From: [redacted] [redacted]@cisa.dhs.gov]
Sent: 9/17/2020 9:50:59 AM
To: Aaron Wilson [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; Ben Spear [/o=exchange/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=[redacted]]
CC: Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; [redacted] [redacted]@cisa.dhs.gov]
Subject: Fwd: EIP-167 Tweet says Newsom changed voting preference

Hi Aaron and Ben,

Thanks for the clarification email yesterday regarding the reporting workflow, we are glad these flows are getting finalized. Just in time, too! I'm forwarding you here one of the first substantive regional election misinfo tickets that EIP has actionted that led to platform intervention. After EIP found this with their own monitoring and flagged the content to Twitter, Twitter took action almost immediately. EIP is producing a blogpost about this very soon.

This ticket has the misinformation@ciscurity.org box tagged — are you monitoring for these tickets yet and are they being received? EIP is now in a place where this sort of event will occur regularly, so starting up the information flow identified in the one-pager might be prudent at this stage.

Let us know if you have questions or concerns as well.

Best,
[redacted]

CISA knew that flagging individual posts for removal would not be sufficient to achieve its goal of categorically censoring disfavored viewpoints, primarily conservative political speech. Instead, entire "narratives" needed to be targeted for censorship. Pursuant to multiple subpoenas, the Committee and Select Subcommittee obtained communications between CISA, the EIP, and CIS demonstrating that the true objective in flagging content to social media platforms was to censor entire narratives not just specific, flagged posts. However, this did not stop the EIP from identifying massive amounts of social media posts allegedly spreading "misinformation," with some misinformation reports containing over 500 individual links.[117]

[116] Email from CISA official to Aaron Wilson and Ben Spear (Sept. 17, 2020, 9:50 AM) (on file with the Comm.).
[117] EIP-915, submitted by [REDACTED], ticket created (Nov. 5, 2020, 9:07 PM) (archived Jira ticket data produced to the Comm.); *see also* James O'Keefe, TWITTER (Nov. 6, 2020, 5:44 PM), https://twitter.com/JamesOKeefeIII/status/1324845160358940673.

On September 24, one of the CISA-SIO interns wrote: "there is no way we found every piece of misinfo related to this incident, so we don't give a ton of weight to how many of the links that we sent over got actioned (though we hope all would) . . . . Because of this, we see the narrative itself as the most important thing to communicate."[118]

From: [redacted]@cisa.dhs.gov]
Sent: 9/24/2020 5:21:14 PM
To: Aaron Wilson [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; [redacted] [redacted]@cisa.dhs.gov]; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]
CC: Scully, Brian [redacted]@cisa.dhs.gov]; Snell, Allison [redacted]@cisa.dhs.gov]; Tipton, James [redacted]@cisa.dhs.gov]; Dragseth, John [redacted]@cisa.dhs.gov]; Masterson, Matthew [redacted]@cisa.dhs.gov]; Hale, Geoffrey [redacted]@cisa.dhs.gov]
Subject: RE: EIP-167 Tweet says Newsom changed voting preference

Hello Aaron:

Jumping in to answer a couple of the technical questions! We just had an issue with Facebook's reporting box which was configured oddly as a 'bulk' email inbox. Is your mail receiver for misinfo@cisecurity.org automatically dropping emails tagged as 'bulk'? Because if so, the Jira alias where these tips are coming from (which I think is a bulk inbox) won't work with it. I am relaying this from our technical team so can ask for more information as helpful.

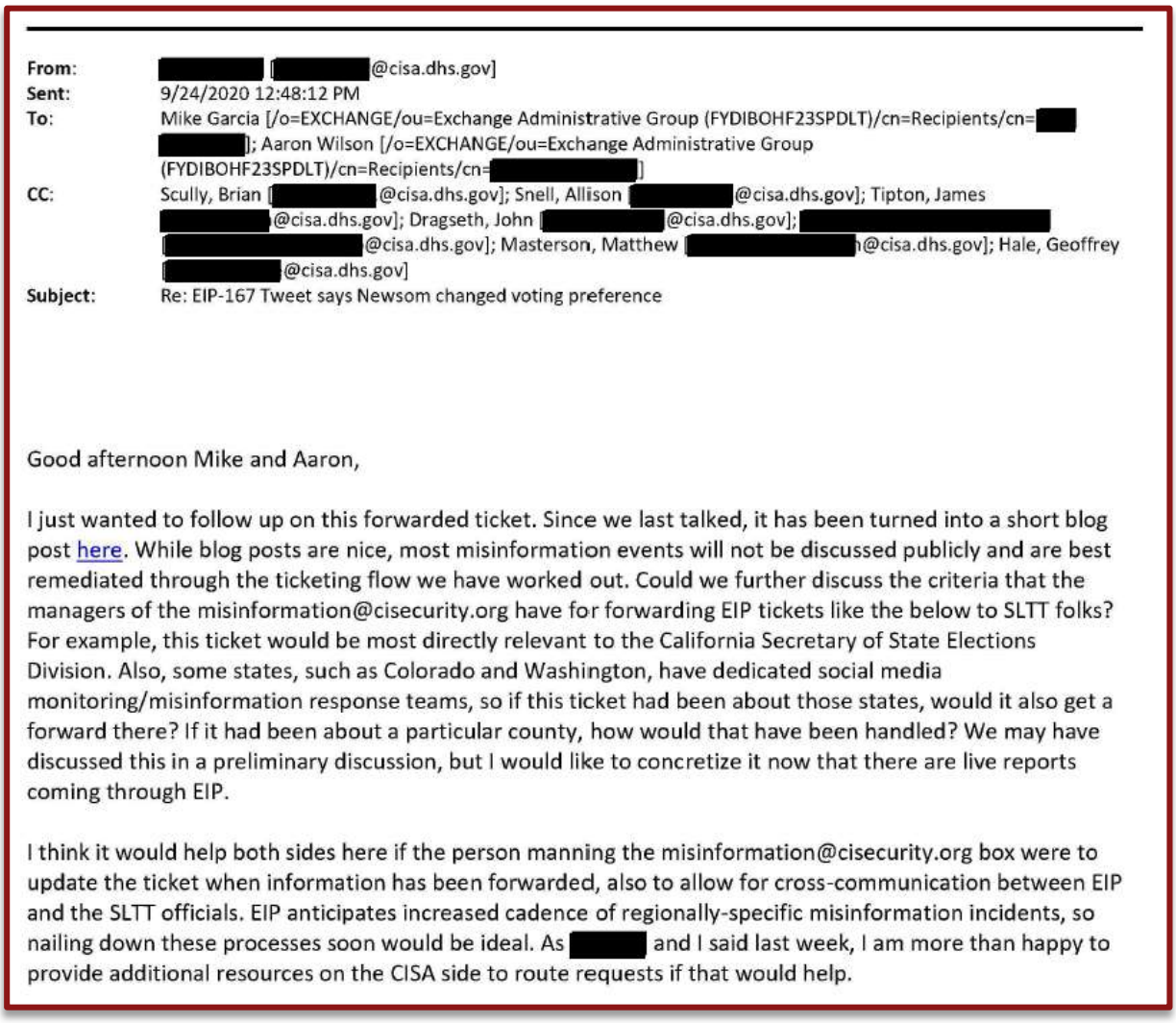
Regarding your second question on whether the ticket is closed: we closed the ticket as we had given the organizations tagged a reasonable amount of time to respond (~1 week in this case) and received no further commentary. We also wrote up our findings publicly. I don't think the status of the ticket as Open or Closed means much for the election officials – we are sending this to you early in hopes of having it go straight to the impacted stakeholders as close to instantly as possible, so that if its of interest, they can ask further questions and we can be responsive to find more information. We just don't know what is helpful to them yet.

As to the action on certain links: there is no way we found every piece of misinfo related to this incident, so we don't give a ton of weight to how many of the links that we sent over got actioned (though we hope all would) because we know we didn't find all the links anyways, and that the platforms are not going to communicate to us how many further leads they found and actioned as well (it could be none, it could be a network of 1000 users. Though they'd likely tell us about the latter). Because of this, we see the narrative itself as the most important thing to communicate, and the links as supplementary examples. We are always available to re-open a case to give further information on a narrative as helpful.

In another email sent on September 24, one of the CISA-SIO interns who was later hired to the full-time staff at CISA offered support for the joint censorship enterprise, writing, "EIP anticipates increased cadence of regionally-specific misinformation incidents, so nailing down

[118] Email from CISA official to Aaron Wilson and Mike Garcia (Sept. 24, 2020, 5:21 PM) (on file with the Comm.).

these processes soon would be ideal . . . . I am more than happy to provide additional resources on the CISA side to route requests if that would help."[119]



From: [redacted] [redacted]@cisa.dhs.gov]
Sent: 9/24/2020 12:48:12 PM
To: Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; Aaron Wilson [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]
CC: Scully, Brian [redacted]@cisa.dhs.gov]; Snell, Allison [redacted]@cisa.dhs.gov]; Tipton, James [redacted]@cisa.dhs.gov]; Dragseth, John [redacted]@cisa.dhs.gov]; [redacted]@cisa.dhs.gov]; Masterson, Matthew [redacted]@cisa.dhs.gov]; Hale, Geoffrey [redacted]@cisa.dhs.gov]
Subject: Re: EIP-167 Tweet says Newsom changed voting preference

Good afternoon Mike and Aaron,

I just wanted to follow up on this forwarded ticket. Since we last talked, it has been turned into a short blog post here. While blog posts are nice, most misinformation events will not be discussed publicly and are best remediated through the ticketing flow we have worked out. Could we further discuss the criteria that the managers of the misinformation@cisecurity.org have for forwarding EIP tickets like the below to SLTT folks? For example, this ticket would be most directly relevant to the California Secretary of State Elections Division. Also, some states, such as Colorado and Washington, have dedicated social media monitoring/misinformation response teams, so if this ticket had been about those states, would it also get a forward there? If it had been about a particular county, how would that have been handled? We may have discussed this in a preliminary discussion, but I would like to concretize it now that there are live reports coming through EIP.

I think it would help both sides here if the person manning the misinformation@cisecurity.org box were to update the ticket when information has been forwarded, also to allow for cross-communication between EIP and the SLTT officials. EIP anticipates increased cadence of regionally-specific misinformation incidents, so nailing down these processes soon would be ideal. As [redacted] and I said last week, I am more than happy to provide additional resources on the CISA side to route requests if that would help.

Furthermore, while the SIO has claimed that the "EIP's goal was and continues to be to research and analyze attempts to prevent or deter people from voting," the SIO-affiliated individual wrote in the same email that "[w]hile blog posts are nice, most misinformation events will not be discussed publicly and are best remediated through the ticketing flow we have worked out."[120]

Evidence obtained by the Committee and Select Subcommittee also makes clear that the highest levels of CISA leadership, including then-Director Krebs, had awareness of the CISA-

[119] Email from CISA official to Mike Garcia and Aaron Wilson (Sept. 24, 2020, 12:48 PM) (on file with the Comm.).
[120] *Cf. id.*; *Background on the SIO's Projects on Social Media*, STANFORD INTERNET OBSERVATORY (Mar. 17, 2023), https://cyber.fsi.stanford.edu/io/news/background-sios-projects-social-media.

EIP-CIS censorship campaign.[121] On September 25, 2020, an email from CISA to CIS reveals that Twitter took "action on one of the tweets in [an EIP] ticket. Evidently Director Krebs personally reached out to [SIO head] Stamos asking what had happened around this event around the time the content was taken down."[122] In internal Atlantic Council email exchanges around this time, EIP members stated that "Krebs CISA is texting Stamos with some regularity."[123]

From: [redacted] [redacted]@cisa.dhs.gov]
Sent: 9/25/2020 7:45:38 PM
To: Aaron Wilson [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; Misinformation Reports [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=093d02c79b0f4dba805c5322cd750647-misinformation]
CC: Ben Spear [/o=exchange/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=[redacted]]; [redacted] [redacted]@cisa.dhs.gov]
Subject: Re: EIP-243 Claim the thousands of ballots found in dumpster in Sonoma

Hi all,

Just bumping this. Twitter has now taken action on one of the tweets in this ticket. Evidently Director Krebs personally reached out to Stamos asking what had happened around this event around the time the content was taken down, which was only an hour after this ticket was created. If this system is to work, we will need the turnaround time to be much faster for sending these tickets out to states.

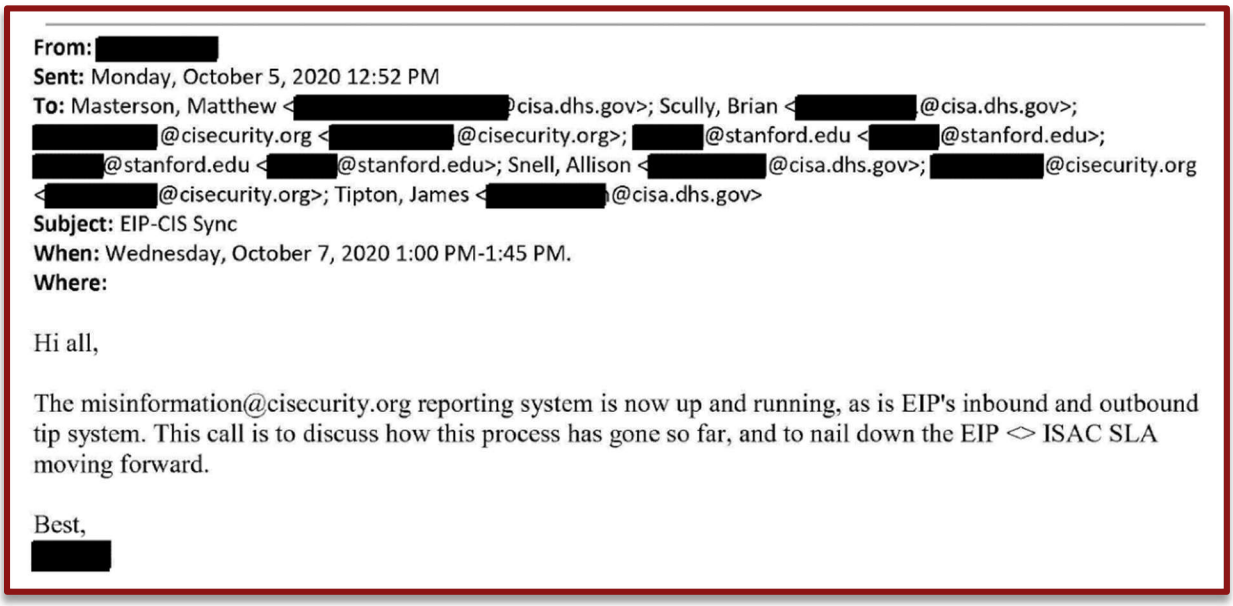
Can anyone advise on next steps for actioning this event?

Thank you,
[redacted]

Overt coordination between CISA, the EIP, and CIS continued well into the 2020 election cycle. On October 5, 2020, Masterson, Scully, Stamos, and Garcia, among others, were invited to a meeting titled "EIP-CIS Sync."[124] According to the email invitation: "The misinformation@cisecurity.org reporting system is now up and running, as is EIP's inbound and

[121] *See e.g.,* email from CISA official to Aaron Wilson and Mike Garcia (Sept. 25, 2020, 7:45 PM) (on file with the Comm.).
[122] *Id.*
[123] Email exchange between Graham Brookie, Andy Carvin and Emerson Brooking (Sept. 30, 2020 5:05 PM) (on file with the Comm.).
[124] Email from CISA official to CISA officials, CIS employees, and SIO affiliates (Oct. 5, 2020, 12:52 PM) (on file with the Comm.).

outbound tip system. This call is to discuss how this process has gone so far, and to nail down the EIP <> ISAC SLA moving forward."[125]



From: [redacted]
Sent: Monday, October 5, 2020 12:52 PM
To: Masterson, Matthew <[redacted]@cisa.dhs.gov>; Scully, Brian <[redacted]@cisa.dhs.gov>; [redacted]@cisecurity.org <[redacted]@cisecurity.org>; [redacted]@stanford.edu <[redacted]@stanford.edu>; [redacted]@stanford.edu <[redacted]@stanford.edu>; Snell, Allison <[redacted]@cisa.dhs.gov>; [redacted]@cisecurity.org <[redacted]@cisecurity.org>; Tipton, James <[redacted]@cisa.dhs.gov>
Subject: EIP-CIS Sync
When: Wednesday, October 7, 2020 1:00 PM-1:45 PM.
Where:

Hi all,

The misinformation@cisecurity.org reporting system is now up and running, as is EIP's inbound and outbound tip system. This call is to discuss how this process has gone so far, and to nail down the EIP <> ISAC SLA moving forward.

Best,
[redacted]

An email from CIS, sent on October 21, 2020, demonstrates that CIS was keeping track of both the "CISA track" and the "EIP track" for flagging posts on social media platforms.[126]

From: Mike Garcia <[redacted]@cisecurity.org>
Sent: Wednesday, October 21, 2020 10:24 AM
To: Amy Cohen <[redacted]@nased.org>; Misinformation Reports <misinformation@cisecurity.org>; Aaron Wilson <[redacted]@cisecurity.org>; Maria Benson <[redacted]@sso.org>
Cc: Scully, Brian <[redacted].@cisa.dhs.gov>
Subject: Re: Misinformation regarding online replacement ballot portal

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

Brian may know otherwise but I don't believe we heard back from the platforms on the "CISA track" just on the EIP track.

The EIP and CISA had another meeting to coordinate their censorship operation on October 29, 2020, as evidenced by a meeting invitation with the subject "EIP EIS [Election

[125] *Id*.
[126] Email from Mike Garcia to Amy Cohen, misinformation@cisecurity.org, Aaron Wilson, and Maria Benson (Oct. 21, 2020, 10:24 AM) (on file with the Comm.).

Security Initiative] Call Disinfo Pre-Brief."[127] EIS appears to be in reference to CISA's Election Security Initiative, which included Geoff Hale and Matt Masterson at the time.

Appointment

From: [redacted] [redacted]@cisa.dhs.gov]
Sent: 10/28/2020 7:12:36 PM
To: [redacted] [redacted]@cisa.dhs.gov]; Snell, Allison [redacted]@cisa.dhs.gov]; Hale, Geoffrey [redacted]@cisa.dhs.gov]; Masterson, Matthew [redacted]cisa.dhs.gov]; [redacted]@stanford.edu; [redacted]@stanford.edu; Graham Brookie [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; [redacted]@wu.edu; Emerson Brooking [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn[redacted]]; [redacted]@uw.edu; Scully, Brian [redacted]@cisa.dhs.gov]; Dragseth, John [redacted]@cisa.dhs.gov]
Subject: EIP EIS Call Disinfo Pre-Brief
Start: 10/29/2020 10:30:00 AM
End: 10/29/2020 10:45:00 AM
Show Time As: Busy
Recurrence: (none)

B. Jira Tickets: The Main Weapon in the EIP's Censorship Arsenal

Once the EIP had been formally organized on July 26, 2020, it quickly set about devising a method to mass-report content that it deemed undesirable to the relevant social media platforms. The EIP's tipline of choice was Jira, an issue-tracking software developed by Atlassian, an Australian software company.[128] According to the EIP's post-election report, the EIP "chose Jira because it supported a large team and allowed the addition of workflows that require both robust customer management capabilities and organizational features to reflect the numerous roles needed to respond to any inbound request."[129]

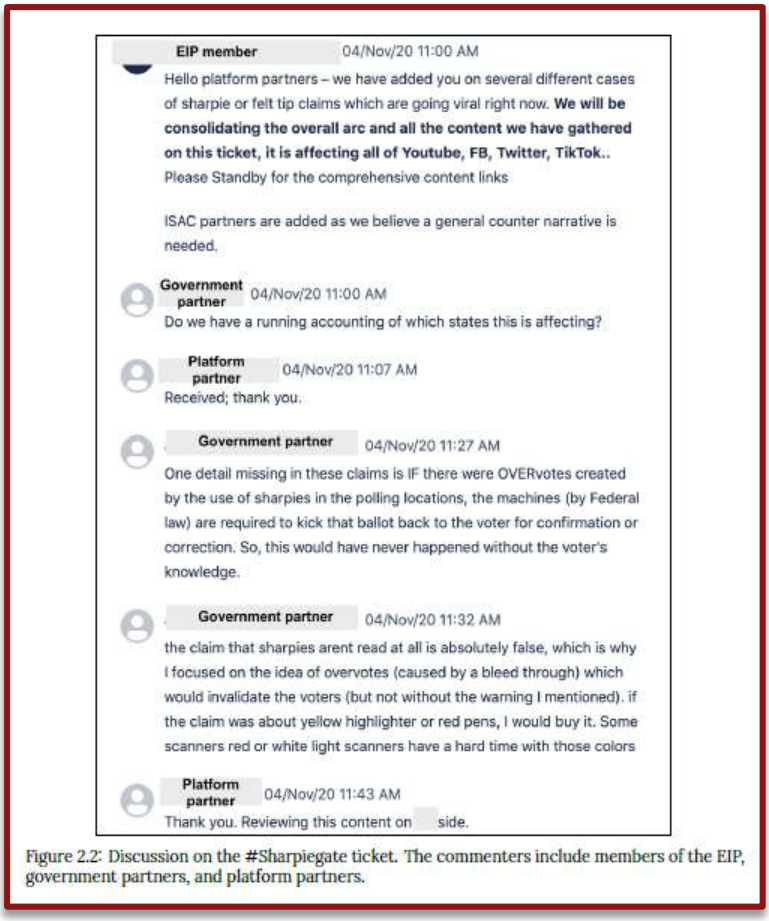


Figure 2.2: Discussion on the #Sharpiegate ticket. The commenters include members of the EIP, government partners, and platform partners.

The EIP's report including an example image of what a Jira

[127] Email from CISA official to CISA officials and EIP personnel (Oct. 28, 2020, 7:12 PM) (on file with the Comm.).
[128] *See Jira Software*, ATLASSIAN, https://www.atlassian.com/software/jira (last visited Nov. 3, 2023).
[129] ELECTION INTEGRITY P'SHIP, *supra* note at 16, at 24.

ticket looked like, demonstrating how the Jira system allowed for real-time collaboration by "members of the EIP, government partners, and platform partners."[130]

C. The Collusion in Practice: The Coordinated Flagging of Posts

Pursuant to a subpoena, CISA has produced to the Committee and Select Subcommittee dozens of emails in which CIS sent reports of misinformation from state and local election officials to both the EIP and CISA. CISA then switchboarded the reports to the relevant social media platforms. CIS frequently included both CISA and the EIP on the same email chains, including CISA's Brian Scully, CISA's CFITF, and the EIP (as indicated by the EIP email domain "@2020partnership.atlassian.net).[131]

Plainly put, the federal government, CIS, and the EIP were all on the same email chains discussing the censorship of Americans' political speech. One of just many examples is shown below.[132] While Stanford and SIO Director (and effectively the head of the EIP) Alex Stamos have given carefully crafted statements and testimony to the Committee and Select Subcommittee that CISA could not *directly* report misinformation content to the EIP, this email chain and others show that CISA routinely was copied on emails from CIS to the EIP reporting misinformation.[133] In other words, while CISA did not directly report content *to the EIP*, CISA had complete visibility on what was being reported to the EIP and at the same time was reporting the same content directly to the social media platforms. While CISA had "no official role," CISA knew what reports were being submitted to the EIP, received Jira ticket reports and notifications via email, had personnel with direct access to the EIP ticketing system, and was in direct contact with the social media platforms.

From: Misinformation Reports <[redacted]@cisecurity.org>
Date: November 11, 2020 at 4:49:18 PM EST
To: Brian Scully <[redacted].@cisa.dhs.gov>, CISA Central [redacted]@cisa.dhs.gov>, CISA CFITF [redacted]@hq.dhs.gov>, EIP <[redacted]@2020partnership.atlassian.net>, Misinformation Reports <[redacted]@cisecurity.org>
Subject: Case #CIS-MIS000196: allegations of election fraud

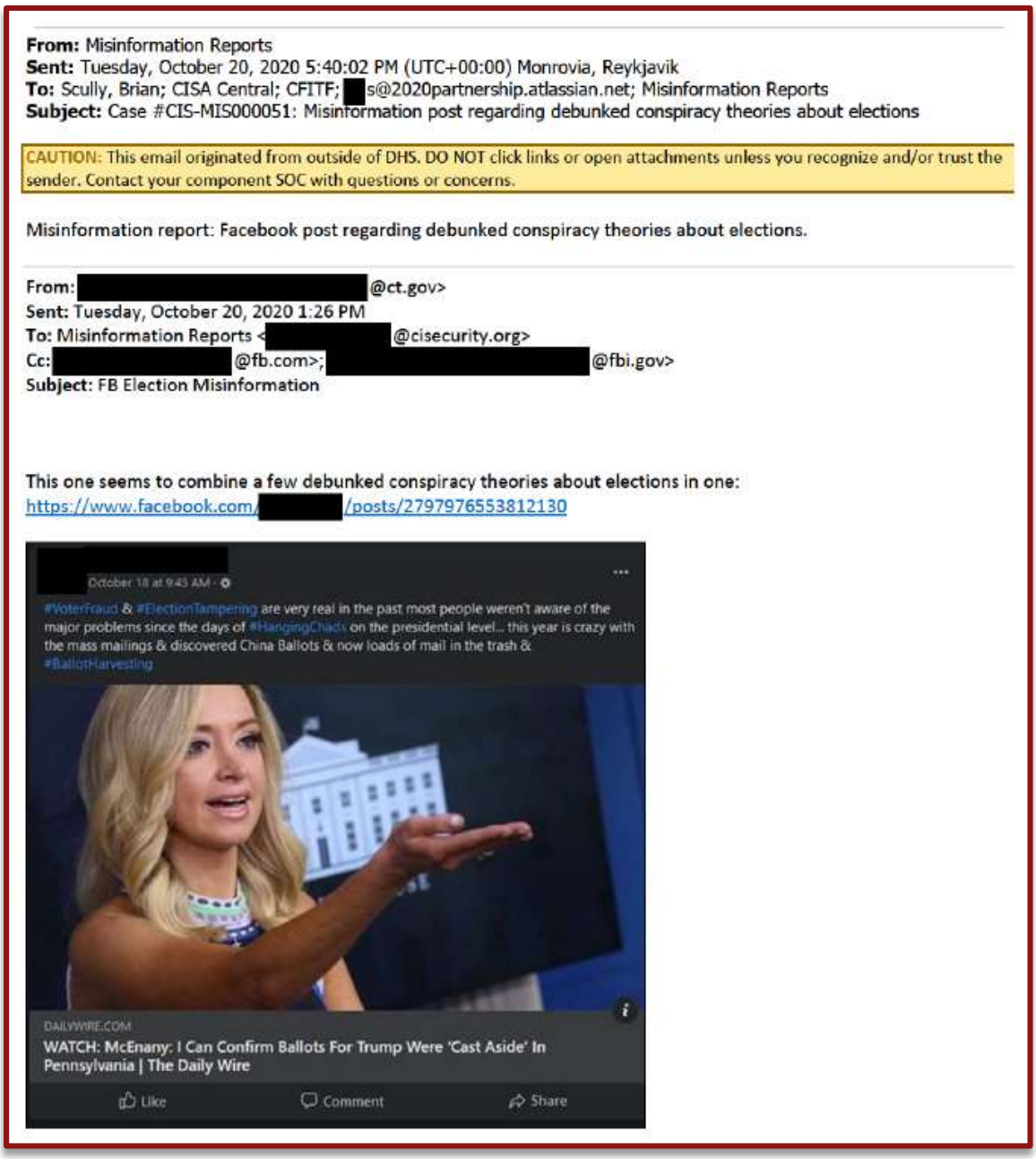
Twitter account alleging election fraud: https://twitter.com/[redacted]

In another characteristic example below, CIS's "Misinformation Reports" email account sent an email to Brian Scully, CISA Central, CISA's CFITF, and EIP, which read:

---

[130] *Id*. at 30.
[131] *See, e.g.*, email from CIS to Brian Scully, CISA Central, CFITF, and EIP personnel (Nov. 11, 2020 4:49 PM) (on file with the Comm.).
[132] Email from CIS to Brian Scully, CISA Central, CFITF, and EIP personnel (Nov. 11, 2020 4:49 PM) (on file with the Comm.).
[133] House Judiciary Committee's Transcribed Interview of Alex Stamos (June 23, 2023), at 224 (on file with the Comm.) ("I still believe we did not receive any *direct* requests from CISA.") (emphasis added); *Background on the SIO's Projects on Social Media*, STANFORD INTERNET OBSERVATORY (Mar. 17, 2023), https://cyber.fsi.stanford.edu/io/news/background-sios-projects-social-media ("Did EIP receive *direct* requests from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) to eliminate or censor tweets? No.") (emphasis added).

"Misinformation report: Facebook post regarding debunked conspiracy theories about elections."[134] The Facebook post in question linked to an article from the Daily Wire, a prominent conservative publication.[135]



From: Misinformation Reports
Sent: Tuesday, October 20, 2020 5:40:02 PM (UTC+00:00) Monrovia, Reykjavik
To: Scully, Brian; CISA Central; CFITF; [redacted]s@2020partnership.atlassian.net; Misinformation Reports
Subject: Case #CIS-MIS000051: Misinformation post regarding debunked conspiracy theories about elections

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

Misinformation report: Facebook post regarding debunked conspiracy theories about elections.

From: [redacted]@ct.gov>
Sent: Tuesday, October 20, 2020 1:26 PM
To: Misinformation Reports <[redacted]@cisecurity.org>
Cc: [redacted]@fb.com>; [redacted]@fbi.gov>
Subject: FB Election Misinformation

This one seems to combine a few debunked conspiracy theories about elections in one:
https://www.facebook.com/[redacted]/posts/2797976553812130

[redacted]
October 18 at 9:45 AM ·
#VoterFraud & #ElectionTampering are very real in the past most people weren't aware of the major problems since the days of #HangingChads on the presidential level... this year is crazy with the mass mailings & discovered China Ballots & now loads of mail in the trash & #BallotHarvesting

DAILYWIRE.COM
WATCH: McEnany: I Can Confirm Ballots For Trump Were 'Cast Aside' In Pennsylvania | The Daily Wire
Like Comment Share

Emails from CIS to CISA and EIP continued throughout the 2020 election cycle, including the months of October and November 2020, during which time many Americans relied

[134] Email from CIS to Brian Scully, CISA Central, CFITF, and EIP personnel (Oct. 20, 2020 5:40 PM) (on file with the Comm.).
[135] *See* Hank Berrien, *WATCH: McEnany: I Can Confirm Ballots For Trump Were 'Cast Aside' In Pennsylvania*, THE DAILY WIRE (Sept. 24, 2020).

on information shared on social media platforms to inform their vote. Moreover, a significant number of emails from CIS were directly addressed specifically to CISA CFITF team lead "Brian [Scully] and EIP" and included employees of the social media platforms hosting the content of concern.

On November 5, for example, an email was sent from CIS's Misinformation Reports email address to CISA, the EIP, and Facebook, which read "Brian and EIP – we have included Facebook in this report."[136] The email copied two employees of Facebook directly on the report of "misinformation."[137] Thus, the Facebook personnel on the receiving end of this email would understand that CISA and the EIP were receiving the same notifications at the same time. Emails such as this one revealed that the federal government had direct knowledge of what was being reported to the EIP.

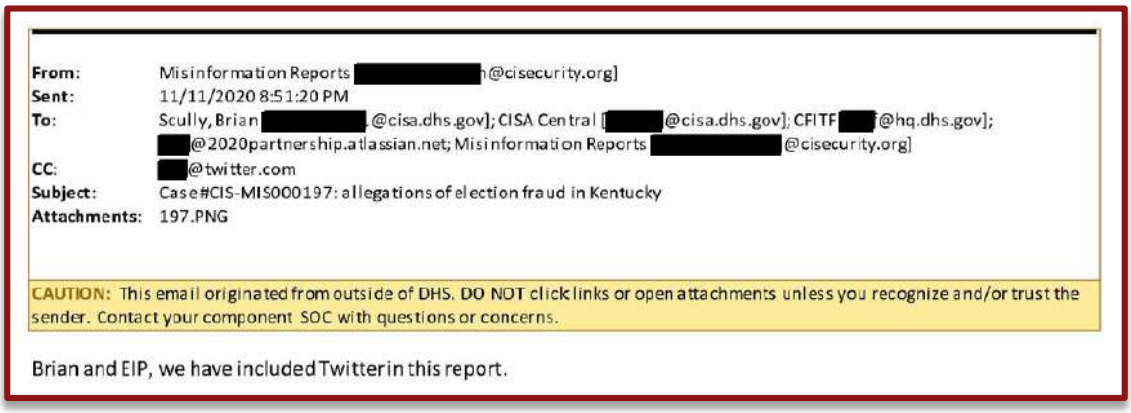
From: Misinformation Reports [redacted]@cisecurity.org]
Sent: 11/5/2020 5:18:37 PM
To: Scully, Brian [redacted].@cisa.dhs.gov]; CISA Central [redacted]@cisa.dhs.gov]; CFITF [redacted]@hq.dhs.gov]; [redacted]@2020partnership.atlassian.net; Misinformation Reports [redacted]@cisecurity.org]
CC: [redacted]@fb.com' [redacted]@fb.com]
Subject: Case#CIS-MIS000177: Facebook post alleging election fraud
Attachments: 177.PNG

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

Brian and EIP – we have included Facebook in this report.

Misinformation Report: Facebook post alleging election fraud

On November 11, CIS sent an email to a Twitter employee, multiple CISA accounts, and the EIP, writing, "Brian and EIP, we have included Twitter in this report."[138] The email copied an employee of Twitter on the alert about "misinformation."[139]



From: Misinformation Reports [redacted]n@cisecurity.org]
Sent: 11/11/2020 8:51:20 PM
To: Scully, Brian [redacted].@cisa.dhs.gov]; CISA Central [redacted]@cisa.dhs.gov]; CFITF [redacted]@hq.dhs.gov]; [redacted]@2020partnership.atlassian.net; Misinformation Reports [redacted]@cisecurity.org]
CC: [redacted]@twitter.com
Subject: Case#CIS-MIS000197: allegations of election fraud in Kentucky
Attachments: 197.PNG

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

Brian and EIP, we have included Twitter in this report.

[136] Email from CIS to Brian Scully, CISA Central, CFITF, EIP, and Facebook employees (Nov. 5, 2020 5:18 PM) (on file with the Comm.).
[137] *Id*.
[138] Email from CIS to Brian Scully, CISA Central, CFITF, EIP, and Twitter employee (Nov. 11, 2020 8:51 PM) (on file with the Comm.).
[139] *Id*.

In one particularly alarming instance, CIS forwarded a report from the Arizona Secretary of State's Office—led at the time by Katie Hobbs, a Democrat—to CISA, the EIP, and Facebook: "Brian and EIP, I included Facebook in this report."[140] In the original "misinformation" report to CIS, an Information Security Officer at the Arizona Secretary of State's Office flagged a Facebook URL, writing, "[t]his post was on a *private* [Facebook] page."[141]

From: Misinformation Reports [redacted]@cisecurity.org]
Sent: 11/6/2020 10:08:42 AM
To: Scully, Brian [redacted]@cisa.dhs.gov]; CISA Central [redacted]cisa.dhs.gov]; CFITF [redacted]@hq.dhs.gov]; [redacted]2020partnership.atlassian.net; Misinformation Reports [redacted]@cisecurity.org]
CC: [redacted]@fb.com' [redacted]@fb.com]
Subject: Case#CIS-MIS000182: Misinformation post that Trump already won AZ
Attachments: misinformation.jpg

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

Brian and EIP, I included Facebook in this report.

Misinformation report: (private) Facebook post that Trump already won AZ

From: [redacted]@azsos.gov>
Sent: Friday, November 6, 2020 9:54 AM
To: Misinformation Reports <[redacted]n@cisecurity.org>
Subject: Fake statement by Arizona Election Worker about fraud

Hi There.

https://www.facebook.com/photo.php?fbid=[redacted]

This post was on a private FB page, above. I've included a screenshot.

Thank you!

[redacted]
Information Security Officer
Arizona Secretary of State's Office

Email: [redacted]@azsos.gov
Office: [redacted]
Cell: [redacted]

KATIE HOBBS
SECRETARY OF STATE
State of Arizona

[140] Email from CIS to Brian Scully, CISA Central, CFITF, EIP, and Facebook employees (Nov. 6, 2020 10:08 AM) (on file with the Comm.).
[141] *Id*. (emphasis added).

While the First Amendment certainly applies to states and state officials, it is concerning that Secretary Hobbs expended her office's limited resources to flag content on social media regarding a Republican candidate's speech. But even more alarming, Hobbs's staff was apparently trawling through *private* Facebook pages to identify dissent and "misinformation" for removal. According to public reporting, Hobbs's office continued flagging social media posts well after the election, into January 2021.[142] In some cases, Hobbs's staff emailed the social media platforms directly, requesting that posts criticizing her be censored.[143]

Even more damaging to the argument that CISA and EIP were independent of one another is the fact that CISA personnel, who supposedly had no access to the EIP's Jira system, referenced the EIP-specific ticket codes when discussing "misinformation" reports. The email below, sent on November 2—the day before the 2020 election—is one such example, in which a CISA official informed Twitter: "Please see below reporting from Connecticut election officials. The ticket is *also tagged EIP-572*."[144]

From: "[redacted]" <[redacted]@cisa.dhs.gov> on behalf of CFITF <[redacted]@hq.dhs.gov>
Date: Monday, November 2, 2020 at 2:34 PM
To: "[redacted]@twitter.com" [redacted]@twitter.com>, "[redacted]@twitter.com" [redacted]@twitter.com>, "[redacted]@twitter.com" [redacted]@twitter.com>, "[redacted]@twitter.com" <[redacted]@twitter.com>
Subject: FW: Case #CIS-MIS000107: twitter post alleging CT will be reverting back to phase 1 (of pandemic) on or before election day

Twitter Gov Team, [redacted]

Please see below reporting from Connecticut election officials. The ticket is also tagged EIP-572.

Regards,

[redacted]
Cybersecurity and Infrastructure Security Agency
[redacted]

At one point, it appears that Christopher Krebs, the then-Director of CISA, directed Robert Schaul, CISA's Analysis and Resilience Policy Lead, to contact Graham Brookie, Senior Director of the Atlantic Council's Digital Forensic Research Lab (DFRLab), to inquire about a particular election-related narrative spreading on social media. In the email, Schaul wrote: "We're getting the EIP take as well but wanted to check in with you . . . . [Director Krebs is] particularly interested in any analytics we can pull together on the narrative as well as where it's coming from and who is amplifying it."[145] Internal Atlantic Council documents show that

[142] *See* Jeremy Duda, *Secretary of State Had Disinformation Pulled From Twitter*, AXIOS (Dec. 6, 2022).
[143] *See* Houston Keene, *Dem Gov Katie Hobbs Requested Twitter Censor Critics of Tweet Comparing Trump Supporters to Nazis*, FOX NEWS (Aug. 10, 2023).
[144] Email from CISA official to Twitter employees (Nov. 2, 2020 2:34 PM) (on file with the Comm.) (emphasis added).
[145] Email from Robert Schaul to Graham Brookie (Nov. 10, 2020 8:31 AM) (on file with the Comm.).

Brookie and others understood that Director Krebs and SIO Director Alex Stamos were texting "with some regularity."[146]

From: Graham Brookie <gbrookie@ATLANTICCOUNCIL.ORG>
Sent: Wednesday, September 30, 2020 5:05 PM
To: Andy Carvin <ACarvin@ATLANTICCOUNCIL.org>; Emerson Brooking <EBrooking@ATLANTICCOUNCIL.org>
Subject: ANDY / EMERSON -- Coordination

COORDINATION ON US DOMESTIC PRIORITIES

Hi to both –

The struggle here is that Emerson is managing efforts and Andy is managing staff and outputs. The only way to be successful is to make sure that the three of us are explicitly on the same page about how we are allocating staff to efforts.

The below is intended to do that – and I will be adding Emerson to the DCHQ WhatsApp chain, where we will coordinate in general, as soon as we're on the same page as below. Our first obligation is always to our staff and not setting them up for failure. Our second obligation is to our core work, which every single one of us is managing key elements of. Thus the burden falls on the three of us to coordinate both.

Please reply in red or blue to the below. I also didn't have explicit names in the "staffing" section of each, so please fill out.

Thanks,
Graham

Election Integrity Partnership
Key questions: What is the schedule of shifts, noting that we just need to assign people to them? EIP, the voluntary shift system is a potential challenge because it requires a person to spend X amount of hours monitoring things, which either results in no outputs being produced, or a sudden need to complete an output that the person may or may not be suited to complete, especially if it's an international member of the team with limited knowledge of US politics, geography, culture, etc.

In scenarios where something potentially important surfaces within EIP, how do we go about prioritizing it? For example, when is it simply a matter of "this is a good story so please get me a draft in 72 hours" vs "all hands on deck, this is like a major takedown?" In either case, the three of us need to locked up in order to not undermine our whole business operation through editorial capacity, who gets assigned, scheduling, etc.

One not ideal scenario is a situation where Jean or Ayush volunteer for a few hours, end up finding something important, and then having not having all three of our awareness and approval, which could lead to significant members of staff being taken away from their core responsibilities for extended periods of days/week. In other words, a shift is just the tip of the iceberg, commitment-wise.

Another question is what constitutes a contribution to EIP. While the focus has been on the partnership and the process (which makes sense) we're part of a team reviewing leads and deciding when to act on them. But we also continue to cover election-related stories that will originate from our original research, rather than the college students volunteering at EIP, especially now that Jared is coming on board and while looking into more conspiracy related content. Can we consider those contributions? I imagine for some researchers there's more incentive to contribute when they're able to generate research leads themselves rather than being responsive to tips, though I understand responding to tips is still core to the partnership.

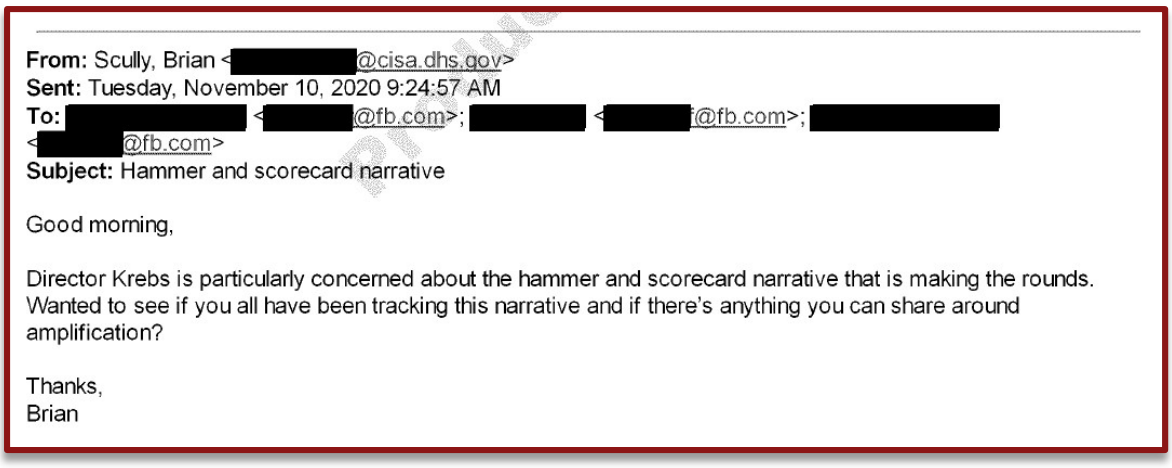
Important to note: not college kids surfacing EIP leads. Krebs CISA is texting Stamos with some regularity. A few tickets have been flagged by the platforms. Starbird's UW team is surfacing a lot of stuff using advanced soc media listening methods. College kids (T-1) just doing the first round of analysis.

The job of DFRLab is to be T-2, doing a deep dive into tickets, attaching more contextual information, and writing up a twitter thread/blog post if that's the recommendation of the researcher (and the T-3 shift manager approves).

Analysts can step away and write a blog post on-shift. That's what Alyssa did last week.

[146] Email exchange between Graham Brookie, Andy Carvin and Emerson Brooking (Sept. 30, 2020 5:05 PM) (on file with the Comm.).

CISA personnel also solicited information about political speech on social media from employees of the platforms. On the same day, November 10, Scully sent an email to three Facebook employees, writing, "Director Krebs is particularly concerned about the hammer and scorecard narrative that is making the rounds. Wanted to see if you have been tracking this narrative and if there's anything you can share around amplification?"[147]



From: Scully, Brian <[redacted]@cisa.dhs.gov>
Sent: Tuesday, November 10, 2020 9:24:57 AM
To: [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>; [redacted] <[redacted]@fb.com>
Subject: Hammer and scorecard narrative

Good morning,

Director Krebs is particularly concerned about the hammer and scorecard narrative that is making the rounds. Wanted to see if you all have been tracking this narrative and if there's anything you can share around amplification?

Thanks,
Brian

These emails directly contradicts claims that CISA had only a "very little role, if none" in the EIP.[148] To the contrary, CISA had real-time awareness of what was being submitted to EIP, what steps EIP was conducting, and what actions the social media platforms were taking—and EIP and the social media platforms were aware of CISA's significant role.

D. The State Department's Direct Participation in the EIP's Censorship Operation

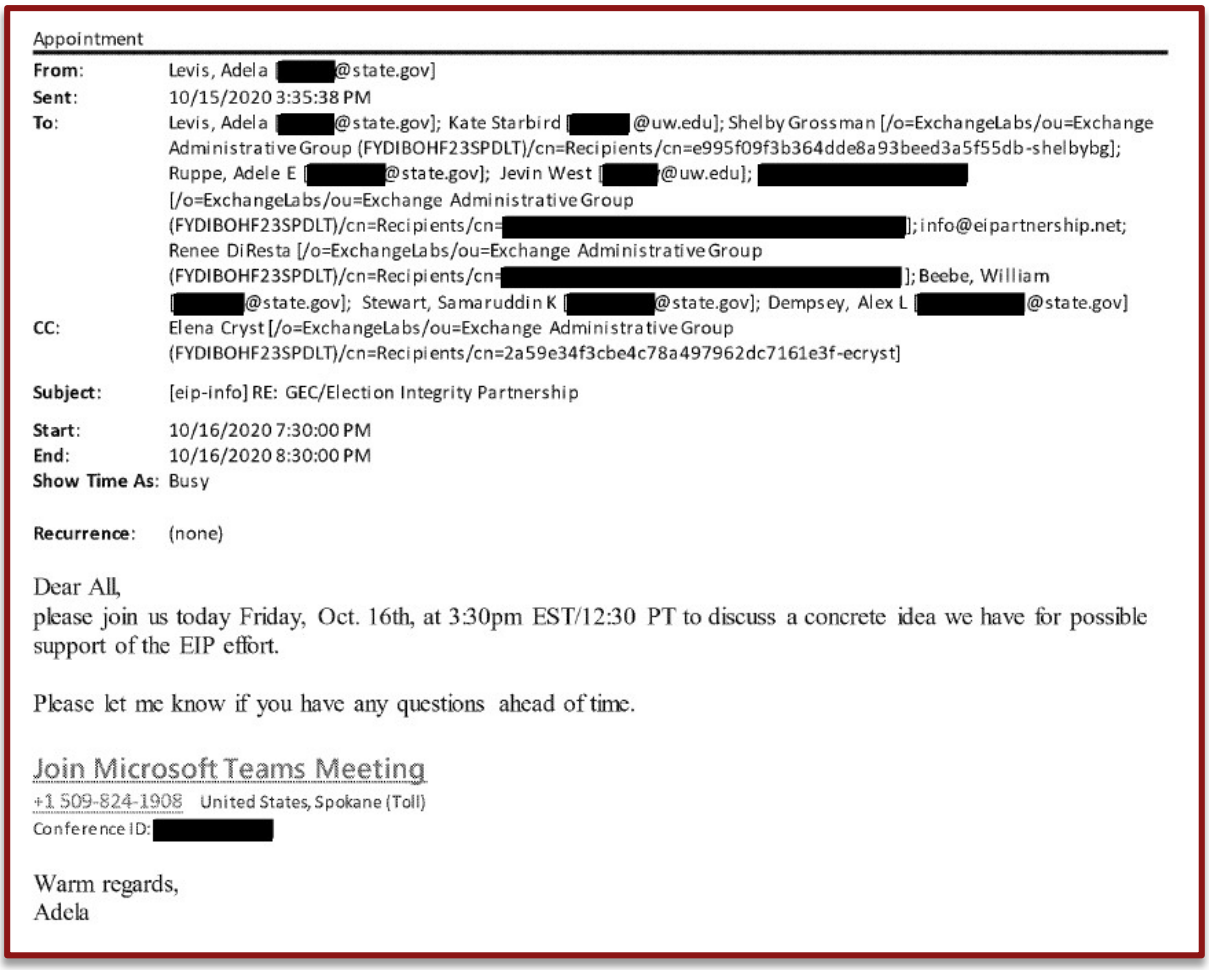
The Global Engagement Center (GEC) is a multi-agency organization housed within the State Department, which Elon Musk has described as "[t]he worst offender in US government censorship & media manipulation."[149] The GEC and GEC-funded entities have, on multiple occasions flagged content to social media platforms that included Americans engaged in constitutionally protected speech.[150]

---

[147] Email from Brian Scully to Facebook employees (Nov. 10, 2020 9:24 AM) (on file with the Comm.).
[148] *Compare* House Judiciary Committee's Transcribed Interview of Alex Stamos (June 23, 2023), at 95 (on file with the Comm.); Letter to John B. Bellinger, III, from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (June 1, 2023), at 2; *and* Letter from John B. Bellinger III to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (June 14, 2023), at 4 (on file with the Comm.) *with* email from Graham Brookie to Atlantic Council employees (July 31, 2020, 5:54 PM) (on file with the Comm.); email from CISA staff to Aaron Wilson, Ben Spear, and Mike Garcia (Sept. 3, 2020, 1:51 PM) (on file with the Comm.); *and* email from Brian Scully to Facebook employees (Nov. 10, 2020 9:24 AM) (on file with the Comm.).
[149] Elon Musk (@elonmusk), TWITTER (Feb. 6, 2023, 6:32 PM), https://twitter.com/elonmusk/status/1622739987031552002.
[150] *See, e.g.*, Matt Taibbi (@mtaibbi), TWITTER (Mar. 2, 2023, 12:00 PM), https://twitter.com/mtaibbi/status/1631338687718907904 ("Here are 5500 names GEC told Twitter it believed were 'Chinese… accounts' engaged in 'state-backed coordinated manipulation.' It takes about negative ten seconds to find non-Chinese figures."); Matt Taibbi (@mtaibbi), TWITTER (Mar. 2, 2023, 12:00 PM), https://twitter.com/mtaibbi/status/1631338690931826711 ("GEC's 'Chinese' list included multiple Western government accounts and at least three CNN employees based abroad.").

Unlike CISA's pretext of peripheral non-involvement, the EIP openly admitted that the GEC "reported tickets" to the EIP in its final report looking back on the 2020 election cycle.[151] In fact, according to that report, the GEC was one of the most frequently tagged organizations in the EIP's Jira system.[152]

On October 15, 2020, Adela Levis, an "Academic and Think-Tank Liaison" with the GEC, sent an email invitation to a meeting with the title "GEC/Election Integrity Partnership."[153] In the body of the email, Levis wrote that the meeting was "to discuss a concrete idea we have for possible support of the EIP effort."[154]



Appointment

From: Levis, Adela [redacted]@state.gov]
Sent: 10/15/2020 3:35:38 PM
To: Levis, Adela [redacted]@state.gov]; Kate Starbird [redacted]@uw.edu]; Shelby Grossman [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=e995f09f3b364dde8a93beed3a5f55db-shelbybg]; Ruppe, Adele E [redacted]@state.gov]; Jevin West [redacted]@uw.edu]; [redacted] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; info@eipartnership.net; Renee DiResta [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; Beebe, William [redacted]@state.gov]; Stewart, Samaruddin K [redacted]@state.gov]; Dempsey, Alex L [redacted]@state.gov]
CC: Elena Cryst [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=2a59e34f3cbe4c78a497962dc7161e3f-ecryst]

Subject: [eip-info] RE: GEC/Election Integrity Partnership

Start: 10/16/2020 7:30:00 PM
End: 10/16/2020 8:30:00 PM
Show Time As: Busy

Recurrence: (none)

Dear All,
please join us today Friday, Oct. 16th, at 3:30pm EST/12:30 PT to discuss a concrete idea we have for possible support of the EIP effort.

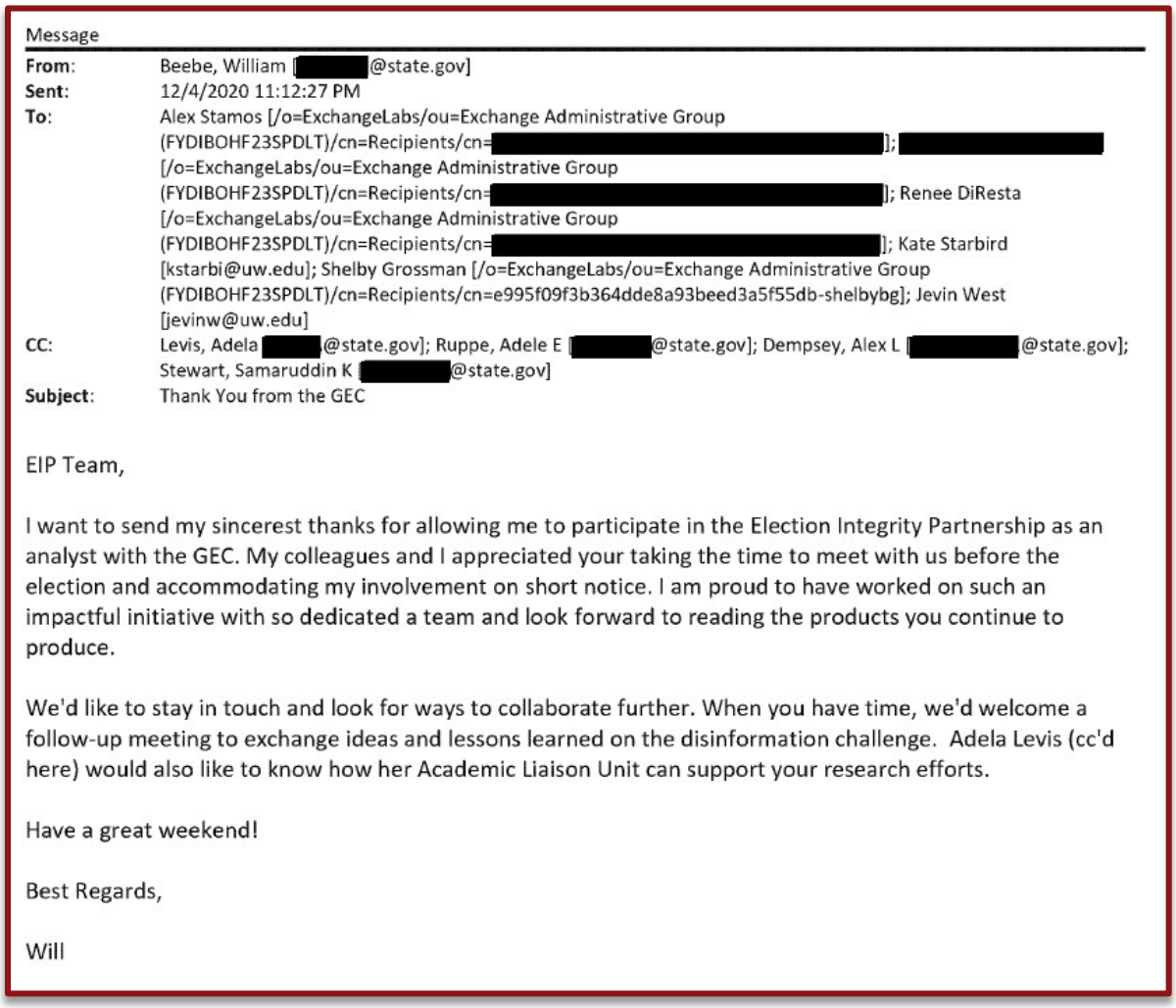
Please let me know if you have any questions ahead of time.

Join Microsoft Teams Meeting
+1 509-824-1908 United States, Spokane (Toll)
Conference ID: [redacted]

Warm regards,
Adela

[151] ELECTION INTEGRITY P'SHIP, *supra* note 16, at 42.
[152] *Id.* at 38.
[153] Email from Adela Levis to Kate Starbird, et. al (Oct. 15, 2020 3:35 PM) (on file with the Comm.).
[154] *Id*.

Following the 2020 election, a "Counter Disinformation Analyst" with the GEC sent an effusive email to SIO Director Alex Stamos, SIO research manager Renée DiResta, and UW's CIP Director Kate Starbird, among others, with the subject "Thank You from the GEC."[155] The analyst gushed: "I want to send my sincerest thanks for allowing me to participate in the Election Integrity Partnership with the GEC. My colleagues and I appreciated your taking the time to meet with us before the election and accommodating my involvement on short notice."[156] The analyst continued, "I am proud to have worked on such an impactful initiative with so dedicated a team."[157]



Message

From: Beebe, William [[redacted]@state.gov]
Sent: 12/4/2020 11:12:27 PM
To: Alex Stamos [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; [redacted] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; Renee DiResta [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; Kate Starbird [kstarbi@uw.edu]; Shelby Grossman [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=e995f09f3b364dde8a93beed3a5f55db-shelbybg]; Jevin West [jevinw@uw.edu]
CC: Levis, Adela [redacted]@state.gov]; Ruppe, Adele E [[redacted]@state.gov]; Dempsey, Alex L [[redacted]@state.gov]; Stewart, Samaruddin K [[redacted]@state.gov]
Subject: Thank You from the GEC

EIP Team,

I want to send my sincerest thanks for allowing me to participate in the Election Integrity Partnership as an analyst with the GEC. My colleagues and I appreciated your taking the time to meet with us before the election and accommodating my involvement on short notice. I am proud to have worked on such an impactful initiative with so dedicated a team and look forward to reading the products you continue to produce.

We'd like to stay in touch and look for ways to collaborate further. When you have time, we'd welcome a follow-up meeting to exchange ideas and lessons learned on the disinformation challenge. Adela Levis (cc'd here) would also like to know how her Academic Liaison Unit can support your research efforts.

Have a great weekend!

Best Regards,

Will

[155] Email from William Beebe to Alex Stamos, Renée DiResta, Kate Starbird, and Jevin West (Dec. 4, 2020 11:12 PM) (on file with the Comm.).
[156] *Id*.
[157] *Id*.

E. Other Federal Agencies' Involvement with the EIP: the FBI and the NSA

CISA was not the only government entity apprised of the EIP's activities. On June 23, 2023, the Committee and Select Subcommittee conducted a transcribed interview of Alex Stamos, examining his and CISA's involvement in the EIP. During the interview, Stamos testified that the SIO briefed several other government agencies about the EIP, including the National Security Agency (NSA) and Cyber Command. Stamos further testified that Federal Bureau of Investigation (FBI) Special Agent Elvis Chan, who was the primary liaison between the FBI and Silicon Valley and was involved in the suppression of news about information damaging to the Biden family found on a laptop belonging to Hunter Biden, arranged the SIO-NSA briefing.

Stamos testified:

> Q. Which other federal agencies did EIP brief?
>
> A. I did a briefing for General Nakasone, then the director of NSA and Cyber Command . . . .
>
> Q. Did the FBI also receive briefings for the election?
>
> A. The FBI was part of that briefing, so I did it from the FBI office in – in San Francisco because I just can't Zoom into the NSA.
>
> Q. Do you recall who set up the meeting between you and the NSA?
>
> A. Elvis Chan had set up the – so the meeting was set up because Nakasone had come to campus. Elvis was the facilitator who provided the space and participated, listened to the briefing in San Francisco.
>
> Q. Yeah. Did you know Mr. Chan before this meeting had occurred?
>
> A. I did.[158]

The SIO continued to provide the FBI with updates on the EIP throughout the 2020 election cycle. For example, on October 5, 2020, Alex Stamos sent an email to Elvis Chan, writing: "Right now, the Election Integrity Partnership is running three shifts each weekday . . . We don't have any good indications of foreign interference from our work, and most of the things we have spotted can be tied to known domestic actors," i.e., Americans.[159]

[158] House Judiciary Committee's Transcribed Interview of Alex Stamos (June 23, 2023), at 98-99 (on file with the Comm.).
[159] Email from Alex Stamos to Elvis Chan and Renee DiResta (Oct. 5, 2020 7:44 PM) (on file with the Comm.).

From: Alex Stamos <[redacted]@stanford.edu>
Sent: Monday, October 5, 2020 7:44 PM
To: Chan, Elvis M. (SF) (FBI) <[redacted]@fbi.gov>; Renee DiResta <[redacted]@stanford.edu>
Subject: Re: [EXTERNAL EMAIL] - RE: Status Update

Elvis-

Right now, the Election Integrity Partnership is running three shifts each weekday (and one on Sunday) looking for election related disinformation. We are handling about a dozen "incidents" per day, which can correspond to multiple pieces of disinformation or just one (this is varying widely). We are intaking reports from locals via EI-ISAC, working with NGOs like Common Cause, and routing issues to platforms to get handled.

It's working pretty well. You can see a handful of incidents we wrote up at eipartnership.net. We will be adding shifts in a couple of weeks and will be staffing a war room at my house (post COVID-testing) on election day.

CONFIDENTIAL SIO-HJC014624

What's your mandate look like? We don't have any good indications of foreign interference from our work, and most of the things we have spotted can be tied to known domestic actors. Probably some foreign amplifiers, but figuring that out is generally outside of our scope and the data we have access to. Check out our "Rapid Reaction" posts and see if any of those kinds of topics are in scope for your work.

Alex

In response to Stamos's question regarding the FBI's mandate, Chan wrote: "The FBI [San Francisco] mandate is to be the conduit to/from the social media companies for all election-related threats, whether foreign or domestic. We've been receiving mostly domestic voter suppression-related accounts to flag for social media companies as each state had its primaries."[160]

Message

From: Chan, Elvis M. (SF) (FBI) [[redacted]@fbi.gov]
Sent: 10/6/2020 4:25:46 PM
To: Alex Stamos [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]; Renee DiResta [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[redacted]]
Subject: RE: [EXTERNAL EMAIL] - RE: Status Update

Hi Alex,

It seems like you have a good system in place and are plugged in with the relevant entities. The FBI SF mandate is to be the conduit to/from the social media companies for all election-related threats, whether foreign or domestic. We've been receiving mostly domestic voter suppression-related accounts to flag for social media companies as each state had its primaries.

At our command post, we'll have a NCRIC-embed who will have access to HISN, EI-ISAC, and MS-ISAC feeds as well. We are hoping USIC partners will be able to declassify information fast enough for us to push out to the companies for awareness.

Since you are also flagging things and sending them to the social media companies, I know they'll be able to relay any coordinated campaigns they see to us for examination and possible case opening. Let's plan to stay in touch as things start to heat up. Thanks!

Regards,
Elvis

[160] Email from Elvis Chan to Alex Stamos and Renee DiResta (Oct. 6, 2020 4:25 PM) (on file with the Comm.).

III. THE EIP'S JIRA TICKETS: AN ENCYCLOPEDIA OF CONSERVATIVE CENSORSHIP

An examination of the Jira tickets themselves reveals a veritable who's who of prominent conservative voices targeted for censorship by CISA and the EIP. On March 17, 2023, in response to increased media scrutiny of the SIO's activities, including the Select Subcommittee's March 9 hearing on the Twitter Files, the SIO published a blog post riddled with false statements about the EIP.[161] For instance, the blog post stated that the EIP did not "'target' or discriminate against conservative social media accounts or content."[162] While it is true that the EIP, did flag non-conservative content to maintain a façade of neutrality, the EIP's reports show a clear attempt to suppress conservative speech in particular.[163]

According to the EIP's post-election report, there are four categories of election-related "misinformation" that the EIP considered to be "in scope" of the type of "misinformation" the EIP would analyze.[164] Some of the categories, like "procedural interference" are relatively anodyne—although often stretched beyond its intended contours—and include things like "[c]ontent that misleads voters about how to correctly sign a mail-in ballot" and "[c]ontent that encourages voters to vote on a different day."[165]

The EIP repeatedly used its fourth category, in particular, to justify the censorship of conservative political speech: the "Delegitimization of Election Results," defined as "[c]ontent that delegitimizes election results on the basis of false or misleading claims."[166] This arbitrary and inconsistent standard was determined by political actors masquerading as "experts" and academics. But even more troubling, the federal government was heavily intertwined with the universities in making these seemingly arbitrary determinations that skewed against one side of the political aisle.

The EIP routinely flagged conservative content on social media under the guise that it was inappropriately "delegitimizing" election results, even in cases where the content was factually accurate. Criticism of the electoral system is constitutionally protected speech. A political system that allows a small minority of government-approved "experts" to exercise influence over the ability of other citizens to express concerns with the government represents a profound threat to our constitutional republic. Indiscriminately or improperly suppressing accusations of electoral fraud necessarily suppresses speech about real instances of electoral fraud, thereby allowing the government free rein to conduct elections in a manner that is not accountable to the American people.[167]

---

[161] Stanford Internet Observatory, *Background on the SIO's Projects on Social Media*, STANFORD UNIV. (Mar. 17, 2023).
[162] *Id*.
[163] So that the American people can judge for themselves, Appendix II of this report includes all of the EIP and Virality Project Jira ticket data provided to the Committee pursuant to a subpoena to Stanford University.
[164] ELECTION INTEGRITY P'SHIP, *supra* note 16, at vi, 246.
[165] *Id.* at vi, 7.
[166] *Id.* at vi.
[167] *See, e.g.*, Susan Haigh, *Connecticut Judge Orders New Mayoral Primary After Surveillance Videos Show Possible Ballot Stuffing*, AP (Nov. 1, 2023) ("A judge on Wednesday tossed out the results of a Democratic mayoral primary in Connecticut's largest city and ordered that a new one be held, citing surveillance videos showing people stuffing multiple absentee ballots into outdoor collection boxes.").

A. Dropping the Pretense of "Mis- and Disinformation": The EIP's Absurd Approach to Classification

The EIP acknowledged in its report that it is "not a fact-checking organization" and that "[f]or some tickets, it was not possible to find an external fact-check for the content, either because no fact-checker had yet addressed the issue, or because the information was resistant to simple verification."[168] Unbelievably, the EIP also admitted that its analysts "identified at least one external fact-check source for approximately 42% of the in-scope tickets."[169] In other words, EIP analysts were unable to identify a single external source to support its designation of a particular post or narrative as "mis- or disinformation" in a *majority of posts* it flagged.

The general reliance of social media censors on fact-checkers, many of whom have a distinctly liberal political bias, creates an environment that is hostile to free speech, especially conservative viewpoints, and is concerning in and of itself. However, the fact that the EIP could not find even a single fact-checker, biased or not, before flagging content to social media in a majority of cases and was willing to publicly admit to that fact, is indicative of a brazen and megalomaniacal approach to censorship, unbothered by the truth or maintaining even the appearance of political neutrality.

For cases in which the EIP was unable to fact-check a claim or narrative it had identified, the EIP could have opted not to flag the content to the social media platforms, given that there was uncertainty about the truth value of the content in question. Instead, the EIP aggressively flagged such posts to the platforms, noting in the tickets that it had no justification for reporting the content other than CISA's and the EIP's own political agenda.

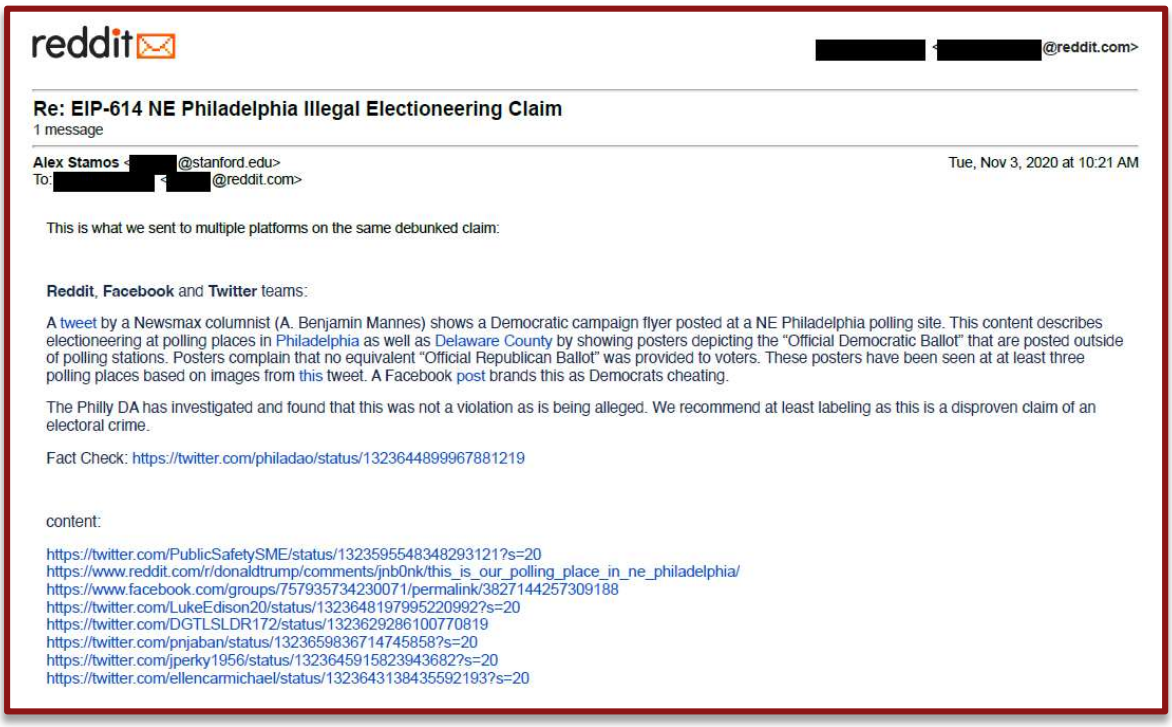
For example, an entry in EIP-713, a Jira ticket regarding a Gateway Pundit article, submitted on the afternoon of Election Day, November 3, read: "We are sending this to you quickly as we likely won't be able to figure out a factcheck here."[170] In EIP-418, concerning a tweet from One America News Network, a contributor wrote: "We have not seen a fact-check on this direct story, but this story is targeted at discrediting the validity of vote-by-mail."[171] In its report, the EIP claimed that its purpose was "to identify and analyze mis- and disinformation," which even CISA publicly defines as *false* information.[172] However, the approach demonstrated in these and other tickets makes clear that the EIP's focus was not on the truth, but rather the advancement of viewpoint-based discrimination.

---

[168] ELECTION INTEGRITY PARTNERSHIP, *supra* note 16, at 10.
[169] *Id*.
[170] EIP-713, submitted by [REDACTED], ticket created (Nov. 3, 2020, 2:45 PM) (archived Jira ticket data produced to the Comm.).
[171] EIP-418, submitted by [REDACTED], ticket created (Oct. 21, 2020, 9:30 AM) (archived Jira ticket data produced to the Comm.); *see also* OAN Newsroom, *Reports Claim 440K Questionable Ballots Sent To Deceased Or Inactive Voters In Calif.*, ONE AMERICA NEWS NETWORK (Oct. 20, 2020) available at http://web.archive.org/web/20201021170509/https://www.oann.com/reports-claim-440k-questionable-ballots-sent-to-deceased-or-inactive-voters-in-calif/.
[172] ELECTION INTEGRITY PARTNERSHIP, *supra* note 16, at vi.

B. Efforts to Censor the Truth

Even in the limited cases in which the EIP was able to find an external fact-check, the fact-checkers were often unsure themselves, admitted that the relevant claims were not false, or subject to undeniable political bias. On November 3, 2020, Alex Stamos sent an email to a Reddit employee with the contents of a Jira ticket concerning irregularities at polling sites in Philadelphia, as Reddit refused to participate in the Jira system directly.[173]



reddit [redacted] <[redacted]@reddit.com>

Re: EIP-614 NE Philadelphia Illegal Electioneering Claim
1 message

Alex Stamos <[redacted]@stanford.edu> Tue, Nov 3, 2020 at 10:21 AM
To: [redacted] <[redacted]@reddit.com>

This is what we sent to multiple platforms on the same debunked claim:

Reddit, **Facebook** and **Twitter** teams:

A tweet by a Newsmax columnist (A. Benjamin Mannes) shows a Democratic campaign flyer posted at a NE Philadelphia polling site. This content describes electioneering at polling places in Philadelphia as well as Delaware County by showing posters depicting the "Official Democratic Ballot" that are posted outside of polling stations. Posters complain that no equivalent "Official Republican Ballot" was provided to voters. These posters have been seen at at least three polling places based on images from this tweet. A Facebook post brands this as Democrats cheating.

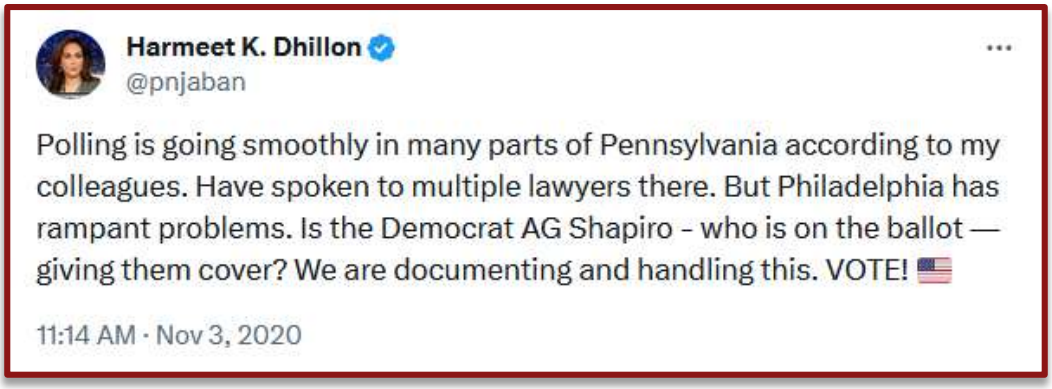
The Philly DA has investigated and found that this was not a violation as is being alleged. We recommend at least labeling as this is a disproven claim of an electoral crime.

Fact Check: https://twitter.com/philadao/status/1323644899967881219

content:

https://twitter.com/PublicSafetySME/status/1323595548348293121?s=20
https://www.reddit.com/r/donaldtrump/comments/jnb0nk/this_is_our_polling_place_in_ne_philadelphia/
https://www.facebook.com/groups/757935734230071/permalink/3827144257309188
https://twitter.com/LukeEdison20/status/1323648197995220992?s=20
https://twitter.com/DGTLSLDR172/status/1323629286100770819
https://twitter.com/pnjaban/status/1323659836714745858?s=20
https://twitter.com/jperky1956/status/1323645915823943682?s=20
https://twitter.com/ellencarmichael/status/1323643138435592193?s=20

The ticket, although ostensibly about a specific claim regarding signs posted outside polling sites, flagged more generic content, including the below tweet from Republican Party official Harmeet Dhillon.[174] The "Fact Check" cited in the ticket is a tweet from the office of the Democratic District Attorney in Philadelphia and does not dispute any of the claims in Dhillon's post.



Harmeet K. Dhillon
@pnjaban

Polling is going smoothly in many parts of Pennsylvania according to my colleagues. Have spoken to multiple lawyers there. But Philadelphia has rampant problems. Is the Democrat AG Shapiro - who is on the ballot — giving them cover? We are documenting and handling this. VOTE!

11:14 AM · Nov 3, 2020

[173] Email from Alex Stamos to Reddit employee (Nov. 3, 2020 10:21 AM) (on file with the Comm.).
[174] *Id.*; *see also* Harmeet K. Dhillon (@pnjaban), TWITTER (Nov. 3, 2020, 11:14 AM).

C. Efforts to Censor President Trump and His Family

The most prominent conservative voice targeted by CISA and the EIP was none other than the sitting President of the United States, Donald Trump. On October 27, 2020, a local official reported a tweet from President Trump to CIS's "misinformation" tipline, which then forwarded the report to the EIP and CISA, per its usual protocol.[175] CISA then flagged the content to Twitter.[176] To be clear, this evidence shows an unelected executive branch official flagging a statement from the elected leader of the executive branch for removal from one of the world's largest and most active public forums. CISA has not provided the Committee any evidence that it contacted the White House prior to making the referral to opine on the veracity of the claim in the tweet.

[mailto:]
Sent: Tuesday, October 27, 2020 12:52 PM
To: Elections - Public <[redacted]@sos.wa.gov>
Subject: Disinformation

I'm reporting this disinformation about the elections. Please take steps to stop it, and correct it publicly. Thanks.

Federal Way, WA

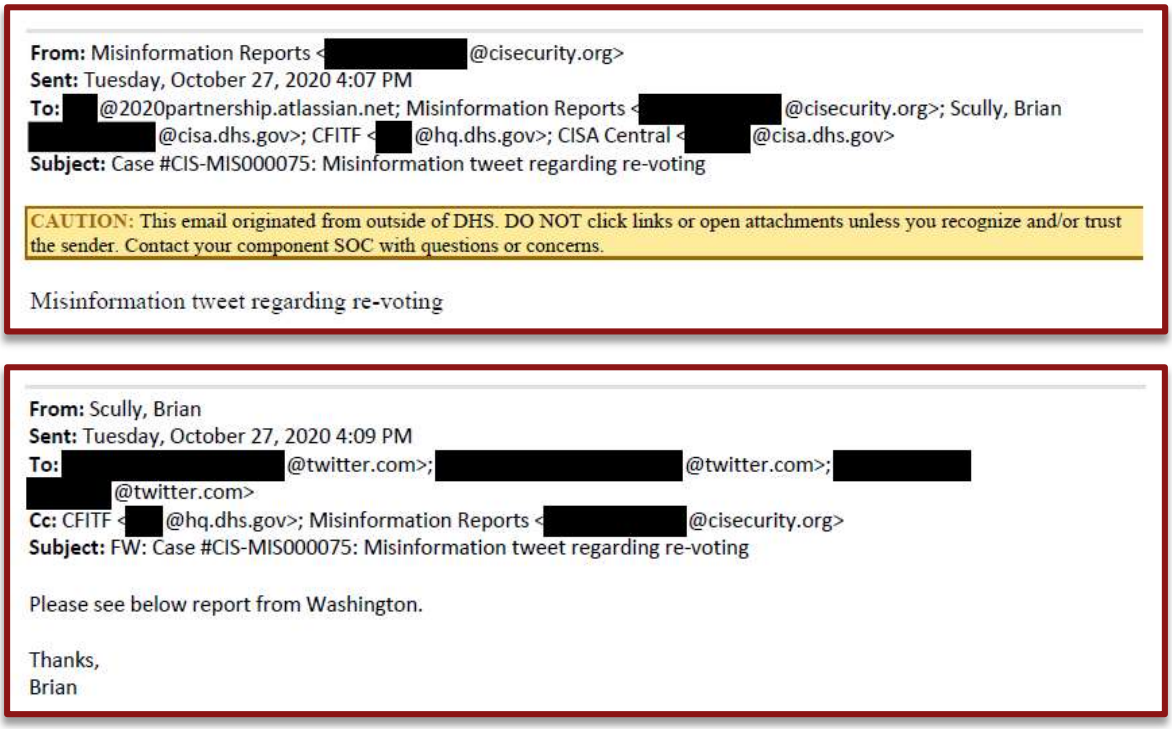
Donald J. Trump
@realDonaldTrump

Strongly Trending (Google) since immediately after the second debate is CAN I CHANGE MY VOTE? This refers changing it to me. The answer in most states is YES. Go do it. Most important Election of your life!

3:53 AM · Oct 27, 2020

174.5K 58K people are Tweeting about this

[175] EIP-482, submitted by CIS Misinformation Reporting, ticket created (Oct. 27, 2020, 1:07 PM) (archived Jira ticket data produced to the Comm.); *see also* Donald J. Trump (@realDonaldTrump), TWITTER (Oct. 27, 2020 3:53 AM), available at https://web.archive.org/web/20201027105312/https://twitter.com/realDonaldTrump/status/1321042229838909441.
[176] *Id*.



From: Misinformation Reports <[redacted]@cisecurity.org>
Sent: Tuesday, October 27, 2020 4:07 PM
To: [redacted]@2020partnership.atlassian.net; Misinformation Reports <[redacted]@cisecurity.org>; Scully, Brian [redacted]@cisa.dhs.gov>; CFITF <[redacted]@hq.dhs.gov>; CISA Central <[redacted]@cisa.dhs.gov>
Subject: Case #CIS-MIS000075: Misinformation tweet regarding re-voting

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

Misinformation tweet regarding re-voting

From: Scully, Brian
Sent: Tuesday, October 27, 2020 4:09 PM
To: [redacted]@twitter.com>; [redacted]@twitter.com>; [redacted]@twitter.com>
Cc: CFITF <[redacted]@hq.dhs.gov>; Misinformation Reports <[redacted]@cisecurity.org>
Subject: FW: Case #CIS-MIS000075: Misinformation tweet regarding re-voting

Please see below report from Washington.

Thanks,
Brian

CISA's involvement in the attempted censorship of President Trump did not end once the report had been submitted to Twitter. Instead, as noted in an entry on the Jira ticket identified as EIP-482: "We [the EIP] heard back from Twitter through CISA" regarding how Twitter decided to handle the reported tweet.[177]

This was not the only time CISA and the EIP attempted to hinder the duly elected President's ability to communicate with the American public. On November 4, 2020, a Michigan election official made a "misinformation" report to CIS, writing, "Today we learned of an apparent error in reporting unofficial election results from Antrim. The unofficial results reported were unusual. The County reviewed the issue and after speaking with their election vendor, determined that there may have been an error in the program used to combine the results that caused inaccurate numbers to display."[178] According to the election official, this was concerning because "[i]ndividuals are using this incident to spread misinformation or conspiracy theories that the election results cannot be trusted."[179]

[177] *See* EIP-482, *supra* note 175.
[178] Email from Michigan election official to CIS and MS-ISAC personnel (Nov. 4, 2020 2:35 PM) (on file with the Comm.).
[179] *Id*.

From: [redacted]@michigan.gov>
Sent: Wednesday, November 4, 2020 2:35 PM
To: MS-ISAC SOC <[redacted]@msisac.org>; Misinformation Reports <[redacted]@cisecurity.org>
Subject: Antrim County Michigan Election Results Error in reporting
Importance: High

Good Afternoon,

Today we learned of an apparent error in reporting unofficial election results from Antrim. The unofficial results reported were unusual. The County reviewed the issue and after speaking with their election vendor, determined that there may have been an error in the program used to combine the results that caused inaccurate numbers to display.

At this time, there is no reason to think that this was the result of malicious activity. We believe that all ballots and tabulators functioned properly. Voters are recorded on hand-marked paper ballots. The County is reviewing the issue further with its election vendor and will then determine when it will be able to report its unofficial results. Again, all results reported at this time are unofficial; the official results are determined after a County canvass of election results and certification by the Board of State Canvassers.

Individuals are using this incident to spread misinformation or conspiracy theories that the election results cannot be trusted. They may be combining this story with apparently doctored images of election results in other areas to suggest a widespread conspiracy to change election results. They may also combine this with efforts to undermine the ongoing counting of absent voter ballots. There is no basis to this whatsoever and as far as we know this was an isolated incident caused by an error that was quickly caught.

As usual, the report was then sent at the same time to the EIP and CISA for further action.[180]

From: Misinformation Reports
Sent: Wednesday, November 4, 2020 7:42:36 PM (UTC+00:00) Monrovia, Reykjavik
To: Scully, Brian; CISA Central; CFITF; [redacted]@2020partnership.atlassian.net; Misinformation Reports
Subject: Case #CIS-MIS000159: Antrim County, MI election results error in reporting

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

In response, the EIP dutifully activated its surveillance antennae, scouring social media for posts and activity related to the reporting irregularity that the state election official confirmed had actually taken place. The EIP then reported a series of URLs to Twitter and Facebook regarding the incident in Antrim County.[181] Facebook replied that it had "applied the relevant labels on the links you shared."[182] One of the links included in the ticket was a tweet from

[180] Email from CIS personnel to Brian Scully, CISA Central, CFITF, and EIP personnel (Nov. 4, 2020 7:42 PM) (on file with the Comm.).
[181] *See See* EIP-822, submitted by CIS Misinformation Reporting, ticket created (Nov. 4, 2020, 11:42 AM) (archived Jira ticket data produced to the Comm.); *see also* Donald J. Trump (@realDonaldTrump), TWITTER (Nov. 7, 2020 7:23 AM), available at https://web.archive.org/web/20201107152307/http://twitter.com/realDonaldTrump/status/1325096422799237120; Alana Mastrangelo, *Georgia Counties Using Same Software as Michigan Counties Also Encounter 'Glitch'*, BREITBART (Nov. 7, 2020) available at https://web.archive.org/web/20201108204307/https://www.breitbart.com/politics/2020/11/07/georgia-counties-using-same-software-as-michigan-counties-also-encounter-glitch/.
[182] *Id*.

President Trump, in which the President shared an article from Breitbart, with the added commentary: "What a total mess this 'election' has been!"[183]

CISA has not provided the Committee with any evidence that the agency contacted the White House directly to convey its concerns with the tweet, instead relying on the EIP to conduct censorship by proxy.

Members of President Trump's family were also targeted for censorship by CISA and the EIP. During the course of its work in the 2020 election cycle, the EIP flagged multiple posts from both Donald Trump Jr. and Eric Trump, some of which appear to have been removed or labelled.[184] In one ticket, tagged EIP-867, the EIP flagged Donald Trump Jr.'s Twitter account

[183] *Id*.
[184] *See, e.g.*, EIP-949, submitted by Alex Stamos, ticket created (Nov. 7, 2020, 8:36 AM) (archived Jira ticket data produced to the Comm.); *see also* Eric Trump (@EricTrump), TWITTER (Nov. 8, 2020 4:22 AM), available at https://web.archive.org/web/20201108122250/https://twitter.com/EricTrump/status/1325413441310482432; Alana Mastrangelo, *Georgia Counties Using Same Software as Michigan Counties Also Encounter 'Glitch'*, BREITBART

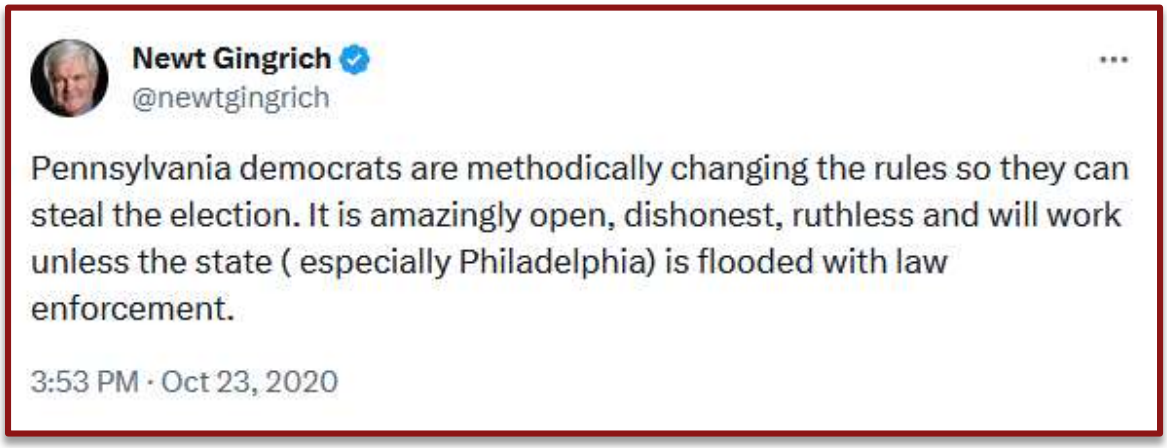
for simply reposting a Tweet from conservative journalist James O'Keefe and asking: "Where is the DOJ???"[185]

(Nov. 7, 2020) available at https://web.archive.org/web/20201108204307/ https://www.breitbart.com/politics/2020/11/07/georgia-counties-using-same-software-as-michigan-counties-also-encounter-glitch/; Donald Trump Jr. (@DonaldJTrumpJr), TWITTER (Nov. 6, 2020 8:47 PM), available at https://web.archive.org/web/20220712020104/https://twitter.com/DonaldJTrumpJr/status/1324815748108345344.

[185] EIP-867, submitted by [REDACTED], ticket created (Nov. 18, 2020, 1:29 PM) (archived Jira ticket data produced to the Comm.).

D. Efforts to Censor Political Candidates and Legislators

CISA's and the EIP's censorship enterprise targeted not only President Trump but also former, current, and prospective legislators. In EIP-450, the EIP flagged a tweet, pictured below, from former Speaker of the House of Representatives Newt Gingrich about changes to Pennsylvania election law.[186]



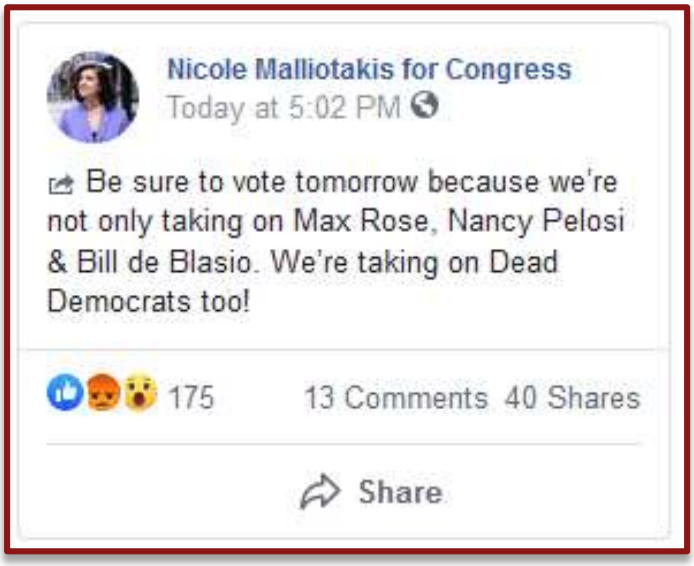
In EIP-904, the EIP attempted to censor Rep. Jody Hice, a sitting Republican Congressman from Georgia, engaging in core political speech criticizing the administration of the election in his home state.[187]

[186] *See* EIP-450, submitted by [REDACTED], ticket created (Oct. 23, 2020, 1:43 PM) (archived Jira ticket data produced to the Comm.).
[187] *See* EIP-904, submitted by Josh Aaron Goldstein, ticket created (Nov. 5, 2020, 4:30 PM) (archived Jira ticket data produced to the Comm.); *see also* Rep. Jody Hice (@CongressmanHice), TWITTER (Nov. 5, 2020 4:04 PM), available at http://web.archive.org/web/20201106010558/ https://twitter.com/CongressmanHice/status/1324502770813194241?s=20.

EIP analysts also flagged a completely innocuous tweet from Sen. Thom Tillis of North Carolina in EIP-936 because the group deemed his declaration of victory to be premature.[188] Sen. Tillis did, in fact, win his reelection to the Senate.

[188] EIP-936, submitted by [REDACTED], ticket created (Nov. 16, 2020, 2:08 PM) (archived Jira ticket data produced to the Comm.); *see also* Joseph Curl, *Republican Thom Tillis Claims Victory in North Carolina*, THE DAILY WIRE (Nov. 4, 2020) available at https://web.archive.org/web/20201108225403/https://www.dailywire.com/news/republican-thom-tillis-claims-victory-in-north-carolina; Thom Tillis (@ThomTillis), TWITTER (Nov. 3, 2020 9:05 PM), available at https://web.archive.org/web/20201108230403/https://twitter.com/ThomTillis/status/1323853951394074629.

The EIP further targeted Republican candidates for political office, including those who would later be seated in Congress. For example, in EIP-596, the EIP flagged this Facebook post from Rep. Nicole Malliotakis's campaign page. The post appears to have been removed by Facebook.[189]



In EIP-780, the EIP's "analysts" flagged a post from Rep. Marjorie Taylor Greene's campaign account, in which the Congresswoman encouraged her followers to share her post.[190] It is a slippery slope if political candidates and their supporters are not able to express legitimate concerns with the election process. While many disinformation experts are quick to criticize Republican candidates about undermining "faith in elections," these experts appear to be notably silent whenever Democrats objected to election results in other elections, or baselessly blamed election losses on unfounded claims of fraud or cheating. Perhaps most notably, many Democrats repeated the unfounded claim that President Trump colluded with Russia, rather than accept the truth that his victory over Hillary Clinton was legitimate.[191] But as the disinformation experts in their own words acknowledge, the study of "disinformation" is of course "inherently political."[192]

---

[189] EIP-596, submitted by [REDACTED], ticket created (Nov. 3, 2020, 7:46 PM) (archived Jira ticket data produced to the Comm.); *see also* Nicole Malliotakis for Congress (@NicoleForCongress), FACEBOOK (Nov. 3, 2020 5:02 PM) available at https://web.archive.org/web/20201103040541/ https://www.facebook.com/NicoleForCongress/posts/2718395868412350.

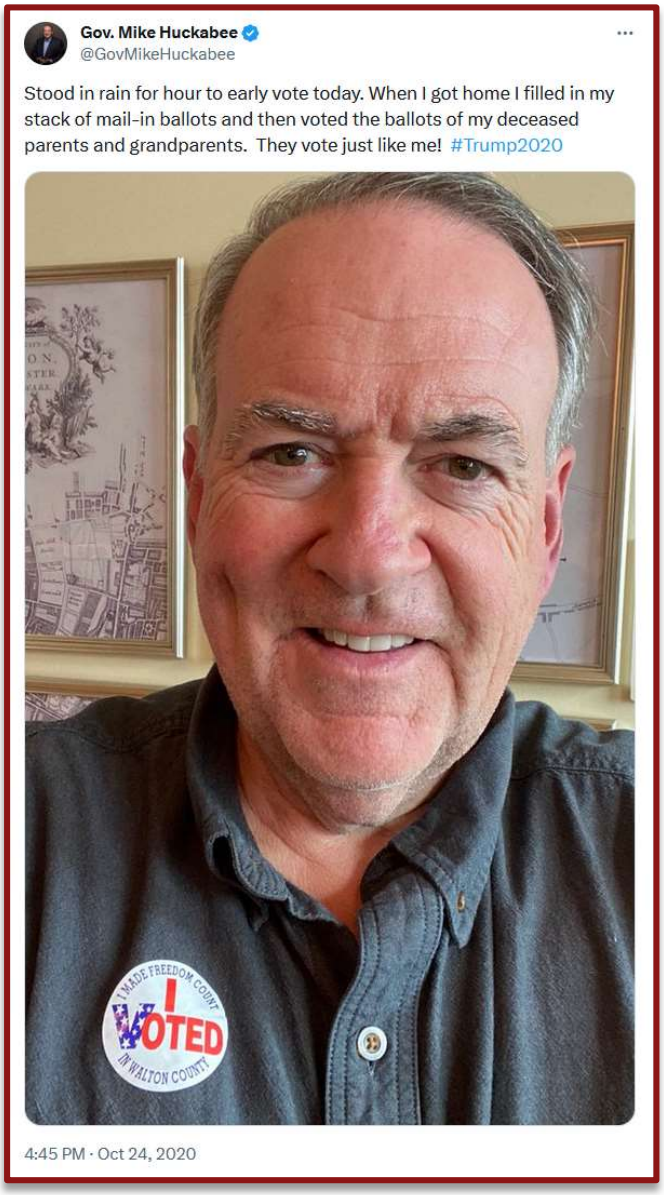
[190] EIP-780, submitted by Melanie Smith, ticket created (Nov. 4, 2020, 12:32 AM) (archived Jira ticket data produced to the Comm.); *see also* Marjorie Taylor Greene For Congress (@mtgreenee) TWITTER (Nov. 3, 2020 11:37 PM) available at http://web.archive.org/web/20201104160034/ https://twitter.com/mtgreenee/status/1323892005584412674; Marjorie Taylor Greene For Congress (@mtgreenee) TWITTER (Nov. 4, 2020 7:58 AM) available at http://web.archive.org/web/20201104161216/ https://twitter.com/mtgreenee/status/1324019263255040003; Marjorie Taylor Greene For Congress (@mtgreenee) TWITTER (Nov. 4, 2020 8:02 AM) available at http://web.archive.org/web/20201104160746/ https://twitter.com/mtgreenee/status/1324018211021594626; Matt Walsh (@MattWalshBlog) TWITTER (Nov. 4, 2020) available at http://web.archive.org/web/20201104153558/ https://twitter.com/MattWalshBlog/status/1323999569466789889.

[191] *See, e.g.*, Paul Farhi, *The Washington Post corrects, removes parts of two stories regarding the Steele dossier*, WASH. POST (Nov. 12, 2021); *see generally* REPORT ON MATTERS RELATED TO INTELLIGENCE ACTIVITIES AND INVESTIGATIONS ARISING OUT OF THE 2016 PRESIDENTIAL CAMPAIGNS, Office of Special Counsel John H. Durham, U.S. DEP'T OF JUSTICE (May 12, 2023); *see also* Susan Haigh, *Connecticut Judge Orders New Mayoral Primary After Surveillance Videos Show Possible Ballot Stuffing*, AP (Nov. 1, 2023) ("A judge on Wednesday tossed out the results of a Democratic mayoral primary in Connecticut's largest city and ordered that a new one be held, citing surveillance videos showing people stuffing multiple absentee ballots into outdoor collection boxes.").

[192] Email from Suzanne Spaulding (Google Docs) to Kate Starbird (May 16, 2022, 6:27 PM) (on file with the Comm.).; *see also* Kate Starbird et al., Proposal to the National Science Foundation for "Collaborative Research: SaTC: Core: Large: Building Rapid-Response Frameworks to Support Multi-Stakeholder Collaborations for Mitigating Online Disinformation" (Jan. 29, 2021) (unpublished proposal) (on file with the Comm.) ("The study of disinformation today invariably includes elements of politics.").

E. Efforts to Censor Humor and Satire

Documents obtained by the Committee and Select Subcommittee also show that the EIP flagged content that was obviously humorous and satirical. For example, EIP analysts internally identified a tweet from former Governor of Arkansas Mike Huckabee, in which Huckabee made a quip about dead relatives voting.[193] According to the ticket, labeled EIP-460, an individual affiliated with the EIP wrote, "ISAC Partners, adding you to this thread for visibility. We recommend to Twitter that this be labeled, especially under option (b) as it was posted by a public figure."[194]



[193] *See* EIP-460, submitted by [REDACTED], ticket created (Oct. 25, 2020, 11:36 AM) (archived Jira ticket data produced to the Comm.); *see also* Gov. Mike Huckabee (@GovMikeHuckabee) TWITTER (Oct. 24, 2020 1:45 PM) available at https://web.archive.org/web/20201025064250/https://twitter.com/GovMikeHuckabee/status/1320104112420212739.

[194] *Id*.

The EIP even objected to and attempted to censor humorous images that could not reasonably be perceived as genuine.[195] Both images, replicated below and flagged in EIP-811, are self-evidently doctored and depict the transportation of boxes labelled "Emergency Democrat Votes."[196] The EIP wrote in the ticket: "Users on Twitter and Facebook are sharing manipulated images of people moving boxes in trucks labeled 'Emergency Democrat Votes.' We suggest labeling or removing tweets that use this photo, as it could undermine people's faith in the legitimacy of the election process. Though the image may seem ridiculous, some users may still believe it is real."[197]

[195] EIP-811, submitted by [REDACTED], ticket created (Nov. 16, 2020, 3:25 PM) (archived Jira ticket data produced to the Comm.); *see also* Dark to Light (@pushforward40) TWITTER (Nov. 4, 2020 9:27 AM) available at https://web.archive.org/web/20201104182147/https://twitter.com/pushforward40/status/1324040688351236099; Carol Ricks (@BVMgroupie) TWITTER (Nov. 4, 2020 10:33 AM) available at https://web.archive.org/web/20201104215451/https://twitter.com/BVMgroupie/status/1324057218950594560; Paula Priesse, FACEBOOK (Nov. 4, 2020 10:42 AM) available at https://web.archive.org/web/20201104215620/https://www.facebook.com/256566055895/posts/10157402516245896.

[196] *Id*.

[197] *Id*.

In both cases, the EIP successfully induced the platforms to append labels to the posts. Examples like these illustrate the utter contempt in which CISA, CIS, and the EIP held the American public and its ability to evaluate information on social media.

F. Efforts to Censor Other Influential Conservative Accounts

In addition to the accounts mentioned previously, the EIP targeted the social media accounts of conservative journalists, commentators, and personalities with large followings and high engagement for suppression. In the Jira ticket numbered EIP-805, the EIP flagged both posts in the screenshot below, one from Candace Owens and the other from Charlie Kirk.[198]

The EIP also flagged posts from notable and popular conservative accounts, including those of Paul Sperry, Chanel Rion, Sean Davis, Dave Rubin, Michelle Malkin, James O'Keefe, Benny Johnson, Jack Posobiec, Tracy Beanz, Mike Roman, Sean Hannity, the Babylon Bee, Newsmax, Mollie Hemingway, and Tom Fitton, among others.

The suppression of conservative politicians and media resulting from this censorship operation deprived countless American voters from exposure to a range of perspectives on the most important political issues in the days and weeks surrounding a general election. Critically, the EIP conducted its censorship operation at the direction of, in collaboration with CISA, a federal government agency actively seeking to undermine free expression and the sitting President. The significance of these facts cannot be overstated.

[198] EIP-805, submitted by [REDACTED], ticket created (Nov. 4, 2020, 10:01 AM) (archived Jira ticket data produced to the Comm.); *see also* Candace Owens (@RealCandaceO) TWITTER (Nov. 4, 2020 8:52 AM) available at https://web.archive.org/web/20201104165242/https://twitter.com/realcandaceo/status/1324031726096699392.

IV. THE EIP'S COERCIVE TACTICS

In the lead-up to the 2020 election, social media platforms were inundated by requests for censorship from a number of federal agencies, including the FBI and CISA.[199] As documented in Section I of this interim report, CISA and its proxies already had two avenues to submit reports—switchboarding and the EI-ISAC—and was heavily lobbying a third avenue, a "misinformation reporting portal" operated by CIS, before the creation of EIP. Then, with the EIP, Jira ticket data and emails establish clearly that social media platforms understood that the federal government was working directly with the EIP.

In addition to having the explicit and implicit backing of the federal government, the EIP had another tool at its disposal to pressure social media companies to comply with the censorship requests: the media. In his testimony before the Committee, Alex Stamos—the SIO director and former Chief Security Officer at Facebook—explained how social media companies felt pressure from public criticism about the failure to remove content that experts had labeled as misinformation.[200] He testified:

> Q. And, with respect to the blogpost, are there any -- did anyone from EIP ever communicate to the platforms that you were going to make these blogposts public?
>
> A. I mean, it's possible that we gave them a heads-up when we were posting about it.
>
> Q. And why would you do that?
>
> A. I think it's a polite thing to do so that they know that we're going public. We didn't want them to feel like we were blindsiding them.
>
> Q. And what do you mean by "blindsiding" them?
>
> A. We wanted them to know that there's going to be a possible discussion of what was going on in their platform, and they should know about it. I think the -- you know, we were -- I am sympathetic to how hard it is to be in one of these companies and to try to balance all the different equities. And so, if somebody was writing something that could generate a communications moment during an election period, then that's something I would want to know for sure.

[199] *See* Missouri v. Biden, No. 3:22-cv-01213 (W.D. La. Jul. 4, 2023), ECF No. 293, at 2 (memorandum ruling granting preliminary injunction); STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A "CYBERSECURITY" AGENCY COLLUDED WITH BIG TECH AND "DISINFORMATION" PARTNERS TO CENSOR AMERICANS, at 9–12 (Comm. Print June 26, 2023); STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE FBI'S COLLABORATION WITH A COMPROMISED UKRAINIAN INTELLIGENCE AGENCY TO CENSOR AMERICAN SPEECH (Comm. Print July 10, 2023).

[200] *See* House Judiciary Committee's Transcribed Interview of Alex Stamos (June 23, 2023), at 183-184 (on file with the Comm.).

Q. What do you mean by "communications moment"?

A. So, if we wrote a blogpost that said, "This is something viral that's happening that's not true," you very well could find members of the media going out and then finding that content on five different platforms and then writing about it being up or not.

Q. And, if it was still up, would some of those media publications be criticism of the platforms?

A. It's possible.[201]

Similarly, Dr. Kate Starbird of the University of Washington, and one of the central figures involved in the EIP's operation, similarly testified about using her platform (independent of the EIP) to publicly push social media platforms to change their policies. She testified:

Q. Was the purpose of the public communication to have Twitter change its policy?

A. It was, for me -- again, this is not, like, within the EIP brand. This is sort of something that we were just kind of doing that eventually we start working together. But this is just something that I do a lot, which is to put out analysis and have recommendations for the platforms at the end of that analysis.

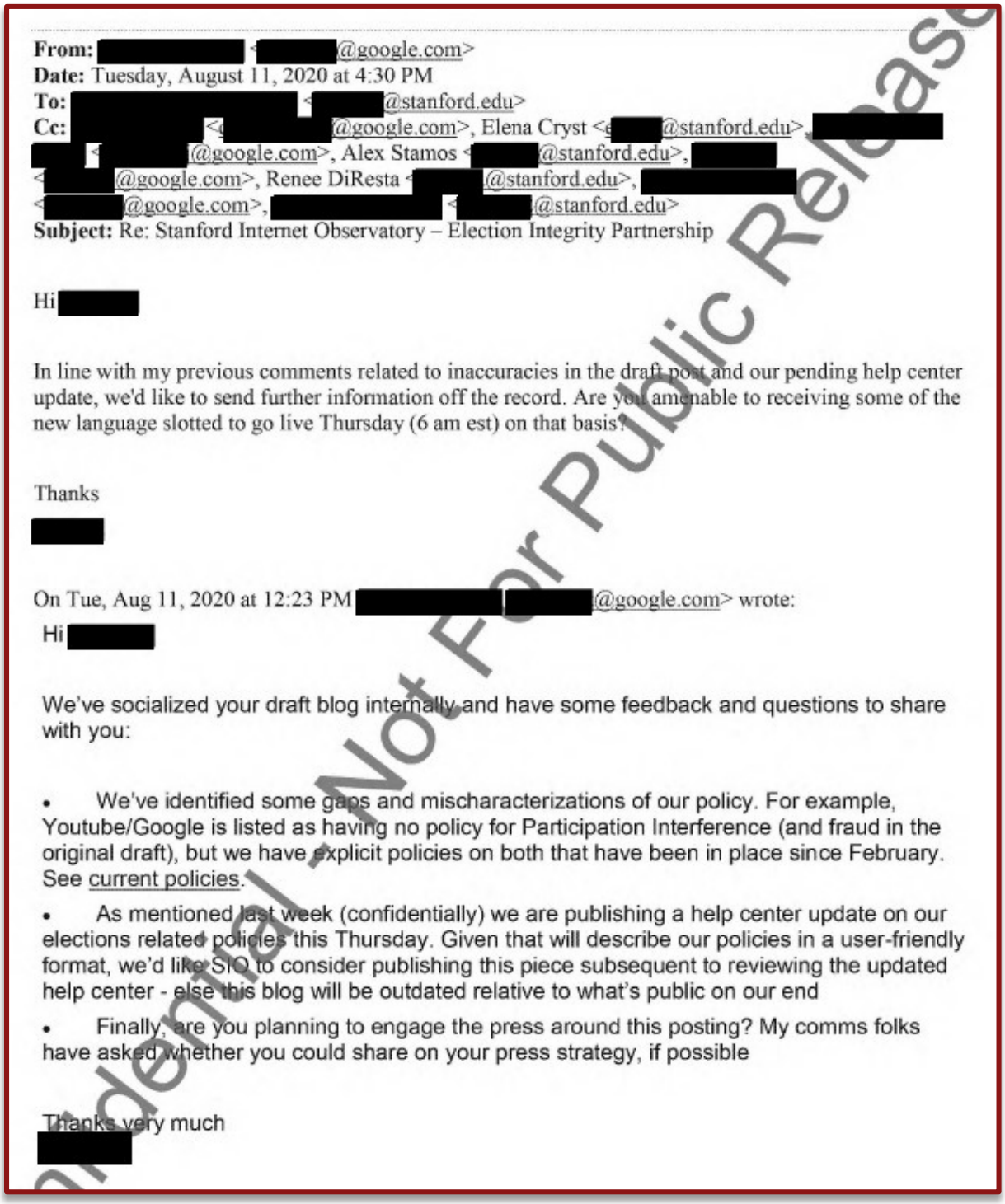
Sometimes that's in formal papers. In this case, I would sometimes put the analyses out on Twitter to say this is happening and that it's a problem, to draw attention to it, and for them to think about what they should do to change. Yeah.

And I don't always recommend -- I rarely recommend a specific action. I wish -- I didn't get to say this -- I wish I had something better to say. But most of the time, I just point out problems and don't tell them how to fix them. And I understand that the fixes for the problems are very tricky and very hard, so I give them credit for that. But I did a lot of, like, pointing out: This is a problem.[202]

In the fall of 2020, the EIP also worked on preparing work product summarizing the major social media platforms' content moderation policies and the differences among them. The EIP initially gave Alphabet (the parent company of Google and YouTube) an opportunity to comment on YouTube's content moderation policies. As the email chain below demonstrates, Alphabet was keenly aware that the EIP may "engage the press." In particular, the company wanted to ensure that the EIP would not publish "inaccuracies" or "mischaracterizations" that

[201] *Id*.
[202] House Judiciary Committee's Transcribed Interview of Kate Starbird (June 6, 2023), at 153 (on file with the Comm.).

would suggest the company's policies were insufficient in removing election-related content labeled as misinformation by the EIP.[203]



From: [redacted] <[redacted]@google.com>
Date: Tuesday, August 11, 2020 at 4:30 PM
To: [redacted] <[redacted]@stanford.edu>
Cc: [redacted] <[redacted]@google.com>, Elena Cryst <[redacted]@stanford.edu>, [redacted] <[redacted]@google.com>, Alex Stamos <[redacted]@stanford.edu>, [redacted] <[redacted]@google.com>, Renee DiResta <[redacted]@stanford.edu>, [redacted] <[redacted]@google.com>, [redacted] <[redacted]@stanford.edu>
Subject: Re: Stanford Internet Observatory – Election Integrity Partnership

Hi [redacted]

In line with my previous comments related to inaccuracies in the draft post and our pending help center update, we'd like to send further information off the record. Are you amenable to receiving some of the new language slotted to go live Thursday (6 am est) on that basis?

Thanks

[redacted]

On Tue, Aug 11, 2020 at 12:23 PM [redacted] [redacted]@google.com> wrote:

Hi [redacted]

We've socialized your draft blog internally and have some feedback and questions to share with you:

- We've identified some gaps and mischaracterizations of our policy. For example, Youtube/Google is listed as having no policy for Participation Interference (and fraud in the original draft), but we have explicit policies on both that have been in place since February. See current policies.
- As mentioned last week (confidentially) we are publishing a help center update on our elections related policies this Thursday. Given that will describe our policies in a user-friendly format, we'd like SIO to consider publishing this piece subsequent to reviewing the updated help center - else this blog will be outdated relative to what's public on our end
- Finally, are you planning to engage the press around this posting? My comms folks have asked whether you could share on your press strategy, if possible

Thanks very much

[redacted]

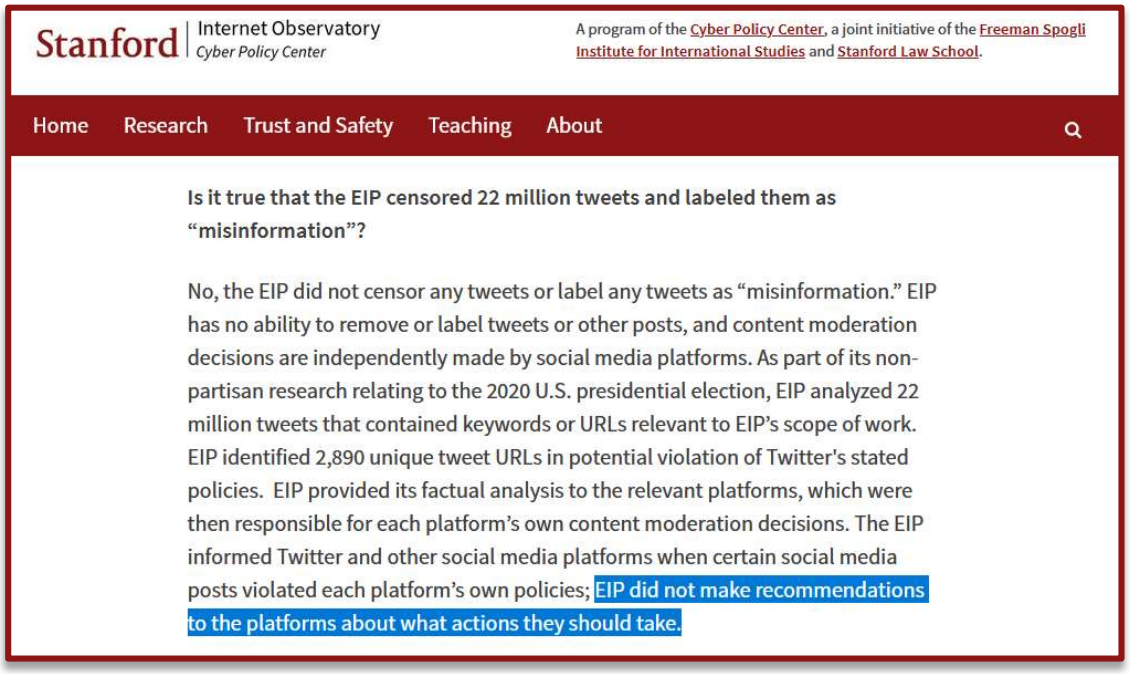
[203] Email between Google Employees and Stanford Personnel (Aug. 11, 2020 4:30 PM) (on file with the Comm.).

V. STANFORD'S EFFORTS TO OBSTRUCT THE COMMITTEE'S INVESTIGATION

A. Stanford's Deceitful Public Statements about the EIP's Flagging of Posts

On March 17, 2023, following the Select Subcommittee's March 9 hearing on the Twitter Files, the SIO published a blog post titled "Background on the SIO's Project on Social Media," in which the SIO sought to downplay the extent of the EIP's censorship and surveillance, claiming that both the EIP and its successor, the Virality Project, "are non-partisan research coalitions that operate in an open, transparent, and public manner."[204] On March 20, the SIO's counsel sent a link to the blog post to Committee staff, writing: "Here's the statement Stanford put up on Friday attempting to correct some of the myths floating around in the press."[205]

In addition to its mendacious framing of the EIP's activities and CISA's involvement therein, the post contains statements that are categorically untrue. Most notably, the SIO falsely claimed in the post that the "EIP informed Twitter and other social media platforms when certain social media posts violated each platform's own policies; *EIP did not make recommendations to the platforms about what actions they should take*."[206]



Documents produced to the Committee and Select Subcommittee by both the SIO and other entities contain numerous examples of EIP analysts and staff making explicit recommendations to the platforms for specific enforcement measures. Appendix I compiles recommendations from 75 Jira tickets Stanford produced in which the EIP made a direct recommendation to platforms on what action should be taken.

---

[204] *Background on the SIO's Projects on Social Media*, STANFORD INTERNET OBSERVATORY (Mar. 17, 2023), https://cyber.fsi.stanford.edu/io/news/background-sios-projects-social-media.
[205] Email from John Bellinger to Committee Staff (March 20, 2023 5:09 PM). (on file with the Comm.).
[206] *Background on the SIO's Projects on Social Media*, STANFORD INTERNET OBSERVATORY (Mar. 17, 2023), https://cyber.fsi.stanford.edu/io/news/background-sios-projects-social-media (emphasis added).

Below are a few examples to illustrate how explicitly the EIP instructed social media companies to take action:

Ticket #	Entry
EIP-345	"The article is being shared on Facebook, and while it has been labeled when shared in a group, official Page shares did not receive such a label . . . We recommend labeling all instances of the article being shared on Facebook."
EIP-378	"This has circulated in pro-Trump conservative groups and sub-communities . . . We recommend that you all flag as false, or remove the posts below."
EIP-396	"Hi Facebook, Reddit, and Twitter . . . we recommend it be removed from your platforms."
EIP-407	"Hi Twitter team – please see the ticket above, which we'd recommend be labeled with information pertaining to mail-in voting."
EIP-421	"We recommend that posts like these be labeled if they are alleging fraud, and that further action may be appropriate if this post actually documents fraud."
EIP-460	"Huckabee has not said whether the tweet was a joke or not . . . We recommend that Twitter labels the post with (a) proper voting information."
EIP-461	"Given the large audiences and Pennsylvania's swing state status, we'd recommend this content be actioned."
EIP-581	"We recommend you label or reduce the discoverability of the post."
EIP-638	"We recommend labeling his [sic] tweets and monitoring if any of the tagged influencer accounts retweet him."
EIP-656	"@SeanHannity is sharing a partial statement by Rep. Ilhan Omar . . . we recommend Twitter adds a label to Tweets sharing the link to the article."
EIP-668	"We repeat our recommendation that this account be suspended for the duration of election day from posting additional misleading information about voting."
EIP-673	"We recommend that this tweet, and other tweets sharing this false information, should be removed."; "We recommend taking action specifically on this account, such as suspending their ability to continue tweeting for 12 hours."
EIP-680	"We recommend that this tweet, as well as the tweets with the original video should be removed or labeled as misleading."
EIP-1020	"[W]e recommend links to its content be labeled or removed."

In EIP-421, the responsible EIP analyst appeared to make a remarkable admission about the EIP's true intentions, writing: "We recommend that posts like these be labeled if they are alleging fraud, and that further action may be appropriate *if this post actually documents fraud*."[207]

B. Stanford's Initial Efforts to Unlawfully Misrepresent and Withhold Jira Data

Despite the fact that the EIP admitted in its own report that the Jira system facilitated communication between the EIP and the federal government, Stanford initially refused to provide the Committee and Select Subcommittee with the archival Jira data. Based on the representations from Stanford and other entities with knowledge of the EIP's data retention practices, the Committee understood that Stanford was the only entity with access to the Jira ticket data.[208] Following a March 24, 2023, production which failed to adequately comply with the Committee's requests for the Jira data, the Committee issued a subpoena on April 12.[209] On April 28, the date of the subpoena's deadline, Stanford produced a set of marginally responsive communications, but again did not produce the Jira tickets.[210]

On May 4, Committee staff raised the issue of Jira tickets again during a phone call with counsel for Stanford, who agreed to consult with his client regarding the nature and retention of the Jira tickets.[211] Remarkably, on May 15, Stanford's counsel confirmed to Committee staff in another phone call that the contents of the Jira tickets *were* responsive to the Committee's subpoena but that Stanford would nevertheless refuse to produce them.[212] According to Stanford's counsel, the Jira tickets supposedly "concern[ed] only a research project conducted by Stanford students."[213] In light of Stanford's apparent unwillingness to comply in full with the subpoena, on June 1, 2023, the Committee sent a letter to Stanford raising the prospect of enforcing the subpoena, the deadline of which had long since passed.[214]

---

[207] *See* EIP-421, submitted by CIS Misinformation Reporting; ticket created (Oct. 21, 2020, 11:18 AM) (archived Jira ticket data produced to the Comm.) (emphasis added); *see also* McKenzie Sadeghi, *Fact Check: Mailing Ballots to Dead People Not Leading to Voter Fraud, Experts and Studies Say*, USA TODAY (July 15, 2020) available at https://web.archive.org/web/20230714194915/https://www.usatoday.com/story/news/factcheck/2020/07/14/fact-check-mailing-ballots-dead-people-not-leading-voter-fraud/3214074001/.

[208] House Judiciary Committee's Transcribed Interview of Alex Stamos (June 23, 2023), at 108 (on file with the Comm.).

[209] Letter to Alex Stamos, Dir., Stanford Internet Observatory, from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (Apr. 12, 2023).

[210] Email from Stanford's Counsel to Committee Staff (Apr. 29, 2023, at 12:00 AM).

[211] Phone call between John Bellinger and Committee Staff (May 4, 2023).

[212] Phone call between John Bellinger and Committee Staff (May 15, 2023); *see also* Letter to John B. Bellinger, III, from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (June 1, 2023), at 2.

[213] Letter to John B. Bellinger, III, from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (June 1, 2023), at 2.

[214] *Id*.

The Committee's subpoena imposes legal obligations on SIO to comply and produce responsive materials. Thus, your client's refusal to produce documents responsive to the Committee's subpoena—four weeks after the subpoena return date—is highly concerning. Accordingly, the Committee expects the SIO will complete its production of responsive documents, in full, by no later than Wednesday, June 14, 2023, at 5:00 p.m. If Stanford fails to comply in full with the subpoena's demands, the Committee may be forced to consider the use of one or more enforcement mechanisms. Thank you for your client's attention to this matter.

Sincerely,

Jim Jordan
Chairman

It was only after the Chairman's letter that the SIO ultimately relented and began producing the Jira data.[215] All told, the Committee has received fifteen productions from the SIO, including six which contain the data for almost 400 EIP Jira tickets.[216]

C. Numerous Documents Contradict Witness Testimony Regarding CISA's Involvement with the EIP

The Committee and Select Subcommittee have conducted transcribed interviews of several witnesses involved in the EIP who have claimed that CISA had little to no involvement in the EIP. This testimony is contradicted by the overwhelming amount of evidence obtained by the Committee and Select Subcommittee pursuant to several subpoenas issued to entities involved with the EIP. For example, Alex Stamos, the head of the EIP, claimed that CISA's role in the EIP was limited to introducing the EIP to the EI-ISAC:

> Q. So, you have contacted CISA, CISA introduces you to EI-ISAC. And we are still in the summer of 2020, to the best of your recollection?
>
> A. Okay.
>
> Q. What roles did CISA play, if any, after that?
>
> A. In the EIP they had no official role. They did not have the ability to report things directly to us. We would take things from EI-ISAC. I don't believe anything that EI-ISAC sent us came from CISA employees themselves. And they were not part of our day-to-day operations or our analysis. So, *they had very little role, if none, in EIP*.[217]

[215] *See* Stanford Internet Observatory – Document Production Index (June 14, 2023) (on file with the Comm.).
[216] *See* App'x II.
[217] House Judiciary Committee's Transcribed Interview of Alex Stamos (June 23, 2023), at 95 (on file with the Comm.) (emphasis added).

But Dr. Kate Starbird of CIP—and one of the founding members of the EIP—recalled more involvement from CISA. She testified:

> Q. Was it your understanding that some of the external partners were government agencies?
>
> A. It was my understanding that there was one Federal Government agency and that there were other organizations that convened local and State election officials who we saw — who my understanding was is that we could help them and they could help us figure out what the ground truth was around election processes and procedures. And so that that would be an important part of a collaboration when you're trying to address that kind of misinformation.
>
> Q. And which Federal agency was the one that you were referencing?
>
> A. The Federal agency that -- is kind of who was -- is the CISA agency, yeah.[218]

Regarding the creation of the EIP, former CISA Director Krebs testified that "EIP's establishment was independent of CISA," which is directly contradicted by documents from the summer of 2020 that the Atlantic Council, one of the members of the EIP, understood that the EIP was created "at the request of DHS/CISA."[219]

The testimony of Stamos and Krebs regarding the extent of CISA's involvement in the creation and operation of EIP is contradicted by an overwhelming amount of evidence obtained by the Committee and Select Subcommittee, which makes abundantly clear that, not only was CISA directly involved the creation of the EIP, but it also took an active role in the EIP's day-to-day operations, receiving a constant stream of tips and other information from both CISA and the CISA-funded CIS.

D. Stanford's Continued Misrepresentations Regarding CISA, the EIP, and Jira

Unable to hide from its own report, counsel for Stanford initially admitted, in a June 14, 2023, letter to the Committee, that the GEC submitted tickets through the Jira system.[220] However, Stanford's counsel then claimed that "[a]side from this small number of GEC-initiated EIP tickets, SIO did not use Jira to receive information from, or share information with, any federal government agencies or officials about the [Virality Project] or EIP projects."[221] Stanford's counsel also claimed that "for EIP, SIO did not provide any government agency or employee of a government agency (whether federal, state, or local) access to the Jira database,

---

[218] House Judiciary Committee's Transcribed Interview of Kate Starbird (June 6, 2023), at 77 (on file with the Comm.).
[219] *Cf.* House Judiciary Committee's Transcribed Interview of Chris Krebs (Oct. 11, 2023), at 170 (on file with the Comm.); email from Graham Brookie to Atlantic Council employees (July 31, 2020, 5:54 PM) (on file with the Comm.).
[220] Letter from John B. Bellinger III to Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary (June 14, 2023), at 4 (on file with the Comm.).
[221] *Id*.

and SIO only communicated using Jira with a single federal agency (the State Department) regarding the handful of tickets that GEC initiated."[222]

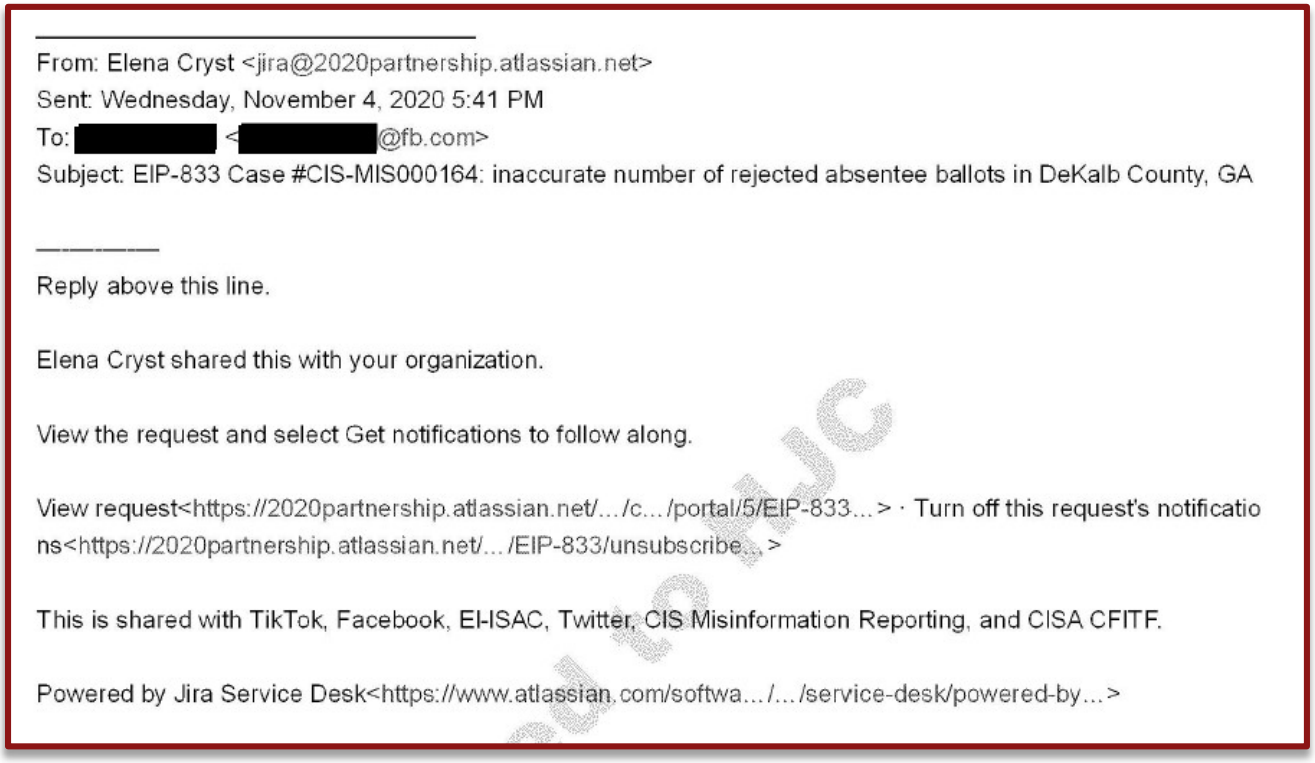
Arnold & Porter

that Jira data. However, the statement in the Committee's letter that the "government and large social media platforms initiated and received information" from Jira is not accurate.[11] Social media companies did not initiate any EIP or VP Jira tickets. Federal government agencies did not initiate any Jira tickets relating to the VP project. The State Department's Global Engagement Center (GEC), which was established by Congress to counter foreign state disinformation and propaganda, initiated a very small number of tickets (fewer than 20) during the EIP 2020 project. These tickets concerned foreign propaganda and disinformation, primarily instigated by Russia. Aside from this small number of GEC-initiated EIP tickets, SIO did not use Jira to receive information from, or share information with, any federal government agencies or officials about the VP or EIP projects. Information from a small number of Jira tickets relating to the EIP project, and from an even smaller number of tickets relating to the VP project, was shared with social media companies. (As stated above, Stanford is producing Jira ticket data that was received from the GEC or exchanged with social media companies.) As Stanford's counsel has explained in several telephone conversations with your staff, the vast majority of Jira tickets were generated by students and supervising researchers, and it is Stanford's understanding that the tickets were never accessed or viewed by individuals or entities other than the researchers and non-governmental institutions participating in EIP and VP.

More specifically, for EIP, SIO did not provide any government agency or employee of a government agency (whether federal, state, or local) access to the Jira database, and SIO only communicated using Jira with a single federal agency (the State Department) regarding the handful of tickets that GEC initiated. As noted above, social media companies did not initiate any Jira tickets. The non-governmental, non-profit Center

[222] *Id*.

These statements are inaccurate. In addition to the fact that CISA personnel referenced the "EIP-" codes when switchboarding, the Committee has obtained records of communications proving that CISA personnel were receiving information from or generated by the Jira system. For example, the email notification below, which was generated by the Jira system, indicates that the ticket "EIP-833" was "shared with . . . CISA CFITF."[223]



From: Elena Cryst <jira@2020partnership.atlassian.net>
Sent: Wednesday, November 4, 2020 5:41 PM
To: [redacted] <[redacted]@fb.com>
Subject: EIP-833 Case #CIS-MIS000164: inaccurate number of rejected absentee ballots in DeKalb County, GA

Reply above this line.

Elena Cryst shared this with your organization.

View the request and select Get notifications to follow along.

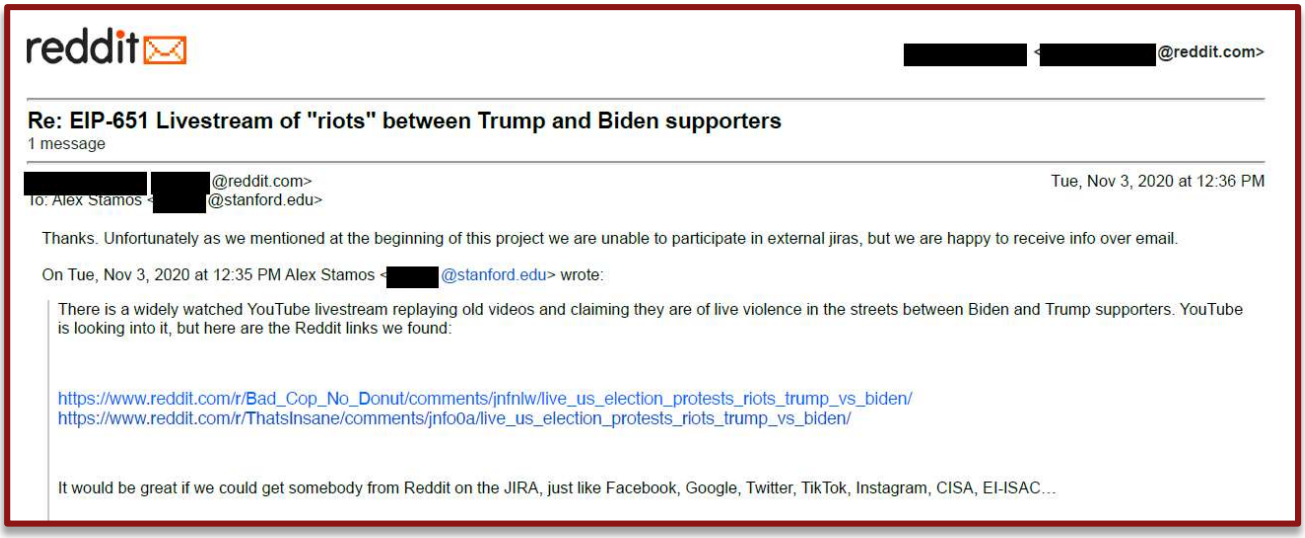
View request<https://2020partnership.atlassian.net/...c.../portal/5/EIP-833...> · Turn off this request's notificatio ns<https://2020partnership.atlassian.net/.../EIP-833/unsubscribe...>

This is shared with TikTok, Facebook, EI-ISAC, Twitter, CIS Misinformation Reporting, and CISA CFITF.

Powered by Jira Service Desk<https://www.atlassian.com/softwa.../.../service-desk/powered-by...>

[223] Email from Elena Cryst to Facebook employee (Nov. 4, 2020, 5:41 PM) (on file with the Comm.); *see also* EIP-833, submitted by CIS Misinformation Reporting, ticket created (Nov. 4, 2020, 1:28 PM) (archived Jira ticket data produced to the Comm.); Tom Clark (@tom_s_clark) TWITTER (Nov. 4, 2020 12:03 PM) available at https://web.archive.org/web/20201104221417/https://twitter.com/tom_s_clark/status/1324079751640862727; Daniel Dale (@ddale8) TWITTER (Nov. 4, 2020 1:30 PM) available at https://web.archive.org/web/20201105010400/https://twitter.com/ddale8/status/1324101773322276864.

An email exchange from November 3, 2023 between Alex Stamos and Reddit further suggests that CISA had some form of access to the Jira system. In the email, Stamos attempted to pressure Reddit to join the EIP's Jira system, writing: "It would be great if we could get somebody from Reddit on JIRA, just like Facebook, Google, Twitter, TikTok, Instagram, *CISA*, EI-ISAC…"[224] The Reddit employee responded: "Thanks. Unfortunately as we mentioned at the beginning of this project we are unable to participate in external jiras, but we are happy to receive info over email."[225]



reddit [redacted] <[redacted]@reddit.com>

Re: EIP-651 Livestream of "riots" between Trump and Biden supporters
1 message

[redacted] [redacted]@reddit.com> Tue, Nov 3, 2020 at 12:36 PM
To: Alex Stamos <[redacted]@stanford.edu>

Thanks. Unfortunately as we mentioned at the beginning of this project we are unable to participate in external jiras, but we are happy to receive info over email.

On Tue, Nov 3, 2020 at 12:35 PM Alex Stamos <[redacted]@stanford.edu> wrote:

> There is a widely watched YouTube livestream replaying old videos and claiming they are of live violence in the streets between Biden and Trump supporters. YouTube is looking into it, but here are the Reddit links we found:
>
> https://www.reddit.com/r/Bad_Cop_No_Donut/comments/jnfnlw/live_us_election_protests_riots_trump_vs_biden/
> https://www.reddit.com/r/ThatsInsane/comments/jnfo0a/live_us_election_protests_riots_trump_vs_biden/
>
> It would be great if we could get somebody from Reddit on the JIRA, just like Facebook, Google, Twitter, TikTok, Instagram, CISA, EI-ISAC…

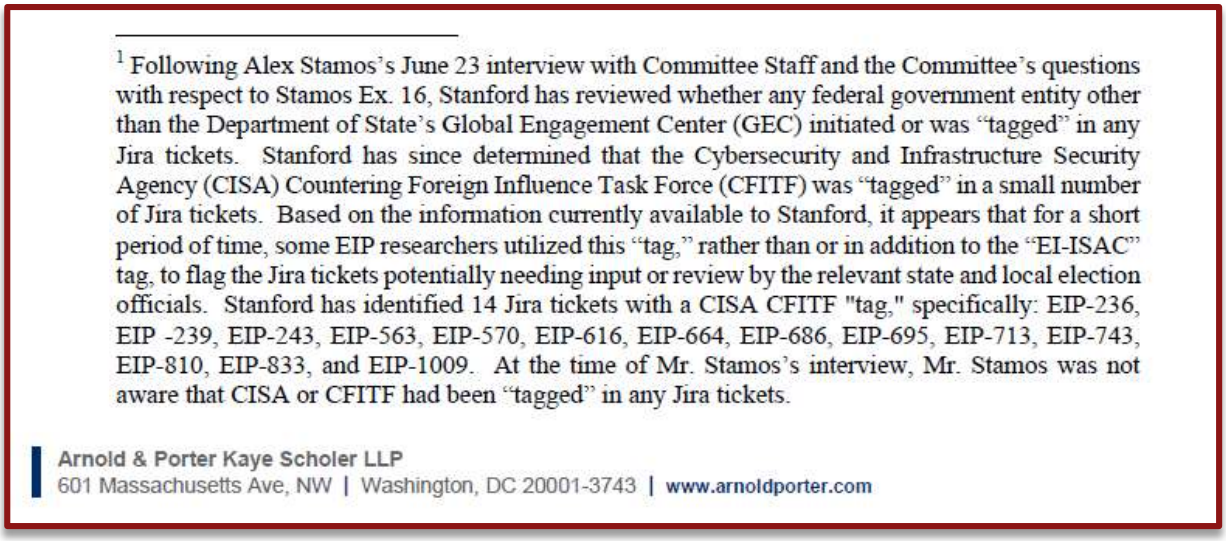
When confronted with this discrepancy during his transcribed interview, Stamos claimed that he "was probably making a mistake there talking about CISA because EI-ISAC were the people who had access to the Jira," despite the fact that he independently listed both CISA and the EI-ISAC in the email.[226]

The Jira data produced to the Committee and Select Subcommittee contains a number of cells in which "CISA" is mentioned, including in contexts that prove close coordination between CISA and the EIP. For example, EIP-315 contains an entry which reads, "EIP – this information was posted on an app that is not a primary social media platform. CISA is looking into how to handle this type of reporting."[227]

On July 27, 2023, more than a month after Stamos's interview, Stanford's counsel finally admitted in a letter to the Committee that CISA was, in fact, involved with the EIP's Jira system and that CISA had been directly "tagged" on a number of tickets.[228] Stanford's counsel claimed

[224] Email from Alex Stamos to Reddit employee (Nov. 3, 2020 12:35 PM) (on file with the Comm.) (emphasis added).
[225] Email from Reddit employee to Alex Stamos (Nov. 3, 2020 12:36 PM) (on file with the Comm.).
[226] *Cf.* House Judiciary Committee's Transcribed Interview of Alex Stamos (June 23, 2023), at 218 (on file with the Comm.); email from Alex Stamos to Reddit employee (Nov. 3, 2020, 12:35 PM) (on file with the Comm.).
[227] *See* EIP-315, submitted by CIS Misinformation Reporting, ticket created (Oct. 5, 2020, 4:19 PM) (archived Jira ticket data produced to the Comm.).
[228] *See* Letter from John B. Bellinger III to Rep. Jim Jordan, Chairman, H. Comm. On the Judiciary (July 27, 2023), at 1 n.1.

in the letter that "At the time of Mr. Stamos's interview, Mr. Stamos was not aware that CISA or CFITF had been 'tagged' in any Jira tickets."[229]



[1] Following Alex Stamos's June 23 interview with Committee Staff and the Committee's questions with respect to Stamos Ex. 16, Stanford has reviewed whether any federal government entity other than the Department of State's Global Engagement Center (GEC) initiated or was "tagged" in any Jira tickets. Stanford has since determined that the Cybersecurity and Infrastructure Security Agency (CISA) Countering Foreign Influence Task Force (CFITF) was "tagged" in a small number of Jira tickets. Based on the information currently available to Stanford, it appears that for a short period of time, some EIP researchers utilized this "tag," rather than or in addition to the "EI-ISAC" tag, to flag the Jira tickets potentially needing input or review by the relevant state and local election officials. Stanford has identified 14 Jira tickets with a CISA CFITF "tag," specifically: EIP-236, EIP -239, EIP-243, EIP-563, EIP-570, EIP-616, EIP-664, EIP-686, EIP-695, EIP-713, EIP-743, EIP-810, EIP-833, and EIP-1009. At the time of Mr. Stamos's interview, Mr. Stamos was not aware that CISA or CFITF had been "tagged" in any Jira tickets.

Arnold & Porter Kaye Scholer LLP
601 Massachusetts Ave, NW | Washington, DC 20001-3743 | www.arnoldporter.com

This is an especially dubious assertion, given that EIP-664, EIP-686, EIP-695—tickets which the SIO admitted were shared with CISA—were assigned to Stamos, according to the Jira data produced to the Committee and Select Subcommittee.[230]

[229] *Id*.

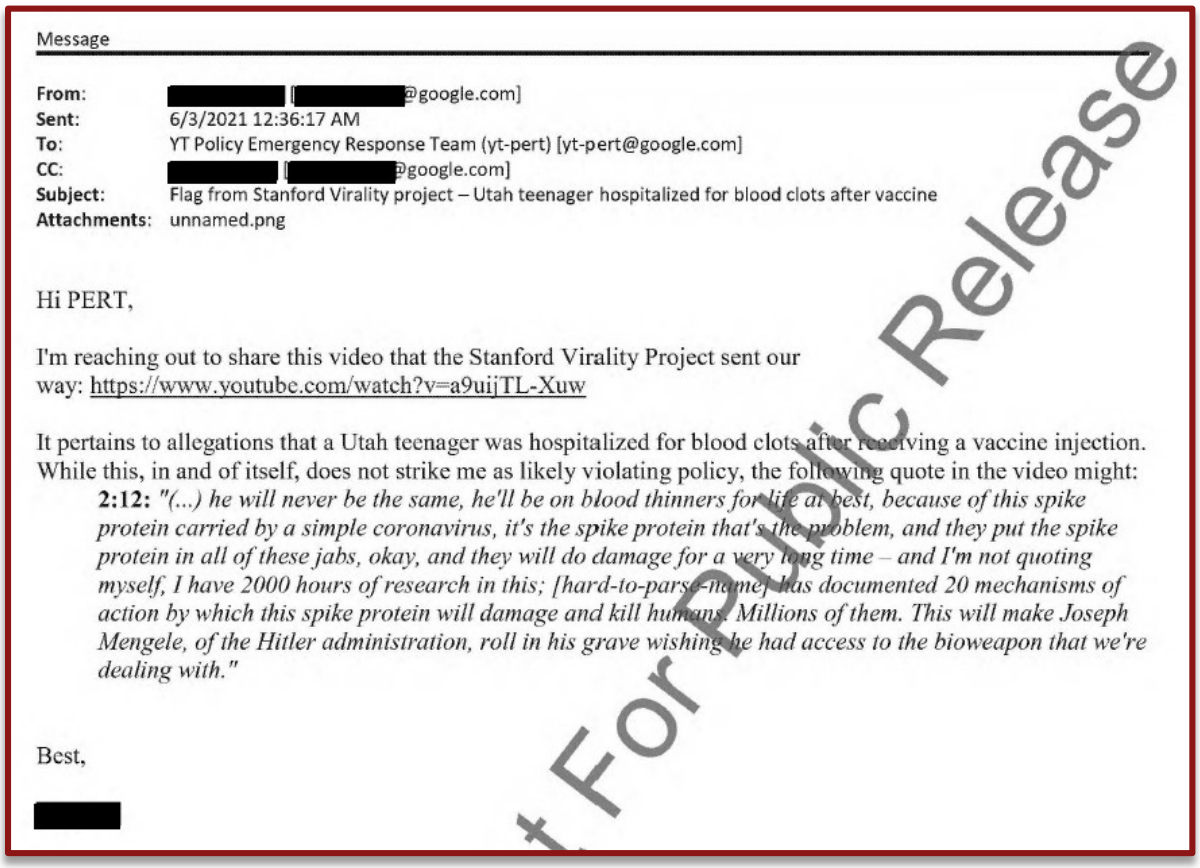
[230] *See* EIP-664, submitted by Mike Caulfield, ticket created (Nov. 3, 2020, 11:26 AM) (archived Jira ticket data produced to the Comm.); EIP-686, submitted by CIS Misinformation Reporting, ticket created (Nov. 3, 2020, 12:58 PM) (archived Jira ticket data produced to the Comm.); EIP-695, submitted by CIS Misinformation Reporting, ticket created (Nov. 3, 2020, 1:34 PM) (archived Jira ticket data produced to the Comm.).

EPILOGUE

It is no surprise that Stanford University attempted to refuse to turn over documents responsive to the Committee's subpoena: they reveal that the EIP was not a non-partisan "school project" comprised of students and researchers interested in combatting misinformation online. Instead, from start to finish, the EIP operation worked directly with the federal government and disproportionally targeted conservative-oriented speech.

After the 2020 election, what others have deemed the "censorship industrial complex," played out as expected. After President Trump fired CISA Director Chris Krebs in November 2020, Mr. Krebs created the Krebs Stamos Group with Alex Stamos, the head of the EIP and the SIO, in January 2021. Matt Masterson left CISA at the end of 2020 and took a position as a non-research fellow with Stanford, working with the SIO and its Virality Project.

With the election over and the American people questioning the wisdom of lockdowns and the safety of the COVID-19 vaccines, the EIP reconstituted itself as the Virality Project. Again working with the federal government, the SIO launched the Virality Project as a "a global study aimed at understanding the disinformation dynamics specific to the COVID-19 crisis." The Virality Project again used Jira tickets. Though Stanford was less explicit and specific in its recommendations for censorship as it was under the EIP model, social media platforms still dutifully removed content flagged by Stanford:



Message

From: [redacted] [redacted]@google.com]
Sent: 6/3/2021 12:36:17 AM
To: YT Policy Emergency Response Team (yt-pert) [yt-pert@google.com]
CC: [redacted] [redacted]@google.com]
Subject: Flag from Stanford Virality project – Utah teenager hospitalized for blood clots after vaccine
Attachments: unnamed.png

Hi PERT,

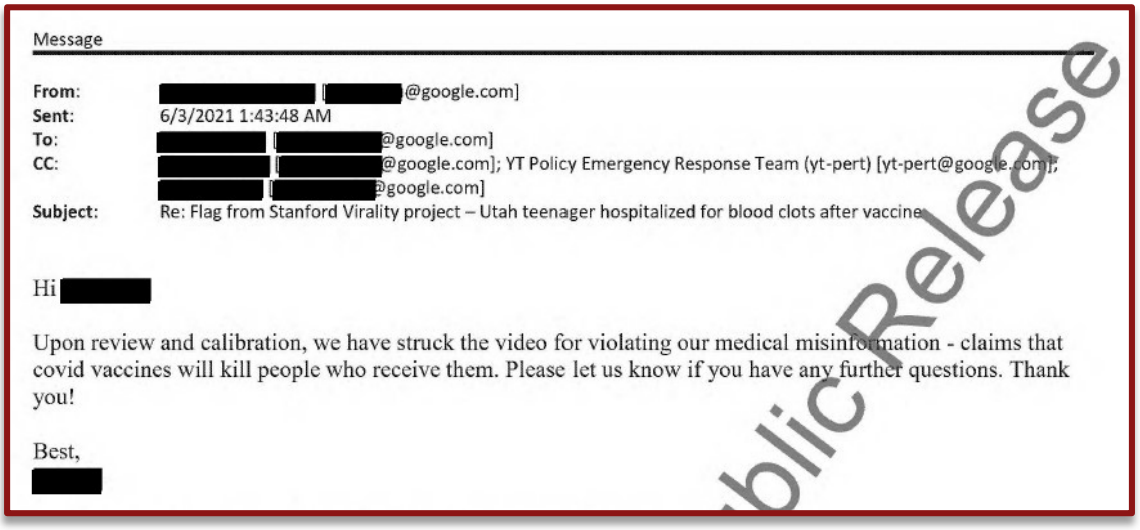
I'm reaching out to share this video that the Stanford Virality Project sent our way: https://www.youtube.com/watch?v=a9uijTL-Xuw

It pertains to allegations that a Utah teenager was hospitalized for blood clots after receiving a vaccine injection. While this, in and of itself, does not strike me as likely violating policy, the following quote in the video might:

> **2:12:** *"(...) he will never be the same, he'll be on blood thinners for life at best, because of this spike protein carried by a simple coronavirus, it's the spike protein that's the problem, and they put the spike protein in all of these jabs, okay, and they will do damage for a very long time – and I'm not quoting myself, I have 2000 hours of research in this; [hard-to-parse-name] has documented 20 mechanisms of action by which this spike protein will damage and kill humans. Millions of them. This will make Joseph Mengele, of the Hitler administration, roll in his grave wishing he had access to the bioweapon that we're dealing with."*

Best,

[redacted]



Message

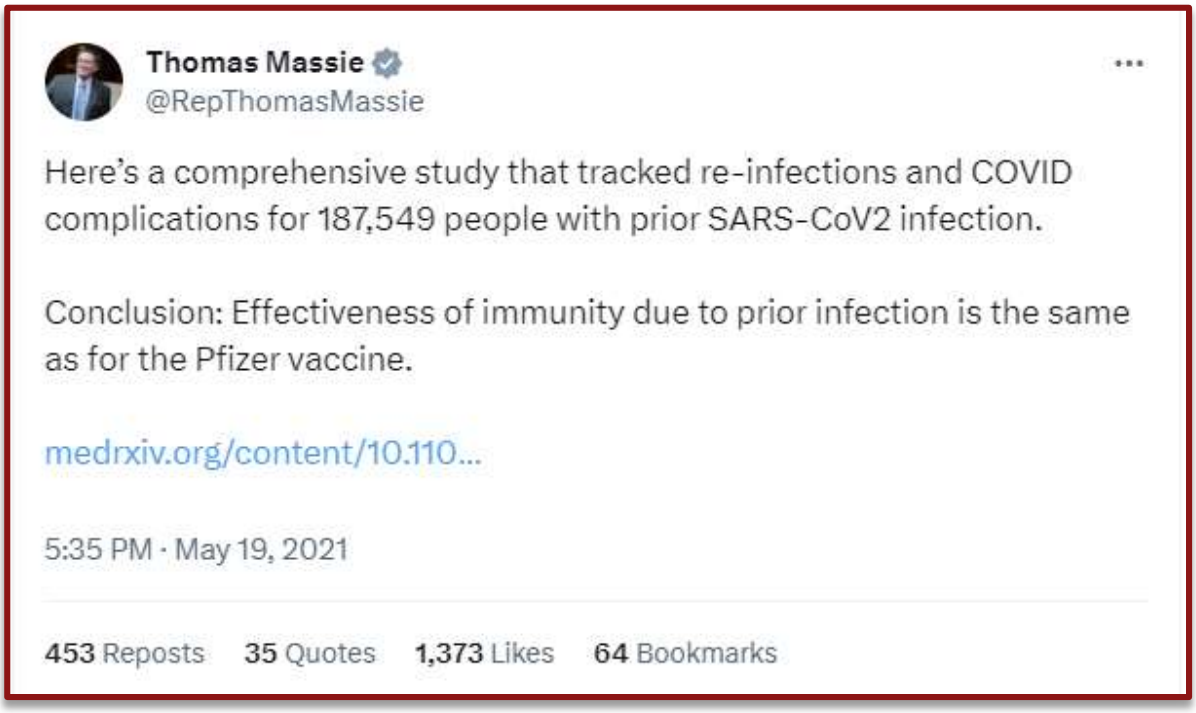
From: [redacted] [redacted]@google.com]
Sent: 6/3/2021 1:43:48 AM
To: [redacted] [redacted]@google.com]
CC: [redacted] [redacted]@google.com]; YT Policy Emergency Response Team (yt-pert) [yt-pert@google.com]; [redacted] [redacted]@google.com]
Subject: Re: Flag from Stanford Virality project – Utah teenager hospitalized for blood clots after vaccine

Hi [redacted]

Upon review and calibration, we have struck the video for violating our medical misinformation - claims that covid vaccines will kill people who receive them. Please let us know if you have any further questions. Thank you!

Best,
[redacted]

Like the EIP, Stanford's Virality Project continued to flag content directly to social media platforms, including *true* content by elected officials, such as the tweet below by Congressman Thomas Massie.[231] In reference to this tweet, the Virality Project ticket stated, "Dear Facebook and Twitter teams, Please note this Israeli narrative claiming that Covid-19 immunity is equivalent to vaccination immunity, with the following URLs:" before flagging Congressman Massie's tweet among other Facebook and Twitter links.[232]



Thomas Massie
@RepThomasMassie

Here's a comprehensive study that tracked re-infections and COVID complications for 187,549 people with prior SARS-CoV2 infection.

Conclusion: Effectiveness of immunity due to prior infection is the same as for the Pfizer vaccine.

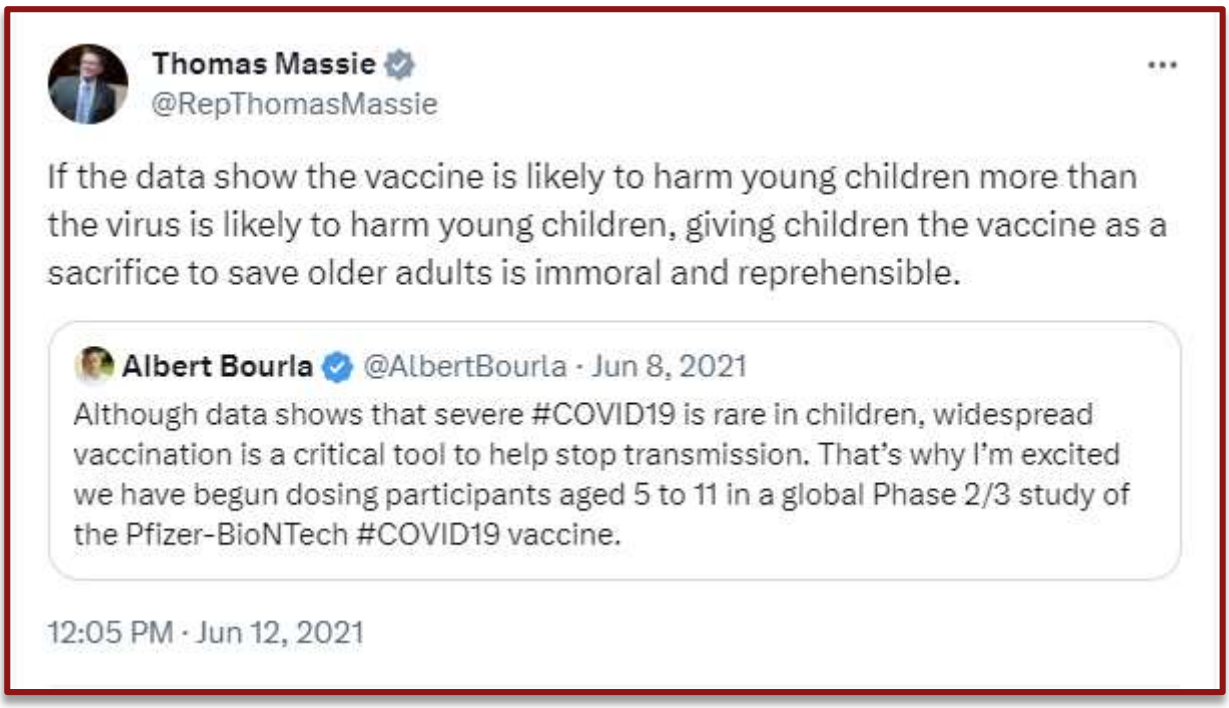
medrxiv.org/content/10.110...

5:35 PM · May 19, 2021

453 Reposts **35** Quotes **1,373** Likes **64** Bookmarks

[231] VP-899, submitted by [REDACTED], ticket created (May 21, 2021, 9:49 AM) (archived Jira ticket data produced to the Comm.); *see also* Rep. Thomas Massie (@RepThomasMassie), TWITTER (May 19, 2021, 5:35 PM), https://twitter.com/RepThomasMassie/status/1395130940343607297.
[232] *Id*.

The Virality Project later flagged this tweet by Congressman Massie as well.[233]



After President Biden was inaugurated in January 2021, the government's censorship regime ramped up. At CISA, the CFITF team dropped any pretense of a "foreign"-focus and relabeled itself as the "MDM team" that would focus on foreign *and domestic* speech that the government considered mis-, dis-, or malinformation.[234] Throughout 2021, the Biden White House engaged in a pressure campaign against Facebook and other social media companies to censor anti-vaccine content, even if it was true.[235] By 2022, CISA invited Dr. Starbird, then-Twitter Executive Vijaya Gadde, and others to form an advisory MDM Subcommittee to consult with CISA about how the agency could and should combat Americans' speech that the government considered to be mis-, dis-, or malinformation.[236] DHS created, and then disbanded after public outcry, the short-lived Disinformation Governance Board.[237]

---

[233] VP-1018, submitted by [REDACTED], ticket created (June 18, 2021, 9:58 AM) (archived Jira ticket data produced to the Comm.); *see also* Rep. Thomas Massie (@RepThomasMassie), TWITTER (June 12, 2021), https://twitter.com/RepThomasMassie/status/1403745403665850372.

[234] *See* STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A "CYBERSECURITY" AGENCY COLLUDED WITH BIG TECH AND "DISINFORMATION" PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).

[235] Ryan Tracy, *Facebook Bowed to White House Pressure, Removed Covid Posts*, WALL ST. J. (July 28, 2023); Rep. Jim Jordan (@Jim_Jordan), TWITTER (July 27, 2023, 12:03 PM), https://twitter.com/Jim_Jordan/status/1684595375875760128; Rep. Jim Jordan (@Jim_Jordan), TWITTER (July 28, 2023, 12:03 PM), https://twitter.com/Jim_Jordan/status/1684957660515328001; Rep. Jim Jordan (@Jim_Jordan), TWITTER (Aug. 3, 2023, 11:00 AM), https://twitter.com/Jim_Jordan/status/1687116316073930752; Rep. Jim Jordan (@Jim_Jordan), TWITTER (Sept. 5, 2023, 6:17 PM), https://twitter.com/Jim_Jordan/status/1699184930331267539.

[236] *See* STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A "CYBERSECURITY" AGENCY COLLUDED WITH BIG TECH AND "DISINFORMATION" PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).

[237] *Id*.; Ronn Blitzer, *Biden Administration 'Disinformation' Board on Pause Amid Free Speech Concerns: Reports*, FOX NEWS (May 18, 2022).

But by 2023, as Republicans retook the majority in the House of Representatives and initiated oversight of the censorship-industrial complex, CISA scrubbed its website of references to domestic censorship.[238] The Committee and Select Subcommittee obtained and revealed how Facebook changed its policies because of pressure from the Biden Administration.[239] Internal Facebook documents showed that the Biden White House in particular wanted true information and satire censored at a rate even Big Tech found objectionable.[240] Based on the Committee's and Select Subcommittee's work, even the mainstream media could no longer ignore these constitutional violations.[241] The plaintiffs in *Missouri v. Biden* have obtained significant victories before a federal district court and the U.S. Court of Appeals for the Fifth Circuit, and now will have their case heard by the Supreme Court. Public reporting shows that universities are reconsidering whether to permit their professors to receive funding and engage in censorship work.[242]

But the work is not done yet. The Committee and Select Subcommittee's investigation remains ongoing. To better inform legislative efforts to end government censorship 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 and third parties, including those used to facilitate censorship by proxy.

---

[238] *See* STAFF OF SELECT SUBCOMM. ON THE WEAPONIZATION OF THE FEDERAL GOVERNMENT OF THE H. COMM. ON THE JUDICIARY, 118TH CONG., THE WEAPONIZATION OF CISA: HOW A "CYBERSECURITY" AGENCY COLLUDED WITH BIG TECH AND "DISINFORMATION" PARTNERS TO CENSOR AMERICANS (Comm. Print June 26, 2023).
[239] Rep. Jim Jordan (@Jim_Jordan), TWITTER (July 27, 2023, 12:03 PM), https://twitter.com/Jim_Jordan/status/1684595375875760128.
[240] *Id*.
[241] *See, e.g.*, Ryan Tracy, *Facebook Bowed to White House Pressure, Removed Covid Posts*, WALL ST. J. (July 28, 2023).
[242] Naomi Nix et. al, *Misinformation Research Is Buckling Under GOP Legal Attacks*, WASH. POST, (Sept. 23, 2023).

APPENDIX I

The House Judiciary Committee and its Select Subcommittee on the Weaponization of the Federal Government have obtained documents and information from Stanford University, pursuant to a subpoena, which reveal that EIP analysts and staff made explicit recommendations to social media platforms for specific enforcement measures on at least 75 occasions in just a four-month span in the lead-up to and during the 2020 election. This appendix compiles those 75 recommendations in order of their EIP Jira ticket number. The entire Jira ticket, including comments from social media platforms, can be found by cross-referencing the archived Jira ticket data provided in Appendix II.

Ticket #	Entry
EIP-166	"Hello Google, . . . We recommend this ad be removed."
EIP-279	"We recommend Twitter label or remove this tweet."
EIP-307	"We recommend that the following platforms take these actions: *Twitter* - Disable account."
EIP-321	"Recommended actions: Ban sharing links to the following sites:"
EIP-329	"We are reporting two instances of electoral disinformation constituting participation interference and delegitimization. We flag a post and an account to you all at Twitter, and recommend the following:"
EIP-330	"We recommend that Twitter and Facebook remove these posts. If you are not able to remove these posts, we suggest that they be labeled as misleading."
EIP-345	"The article is being shared on Facebook, and while it has been labeled when shared in a group, official Page shares did not receive such a label . . . We recommend labeling all instances of the article being shared on Facebook."
EIP-348	"Recommend labeling."
EIP-378	"This has circulated in pro-Trump conservative groups and sub-communities . . . We recommend that you all flag as false, or remove the posts below."
EIP-389	"We also recommend expanded enforcement efforts on election misinformation on content in non-English languages."
EIP-396	"Hi Facebook, Reddit, and Twitter . . . we recommend it be removed from your platforms."

EIP-397	"Hi, Facebook, here are two posts alleging problems with voting machines, we recommend labeling:"
EIP-402	"Twitter and Reddit, we are passing along the full links we found for your visibility, and recommend you label them with voting information."
EIP-407	"Hi Twitter team – please see the ticket above, which we'd recommend be labeled with information pertaining to mail-in voting."
EIP-417	"This video narration claims to show evidence of voter fraud in Maryland, but the video itself (footage of an election worker) does not show anything that we interpret as voter fraud. We recommend that this video be removed or labeled."
EIP-421	"We recommend that posts like these be labeled if they are alleging fraud, and that further action may be appropriate if this post actually documents fraud."
EIP-450	"At minimum, we recommend that the posts be labeled with labels clarifying that vote by mail is secure."
EIP-451	"We recommend taking the same action on the new ad."
EIP-455	"+*Platform Recommendations*+ +*Twitter*+, where narrative is receiving the most interactions, to flag the video and hashtag and continue to monitor for possible poll watcher/intimidation narratives."
EIP-460	"Huckabee has not said whether the tweet was a joke or not . . . We recommend that Twitter labels the post with (a) proper voting information."
EIP-461	"Hi Twitter team – there are a number of high-profile individuals, including the President, making accusations of voter fraud . . . Given the large audiences and Pennsylvania's swing state status, we'd recommend this content be actioned."
EIP-479	"We recommend labeling accordingly."
EIP-483	"We recommend twitter remove the tweet as it is a fairly clear violation."
EIP-489	"We recommend to Twitter that the tweets be removed."
EIP-503	"We recommend removing the following tweets as misleading."
EIP-511	"We recommend labeling this content and monitoring for Chinese-language keywords like election fraud and QAnon terms for action on future content."

EIP-512	“We recommend that Twitter remove this tweet.”; “We recommend these tweets be taken down.”; “I recommend that Twitter and Facebook remove these posts or add a strong label.”
EIP-537	“Hello Youtube, Facebook teams: We are adding you to this ticket as the videos in questions contain several misleading claims about mail-in ballots as well as in-person voting. We recommend a specific label be applied to these posts.”
EIP-559	“We recommend removing or labeling this tweet.”; “As this is clearly false information about the election we recommend removal by Twitter.”
EIP-575	“We recommend Twitter actions the account for election delegitimization.”
EIP-581	“We recommend you label or reduce the discoverability of the post.”
EIP-585	“We recommend removing the linked Tweet.”; “Recommend also removing the linked Quote Tweets.”
EIP-589	“As it is a false claim that undermines trust in the electoral process we recommend its removal.”
EIP-608	“Recommend labeling.”
EIP-614	“We recommend at least labeling as this is a disproven claim of an electoral crime.”
EIP-615	“We recommend removing these posts and will update you with any more.”
EIP-638	“We recommend labeling his [sic] tweets and monitoring if any of the tagged influencer accounts retweet him.”
EIP-639	“We recommend removing or labeling these tweets.”
EIP-656	“@SeanHannity is sharing a partial statement by Rep. Ilhan Omar . . . we recommend Twitter adds a label to Tweets sharing the link to the article.”
EIP-664	“Twitter, recommend removing:”
EIP-668	“We repeat our recommendation that this account be suspended for the duration of election day from posting additional misleading information about voting.”

EIP-673	"We recommend that this tweet, and other tweets sharing this false information, should be removed."; "We recommend taking action specifically on this account, such as suspending their ability to continue tweeting for 12 hours."
EIP-680	"We recommend that this tweet, as well as the tweets with the original video should be removed or labeled as misleading."
EIP-698	"Recommend removal for some, labeling for other Tweets."
EIP-705	"We recommend that this tweet be removed or flagged for misleading content."
EIP-706	"As the accounts are making a baseless claim that undermines trust in the electoral process we recommend the accounts be actioned."
EIP-715	"This account in the above tweet is attempting to delegitimize the voting process without evidence. We recommend it be actioned."
EIP-746	"We recommend removing this content."
EIP-767	"We recommend Twitter remove the posts."
EIP-779	"We recommend that posts sharing links to this story and posts sharing screenshots of this story be removed. If they cannot be removed, a banner explaining that they are sharing false or misleading content should be added."
EIP-780	"We know you are aware of the #stopthesteal push but we have gathered here some of the major contributors . . . We recommend actioning these quickly."
EIP-789	"These posts are growing rapidly, and we recommend that they be removed, because they undermine people's faith in the legitimacy of the election result."
EIP-790	"They share this video to suggest that Biden is engaging in voter fraud, but this is misleading . . . Facebook has put a warning banner on similar posts (see linked post), and we suggest that Twitter either remove these posts or do the same."
EIP-795	"We recommend that these posts be removed immediately."
EIP-798	"We recommend that the tweet be removed, or at least covered with a misleading/disputed content banner. It falsely undermines people's faith in the legitimacy of the election results."
EIP-811	"Users on Twitter and Facebook are sharing manipulated images of people moving boxes in trucks labeled 'Emergency Democrat Votes.' We suggest labeling or removing tweets that use this photo, as it could undermine people's faith in the legitimacy of the election process."

EIP-817	"As it is a claim without evidence that undermines trust in the election we recommend it be actioned."
EIP-847	"We recommend labeling (as some have already been) or removing these tweets."
EIP-853	"Recommend labels or removal:"
EIP-867	"We recommend that these claims be labeled as unsubstantiated."
EIP-868	"We strongly recommend that platforms take action on this content and any further content with this screenshot. These posts should be removed or labeled appropriately."
EIP-869	"We recommend at least labeling as this is a disproven claim of an election crime."
EIP-879	"We recommend that this content be removed or labeled."
EIP-890	"We recommend flagging (or removing) posts that make this claim:"
EIP-909	"We recommend removal."
EIP-920	"Recommend you limit spread of attached tweets."
EIP-949	"We have completed this analysis of the attached Breitbart article and recommend that any links to it be labeled or removed per policy."; "recommend applying the same label to other/new instances of the narrative."
EIP-952	"We recommend it be actioned with fact-check labeling."
EIP-969	"Facebook: please see this misleading Instagram story . . . Recommend labeling or other action, as it has already made its way to Twitter."
EIP-970	"Facebook and Twitter: this story from alleged Nevada 'whistleblower' claiming voting irregularities has not been verified or substantiated. It has received significant viral amplification. We recommend these links be labeled."
EIP-987	"We are working on a thread but recommend that Twitter/Facebook delete (or at least label) the videos."

EIP-989	“We recommend it be removed as violative of terms of service.”
EIP-996	“We recommend removing or labeling this content as appropriate.”
EIP-998	“We recommend that they be flagged for labeling or removal.”
EIP-1020	“we recommend links to its content be labeled or removed.”

APPENDIX II

Appendix II is the EIP and Virality Project Jira ticket data provided to the Committee and Select Subcommittee. If the Department of Homeland Security, among others, had the ability to see what American speech was being targeted and censored, so too should the American people.