ENVIRONMENTAL PROGRESS

NATURE, PEACE & FREEDOM FOR ALL

Censorship Laundering By The U.S. Department Of Homeland Security

Testimony by Michael Shellenberger to Homeland Security Subcommittee for Oversights, Investigations, and Accountability

For a hearing on:

"Censorship Laundering Part II: Preventing the Department of Homeland Security's Silencing of Dissent"

December 13, 2023

Chairman Green, Chairman Bishop, Chairman Ivey, and members of the Subcommittee, thank you for inviting my testimony.

Researchers asked by the U.S. Department of Homeland Security (DHS) to flag election and Covid misinformation to social media platforms in 2020 and 2021 say that they didn't break the law. According to the leaders of the Stanford Internet Observatory, and the other groups, they simply alerted social media platforms to potential violations of their Terms of Service. What the platforms chose to do after that was up to them.

But during the two years that these DHS-empowered researchers were asking social media platforms to take down, throttle, or otherwise censor social media posts, the President of the United States was accusing Big Tech of "killing people," his then-press secretary said publicly that the administration was "flagging violative posts for Facebook," members of Congress threatened to strip social media platforms of their legal right to operate because, they said, the platforms weren't censoring enough, and many supposedly disinterested researchers were aggressively demanding that the platforms change their Terms of Service.

It's true that social media platforms are private companies technically free to censor content as they see fit and are under no clearly stated obligation to obey demands by the US government or its authorized "researchers" at Stanford or anywhere else.

But the First Amendment of the U.S. Constitution states clearly that the government should take no action that would limit free speech, and the record shows that the US government, in general, and the DHS in particular, did just that.

DHS supported, created, and participated in the 2020 Cyber Threat Intelligence League, or CTIL; the 2020 Election Integrity Partnership, or EIP; and the 2021 Virality Project, or VP. In the case of the EIP and VP, four think tanks led by Stanford Internet Observatory, or SIO, and reporting to CISA, demanded and achieved mass censorship of the American people in direct violation of the First Amendment and the prohibition on government agencies from interfering in an election.

A longtime US Navy officer and a UK military contractor created the so-called anti-disinformation wing of the CTIL in 2020. In so doing, they pioneered the misdescription of censorship laundering as "cyber-security." They used CTIL as a front group to demand censorship and demanded that "cognitive security" be viewed as their responsibility, in addition to physical security and cyber-security.

CTIL created a handbook full of tactics, including demanding social media platforms change their terms of service. Another explains that while such activities overseas are "typically" done by "the CIA and NSA and the Department of Defense,"

censorship efforts "against Americans" have to be done using private partners because the government doesn't have the "legal authority."

DHS publicly blessed this project, and its staff helped create CTIL's "anti-disinformation" efforts.

The CTI League aimed to implement something called "AMITT," which stood for "Adversarial Misinformation and Influence Tactics and Techniques." AMITT was a disinformation framework that included many offensive actions, including working to influence government policy, discrediting alternative media, using bots and sock puppets, pre-bunking, and pushing counter-messaging. The specific "counters" to "disinformation" in AMITT and its successor framework, DISARM, included the following:

- "Create policy that makes social media police disinformation"
- "Strong dialogue between the federal government and private sector to encourage better reporting"
- "Marginalize and discredit extremists"
- "Name and Shame influencers"
- "Simulate misinformation and disinformation campaigns, and responses to them, before campaigns happen"
- "Use banking to cut off access"
- "Inoculate populations through media literacy training"

The explanations and justifications by the creators and leaders of the EIP and VP have shifted over the last nine months. At first, an SIO executive claimed in a video for DHS that the idea for EIP came from SIO's interns, who happened to be working at DHS. More recently, another SIO executive claimed that the idea was his.

Then, last month, this committee released documents establishing that the DHS-authorized groups believed the idea had come from DHS. "We just set up an election integrity partnership at the request of DHS/CISA," said an Atlantic Council senior executive, Graham Brookie, in an email sent on July 21, 2020.

After Matt Taibbi and I testified before Congress in March, an SIO spokesperson says it "did not censor or ask social media platforms to remove any social media content regarding coronavirus vaccine side effects."

That turned out not to be true, as internal messages from its operation, released publicly by this committee last month, proved.

- Consider the language that these DHS-authorized individuals used:
- "Hi Facebook, Reddit, and Twitter . . . we recommend it be removed from your platforms."
- "We repeat our recommendation that this account be suspended…."
- "We recommend labeling…."

- "We recommend that you all flag as false, or remove the posts below."

Under the guise of a research project, EIP was enmeshed with the federal government leading up to the 2020 election. Four students involved with EIP were even employed by CISA. One Stanford student, for example, worked as a DHS intern "inside the EIP network."

It is clear from the emails released by this committee that the supposedly independent Election Integrity Partnership (EIP) and CISA were working together and interacted. One email from a Colorado official was addressed to "EI-ISAC, CISA and Stanford partners," directly referring to EIP. The CISA-funded non-profit, Center for Internet Security (CIS), also sent alleged misinformation to social media companies.

CIS had previously claimed that its definition of election mis- and disinformation did not include "content that is polarizing, biased, partisan or contains viewpoints expressed about elections or politics," "inaccurate statements about an elected or appointed official, candidate, or political party," or "broad, non-specific statements about the integrity of elections or civic processes that do not reference a specific current election administration activity."

But the DHS emails reveal that CISA and CIS did, in fact, consider such content to be subject to censorship. The emails show that CISA and its non-profit partners reported political speech to social media companies, including jokes, hyperbole, and the types of "viewpoints" and "non-specific statements" that CIS once claimed it would not censor. Using the pretext of "election security," DHS sought to censor politically inconvenient speech about election legitimacy.

Messages one year later also showed VP researchers urging censorship of "general anti-vaccination" posts, of the CDC's own data, of accurate claims of natural immunity, of accurate information from the journal Lancet, of anti-lockdown protests, and even of someone's entire Google Drive.

In 2020, Department of Homeland officials and personnel from EIP were often on emails together, and CISA's personnel had access to EIP's tickets through an internal messaging system, Jira, which EIP used to flag and report social media posts to Twitter, Facebook, and other platforms. And CISA included a threatening disclaimer in its email. It stated that "information may also be shared with law enforcement or intelligence agencies."

CISA was not supposed to have involvement in EIP's flagging activities, but, notes the House Judiciary, numerous Jira tickets mention CISA, and CISA referenced EIP Jira codes when switchboarding. Stanford's legal counsel insisted that EIP and SIO "did not provide any government agency… access to the Jira database," but in one November 2020 email, SIO Director Alex Stamos told a Reddit employee, "It would be great if we could get somebody from Reddit on JIRA, just like Facebook,

Google, Twitter, TikTok, Instagram, CISA, EI-ISAC…" Stamos's statement indicated that CISA had access to EIP's Jira system.

In communications with social media platforms, the House report states, Stamos made it clear "that the EIP's true purpose was to act as a censorship conduit for the federal government." In an email to Nextdoor, Stamos wrote that EIP would "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."

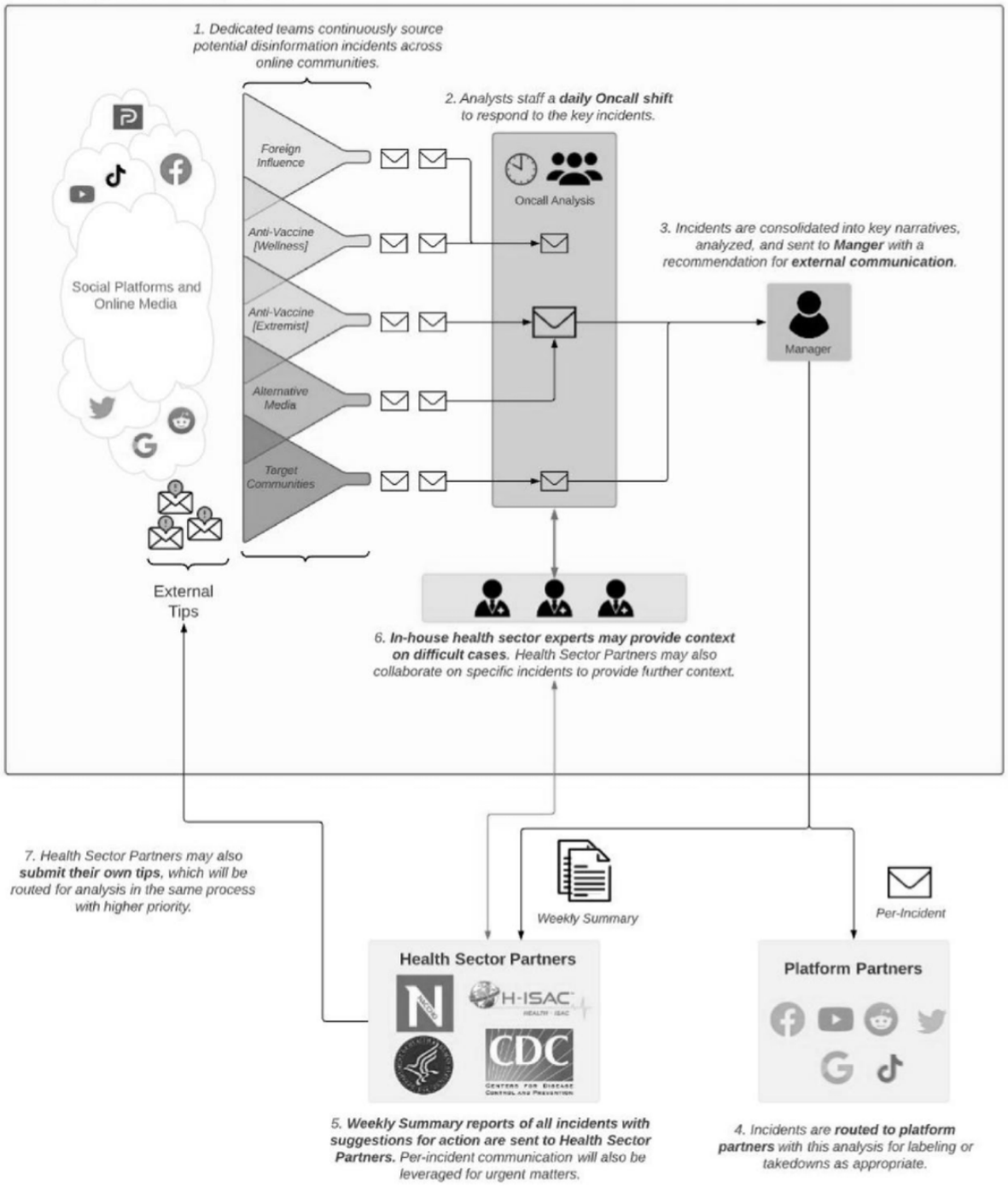
Anyone who doubts that the DHS-authorized organizations, SIO chief among them, need only look at the "Internal Workflow" graphic in a VP proposal obtained earlier this week through a FOIA request by Taibbi. It shows how disinformation "Incidents are routed to platform partners... for... takedowns."

Exhibit: Internal Workflow (Link)

Core Virality Project Partners

FIRST DRAFT · Stanford Internet Observatory Cyber Policy Center · CENTER FOR AN INFORMED PUBLIC UNIVERSITY of WASHINGTON · CSMaP

Virality Project Internal Organization



"Psychological and influence operations have long been used to secure military objectives," noted my colleague Alex Gutentag last week. "We now have clear evidence that, with the creation of CTIL and its partnership with CISA, [the censorship leaders] pioneered the use of psychological strategies to combat populism at home by censoring information and narratives associated with populist discontent."

Today, the Defense Department and its contractors openly discuss the importance of "cognitive warfare," not just "security," aimed at the American people.

While I believe all of the above is transparently unconstitutional, there is the possibility that The Supreme Court will not rule against it after it hears the Missouri v Biden censorship lawsuit next year. Some justices may conclude that somehow the First Amendment does not cover the Internet, or that governments outsourcing censorship to third-party "cut-outs" or front groups is justified even though the Supreme Court has called it "axiomatic" that the government cannot facilitate private parties violating the Constitution on its behalf. Still other justices may claim that the First Amendment requires a very high bar for government coercion of private actors, even though the First Amendment prohibits government limitations on freedom of speech broadly, not just through coercion

As such, the importance of this DHS oversight committee in protecting our freedom of speech is essential.

Setting aside the clear and present threat that DHS poses to our first and most fundamental freedom, there is another problem related to DHS's censorship activities, and that's the ways in which it distracts from and thus undermines our nation's cybersecurity.

As this committee knows well, the Internet is more essential than any other piece of America's infrastructure because every major aspect of civilization depends upon it, including our electrical grids, our transportation networks, and our policing and security systems. If cyber-attacks take down or undermine the Internet, the consequences could be catastrophic.

Given that, does this committee believe it makes sense for the head of the DHS's so-called "Cybersecurity and Information Security Agency," CISA, to be involved in policing what people say, hear, and think?

Set aside for a moment the Orwellian aspects of CISA's efforts at mind control. What do we think the consequences could be of CISA taking its eye off the cybersecurity ball so that it can crusade with Stanford interns against wrongthink? Should we be able to sleep soundly at night knowing that CISA is focused on the problem of people being wrong on the Internet rather than on China, Russia, Iran, and other malicious actors seeking to harm American businesses, government agencies, and our citizens?

Over the last 100 years, the Supreme Court created a tiny number of exceptions to the radical commitment to freedom of speech enshrined in our constitution. Nobody questions the need for governments to fight fraud, child exploitation, and the *immediate* incitement of violence.

What's at stake here is our fundamental freedom to express our views on controversial social and political issues without fear of government censorship. CISA drifted so far from its mission that it slid down the slipperiest slope in American political life.

I believe this dramatic situation requires the abolition of CISA. If it is doing good cybersecurity work, then it should be placed under the supervision of different leadership at a different agency free from the awful and unlawful behaviors of the last three years.

However, I am also a realist and recognize that guardrails may be all that can be imposed. If that is the direction in which this committee chooses to go, then I would encourage very bright lines between cyber security and "cognitive security." While censorship advocates have tried to blur that line, it is, in reality, quite clear to everyone what constitutes security and what constitutes censorship.

Nonetheless, something must be done to make clear, in DHS-CISA's mandate, that the agency recognizes the distinction and will never again transgress its mandate in violation of our Constitution.

The turning against the American people of counterterrorism tactics once reserved for foreign enemies should terrify all of us and inspire a clear statement that never again shall our military, intelligence, and law enforcement guardians engage in such a recklessly ideological and partisan "warfare" against civilians.