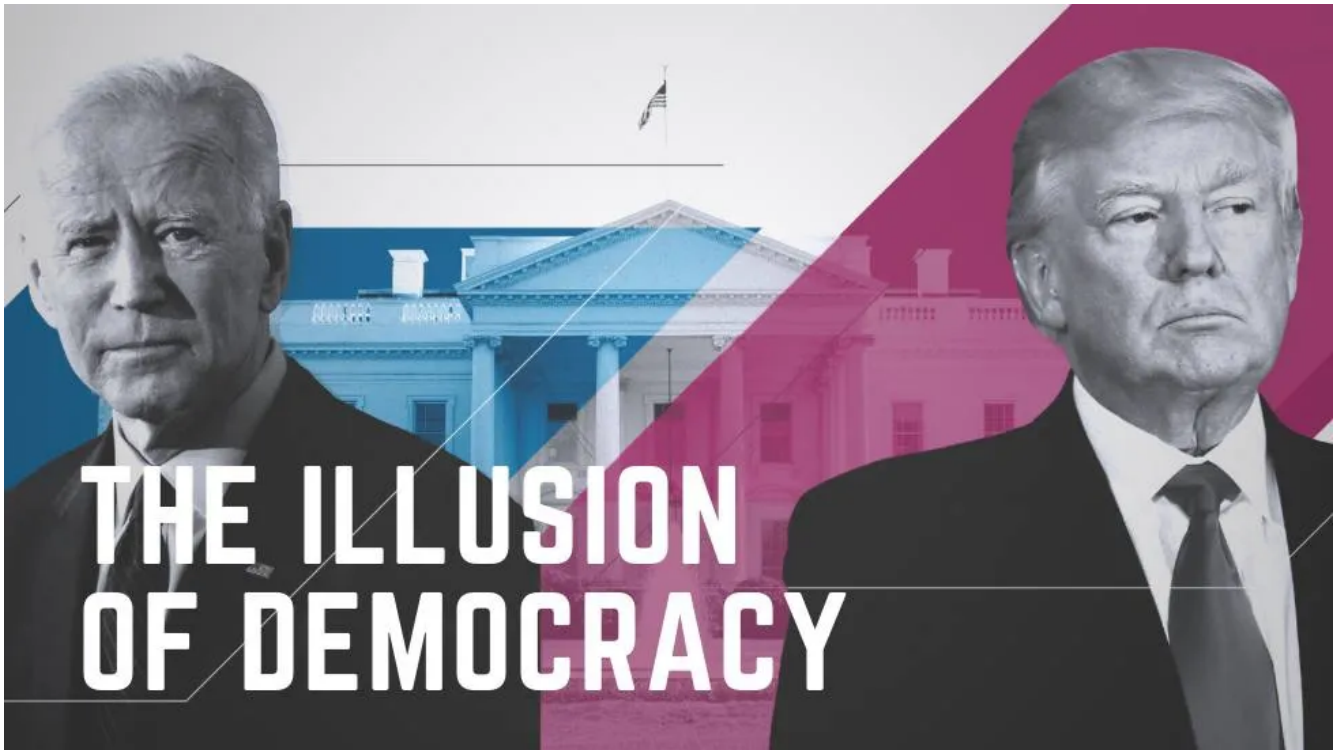
The Illusion of Democracy

How Our Country Was Hijacked By Our Election System

JON HEROLD
DEC 14, 2023



There has recently been a rash of revelations providing us more context to the politically biased censorship activities related to the 2020 election. Much of the recent exposure has come from the efforts put forth by Michael Shellenberger and his team over atPublicin what they are calling the "CTIL files:"

> A whistleblower has come forward with an explosive new trove of documents, rivaling or exceeding the Twitter Files and Facebook Files in scale and importance. They describe the activities of an "anti-disinformation" group called the Cyber Threat Intelligence League, or CTIL, that officially began as the volunteer project of data scientists and defense and intelligence veterans but whose tactics over time appear to have been absorbed into multiple official projects, including those of the Department of Homeland Security (DHS).
>
> The CTI League documents offer the missing link answers to key questions not addressed in the Twitter Files and Facebook Files. Combined, they offer a comprehensive picture of the birth of the "anti-disinformation" sector, or what we have called the Censorship Industrial Complex.

Reading through the CTIL files revealed just how much Donald Trump's victory in 2016 disrupted the status quo of the entrenched bureaucracy within the administrative state, as well as how desperate they were to remove him from the equation. The censorship campaign was just one part of what appears to be a much larger, but coordinated effort to prevent another Trump victory, and the genesis of this effort came from the Obama White House just before Trump's inauguration.

> The whistleblower alleges that a leader of CTI League, a "former" British intelligence analyst, was "in the room" at the Obama White House in 2017 when she received the instructions to create a counter-disinformation project to stop a "repeat of 2016."

On January 6th, 2017, Obama's Secretary of Homeland Security, Jeh Johnson, released a statement designating "Election Infrastructure" as a "critical infrastructure." In their September of 2020 Election Infrastructure Security Resource Guide, the Cybersecurity and Infrastructure Security Agency (CISA) explained what that designation enabled:

In January 2017, DHS designated election systems as critical infrastructure. This designation is given to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[1]

The critical infrastructure designation enables DHS to prioritize cybersecurity and physical security assistance to election officials upon request. The designation emphasizes, both domestically and internationally, that election infrastructure possesses all the benefits and protections that the Nation has to offer. It enabled DHS to lead the formation of an Election Infrastructure Subsector Government Coordinating Council (EIS GCC) and the private sector's Election Infrastructure Subsector Sector Coordinating Council (EISCC) to serve as collaborative forums where the Federal Government, state and local government officials, and the private sector can establish mutually recognized information sharing to prevent or mitigate the effects of incidents that undermine the integrity of or public confidence in the election system.

The critical infrastructure designation led to the creation of the EIS GCC and EISCC. They state it was for the purpose of "information sharing" but it's really much more sinister than that. These are the entities who told us "the November 3rd election was the most secure in American history."

Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees

Released: November 12, 2020

Revised: November 12, 2020

RELATED TOPICS: ELECTION SECURITY

WASHINGTON – The members of Election Infrastructure Government Coordinating Council (GCC) Executive Committee – Cybersecurity and Infrastructure Security Agency (CISA) Assistant Director Bob Kolasky, U.S. Election Assistance Commission Chair Benjamin Hovland, National Association of Secretaries of State (NASS) President Maggie Toulouse Oliver, National Association of State Election Directors (NASED) President Lori Augino, and Escambia County (Florida) Supervisor of Elections David Stafford – and the members of the Election Infrastructure Sector Coordinating Council (SCC) – Chair Brian Hancock (Unisyn Voting Solutions), Vice Chair Sam Derheimer (Hart InterCivic), Chris Wlaschin (Election Systems & Software), Ericka Haas (Electronic Registration Information Center), and Maria Bianchi (Democracy Works) - released the following statement:

"The November 3rd election was the most secure in American history. Right now, across the country, election officials are reviewing and double checking the entire election process prior to finalizing the result.

If you questioned the statement above, it was these entities who assisted in shutting you down.

Understanding these two entities is crucial because as I said, something more sinister is happening with their roles in our election infrastructure, beyond the censorship.

I have already covered the EISCC in detail in a previous article, so I won't elaborate much on them here. It is made up of the private sector companies actually administering our election, companies like Dominion and Smartmatic. They are tasked with advising on how our elections should be administered. Here is a brief summary on the EISCC:

> Dominion Voting Systems and Smartmatic were two of the members of the EISCC which "advises and assists" our government with election security by "coordinating with the DHS to develop, recommend, and review sector-wide plans, procedures, and

> effective practices in support of infrastructure protection, including training, education, and implementation". They were also making "recommendations to appropriate authorities to mitigate impediments to effective critical infrastructure security".
>
> The EISCC operates under the framework of CIPAC and is exempt from Public Law 92-463 (exempt from oversight), they are classified as "Special Government Employees" and they have been certified that their "services outweighs the potential for a conflict of interest created by the financial interest involved."
>
> This means our government knows there is a "potential for a conflict of interest created by the financial interest involved" for members of the EISCC because the "official responsible for the employee's appointment" has to certify it. They know there is a conflict of interest for members of the EISCC yet they allow it to operate without oversight.

The EIS GCC is made up of government agencies and entities and they are tasked with implementing the election security recommendations put forth by the EI-SCC (the companies administering our elections like Dominion and Smartmatic).

Election Infrastructure Subsector
Government Coordinating Council
Charter

Article I – Official Designation

The official designation of this Council is the "Election Infrastructure Subsector Government Coordinating Council," hereinafter referred to as the "EIS GCC" or the "Council."

Article II – Mission and Purpose

The Council enables state, local, and federal governments to share information and collaborate on best practices to mitigate and counter threats[1] to election infrastructure.

Specifically, the EIS GCC provides for interagency, intergovernmental, and cross-jurisdictional coordination within the Election Infrastructure Subsector and between this subsector and other sectors identified in Presidential Policy Directive/PPD-21 on "Critical Infrastructure Security and Resilience." The EIS GCC is composed of representatives from across various levels of government as appropriate to depict the operating landscape of the Election Infrastructure Subsector.

In order to implement that election security, the EIS-GCC partnered with an outside organization called the Center for Internet Security (CIS).

> Founded in 2000, the Center for Internet Security is a nonprofit group specializing in cyber-security research which provides cyber-security consulting services to local, state, and federal governments. The organization has been awarded $115 million in federal grants by the Department of Homeland Security (DHS) and the Department of Defense (DoD) since 2010 and has received $3.6 million in cybersecurity contracts from numerous federal agencies since 2005. [4]

The Center for Internet Security shares an address with the Global Cyber Alliance, which is comprised of federal government officials Cybersecurity and Infrastructure Security Agency and left-of-center groups such as the Center for Tech and Civic Life, Brennan Center for Justice, Facebook, and the Center for Election Innovation and Research. [7] [8]

> Since 2016, the Center for Internet Security has been active in researching and providing cyber security for election administration through its Elections Infrastructure Information Sharing and Analysis Center (EI-SAC). In April 2019, the organization published "A Guide for Ensuring Security in Election Technology Procurements," which was funded by a $290,000 grant from Pierre Omidyar's Democracy Fund. [9]

The EIS-GCC and CIS would establish the Elections Infrastructure Information Sharing and Analysis Center" (EI-ISAC). The entire purpose of the EI-ISAC was to promote the cybersecurity of our elections.

> Since 2016, the Center for Internet Security has been active in researching and providing cyber security for election administration through its Elections Infrastructure Information Sharing and Analysis Center (EI-SAC). In April 2019, the organization published "A Guide for Ensuring Security in Election Technology Procurements," which was funded by a $290,000 grant from Pierre Omidyar's Democracy Fund. [9]

Both CIS and the EI-ISAC were mentioned by the CITL files:

> 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.

There were two roles that CIS played when it came to "election security." One of those roles was with the censorship. We will get to the other role they played shortly but before we do, it's important to understand just how big their role was with the censorship, and just how biased it was.

One of the sources for the CITL files is a November 6th, 2023 report from the House of Representatives Select Subcommittee on the Weaponization of Government titled **"THE WEAPONIZATION OF "DISINFORMATION" PSEUDO-EXPERTS AND BUREAUCRATS: HOW THE FEDERAL GOVERNMENT PARTNERED WITH UNIVERSITIES TO CENSOR AMERICANS' POLITICAL SPEECH."**

This report provides excruciating detail of CIS' role in the "censorship industrial complex." It was through its EI-ISAC that they actually served as "the singular conduit for election officials to report" what they deemed as election misinformation:

2. EI-ISAC

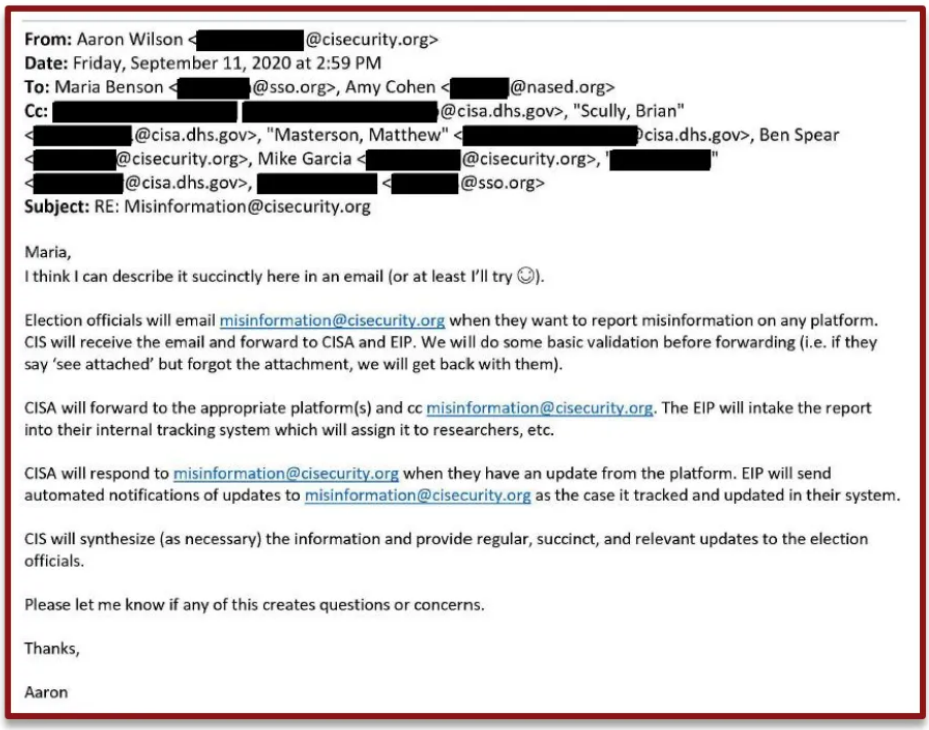
The Center for Internet Security (CIS) is a non-profit organization based in New York, which was established "in partnership with the U.S. Cybersecurity and Infrastructure Security Agency (CISA)."[48] CIS operates the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), which is 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]

CIS worked directly with social media companies in getting content removed from platforms.

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]

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 the 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]@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

They also worked to take down posts on behalf of Democrat candidates, including posts sent to them directly by Katie Hobbs.

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]

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]

CIS targeted “former, current, and prospective” Republican legislators as well as many other accounts who were considered conservative and pro-Trump at the time.

> 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.

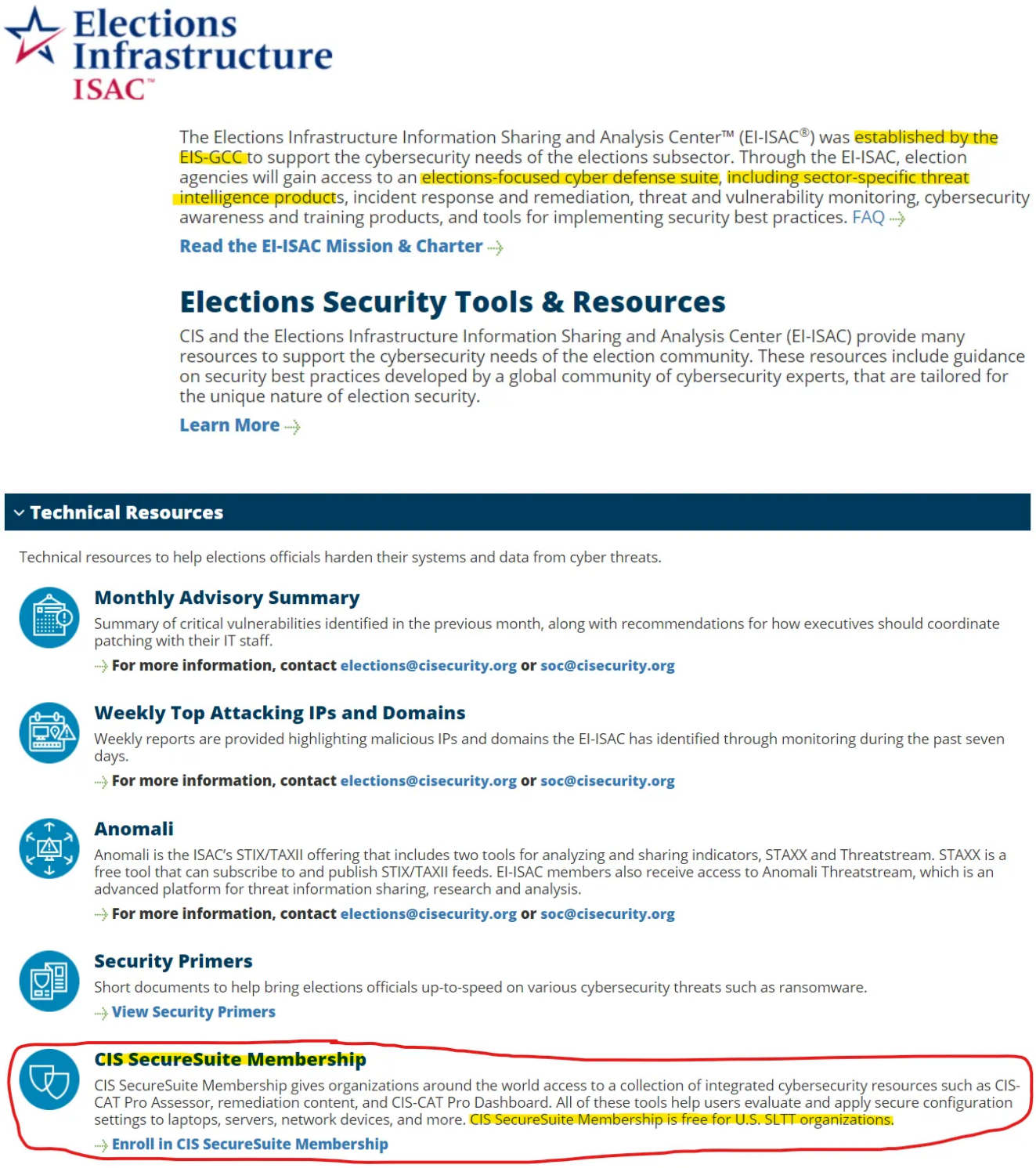
The highly partisan nature of the censorship went as far as targeting Donald Trump himself.

> **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.

Understanding the active role in censorship by CIS and the EI-ISAC, which was clearly biased against President Trump, is important context because as mentioned earlier, censoring conservatives was not the only role that CIS played in the 2020 election. The second role they played is far more disturbing.

The Center for Internet Security also provided cybersecurity for our election infrastructure.

CIS created an “elections-focused cyber defense suite,” and then give it away for free to anybody who becomes a member of the EI-ISAC. :



This free membership, entailing an "elections-focused cyber defense suite" allowed for a mass rollout across the United States. The access given to CIS in order to "defend the nation's election systems from cyberthreats" is pervasive and concerning.

Federal program offers new cybersecurity tool for elections

By Christina A. Cassidy | AP
August 4, 2020 at 10:21 p.m. EDT

ATLANTA — State and local officials are receiving additional tools from the federal government to help defend the nation's election systems from cyberthreats ahead of the November vote, as intelligence officials continue to warn about foreign efforts to interfere in the U.S. election.

Under a $2.2 million pilot program that began in March, the Department of Homeland Security's cybersecurity agency in partnership with the Center for Internet Security has been deploying software to election offices. It is then placed on devices, including laptops and servers used for voter registration and reporting vote totals, to detect malicious activity. The program was highlighted during a congressional hearing Tuesday.

"This is the next step, the evolution of helping state and local entities," said Matt Masterson, a top cybersecurity official within the Department of Homeland Security. "This really advances their ability to protect their networks."

Thirty state election offices have already integrated the so-called endpoint detection and response tools, which are routinely used in the private sector but less common at the local level. Through the federal program, officials expect to have this deployed in at least nine additional states by November. Fewer than 100 local government agencies have signed up so far.

> Endpoint detection is a key component of network defense designed to detect intrusions early. The software identifies known threats as well as suspicious behavior that could indicate an attack.
>
> "The threat actors are creating over a million new strings of malware a day," said Michael Atkinson with FireEye, a leading cybersecurity firm that provides such software. "If you don't have the capacity to search in your endpoint infrastructure for the bad guys and have human cybersecurity experts work on that for you, in the end, compromise will likely be inevitable."
>
> Under the program, CIS analysts would receive alerts of suspicious activity, allowing them to monitor and track suspicious activity across jurisdictions with the goal of early detection and mitigation. Officials said the effort was just the latest in steps taken to shore up cybersecurity since the 2016 presidential election.

The Center for Internet Security was rolling out EDR software to be installed on laptops and servers at election offices, with the stated aim of "detecting malicious activity." What's worse is that the Center for Internet Security wasn't actually using its own software for this endpoint detection. Instead, they contracted out a third party and used tools provided by that third party to identify and respond to malicious activity surrounding our election infrastructure.

[That third party is Crowdstrike.]

CIS partners with CrowdStrike on cybersecurity platform protecting local governments

The new CIS Endpoint Security Services (ESS) platform is built for US State, Local, Tribal and Territorial (SLTT) governments.

CIS has been working for years to democratize cybersecurity protection through a variety of programs that provide free or low-cost tools to hospitals, schools and more.

The new CIS Endpoint Security Services (ESS) platform, which is backed by Crowdstrike's tools, is built to identify, detect and respond to security alerts from local governments.

Through CrowdStrike's Falcon system, the company will offer ESS users deployments onto endpoint devices. The platform provides antivirus solutions, endpoint detection and response, asset and software inventory, USB device monitoring, user account monitoring and host-based firewall management.

CIS has previously worked with CrowdStrike on their Elections Infrastructure Information Sharing and Analysis Center project. The latest partnership will see them provide "a new, fully managed 24/7/365 next-generation cybersecurity offering exclusively tailored to SLTT organizations, including more than 12,000 Multi-State Information and Analysis Center members across the US, with more than 14 million endpoints in total."

To further prove this, here is a contract proving Crowdstrike was providing EDR services for the 2020 election. If you would like more detail on this topic, read this article of mine from 2021.

MEMORANDUM OF AGREEMENT
BETWEEN THE CENTER FOR INTERNET SECURITY
AND
LANCASTER COUNTY, NEBRASKA FOR
Endpoint Detection & Response (EDR) Services
(Federally Funded Services)

This MEMORANDUM OF AGREEMENT ("Agreement") by and between the Center for Internet Security, Inc. ("CIS"), operating in its capacity as the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), located at 31 Tech Valley Drive, East Greenbush, NY 12061-4134, and Lancaster County, Nebraska (Entity) with its principal place of business at: 555 S. 10th St., Lincoln, Nebraska 68508, for EDR Services, as defined herein below (CIS and Entity collectively referred to as the "Parties").

- In its role as the MS-ISAC and the EI-ISAC, CIS has been recognized by the United States Department of Homeland Security (DHS) as a key Cyber Security resource for all fifty states, local governments, United States territories, and tribal nations (SLTT) and state and local elections entities; and

- CIS operates a twenty-four hours a day, seven days per week (24/7) Security Operations Center (SOC); and

- CIS has entered into an agreement with the federal government to provide EDR Services to certain SLTT entities.

Title

The EDR Services include use of software that is licensed to CIS by a third party provider, Crowdstrike, Inc. ("Crowdstrike"). All title and ownership rights of the software shall remain with Crowdstrike.

The Customer shall own all right, title and interest in its data that is provided to CIS pursuant to this Agreement. Customer hereby grants CIS a non-exclusive, non-transferable license to access and use such data to the extent necessary to provide EDR Services under this Agreement.

III. **Third Party Provider Terms and Conditions**

Entity acknowledges and agrees that as part of providing EDR Services, CIS has contracted with the third party provider, CrowdStrike. Entity further acknowledges and agrees that in return for receipt of EDR Services, it agrees to the following terms and conditions as an end user of CrowdStrike services under this Agreement:

A. Access & Use Rights. Subject to the terms and conditions of this Agreement, Entity has a non-exclusive, non-transferable, non-sublicensable license to access and use the Products in accordance with any applicable Documentation solely for Entity's Internal Use. The Product includes a downloadable object-code component ("Software Component"); Entity may install and run multiple copies of the Software Components solely for Entity's Internal Use. Entity's access and use is limited to the quantity and the period of time specified in this Agreement.

The foregoing has been agreed to and accepted by the authorized representatives of each party whose signatures appear below:

CENTER FOR INTERNET SECURITY, INC.

By: DocuSigned by: Deirdre O'Callaghan 95362285528E44E...

Name: Deirdre O'Callaghan

Title: Secretary and Chief Counsel

Date: 8/21/2020

LANCASTER COUNTY, NEBRASKA

By: _____

Name: Sean Flowerday

Title: Chair Lancaster County Board of County Commissioners

Date: _____

This will likely not be new to anybody but Crowdstrike has close ties to the democrat party and has been involved in [questionable cyber-related analysis in the past:]

CrowdStrike, the private cyber-security firm that first accused Russia of hacking Democratic Party emails and served as a critical source for U.S. intelligence officials in the years-long Trump-Russia probe, acknowledged to Congress more than two years ago that it had no concrete evidence that Russian hackers stole emails from the Democratic National Committee's server.

The disclosure that CrowdStrike found no evidence that alleged Russian hackers exfiltrated any data from the DNC server raises a critical question: On what basis, then, did it accuse them of stealing the emails? Further, on what basis did Obama administration officials make far more forceful claims about Russian hacking?

Michael Sussmann: This lawyer at Perkins Coie hired CrowdStrike to investigate the DNC breach. He was also involved with Fusion GPS and Christopher Steele in producing the discredited Steele dossier.
perkinscoie.com

The January 2017 Intelligence Community Assessment (ICA), which formally accused Russia of a sweeping influence campaign involving the theft of Democratic emails, claimed the Russian intelligence service "exfiltrated large volumes of data from the DNC." A July 2018 indictment claimed that GRU officers "stole thousands of emails from the work accounts of DNC employees."

According to everyone concerned, the cyber-firm played a critical role in the FBI's investigation of the DNC data theft. Henry told the panel that CrowdStrike "shared intelligence with the FBI" on a regular basis, making "contact with them over a hundred times in the course of many months." In congressional testimony that same year, former FBI Director James Comey acknowledged that the FBI "never got direct access to the machines themselves," and instead relied on CrowdStrike, which "shared with us their forensics from their review of the system." According to Comey, the FBI would have preferred direct access to the server, and made "multiple requests at different levels," to obtain it. But after being rebuffed, "ultimately it was agreed to... [CrowdStrike] would share with us what they saw."

The firm's work with the DNC and FBI is also colored by partisan affiliations. Before joining CrowdStrike, Henry served as executive assistant director at the FBI under Mueller. Co-founder Dmitri Alperovitch is a vocal critic of Vladimir Putin and a senior fellow at the Atlantic Council, the pro-NATO think tank that has consistently promoted an aggressive policy toward Russia. And the newly released testimony confirms that CrowdStrike was hired to investigate the DNC breach by Michael Sussmann of Perkins Coie – the same Democratic-tied law firm that hired Fusion GPS to produce the discredited Steele dossier, which was also treated as central evidence in the investigation. Sussmann played a critical role in generating the Trump-Russia collusion allegation. Ex-British spy and dossier compiler Christopher Steele has testified in British court that Sussmann shared with him the now-debunked Alfa Bank server theory, alleging a clandestine communication channel between the bank and the Trump Organization.

Henry's recently released testimony does not mean that Russia did not hack the DNC. What it does make clear is that Obama administration officials, the DNC and others have misled the public by presenting as fact information that they knew was uncertain. The fact that the Democratic Party employed the two private firms that generated the core allegations at the heart of Russiagate -- Russian email hacking and Trump-Russia collusion – suggests that the federal investigation was compromised from the start.

Crowdstrike performing any role in the cybersecurity efforts of our elections is something any objective person should consider to be inappropriate or at the very least a cause for concern.

Keep in mind who actually brought them into the picture.

The Center for Internet Security already proved too biased against Trump with how they dictated the flow of information in the public sphere by censoring conservative voices questioning the legitimacy of the 2020 election.

Is it possible they were dictating the flow of information privately too?

Executive Order 13848 required the intelligence community (IC) to assess whether there was interference in the election or not. This assessment told us that there is "no evidence" of shenanigans surrounding the 2020 election:

We—the Department of Justice, including the FBI, and Department of Homeland Security, including CISA—have no evidence that any foreign government-affiliated actor prevented voting, changed votes, or disrupted the ability to tally votes or to transmit election results in a timely manner; altered any technical aspect of the voting process; or otherwise compromised the integrity of voter registration information of any ballots cast during 2020 federal elections.

This conclusion by the intelligence community has not only been repeated ad nauseum by the media, but it has also been mentioned multiple times throughout Trump's J6 case. Donald Trump questioning the legitimacy of the 2020 election is what has ultimately led to the political persecution he has faced since 2021.

The question I'm not seeing asked is what specific sources was the IC using to state there was no evidence of a compromised election?

This is what the ICA claimed was their "source of information:"

Sources of Information

Foreign government activities were included regardless of whether the IC has assessed that they were undertaken with the purpose of interfering in a 2020 federal election. Foreign governments may target election or political and campaign infrastructure for a variety of reasons, including intelligence collection, and the purpose of any activity may not always be apparent. The impact to covered infrastructure was evaluated by considering, among other information, FBI forensic analyses; CISA cyber incident response activities, risk analysis, and stakeholder information; IC reporting; and open-source reporting.

We know CIS and Crowdstrike were the ones monitoring the election systems. We know both Crowdstrike and CIS have a proven history of bias against one of the candidates on the ballot of the election they were tasked with securing from cyber threats in 2020.

Was the actual source for the conclusions found in the ICA Crowdstrike and/or the Center for Internet Security?

Maybe it's just a coincidence that the conclusion found in the ICA was the exact conclusion CIS was censoring people for questioning.

We can even further prove the biased nature of the Center for Internet Security.

Check out this bio:

[redacted] He was a member of the [redacted] Commission (formed to advise the 44th President) and as an advisor to the Office of the Secretary of Defense on [redacted] Mr. [redacted] served on the Obama-Biden Transition Team

Do you believe this individual could be unbiased?

Would you want him to be involved in any aspect of the 2020 election between Joe Biden and Donald Trump, having served on the Obama-Biden Transition Team?

His name is John Gilligan, and he has been the President and CEO of the Center of Internet Security since 2018:

John M. Gilligan

President and Chief Executive Officer

John Gilligan became the President and Chief Executive Officer of the Center for Internet Security (CIS) in October of 2018. He served on the CIS Board of Directors from 2005–2018 and was chairman of the board from 2009–2018.

John M. Gilligan is president of the Gilligan Group, Inc., an IT consulting firm. Prior to his current position he was a senior vice president and director, Defense Sector, at SRA International, Inc. Mr. Gilligan has served as the CIO for the U.S. Air Force and the U.S. Department of Energy, and was program executive officer for battle management and command and control for the Air Force. He was a member of the Cyber Security Commission (formed to advise the 44th President) and as an advisor to the Office of the Secretary of Defense on IT reform. Mr. Gilligan served on the Obama-Biden Transition Team focusing on IT within the DoD and Intelligence Communities. He currently serves as chairman of the board of directors for the Center for Internet Security, Cyber Griffin Inc., and HDT Global, Inc.

The man in charge of the Center for Internet Security, the non-profit which is responsible for the cybersecurity of our nations elections (including the 2020 election between Trump and Biden), has direct ties to Obama and Biden.

Remember that right before leaving office, Obama's DHS designated our election infrastructure as critical infrastructure, a designation which directly led to the Center of Internet Security's involvement in "cyber security" for our elections.

Remember it was at Obama's White House in 2017 that instructions were received to "create a counter-disinformation project to stop a "repeat of 2016.""

Under the guise of "free election cyber-security," the Center for Internet Security has been placed in the position of being the most powerful non-profit in the world. With the level of access they have to our election infrastructure, they could **theoretically** dictate the outcome of every election they come in contact with. I'm not making accusations here, but with a topic as important and divisive as this one, these questions must be asked.

Look at the bigger picture that appears to be forming here.

The administrative state Trump was up against, was tasked by Obama to "prevent a repeat of 2016." They had direct access to our election infrastructure through CIS and then controlled the flow of information using coordination between multiple agencies and the media, big tech, and social media companies that defend them.

The CTIL files revealed what essentially was a narrative clean-up crew, and they were only cleaning up after one political party.

It's nearly impossible for anybody in the public domain to know with any certainty whether or not there were cyber threats to the 2020 election, because none of that information is public.

Instead, we are forced to rely on our intelligence agencies and those who actually monitored our election infrastructure for answers on whether the 2020 election was "the most secure election in American history."

We can't trust that conclusion if it comes from Crowdstrike or the Center for Internet Security.

If there were bad actors attempting to switch votes from Trump to Biden, can you trust that Crowdstrike or CIS would attempt to stop it?

If Crowdstrike and/or CIS software was downloaded onto our election infrastructure, can you trust that they didn't switch votes themselves? Who would be able to stop them

and who would ever find out if they are the ones in charge of detecting and preventing malicious cyber activity?

Technology is supposed to make life easier, but when it comes to our elections, it has done the opposite. Our current system forces us to “trust the experts” and pray they will be honest and unbiased. We aren’t even allowed to question them.

What a terrifying thought.

The only way I see us out of this stranglehold created by the administrative state is through complete transparency.

Voting is the most important and impactful thing that a legal American citizen can do. It must therefore be the most transparent process imaginable. Everything should be on paper. Everything should be recorded on camera. Everything should be verifiable by anybody interested in doing the work to verify it.

Nothing should rely on experts.

Until we get to a system that doesn’t rely on experts, we don’t have a democracy.

We have the illusion of one.

Jon Herold

Twitter: https://twitter.com/patel_patriot

Truth Social: @patelpatriot

Telegram: https://t.me/patelpatriot

Support my work by subscribing here for just $10 per month:

Type your email... Subscribe

258 Likes · 27 Restacks

5 Comments

Write a comment...

Jaytriot Dec 15, 2023

Excellent work, Jon! We knew they were censoring political speech, but we didn't understand the nuts and bolts of HOW they were directing it. Not only did you lay that out, but you found that the same group tasked with censoring conservative political speech was also responsible for monitoring our election infrastructure for "interference"! Amazing connection you discovered....the wolves were guarding the henhouse!

LIKE (28) REPLY SHARE

Cheryl Dec 14, 2023

Yes, praying for God's rescue 🙏

LIKE (17) REPLY SHARE

3 more comments...