ail Watch - November 2, 2020	Amtrak Intelligence Team
riminal and Terrorism Intelligence Report - November , 2020	The Army Threat Integration Center (ARTIC)
uthorities Attribute Islamist Terrorist Motive to hooting Attack at the City Center of Vienna Austria	Railway Alert Network (RAN)
riminal and Terrorism Intelligence Report - November , 2020	The Army Threat Integration Center (ARTIC)

OTHER DOCUMENTS	
Current Situation Reports	Daily Reports
BATS	PT/ST-ISAC Cyber Report
Counterterrorism Daily - NCTC	Joint Counterterrorism Assessment Team (JCAT)
IT-ISAC Open Source News	IED News
Emerging Diseases	FEMA Disaster Emergency Communications Division Newsletter
NH-ISAC Daily Security Intelligence Report	Training & Conference Calendar

For HSIN password resets, click here. For further assistance with your HSIN account, contact the HSIN 24/7 Help Desk at 866-430-0162. For other difficulties opening FOUO documents (e.g., not nominated and validated), contact the EMR-ISAC at emr-isac@fema.dhs.gov or at 301-447-1325.

Update your subscriptions, modify your password or e-mail address, or stop subscriptions at any time on your Subscriber Preferences Page. You will need to use your e-mail address to log in. If you have questions or problems with the subscription service, please contact subscriberhelp.govdelivery.com.

Privacy Policy | GovDelivery is providing this information on behalf of U.S. Department of Homeland Security, and may not use the information for any other purposes.

This email was sent to (b) (6) using GovDelivery Communications Cloud on behalf of: U.S. Fire Administration · U.S. Department of Homeland Security · Emmitsburg, MD 21727 · (301) 447-1325

GovDelivery logo

Sender:	emr-isac <emr-isac@service.govdelivery.com>
Recipient:	(b) (6)

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH FOIA

Sent Date:	2020/12/03 13:32:14
Delivered Date:	2020/12/03 13:34:03
Message Flags:	Unread

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

US ELECTION SECURITY UPDATE
COGEL CONFERENCE

Matt Masterson
Senior Cybersecurity Advisor,
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

OBTAINED BY JUDICIAL WATCH FIRST LEGAL FOUNDATION THROUGH LITIGATION

DHS-1255-003041 04/25/2024

Growth of CISA's Election Security Mission

2016 — Reactive Response to Incidents in the 2016 Election

- Triggered by cyber incidents in two states and a breach of a political organization.
- DHS tried to rapidly engage the election stakeholder community.
- Unsure of the best lines of communication and reached out to state CIOs instead of election officials.

2017 — Recovering from a Deficit of Trust

- Critical Infrastructure designation issued on January 6, 2017.
- Notified 21 states that they had been scanned by an adversary.
- Stood up the Election Task Force, began meeting with state election officials, established the Government Coordinating Council (GCC).

2018 — Proactively building trust and elevating security

- Funded the creation of the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).
- Provided classified and unclassified threat briefings.
- Hosted Tabletop the Vote 2018.

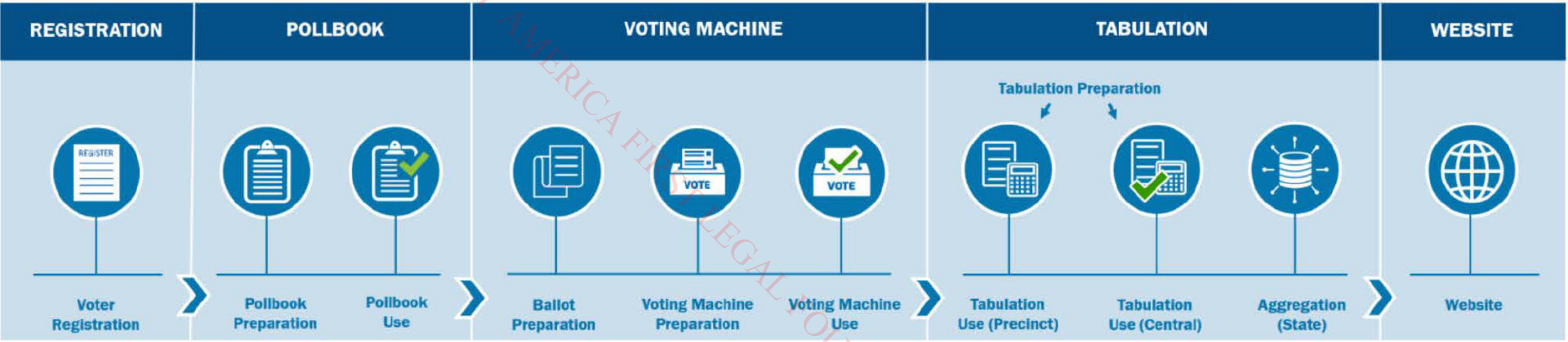
2019-2020 — Partnering for more secure elections

- Increased engagement at local level via Last Mile initiative.
- #Protect2020 Strategic Plan with four Lines of Effort (LOE) ahead of the 2020 Election Cycle.

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATIO

DHS-1255-003042 04/25/2024

Election Infrastructure and Processes



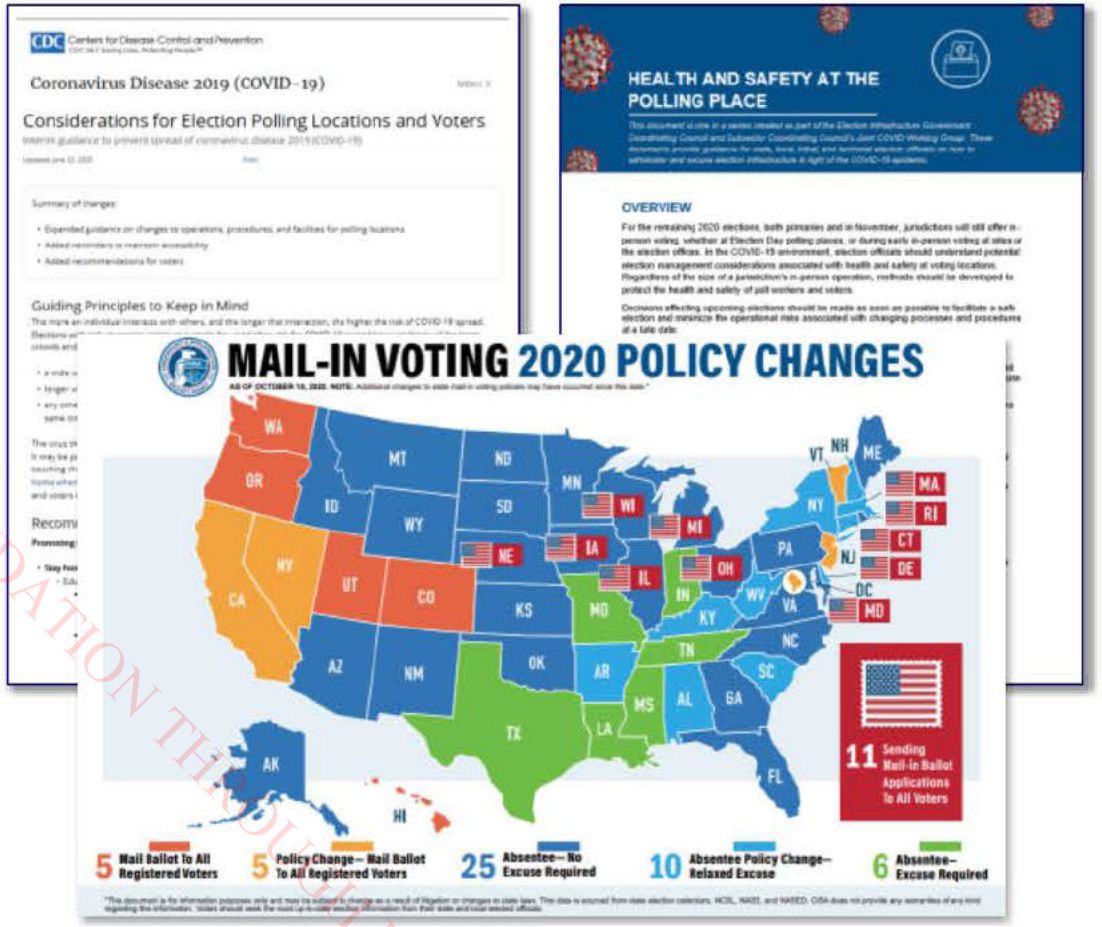
- Attack Surface for Election Infrastructure is broad and diverse and is characterized by:Systems managed by county/sub-county jurisdictions with less cybersecurity expertiseInvolvement by voting system manufacturers, ballot printers, database/website hosting services, etc.Expanded use of mail-in voting shifts some risk to outside entities like ballot printers, mail processing facilities, and U.S. Postal Service

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATIO

DHS-1255-003043 04/25/2024

Impact of COVID-19 Pandemic

- Response measures and policy/procedural changes varied widely by stateMail-in voting: many states expanded voting options and/or relaxed requirements, driven in part by voter demandIn-person: all states implemented COVID-19 mitigation measures, some expanded early voting, some localities consolidated voting sites, poll worker recruitment incentivesChanges tested during primariesOverall, election officials were well prepared to handle the challenges of COVID-19 before, on, and after Election Day

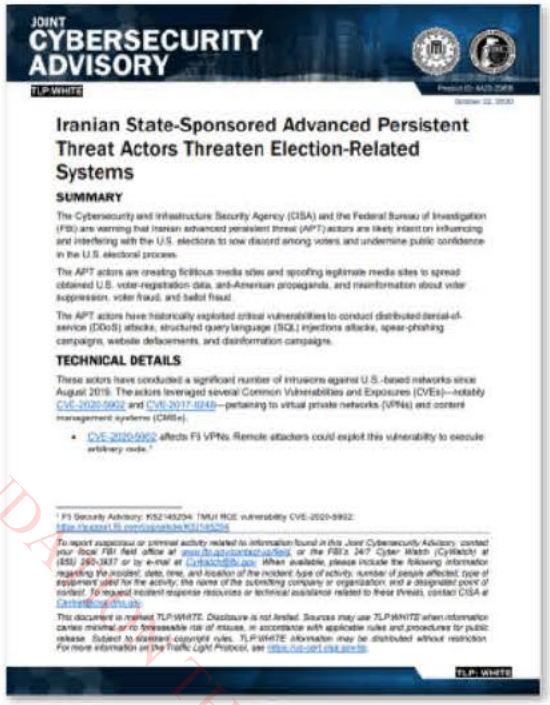


DBT ARCHIVED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATIO

DHS-1255-003044 04/25/2024

CISA Activities up to and on Election Day

- Provided risk advice and services to support security efforts by election officials and private sectorHeightened readiness posture beginning 45 days before Election DayElection Day operations: Classified and unclassified ops centers, cyber situational awareness roomsShared threat information faster than ever before (e.g. Iranian voter suppression emails)



JOINT CYBERSECURITY ADVISORY

TLP:WHITE

Iranian State-Sponsored Advanced Persistent Threat Actors Threaten Election-Related Systems

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) are warning that Iranian advanced persistent threat (APT) actors are likely intent on influencing and interfering with the U.S. elections to sow discord among voters and undermine public confidence in the U.S. electoral process.

The APT actors are creating fictitious media sites and spoofing legitimate media sites to spread obtained U.S. voter-registration data, anti-American propaganda, and misinformation about voter suppression, voter fraud, and ballot fraud.

The APT actors have historically exploited critical vulnerabilities to conduct distributed denial-of-service (DDoS) attacks, structured query language (SQL) injections attacks, spear-phishing campaigns, website defacements, and disinformation campaigns.

TECHNICAL DETAILS

These actors have conducted a significant number of intrusions against U.S.-based networks since August 2018. The actors leveraged several Common Vulnerabilities and Exposures (CVEs)—notably CVE-2020-5902 and CVE-2017-6049—pertaining to virtual private networks (VPNs) and content management systems (CMSs).

- CVE-2020-5902 affects F5 VPNs. Remote attackers could exploit this vulnerability to execute arbitrary code.*

* F5 Security Advisory: K52145254: TMUI RCE vulnerability CVE-2020-5902: https://support.f5.com/csp/article/K52145254

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.dhs.gov.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://us-cert.cisa.gov/tlp.

TLP:WHITE

JOINT CYBERSECURITY ADVISORY

TLP:WHITE

Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets

SUMMARY

Cyfinot Box: This joint cybersecurity advisory uses the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise framework for all referenced threat actor tactics and techniques.

This joint cybersecurity advisory—written by the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA)—provides information on Russian state-sponsored advanced persistent threat (APT) actor activity targeting various U.S. state, local, territorial, and tribal (SLTT) government networks, as well as aviation networks. This advisory updates joint CISA-FBI cybersecurity advisory AA20-283A, APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations.

Since at least September 2020, a Russian state-sponsored APT actor—known variously as Berserk Bear, Energetic Bear, TeamSpy, Dragonfly, Havex, Crouching Yeti, and Koala in open-source reporting—has conducted a campaign against a wide variety of U.S. targets. The Russian state-sponsored APT actor has targeted dozens of SLTT government and aviation networks, attempted intrusions at several SLTT organizations, successfully compromised network infrastructure, and as of October 1, 2020, exfiltrated data from at least two victim servers.

The Russian-sponsored APT actor is obtaining user and administrator credentials to establish initial access, enable lateral movement once inside the network, and locate high value assets in order to exfiltrate data. In at least one compromise, the APT actor laterally traversed an SLTT victim network and accessed documents related to:

- Sensitive network configurations and passwords.
- Standard operating procedures (SOP), such as enrolling in multi-factor authentication (MFA).
- IT instructions, such as requesting password resets.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at CISAServiceDesk@cisa.dhs.gov.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.us-cert.cisa.gov/tlp.

TLP:WHITE

Elections Infrastructure ISAC™

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

DHS-1255-003045 04/25/2024

#Protect2020 and Resilience Messaging

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION VIA FOIA IN LITIGATION

DHS-1255-003046 04/25/2024

CISA Activities Post Election Day

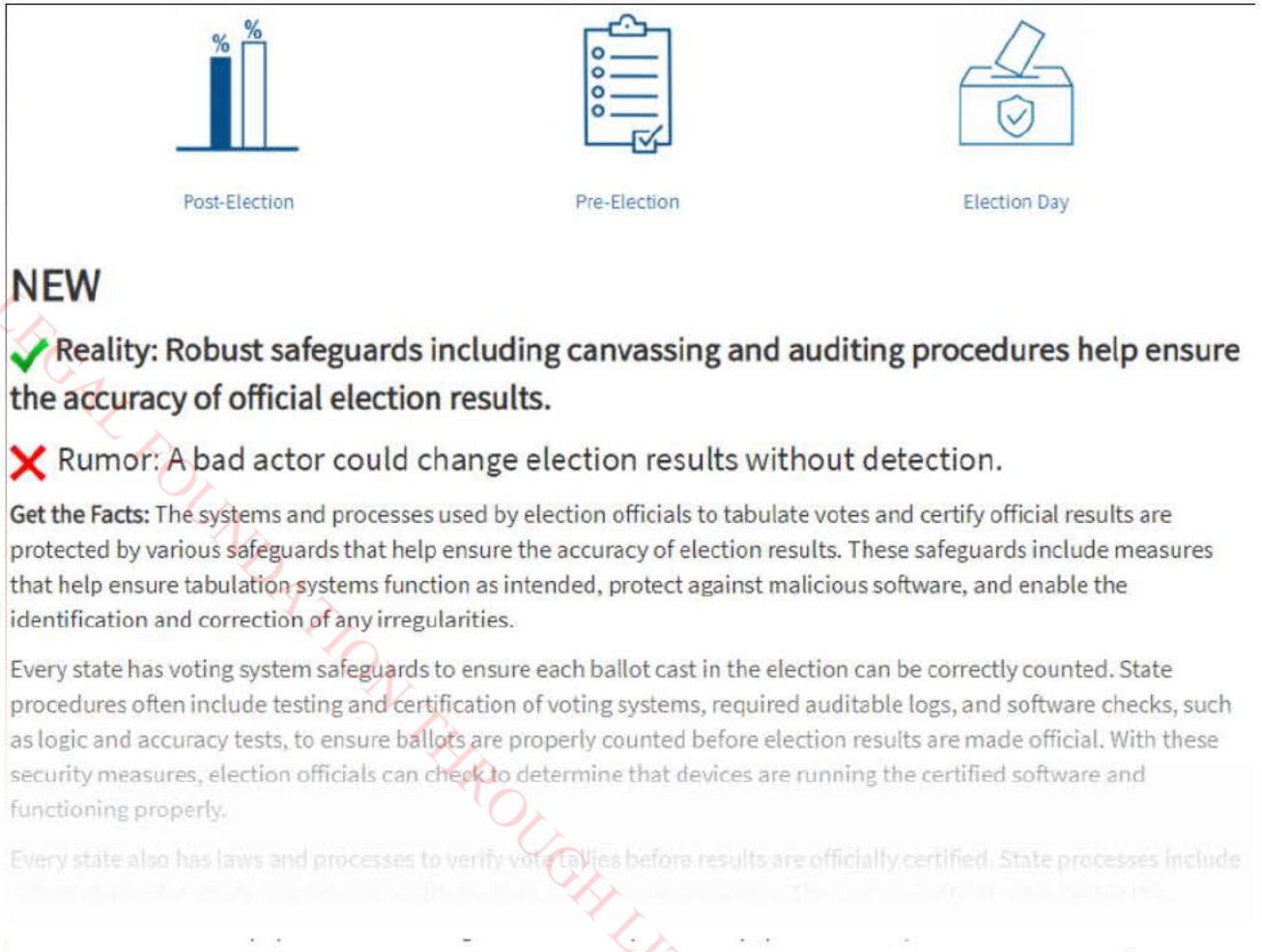
- No evidence that election infrastructure was compromised during the 2020 election, nor that any voting system deleted, lost, or changed votesHeightened readiness posture continues through states' certification of elections (mid-December)Continue to offer support to federal, SLTT, and private sector partners Continue to update our Rumor Control website as necessary to counter disinformation on election processesFollowing certification, CISA will develop an After-Action Report

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

DHS-1255-003047 04/25/2024

CISA Rumor vs Reality Website

- Available at cisa.gov/rumorcontrol Designed to preemptively debunk potential areas for disinformationRumors divided into Pre-Election, Election Day, and Post-Election categories20+ rumors published to date

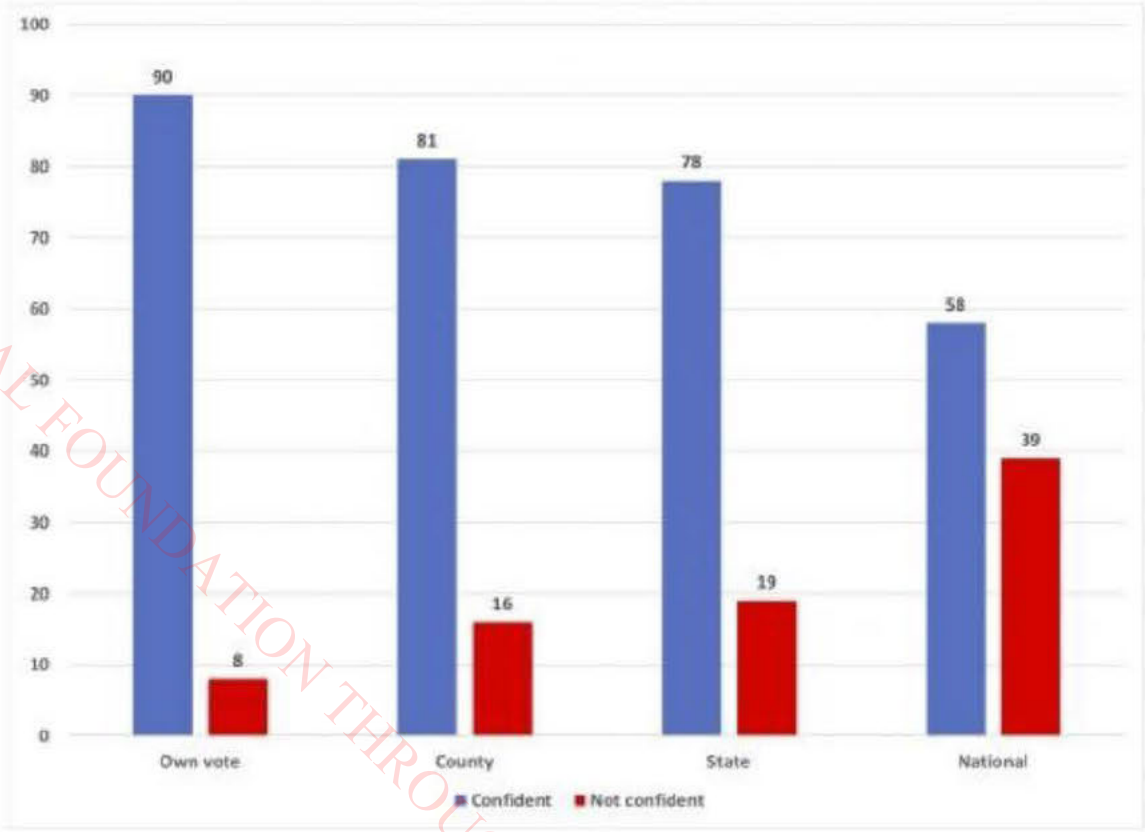


OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATIO

DHS-1255-003048 04/25/2024

Trust in the Election Process

- **High Degree of Confidence in Election Administration at the Local Level:According to a recent survey by Caltech, 90% of voters expressed confidence their own ballot was counted as intended – including high levels of trust for Democrats and RepublicansHowever, Less Confidence at the National Level:Only 58% of voters had confidence in the administration of elections nationwide with a large gap between the two parties:84% of Democrats expressing confidence31% of Republicans expressing confidence**



Alvarez et al. "Voter Confidence in the 2020 Presidential Election: Nationwide Survey Results." California Institute of Technology, Nov. 19, 2020

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATIO

DHS-1255-003049 04/25/2024

Key Milestones for US Elections

- December 14, 2020: Meeting of the Electoral College December 18, 2020: Latest certification deadline (Arkansas) December 23, 2020: Deadline for states to submit Certificate of Vote January 3, 2021: Swearing in of 117th Congress January 5, 2021: Georgia Senate runoff elections January 6, 2021: Joint Meeting of Congress to count electoral votes and declare winners of the presidential and vice-presidential election January 20, 2021: Presidential and VP terms begin at noon ET

OBTAINED BY AMERICAN FIRST LEGAL FOUNDATION THROUGH LITIGATION

DHS-1255-003050 04/25/2024

For more information: www.cisa.gov/protect2020www.cisa.gov/rumorcontrol

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

DHS-1255-003051 04/25/2024

From:	(b) (6) (b) (6)
To:	Election Infrastructure SSA (b) (6) (b) (6)
Subject:	RE: Question about Watermark Visibility on Ballots
Date:	2020/11/09 16:42:20
Priority:	Normal
Type:	Note

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.

Forgive me, because perhaps I don't understand, but what is the point of 'transparency in transmitting information quickly' if that information is incorrect?
Is CISA involved or Is CISA NOT involved in securing the Dominion Voting Systems electronic voting machines, and if not, then what is the acutal purpose of your organization? Which agency caught the DVS system flipping 6000 votes to the democrats

I want to speak with THAT organization, not an inert shell organization whose purpose seems to be to confabulate PUBLIC TRUST in a voting system they absolutely play no meaningful or legitimate role in securing
Perhaps I'm wrong. Explain to me exactlyu what your agency does other than put out PDFs with generic platitudes like 'ensure transparency'? That is not good enough in 2020.

Sorry. I'm an IT expert and I have a background in linux administration and security. Your glossy PDFs don't convince me of anything.

Thank you. I dont' want to be combative. I want the truth. I'm looking out for the american voters just as much as you are. Let's work together. Tell me in a fulsome and helpful way what CISA really does. As the kids say, 'be real with me'

Thank you.

(b) (6) ----------

a serie certe rectificari verum videre
"Not going to say I told you so, but at some point, it might be wise for you to start listening to me" --Laotzu, or someone, whatever, who cares
------- Original Message -------
On Monday, November 9, 2020 8:21 AM, Election Infrastructure SSA (b) (6) wrote:

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

Thank you for the inquiry. CISA defers to state and local election officials as trusted sources on specific questions on the conduct of elections. For general information about election security please see cisa.gov/protect2020 and for updated information on some common misconceptions see cisa.gov/rumorcontrol. Suspected criminal activity, if any, can be reported to local law enforcement and/or the FBI.

EI SSA

EI SSA/ESI, National Risk Management Center

Cybersecurity and Infrastructure Security Agency

Emai(b) (6)

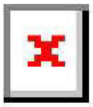


image001.png

From: (b) (6)
Sent: Saturday, November 7, 2020 2:07 AM
To: Election Infrastructure SSA <(b) (6)
Subject: Question about Watermark Visibility on Ballots

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.

Dear CISA,
Independent Journalist here seeking request for comments regarding the guidelines for "approved printing authorites'" watermarking of ballots.

https://cdn-0.stillnessinthestorm.com/wp-content/uploads/2020/11/watermarked-ballots-CISA-Gov-Agency.png

Specificially, I'd like to know if any or all of the "approved (ballot) printing authorities" are required or suggested to use invisible ink such as UV-sensitive toner or inkjet ink that that is only visible by using UV light?

I'd like to know if the watermarks are simply overt watermarks that any counterfeiter would be able to easily reproduce.

I'd like to know if the watermarks on ballots are a fixed mark or a changing mark that matches the ballot id, or in some way can ensure an auditor that the ballot was, in fact, printed by the authorized printer by means of some anti-counterfeit technology, such as MIC machine identification code (discrete and invisible to the human eye, small typically yellow dot patterns printed in empty space).

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

I'd like to know if CISA has given any additional firmware updates, patches, or additional configuration software to be used on "authorized (ballot) printing authority"; or authorized or overseen or coordinated with the USPS the use thereof.

I'd like to know, if CISA has coordinated with the USPS regarding WATERMARKING and/or Ballot Security in any way; and I'd like to know the purview of CISA in that matter.

Please consider this and my last email to you to be a FOIA request for all documents responsive to "BALLOT" and "WATERMARK", with a specificity to the above questions; or if you can simply field my questions in a fulsome manner with a good level of effort to ascertain the information I am looking for, that would suffice.

I am a US citizen, resident of NC, and my name is (b) (6) . Thank you. (b) (6) ; and excluding the possibility of an enormous comet impacting the earth, President Donald Trump is my president AND YOURS until Jan 20, 2021.

Thank you.

(b) (6)

(b) (6)

e: (b) (6)

a serie certe rectificari verum videre

"Not going to say I told you so, but at some point, it might be wise for you to start listening to me" --Laotzu, or someone, whatever, who cares

Sender:	(b) (6)
Recipient:	Election Infrastructure SSA (b) (6) (b) (6)
Sent Date:	2020/11/09 16:41:59
Delivered Date:	2020/11/09 16:42:20

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

From:	(b) (6)
To:	Election Infrastructure SSA / (b) (6) (b) (6)
Subject:	Question about CFITF and Social Media
Date:	2020/11/09 16:58:41
Priority:	Normal
Type:	Note

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.

CISA,

You say in your PDF about securing elections that CISA has direct interactions with the following "private" organizations: TWITTER, FACEBOOK, GOOGLE /ALPHABET(YOUTUBE), REDDIT.
> CFITF is charged with helping CISA's leadership understand the scope and scale of this challenge; ***identifying the policy options available to the government; and working with social media companies***, academia, international partners and across the executive branch on a variety of projects to build resilience against foreign influence operations.
What POLICY OPTION(S) DID CFITF and TWITTER (and/or FACEBOOK, GOOGLE/ALPHABET (YOUTUBE), REDDIT) PROPOSE, DISCUSS, AND/OR AGREE TO IMPLEMENT?
Please give an answer in a fulsome manner as if you are before Congress answering, or I will be forced to make a FOIA request for every document CFITF has produced and yes I'd be glad to pay for that.
Thank you.

(b) (6)

a serie certe rectificari verum videre
"Not going to say I told you so, but at some point, it might be wise for you to start listening to me" --Laotzu, or someone, whatever, who cares

Sender:	(b) (6)
Recipient:	Election Infrastructure SSA (b) (6) (b) (6)
Sent Date:	2020/11/09 16:58:29
Delivered Date:	2020/11/09 16:58:41

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

From:	(b) (6)
To:	Election Infrastructure SSA (b) (6) (b) (6)
Subject:	DVS Smartmatic is a problem
Date:	2020/11/10 01:54:53
Priority:	Normal
Type:	Note

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.

Instead of doing your job, you allowed the UK to come in the backdoor and attempt yet another coup d'etat against the American voter. Congratulations. You're fired.
https://canadafreepress.com/article/unbelievable-george-soros-employee-owns-defective-switch-vote-biden-machine

scrap-election-corruption.jpg

(b) (6)

"Not going to say I told you so, but at some point, it might be wise for you to start listening to me" --Laotzu, or someone, whatever, who cares

Sender:	(b) (6)
Recipient:	Election Infrastructure SSA (b) (6) (b) (6)
Sent Date:	2020/11/10 01:53:42
Delivered Date:	2020/11/10 01:54:53

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

From:	(b) (6)
To:	Election Infrastructure SSA (b) (6) (b) (6)
Subject:	Re: DVS Smartmatic is a problem
Date:	2020/11/10 02:09:41
Priority:	Normal
Type:	Note

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.

aim4truth.org exposed this problem with voting machines 2.5 yrs ago
https://aim4truth.org/2020/11/09/cat-report-596/
Should we give your job to them?

(b) (6)

a serie certe rectificari verum videre
"Not going to say I told you so, but at some point, it might be wise for you to start listening to me" --Laotzu, or someone, whatever, who cares

------- Original Message -------
On Tuesday, November 10, 2020 1:53 AM, M(b) (6)@protonmail.com> wrote:
Instead of doing your job, you allowed the UK to come in the backdoor and attempt yet another coup d'etat against the American voter. Congratulations. You're fired.
https://canadafreepress.com/article/unbelievable-george-soros-employee-owns-defective-switch-vote-biden-machine

scrap-election-corruption.jpg

(b) (6)

a serie certe rectificari verum videre
"Not going to say I told you so, but at some point, it might be wise for you to start listening to me" --Laotzu, or someone, whatever, who cares

Sender:	(b) (6)
Recipient:	Election Infrastructure SSA (b) (6) (b) (6)
Sent Date:	2020/11/10 02:06:49
Delivered Date:	2020/11/10 02:09:41

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

From:	(b) (6)
To:	Election Infrastructure SSA (b) (6) (b) (6)
Subject:	Every Point you've made in /rumorcontrol has been shown to be FALSE
Date:	2020/11/12 23:09:50
Priority:	Normal
Type:	Note

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

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.

https://www.cisa.gov/rumorcontrol
Director Chris Krebs should resign immediately for the above url and video. Every single point on this page has been debunked. These 'mitigation techniques' sound very good in practice, however, we have many witnesses that demonstrate very clearly how your 'mitigation techniques' have failed. There have been people altering voting machines, dominion voting systems IT support staff saying they were malfunctioning before her eyes, and when she reported it, she was told basically to STFU. This woman went on FOX I believe, or newsmax. The DVS machine flipped 6000 votes and this is happening in multiple places. There is mountains of fraud. This is the very tip of that iceberg.
Chris Krebs and your entire department are now guilty of fiduciary negligence in the minds of 71M US citizens because of this voting machine issue.
https://greatawakening.win/p/11PpFuNh5d/copypasta-compilation-of-voter-f/
I can tell you now, I was an expert IT witness in 2005 regarding DIEBOLD voting machines in Georgia. I was able to 'hack' the windows kiosk based system easily and open the voting database in microsoft jet application and thus bypass the administrative password implementation and in that system I was able to see and modify votes on a mock voter database they set up for me. I was just there to confirm a process and I did, and swore an affidavit to that effect to the georgia grand jury. I KNOW these things are easy as hell and wildly insecure. What I witnessed most of all, coming from a mixed background of windows, mac and linux; that these voting machines represented a total fleecing of the US taxpayer to recieve the most inept and frankly goofy and non secure machines I could possibly imagine. Going from NOVELL netware systems used in an enterprise situation or even citrix thin clients to a goofy half assed window system would make anyone cringe. You guys, being a CYBER division of DHS ought to understand where I'm coming from, OK? I know you do. I know it. Your'e cyber experts, I am not. I am an expert in IT and fullstack linux web programmer, and I get these to a degree so If I do, YOU certainly do.

We aren't going to accept this rumorcontrol

And I'll be honest with you: i'm going to find out if CISA played a role in deplatforming me from Twitter and google. It will not be good when it happens because I will sue you. Sovereign

immunity will not apply, sorry. It's called ***18 U.S. Code § 242.Deprivation of rights under color of law***
Expect a FOIA soon
I'm working on it.

Bigger fish to fry for now.

(b) (6)

a serie certe rectificari verum videre
"Not going to say I told you so, but at some point, it might be wise for you to start listening to me" --Laotzu, or someone, whatever, who cares

Sender:	(b) (6)
Recipient:	Election Infrastructure SSA (b) (6) (b) (6)
Sent Date:	2020/11/12 23:09:30
Delivered Date:	2020/11/12 23:09:50

OBTAINED BY JUDICIAL WATCH, INC. FIRST LEGAL FOUNDATION THROUGH LITIGATION

From:	(b) (6)
To:	Election Infrastructure SSA (b) (6) (b) (6)
Subject:	watch this
Date:	2020/11/13 15:44:11
Priority:	Normal
Type:	Note

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.

refutation of your bs claims and rumorcontrol
https://www.bitchute.com/embed/KkXOScyBQLc/

(b) (6)

a serie certe rectificari verum videre

"In Georgia in 2005, I was asked by a member of a Georgia grand jury on evaluating Diebold voting machine election fraud to be an expert IT/cybersecurity witness to participate in a mock hacking of a machine. I was able to easily access the windows kiosk machine, bypass the password feature by opening the database in an alternative program and modify and change mock votes. It was a matter of about 5 minutes tops. Fraudulent and inept Diebold rebranded itself to Sequoia, which is now owned by Dominion Voting Systems, which is itself part of Smartmatic. See the problem?" (b) (6)

Sender:	(b) (6)
Recipient:	Election Infrastructure SSA /o (b) (6) (b) (6)
Sent Date:	2020/11/13 15:43:49
Delivered Date:	2020/11/13 15:44:11

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

From:	(b) (6)
To	Election Infrastructure SSA (b) (6) (b) (6)
Subject:	Panic in DC
Date:	2020/11/14 04:48:38
Priority:	Normal
Type:	Note

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.

https://www.bitchute.com/embed/HnQ9FIBLCGxC/
pain is coming

(b) (6)

a serie certe rectificari verum videre

"In Georgia in 2005, I was asked by a member of a Georgia grand jury on evaluating Diebold voting machine election fraud to be an expert IT/cybersecurity witness to participate in a mock hacking of a machine. I was able to easily access the windows kiosk machine, bypass the password feature by opening the database in an alternative software program and modify mock votes. It was a matter of about 5 minutes tops. Fraudulent and inept Diebold rebranded itself to Sequoia, which is now owned by Dominion Voting Systems, which is itself part of Smartmatic. See the problem?" --(b) (6)

Sender:	(b) (6) Election Infrastructure SSA (b) (6)
Recipient:	(b) (6)
Sent Date:	2020/11/14 04:48:16
Delivered Date:	2020/11/14 04:48:38

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

From:	(b) (6) [redacted]
To:	Election Infrastructure SSA /(b) (6) [redacted] (b) (6) [redacted]
Subject:	Told you
Date:	2020/11/18 02:21:27
Priority:	Normal
Type:	Note

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.

You're whole department is under active investigation now.
This is what you get by doing your job badly and politicizing the facts and the truth.
https://twitter.com/realDonaldTrump/status/1328852352787484677?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1328852352787484677%7Ctwgr%5E&ref_url=https%3A%2F%2Fthedonald.win%2Fp%2F11Q8uv0Z0S%2Ftrump-tweet-chris-krebs-fired-dr%2Fc%2F

(b) (6) [redacted]

a serie certe rectificari verum videre

"In Georgia in 2005, I was asked by a member of a Georgia grand jury on evaluating Diebold voting machine election fraud to be an expert IT/cybersecurity witness to participate in a mock hacking of a machine. I was able to easily access the windows kiosk machine, bypass the password feature by opening the database in an alternative software program and modify mock votes. It was a matter of about 5 minutes tops. Fraudulent and inept Diebold rebranded itself to Sequoia, which is now owned by Dominion Voting Systems, which is itself part of Smartmatic. See the problem?" --(b) (6) [redacted]

Sender:	(b) (6) [redacted]
Recipient:	Election Infrastructure(b) (6) [redacted] (b) (6) [redacted]
Sent Date:	2020/11/18 02:20:59
Delivered Date:	2020/11/18 02:21:27

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

From:	(b) (6)
To:	Election Infrastructure SSA (b) (6) (b) (6)
Subject:	Fired CISA directors crime keeps getting worse
Date:	2020/11/19 05:51:53
Priority:	Normal
Type:	Note

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.

Alledge friends with dishonest NYTimes leaker
Held Watch party on election night with 2 dominion voting systems staffers; systems that were backdoored and flipped votes, 'ballot counting' machines that required "INK" (had ability to print, also)
He's under investigation now. Whether official or unofficial. Maybe ALL of you at CISA are under investigation now. You ought to be
https://nypost.com/2020/11/17/trump-fires-cyber-head-chris-krebs-for-dismissing-voter-fraud-claims/

(b) (6)

a serie certe rectificari verum videre

"In Georgia in 2005, I was asked by a member of a Georgia grand jury on evaluating Diebold voting machine election fraud to be an expert IT/cybersecurity witness to participate in a mock hacking of a machine. I was able to easily access the windows kiosk machine, bypass the password feature by opening the database in an alternative software program and modify mock votes. It was a matter of about 5 minutes tops. Fraudulent and inept Diebold rebranded itself to Sequoia, which is now owned by Dominion Voting Systems, which is itself part of Smartmatic. See the problem?" --(b) (6)

Sender:	(b) (6)
Recipient:	Election Infrastructure SSA (b) (6) (b) (6)
Sent Date:	2020/11/19 05:51:35
Delivered Date:	2020/11/19 05:51:53

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

From:	(b) (6)
Subject:	Here is the Evidence dot com
Date:	2020/11/21 13:15:24
Priority:	Normal
Type:	Note

OBTAINED BY AMERICAN FIRST LEGAL FOUNDATION THROUGH LITIGATION

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.

Crowdsourced catalogue of 2020 election fraud events throughout the country
https://hereistheevidence.com/
note, I say election, not voter fraud. I think voter fraud is minimal, because the cost is high and the gain is unclear. I think 99.99% of people vote in earnest, which is the american / democratic way. I know for certain, and have witnessed first hand (see below) that voting machines are easily compromised, and are in fact designed to be.
Voting machines in 2020 are still using Microsoft access, which is a toy database that is useful for prototyping applications but not real world applications. I am an expert in access, having worked with it for years at UGA, tweny years ago, at three different colleges there as IT person who routinely had to fix data issues, repair databases and the application itself used by grad students, staff and professors.
I know that access is an extremely inappropriate tool for more than 1M records, but it's still being used today. If security isn't an issue, data integrity is; but most of the problems with the voting machines have to do with tally and reporting... Reporting is where most of the fraud is occurring due to, I believe, and reportage is now demonstrating, falsified votes, purposeful miscounting, machinefilled ballot drops after polls close, electronic vote flipping in a collection database further up the chain (collating results of collections of counties--state region level), and various activities such as the "salami slicing" technique that exploits improper application logic and the maths discrepancies between integer fields and floating point fields, stealing hidden fractions (decimals) and then utilizing them to reconstruct ballots. This post explains fractional magic
https://greatawakening.win/p/11QRfUJ5c9/fraction-magic-video-demonstrate/
Gatewaypundit explains drop and roll
https://www.youtube.com/watch?v=1_P3-Z2MV5I

(b) (6)

"In Georgia in 2005, I was asked by a member of a Georgia grand jury on evaluating Diebold voting machine election fraud to be an expert IT/cybersecurity witness to participate in a mock hacking of a machine. I was able to easily access the windows kiosk machine, bypass the password feature by opening the database in an alternative software program and modify mock votes. It was a matter of about 5 minutes tops. Fraudulent and inept Diebold rebranded itself to Sequoia, which is now owned by Dominion Voting Systems, which is itself part of Smartmatic. See the problem?" --(b) (6)

Sender: (b) (6)

Sent Date:	2020/11/21 13:14:59
Delivered Date:	2020/11/21 13:15:24

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

From:	(b) (6)
To:	Election Infrastructure SSA (b) (6) (b) (6)
Subject:	Question about Watermark Visibility on Ballots
Date:	2020/11/07 02:06:52
Priority:	Normal
Type:	Note

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

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.

Dear CISA,

Independent Journalist here seeking request for comments regarding the guidelines for "approved printing authorites'" watermarking of ballots.
https://cdn-0.stillnessinthestorm.com/wp-content/uploads/2020/11/watermarked-ballots-CISA-Gov-Agency.png
Specificially, I'd like to know if any or all of the "approved (ballot) printing authorities" are required or suggested to use invisible ink such as UV-sensitive toner or inkjet ink that that is only visible by using UV light?

I'd like to know if the watermarks are simply overt watermarks that any counterfeiter would be able to easily reproduce.
I'd like to know if the watermarks on ballots are a fixed mark or a changing mark that matches the ballot id, or in some way can ensure an auditor that the ballot was, in fact, printed by the authorized printer by means of some anti-counterfeit technology, such as MIC machine identification code (discrete and invisible to the human eye, small typically yellow dot patterns printed in empty space).
I'd like to know if CISA has given any additional firmware updates, patches, or additional configuration software to be used on "authorized (ballot) printing authority"; or authorized or overseen or coordinated with the USPS the use thereof.
I'd like to know, if CISA has coordinated with the USPS regarding WATERMARKING and/or Ballot Security in any way; and I'd like to know the purview of CISA in that matter.
Please consider this and my last email to you to be a FOIA request for all documents responsive to "BALLOT" and "WATERMARK", with a specificity to the above questions; or if you can simply field my questions in a fulsome manner with a good level of effort to ascertain the information I am looking for, that would suffice.
I am a US citizen, resident of NC, and my name is (b) (6) Thank you. (b) (6) and excluding the possibility of an enormous comet impacting the earth, President Donald Trump is my president AND YOURS until Jan 20, 2021.

Thank you.

(b) (6)

a serie certe recitficari verum videre

"Not going to say I told you so, but at some point, it might be wise for you to start listening to me" --Laotzu, or someone, whatever, who cares

Sender:	(b) (6)
Recipient:	Election Infrastructure SSA /(b) (6) (b) (6)
Sent Date:	2020/11/07 02:06:37
Delivered Date:	2020/11/07 02:06:52

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

From:	Snell, Allison </O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (b) (7)(A)
To:	(b) (6)
CC:	Election Infrastructure (b) (6) (b) (6)
Subject:	FW: FOIA request
Date:	2020/12/07 09:56:00
Priority:	Normal
Type:	Note

We do not have responsive records for this.

Allison L. Snell
Election Security Initiative
Cybersecurity and Infrastructure Security Agency
Cell: (b) (6) Email (b) (6)

From: Election Infrastructure SSA (b) (6)
Sent: Monday, December 7, 2020 8:03 AM
To: Snell, Allison (b) (6) ; Masterson, Matthew (b) (6) , Hale, Geoffrey (b) (6)
Cc: (b) (6)
(b) (6)
Subject: FW: FOIA request

Good morning,

Sharing for everyone's situational awareness. For additional context, we've received about 10-15 additional emails from this individual since the election (attached above). Please let me know if I should forward to any others.

Thanks,

(b) (6)
Contract Support, Election Security Initiative
Cybersecurity and Infrastructure Security Agency
Phone (b) (6) Email: (b) (6)

From: (b) (6)
Sent: Saturday, December 5, 2020 7:07 PM
To: Election Infrastructure SSA (b) (6)
Subject: FOIA request

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.

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

Dear CISA FOIA Dept,

I would like to know if China is an ***"approved printing authority"***

https://www.cisa.gov/sites/default/files/publications/mail-in-voting-election-integrity-safeguards_508.pdf

This video would suggest that China is an approved printing authority because CISA assures us with /rumorcontrol that this was a completely secure election. I mean, if it's secure and China DID print, then clearly someone at CISA approved a location in China to print ballots, unless this is fake news, which it probably is.

https://www.youtube.com/watch?v=V0nAS_jLn7A

But just to be sure, I'd like a list of all approved printing authorities.

This is a FOIA request. I would like for CISA to provide for me list of all entities that are designated as "approved printing authories". I don't know what a responsive search would be, but try the token search for case-insensitive "Printing Authorities" as a full-text search through every human readable string field of every database, excel file, eml, html, txt, PDF and human readable text file of any extension.

I am a journalist writing about approved printing authorities authorized by CISA or a downstream or peer authority that so-authorizes printing authorities.

If you need help with this, I am a linux administrator who has done plenty of research on government documents scraped from the US State Dept electronic library and I am familiar with secure, safe open source tools that can search through large amounts of PDFs and text. The tool of choice I use now is "ack-grep" (or just "ack" in the latest version) with the -i flag (case insensitive) and a quotation enclosed search phrase.

I would like to receive this electronically in any format that is human-readable in English language with no hidden malware, tracking mechanisms such as image beacons, javascript, xml based or microsoft office compatible remote execution exploits, or funny tradecraft soundex swizzles such as comey<->corney or cannabus<->cannabis to inhibit searchability or any other inhibitory, obstructionist, petty or passive aggressive mechanisms which we've catalogued from other agencies begrudging fulfillment of FOIA requests

Please notify me if there are any additional fees you may require to fulfill this request and I'd gladly be able to provide that for you, up to but not beyond 1000 USD.

Please let me know if you need more information from me. I am a US citizen, (b) (6) [redacted] That should be enough for an advanced cybersecurity group such as yourselves to be able to positive validate me as a US citizen empowered to make a FOIA request of your dept.

Thank you.

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

(b) (6)

a serie certe rectificari verum videre

Sender:	Snell, Allison <(b) (6) (b)(5)
Recipient:	(b) (6)
Sent Date:	2020/12/07 09:56:20
Delivered Date:	2020/12/07 09:56:00

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

From:	(b) (6)
To:	Election Infrastructure SSA (b) (6) (b) (6)
Subject:	DVS Smartmatic is a problem
Date:	2020/11/10 01:54:53
Priority:	Normal
Type:	Note

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.

Instead of doing your job, you allowed the UK to come in the backdoor and attempt yet another coup d'etat against the American voter. Congratulations. You're fired.
https://canadafreepress.com/article/unbelievable-george-soros-employee-owns-defective-switch-vote-biden-machine

scrap-election-corruption.jpg

(b) (6)

"Not going to say I told you so, but at some point, it might be wise for you to start listening to me" --Laotzu, or someone, whatever, who cares

Sender	(b) (6)
Recipient:	Election Infrastructure SSA (b) (6) (b) (6)
Sent Date:	2020/11/10 01:53:42
Delivered Date:	2020/11/10 01:54:53

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

From:	[redacted]
To:	Election Infrastructure SSA (b) (6) [redacted]
Subject:	Question about Watermark Visibility on Ballots
Date:	2020/11/07 02:06:52
Priority:	Normal
Type:	Note

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

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.

Dear CISA,

Independent Journalist here seeking request for comments regarding the guidelines for "approved printing authorites'" watermarking of ballots.
https://cdn-0.stillnessinthestorm.com/wp-content/uploads/2020/11/watermarked-ballots-CISA-Gov-Agency.png
Specificially, I'd like to know if any or all of the "approved (ballot) printing authorities" are required or suggested to use invisible ink such as UV-sensitive toner or inkjet ink that that is only visible by using UV light?

I'd like to know if the watermarks are simply overt watermarks that any counterfeiter would be able to easily reproduce.
I'd like to know if the watermarks on ballots are a fixed mark or a changing mark that matches the ballot id, or in some way can ensure an auditor that the ballot was, in fact, printed by the authorized printer by means of some anti-counterfeit technology, such as MIC machine identification code (discrete and invisible to the human eye, small typically yellow dot patterns printed in empty space).
I'd like to know if CISA has given any additional firmware updates, patches, or additional configuration software to be used on "authorized (ballot) printing authority"; or authorized or overseen or coordinated with the USPS the use thereof.
I'd like to know, if CISA has coordinated with the USPS regarding WATERMARKING and/or Ballot Security in any way; and I'd like to know the purview of CISA in that matter.
Please consider this and my last email to you to be a FOIA request for all documents responsive to "BALLOT" and "WATERMARK", with a specificity to the above questions; or if you can simply field my questions in a fulsome manner with a good level of effort to ascertain the information I am looking for, that would suffice.
I am a US citizen, resident of NC, and my name is (b) (6) [redacted] Thank you. (b) (6) [redacted] and excluding the possibility of an enormous comet impacting the earth, President Donald Trump is my president AND YOURS until Jan 20, 2021.

Thank you.

(b) (6)

a serie certe recitficari verum videre

"Not going to say I told you so, but at some point, it might be wise for you to start listening to me" --Laotzu, or someone, whatever, who cares

Sender:	(b) (6)
Recipient:	Election Infrastructure SSA / (b) (6) (b) (6)
Sent Date:	2020/11/07 02:06:37
Delivered Date:	2020/11/07 02:06:52

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

From:	Snell, Allison (b) (8) (b) (6)
To:	Masterson, Matthew (b) (6) (b) (6) Hale, Geoffrey (b) (6) (b) (6)
Subject:	FW: Post Briefing Documents resent wo PW
Date:	2020/12/07 14:53:00
Priority:	Normal
Type:	Note

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

Allison L. Snell
Election Security Initiative
Cybersecurity and Infrastructure Security Agency
Cell: (b) (6) Email: (b) (6)

From: (b) (6)
Sent: Monday, July 13, 2020 1:38 PM
To: (b) (6); Snell, Allison (b) (6)
Cc: Wieczorek, Erin <(b) (6)
Subject: FW: Post Briefing Documents resent wo PW

FYI - This is the group (Russ Ramsland) that talked to (b) (6) and I a few weeks ago. They've sent me a bunch of materials (attached) and have asked for a follow-up meeting, including an in-person follow-up, about 5 times in the past week. It's a lot of random information. I'll see if they can distil it down to one page so we can determine if there's anything there.

(b) (6)
Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
(b) (6)
Cell (b) (6)

From: (b) (6)
Sent: Monday, July 6, 2020 6:07 PM
To: (b) (6)
Cc: (b) (6) @hsgac.senate.gov
Subject: Post Briefing Documents resent wo PW

(b) (6)

My computer at ASOG was having problems this afternoon and would not send the files...
I came to my other office to try from here....I apologize if you get multiple copies of this email ...went th other server wakes up

1. Exec Sum
2. Briefing Outline
3. Dallas Irregularities
4. 2020 Black site report – brek in chain of custody of flash drives Dallas County
5. 2020 election judge report
6. 2020 Commissioners report

Sender:	Snell, Allison <[redacted]>
Recipient:	Masterson, Matthew [redacted] Hale, Geoffrey [redacted]
Sent Date:	2020/12/07 14:54:21
Delivered Date:	2020/12/07 14:53:00

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

ELIMINATE SYSTEM-WIDE ELECTION FRAUD THREAT

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

EXECUTIVE SUMMARY: ***(The Problem)***

The entire U.S. election system is vulnerable and likely compromised by illegal access and the actual perpetrators may be veiled in secrecy. It is open to system-wide manipulation. We have observed and gathered compelling evidence of dangerous, substantial interference.

- Election Fraud** has been perpetrated on a massive scale in this country going back to at least 2008 and continues to be perpetrated. Entire outcomes have been shifted. This completely eclipses mere Voter Fraud*; it is the difference between the entire Navy and a few sporadic vessels. *(See Election Fraud -vs- Voter Fraud* defined on page 2)*

- Examples include the Presidential race in 2016 that was saved only by unprecedented turnout from Trump supporters (wholly unexpected by the perpetrators) and reported denial of service attacks against illegal servers that prevented uploads of wholesale changes in vote databases of key electoral states.

- The recent 2019 race in Kentucky was an example where votes *were* manipulated. Vote changing from one candidate to the other at the database level was captured in real time on CNN footage in this race.

- It is so easy to electronically change votes with today's technology and we have comprehensive proof. While it sounds like a Tom Clancy thriller, the fact is that entire databases are being systematically stolen, manipulated and replaced in real time during elections.

- Current domestic chaos, Mail-in ballots and other Voter Fraud initiatives are a smokescreen to overwhelm the system and distract the administration from the true threat: the biggest and most crucial opportunity to exploit mass scale election fraud to enact a make-or-break outcome for these enemies of the state.

- ***ALL Elections are outsourced to private companies with no transparency. The companies all upload the votes to a single, offshore, multi-national company that houses the votes and reports the results, with no oversight. The software used by virtually all the voting companies comes from a single, original source. The fraudulent system includes a shadowy Soros-backed entity, offshore servers and a prominent DNC-linked entity.***

- This can be stopped or ameliorated before the 2020 Election with immediate action from the Executive Branch, AG Barr, and elements the government that are still regarded as reliable, combined with network resources, key trusted personnel and a well-defined, coherent short term and long term strategy.

DHS-1255-003076 04/25/2024

PROACTIVE MEASURES & REMEDIES: ***(The Short-Term Solution)***

This system-wide vulnerability can be eliminated before the 2020 Election with immediate action from the Executive Branch, AG Barr, and elements of the government that are still regarded as reliable, combined with network resources, key trusted personnel and a well-defined, coherent short term and long term strategy.

The Short-Term Strategy* has 4 aspects:**

1) Make it safe for media to begin a rational discussion about the ease and prevalence of Election Fraud using private and federal lawsuits against voting companies (and the offshore company that ultimately holds, controls and reports the overwhelming majority of US election votes) as a stepping stone for wider and more in-depth coverage.

2) Use Legislation already enacted but not fully implemented, such as the Real ID Act of 1998 that deemed Federal elections as "critical infrastructure", opening the door for the DHS to get directly involved and responsible for the implementation. Implementation by October 2020, required per the legislation, would greatly help to interrupt and disrupt plans and operations currently underway to commit Voter and Election Fraud in a variety of ways.

3) Work with select members of the U.S. Senate to generate a criminal referral to the DoJ.

4) Have a fully briefed government operations center set up and operational to protect vote databases. The effort would require all authorized servers involved in the election system to be registered ahead of time and only accessible via a government VPN (jump server) similar to those of the NSA, CIA and FBI. Also, the users (anyone authorized to legally login from election company workers to news agencies) would be required to register their IP address and a unique identifier. Those registered would then login via the government-controlled VPN (jump server). Anyone wishing access to the databases (including news agencies) would be required to go through the system. No data would be allowed to go offshore or sent to any server not controlled by the government VPN. The government operations center would monitor, police and log all the traffic over the VPN. This could be enacted by Executive Order and accomplished within a few days as the setups already exist within various government agencies and even some State agencies.

Allied Special Operations Group has a full briefing on their findings to date, which echo those presented in the recent HBO Documentary "Kill Chain", and then expand past it to demonstrate the overall voting structure's vulnerabilities.

DEFINITIONS:

***Voter Fraud** – Illegal Voters/Voter Ballot Harvesting/Mail-in Ballots/Voter Intimidation.
****Election Fraud** – Deals with electronic cheating via software changes and database manipulation for votes already captured inside election computers. It is the quintessential example of Stalin's quote that who votes doesn't matter, it only matters who controls and counts the votes.
*****Short-Term Strategy** – This is what ASOG believes can be accomplished before the 2020 General Election. This is really just a patch which allows time for the development of a secure election system.

DHS-1255-003077 04/25/2024

OBTAINED BY AMERICA'S FIRST LEGAL FOUNDATION THROUGH LITIGATION

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

ELECTION FRAUD - A Real Threat to Our Democracy

Introduction Briefing Outline

Shallow Dive with Related Attachments

Revised: May 15, 2020

Election Fraud - Intro Briefing Outline – Shallow Dive – *Update May 15, 2020*

In 2017, Allied Special Operations Group, LLC ("ASOG") was formed as a security (cyber intelligence & personal) support company for litigation, and various other commercial services as well as for limited, discreet government support. It is comprised of specialists in several areas including former operators from various 3 letter Federal agencies that have very deep cyber and HUMINT capabilities.

After the 2018 mid-term elections, we began an investigation into irregularities in election results using an 1,100-page Audit Log of the central tabulation server printed at the request of a citizen's group late on election night at the Dallas County Central Counting office. The audit logs included early vote totals as well as election night totals. The detailed logs documented entries into the tabulation system for the election itself and we saw many areas of concern.

In the audit logs of the Central Counting computer, we found vote totals in the database were zeroed out then reloaded several times between early vote ending and the Election Day close from sources outside of the election system. We also saw statistically strong evidence suggesting vote harvesting of under votes.

The ASOG cyber team in conjunction with other cyber experts took a deep dive into the election system and mapped the voting process from ballot casting to central tabulation to national collection and dissemination via SCYTL, a Spanish multinational corporation. Additionally, we mapped the top 5 or 6 of the major voting companies that are contracted by counties to run the bulk of our US elections (and around the world as well). Most Americans are unaware that our U.S. elections are run entirely by private companies under contract to counties, and these private companies assemble the software, sell the machines, conduct the elections, keep the voter roles and information, collect the votes, tally the votes and post the results. All of this has virtually no transparency. Through Open Source Intel techniques and Tor contacts in the Dark Web, the experts could look into the source code of several of these companies and even see administrator level passwords for database access out in the open. They determined there were significant vulnerabilities in which unseen intruders could take advantage of and actually change votes. The investigation has lasted for 18 months and cost over $1 million.

In November 2019, we were asked to send a small team to Kentucky to look at the hugely anomalous gubernatorial race wherein every statewide race was won by Republicans with significant vote margins (200,000+ votes) except for the top of the ticket. The governor lost by 5,086 votes and members of his campaign thought something looked odd and wanted to get to the bottom of it. We had previously advised them that, based on our research, their race had all the earmarks of a potentially targeted race for vote tampering.

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

Within a few days after the election, our cyber team uncovered a split second in the election night video feed from Clarity Elections to CNN that actually displayed the findings of our investigation. This live feed from CNN accidentally showed reported votes to Governor Bevin ***decrease*** by 560 votes at the exact same instant his opponent, Andy Beshear, had an ***identical increase*** of 560 votes. This vote change is a 1,120 vote swing in a race that was decided by just over 5,000 votes hence about 20% of the vote swing is seen occurring in a split second with votes being subtracted from Bevin and added to Beshear. This can only demonstrate access into central tabulation, probably by uncredentialed outsiders changing vote totals virtually undetected and without an audit trail as we and others have demonstrated and written about. While several groups looked at the CNN clip, no one has been able to offer any other explanation of what we saw happen on CNN. CNN refused to comment. This video clip can be view on the EWR link Election Fraud Battle Plan.

In our briefing we show the clip and play it back to pause at the exact before and after frames where votes appear to have been switched. Additional clips have also been discovered.

Media Strategy ***Note:*** *We have a Litigation Strategy (working with former Kansas AG now living in VA to ID local prosecution with friendly judges to obtain evidence via subpoena) and a Legislative Strategy but time is sort so we began to focus on the media strategy.*

We have begun to make public our election fraud information through various channels. We have recorded 4 explanatory video sessions, collected a compendium of many excellent source articles on this subject and supported several other investigatory groups.

We are now getting significant, national investigative reporters asking us to take them through our detailed 1-hour 15-minute briefing so they can choose the angle they want to write on. Starting Thursday, April 30th, articles started to appear on certain aspects of voter fraud and election fraud. See April 29, 2020 Western Journal: Cyber Experts Warning About 2020 Election.

Our decision to go public was based on the clock ticking towards the general election in November wherein altering the outcome of 5 or 6 key electoral states would change and defeat the actual will of the American people in selecting their President. Two other factors also determined this course. First, the President began to discuss requiring Voter ID in a COVID-19 Task Force Briefing that we took as a cue to move forward with disclosure, and secondly, on April 6, 2020, HBO launched (now on YouTube) an Election Fraud Documentary: "**Kill Chain**"

This was amazing timing. HBO released this 1 $^{1}/_{2}$ hour documentary narrated by Hari Hursti the Finnish voter fraud cyber expert. In the documentary he shows how porous the system is when 11, 12 and 15 year old kids are able to hack the election system in only minutes. He makes clear the ridiculous posture of various government officials who claim in hearings before Congress that the system is not connected to the internet and is not hackable. He puts into a documentary many of the things we have been saying for the last year. What he did not cover is what we found out

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

when we mapped the entire network and ownership and found out the entire system rolls up to SCYTL, a Barcelona, Spain company. It is SCYTL that has the final control on the vote counting and reporting (and which the CNN video shows changing votes). Both the Chicago Sun Times and Forbes say it raises troubling concerns about election cyber security. But make no mistake, the underlying purpose of the documentary is clearly to suggest this was how the Russians changed the last election, undetected, and to establish the Democrats as the thought leaders on Election Fraud in order to help pass their mail-in ballot bill.

Kill Chain https://www.youtube.com/watch?v=3c8LMZ8UGd8

Also see: The Election Fraud Battle Plan: A NEW LANDING PAGE on Kevin Freeman's Economic War Room was set up to aggregate articles and other resources. *(additional videos are added as needed)*

Election Fraud – Our Democracy is Under Threat and It Impacts Your Money, Your Livelihood and Your Way of Life

1. This landing page opens with our 2019 Update Video on Kentucky Governor's Race
   Additional videos –2016 What Happened? 2018 Update "Blue Wave?", 2020 Update
2. You can download the FREE Economic Battle Plan™
3. You can download the FREE Resource Guide with Links to Videos and Articles

Request: Take a briefing and hear our suggestions.

We are business people who believe solutions, not just recital of problems, are the way forward. We would like an opportunity to give our briefing in order to leave no doubt in people's minds as to the seriousness of this. We would also like to offer a short-term solution to help secure an honest 2020 election and then a longer-term course of action. Both the short-term and long-term strategies involve combining and immediately re-implementing the ILLEGAL IMMIGRATION REFORM AND IMMIGRANT RESPONSIBILITY ACT OF 1996, signed into law by President Clinton, with the REAL ID ACT – Public Law 109-13 Title II Section 201 (3). Recently, a friended posted this MEMO to POTUS regarding REAL ID ACT. *Together, these can accomplish 3 things.* ***First,*** *all the ballot-harvesting and mail-in fraud ends.* ***Second,*** *it allows DHS to exercise its power over "critical infrastructure" to require real paper ballots (not those generated by illusory ballot marking devices) so that audits will mean something, and* ***third*** *it allows DHS time to create real oversight of the system, something that doesn't exist today.*

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

Exhibit 1-6

Table of Contents

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

Exhibit 1

April 29, 2020 Western Journal:

Cyber Experts Warning About 2020 Election

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

Cyber Experts Warn of Major Election Vulnerabilities Going into 2020

Randy DeSoto
Published April 29, 2020 at 6:08am

With the November elections quickly approaching, election security experts are warning that the United States is very vulnerable to cyberattacks that could change the results of races, including the presidential contest.

Further, some simple changes could be made that would do much to ensure accurate election reporting, the experts say.

Harri Hursti — one the the world's foremost election security experts — observed in his newly released HBO documentary, "Kill Chain: the Cyber War on America's Elections," that due to the way electronic voting is conducted and the results reported throughout the United States, the system is vulnerable to hacking.

"The problem is once you understand how everything works, you understand how fragile everything is," Hursti says in the film.

"I keep hearing that the system is unhackable. Everything is hackable, always," the cyber expert added.

TRENDING: NBC Admits to Airing Highly Deceptive Edit of Attorney General Barr's Comments

Hursti famously demonstrated to Florida election officials just how easy it was to overwrite voting machine software to change results for his 2006 documentary film, "Hacking Democracy."

Last month, he told WCBS: "The most frightening thing is that from 2006 to now, nothing changed. The actual software that I hacked in 2005 is still in use. Those machines are still in 20 states."

Beyond the vulnerability of voting machines themselves to hacking, other vulnerabilities exist in the tallying and transmission of the results.

Do you support paper ballots and risk-limiting audits of election results?

Two of the biggest misconceptions Americans likely have about how elections are conducted are that votes are counted by state and local election officials and that the vote tallies themselves, even if backed up by paper ballots, are not vulnerable to hacks.

In October 2016, then-President Barack Obama made the oft-repeated argument that due to the decentralized nature of voting in the United States, elections, especially at the presidential level, cannot be hacked or significantly altered.

"There is no serious person out there who would suggest somehow that you could even rig America's elections in part because they are so decentralized and the numbers of votes involved," Obama said.

Election security expert Russell Ramsland told The Western Journal Americans need to understand that state and local officials, by and large, do not count the votes on election night, but have contracted private companies to do so.

"It is incredible how many people believe that their county or their state run their elections," Ramsland said. "They have no idea that all elections are actually conducted by private companies, with virtually no oversight, no transparency."

RELATED: Amy Klobuchar Issues Threat Against Republicans if Vote-by-Mail Is Not Funded

"And that private company writes the software, makes and sells the machines, keeps all the voter rolls, and tallies all the votes and reports them," he added. "It's totally and completely jobbed out to a private company with private shareholders."

Far from being decentralized, there are three main companies that tally the votes for election officials, according to "Kill Chain": Election Systems & Software, Dominion Voting Systems and Hart Voting Systems.

Hursti noted that none of these companies agreed to be interviewed for "Kill Chain."

There are "commonalities" between all the major companies in their election night reporting, he told The

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

DHS-1255-003084 04/25/2024

Western Journal.

One thing all the electronic voting systems have in common is a removable drive or memory device, which engages in two-way communication with the database when results from each voting machine are uploaded.

Hursti explained that all these devices are programmed how to organize and communicate the data to the central database.

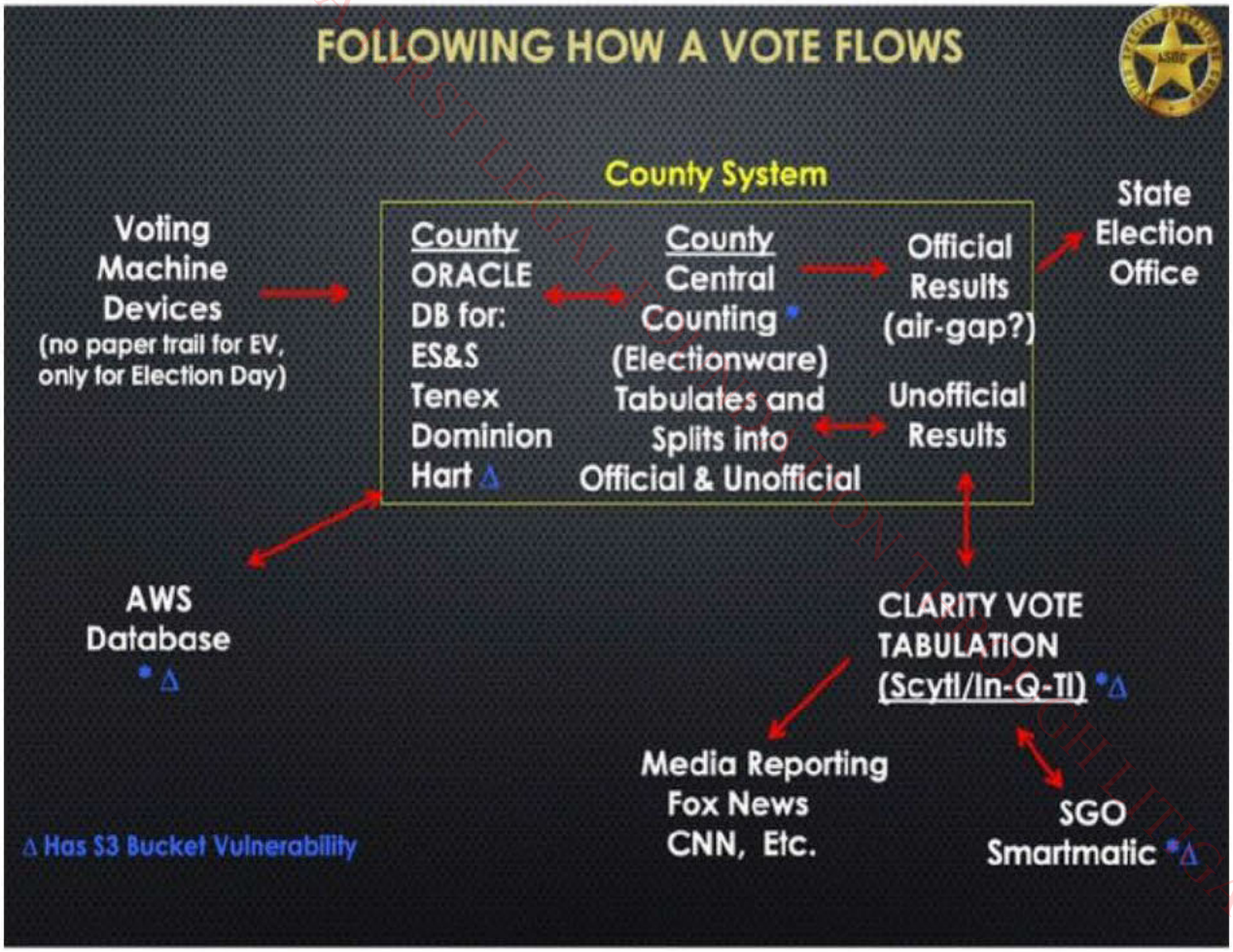
"The memory cards actually have a programming side," he said. "Programming can have a lot of logic. So the program can dynamically look [at] what is happening and decide on the spot what is needed to be done in this precinct on this machine" as part of changing the overall result.

"Once you can send that instruction to the election management system, the election management system is sending the same programming into every voting machine," Hursti continued.

"So the only thing you need to do is to modify that program, and there are so many different ways."

Ramsland created a diagram (shown below) to illustrate how votes typically flow from the precinct voting machines to databases maintained by companies like ES&S, Dominion and Hart to be tallied for the election results.

All this information travels over the internet to different databases (as signified by the blue triangles) along the way, which can be hacked.



The "unofficial results" are then made public through companies like Clarity Elections, which is the U.S. division of the Barcelona, Spain-based company Scytl.

The company proudly states on its website that it has "successfully delivered election modernization projects in the US since 2008, and most recently for the 2018 Midterm Elections, when over 70 [million] voters from more than 900 U.S. counties successfully leveraged Scytl's technology."

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

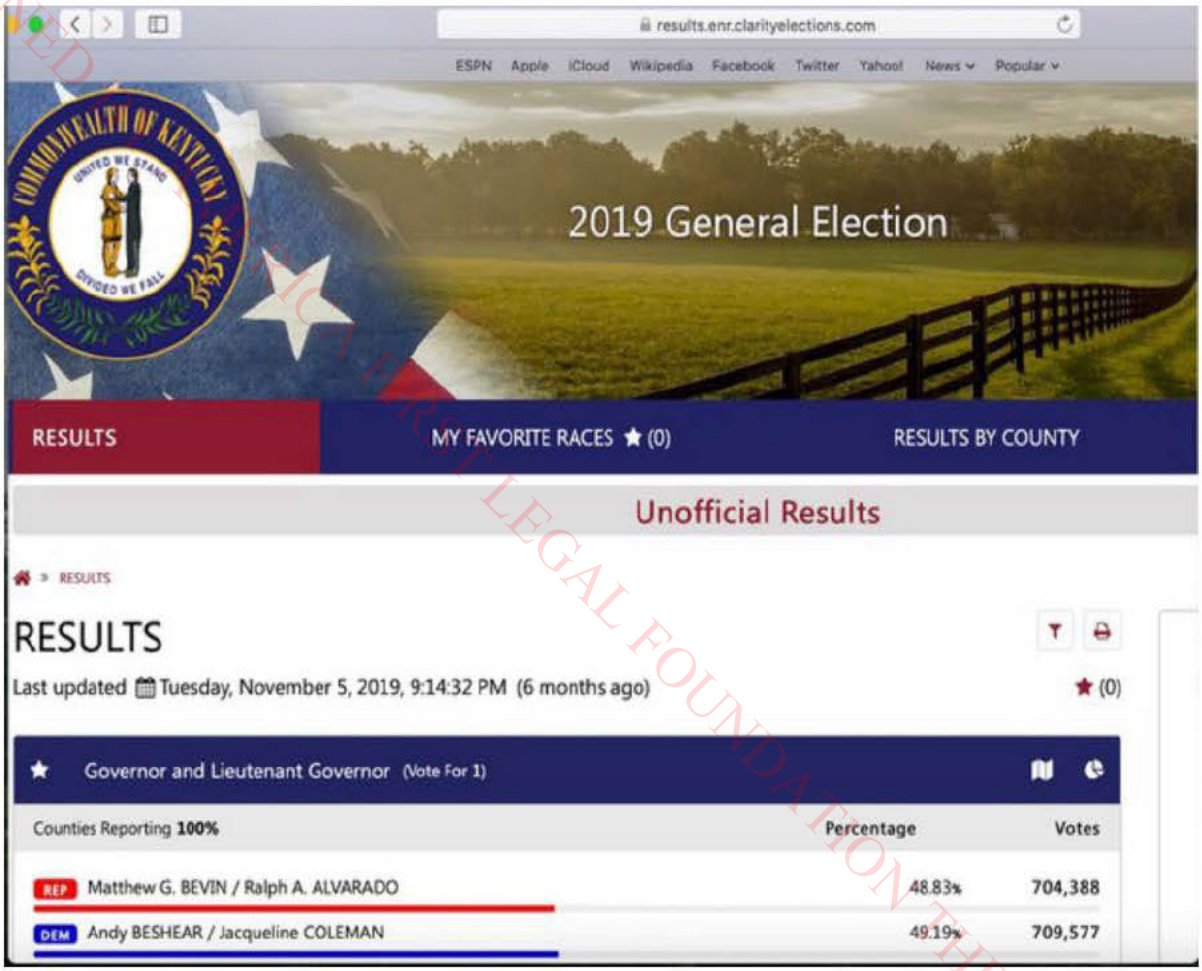
DHS-1255-003085 04/25/2024

The "unofficial results" are then made public through companies like Clarity Elections, which is the U.S. division of the Barcelona, Spain-based company Scytl.

The company proudly states on its website that it has "successfully delivered election modernization projects in the US since 2008, and most recently for the 2018 Midterm Elections, when over 70 [million] voters from more than 900 U.S. counties successfully leveraged Scytl's technology."

Kentucky is one of its customers, which can be seen in the election results from last fall's gubernatorial race between Democrat Andy Beshear and then-Republican incumbent Matt Bevin.

Beshear edged out Bevin by less than a percentage point.



OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

DHS-1255-003086 04/25/2024

According to Hursti, one of the problems with the relatively new trend of private companies running elections is the inability of election officials to provide adequate oversight.

"The election services company tells how the show is run," he said, pointing out that those overseeing the election are often elected officials themselves, who may have very little or no IT expertise.

Nonetheless, he said, "the elected official, who does not know what is going on, is legally responsible" for the overall election results.

There would seem to be a perverse incentive if a hack were discovered by the private company not to report it or the extent of it to election officials, so as to not hurt the company's reputation and its potential opportunity to run future contests.

At the same time, the motivation is high for hostile actors (whether they be foreign powers, or political or business interests) to try to rig the outcome for their favored candidates or to simply sow seeds of distrust in the election process.

For his documentary "Kill Chain," Hursti traveled to Juneau, Alaska, to investigate the hacking of the state's Division of Election's website on election night in November 2016.

The Associated Press reported that election officials determined the India-based hacker did not manipulate any information.

Hursti believes — based on a review of documents obtained by a Freedom of Information Act request — the truth in terms of the extent of the breach was "likely ... clearly worse" than what the officials admitted.

"There was no containment in effect," he said in the documentary.

He then went to India to speak with the hacker, known as CyberZeist, who took credit for the breach.

"I had root access, which just not only allowed me access to make small changes, but granted me full access of the system," including the real-time data to the presidential race, the hacker said.

"I could have made any changes in the system," he added. "I could alter any data, any vote."

CyberZeist chose not to out of fear of being caught, recounting that he reasoned, "Do not edit anything. Just see what is going on. Then we can plan or take out or execute our next steps."

Hursti thinks the hacker likely deployed a cyber tool in the Alaska Division of Elections website.

CyberZeist told the documentarian that Russian interests are seeking to scan state election servers throughout the United States.

The AP reported in September 2017 that the Department of Homeland Security notified 21 states that attempts had been made to hack their election systems during 2016 election cycle.

Among those hit were the key battleground states of Florida, Ohio, Pennsylvania, Virginia and Wisconsin.

Ramsland explained that cyberattackers, whether they are working for the Russian government or some other entity, would likely just need to focus their efforts on a few key states like these to change the outcome of the 2020 presidential race.

"So if you want to change the presidency of this country, all you really have to do is put your whole team on making sure that your guy wins precinct by precinct in at least a semi-believable number in five states and probably only the big metropolitan areas of five states," he said.

Republican Sen. James Lankford of Oklahoma is among the bipartisan supporters of some key election reforms, most importantly the ability to verify the results of a contest.

Last summer, Lankford spoke out in opposition to Democratic Sen. Amy Klobuchar's "Election Security Act" on the grounds that it contained a partisan provision, but agreed with her on the importance of paper ballots and other cyber protection measures.

"Every state, every precinct, should be able to verify [an election], to be able to go to back to the people in their area and to say, 'This is how you voted, and this is how we verified the number is accurate.'"

"It's not just about the voting machine, or it's not just about the piece of paper," he added. "It's how it's counted, how it's presented, how the unofficial results even go out from the state the night of the election. All those things matter."

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

DHS-1255-003087 04/25/2024

"Every state should have a system with a backup paper ballot," Lankford said. "Every state, every precinct. Right now, that's not so."

Hursti and Ramsland agreed that human readable paper ballots must be required.

Some states and precincts use voting machines that generate paper ballots with barcodes, which of course are not human readable and therefore subject to manipulation.

This is true even if the ballot shows in writing the candidates chosen because what the barcode says is what is counted.

The experts also called for risk-limiting audits of election results, regardless of how large the margin of victory.

Such audits are conducted by randomly doing a hand recount of paper ballots until a preset statistical measure of certainty is achieved when the reviewers can conclude the computer-tabulated election results reflect the actual votes cast.

"Elections are an American event," Lankford observed. "They have partisan results, but the act of voting is an American event."

"Election security should never be a partisan issue," he went on to state.

"This is about the preservation of our democracy, and it's something both parties — in fact independents, Republicans, Democrats, all parties — agree, that this should be a central issue for us."

We are committed to truth and accuracy in all of our journalism. Read our editorial standards.

OBTAINED BY AMERICA FIRST LEGAL FOUNDATION THROUGH LITIGATION

DHS-1255-003088 04/25/2024