What Went Right: Addressing Claims of Widespread Voter Fraud in One of the Most Secure Elections in American History

January 19, 2021

ABA Standing Committee on Election Law & ABA Cybersecurity Legal Task Force

Benjamin E. Griffith

"Someone struggled for your right to vote. Use it."

~Susan B. Anthony

Introduction

We count the right to vote as one of the most sacred rights of our democracy. It uniquely defines us as Americans. As Susan B. Anthony made clear by her actions, words and sheer force of will, the American struggle to achieve the right to vote has been hard fought and cherished throughout our nation's history. Elections at the federal, state and local level give voice to this right through the ballot. Elections that count each vote celebrate and secure this cherished right. These principles are the bedrock of American democracy and are woven into the fabric of this country. That said, the 2020 election has provided a startling reminder of the fragility of democracy and how close our nation came to a repeat in 2020 of the nation-state interference in the 2016 electoral process.

This presentation is based on the inseparable nature of election security and election administration. Our intent is to show how those state and local election officials charged with the conduct of the electoral process got it right in 2020. They did so notwithstanding our close encounter with the political cowardice of electoral McCarthyism and its threat to political fair play and fundamental democratic principles.

As we survey the electoral process more than two months after the November 3, 2020 presidential election, we are more than ever able to assure the voters that the

election was largely free of the anticipated cyber and technical issues that plagued even the 2020 primary elections this Spring, and indeed was one of the most secure elections in our history. See EFF Open Letter on Election Security, *Elections are Partisan Affairs. Election Security Isn't*. https://www.eff.org/deeplinks/2020/11/elections-are-partisan-affairs-election-security-isnt

Emerging from an adjudication of over 60 election challenges and contests filed and litigated mostly in the battleground states, we can see what went right in the 2020 Presidential Election from the standpoint of cybersecurity, technological preparedness and fairness. Indeed, many lessons have been learned in the election's aftermath, and a key role in underscoring those lessons was played by the Cybersecurity and Infrastructure Security Agency (CISA) before, during and after the election.

Lessons Learned in and after 2016

To fully appreciate the lessons learned in the 2020 election and how they did not emerge in a vacuum, go back to 2016, when the Russian Federation attempted to advance its candidate of choice and to corrode public faith in American democracy through cyberattacks and a coordinated disinformation campaign that put our country on its heels. In the run-up to the 2020 election, CISA's mission included protecting the American public from both disinformation warfare and cyberattacks from foreign and domestic sources.

There were also U.S. election security concerns both prior to and in the aftermath of the 2016 election that focused in part on digital recording electronic voting machines (DREs) declared by the U.S. Department of Homeland Security to be a "national security concern" and, according to the U.S. Senate Select Committee on Intelligence, "at highest risk of security flaws." *Curling v. Raffensperger*, 403 F. Supp. 3rd 1311 (N.D. Ga. 2019) ("national security experts and cybersecurity experts at the highest levels of our nation's government and institutions have weighed in on the specific issue of DRE systems in upcoming elections and found them to be highly vulnerable to interference, particularly in the absence of any paper ballot audit trail."). See generally *Stein v. Boockvar*, 2020 U.S. Dist. LEXIS 75476 (E.D. Pa. April 29, 2020) (noting Pennsylvania's decision to replace its aging voting equipment with modern machines including a voter-verifiable paper record, as part of a "national movement away from Direct Recording Electronic voting machines (DREs) that record votes only electronically"), and *Shelby Advocates for Valid Elections v. Hargett*, 947 F. 3rd 977 (6th Cir. 2020) (challenging county's use of digital voting machines which, when connected to the internet, were allegedly vulnerable to hacking and cyberattacks, sometimes "flipping" voters, recording a vote cast for candidate A as a vote for candidate B due to programming or

maintenance problems; the court of appeals found that future vote flipping was not shown to be certainly imminent and that plaintiffs had not "plausibly shown that there was a substantial risk of vote-flipping").

While no election will ever be conducted perfectly in every respect, the 2020 election was carried out successfully in all 50 states and territories because (1) a multitude of trained, dedicated and competent election personnel did their job, (2) the nation's independent judiciary applied the rule of law in deciding each challenge, and (3) CISA in collaboration with the FBI and other federal agencies, technology companies, state and local election agencies and officials, and the private sector, helped safeguard the election from a cybersecurity standpoint through planning, coordination, practice, and implementation.

The judicial process worked following the 2020 presidential election despite an unprecedented hyper-partisan environment, as judge after judge eschewed speculation and conjecture and insisted on being presented with facts. The scores of opinions and rulings provided a resounding reaffirmation of the judiciary's nonpartisan commitment to basic principles of reason, fact, and law. Some of those opinions were short and to the point, while others were sweeping defenses of American democracy. The judiciary grounded each decision on actual, provable facts, established legal principles of election law and evidence that confirmed the security and integrity of our electoral process, and consistently applied the procedural and substantive law each time.

Finally, it is illuminating to assess the many pre-election cybersecurity concerns, post-election audits and recounts, and implications for best practices with respect to election security, resilient voting systems that were not compromised, technological security of the electoral process, absence of evidence of systemic fraud that would have changed the outcome, absence of successful cyberthreats or state-sponsored hackers, and specific attributes of what the former Director of CISA called the most secure election in American history.

Releasing the Kraken

The much-touted Kraken[1] was unleashed by the incumbent President's "elite strike force team", led at the time by former Trump counsel Sidney Powell. Its tentacles were lobbed off one at a time. Powell was not horsing around when she announced in a post-election Fox Business interview with Lou Dobbs that "I'm going to release the Kraken."

In her invocation of the legendary sea monster from ancient Norse mythology, it may be that Powell was referring to some illusory mountain of evidence that provided factual and legal support for her claim that Joe Biden stole the Presidential Election through massive fraud, involving possibly thousands if not

millions of illegal votes- evidence that could survive a Rule 11 challenge, perhaps. There was a little problem with the Kraken invoked by Powell, however: there was not such evidence.

Instead, the courts and the American public were inundated with baseless claims of widespread voting irregularities and rampant voter fraud, false conspiracy claims of election fraud, and post-election claims of a "rigged" election propagated by the loser of the 2020 presidential election. These continued assaults on the outcome of the election, even after the Electoral College vote cemented Joe Biden's and Kamala Harris' victory as President and Vice-President, are assaults on democracy and are ultimately corrosive to the institutions that support elections.

Pre-election cybersecurity concerns

Specific pre-election cybersecurity concerns were addressed in the run-up to the 2020 presidential election. See Braun, *A Perfect Storm of Vulnerabilities Could Determine the 2020 Election*. http://bostonreview.net/politics-law-justice/jake-braun-perfect-storm-vulnerabilities-could-determine-2020-election
The following are among the most significant.

1. **Election Security**: In the three years leading up to the November 3, 2020 election, election security and the integrity of the electoral process were the focus of CISA's work. Relationships between federal agencies and state and local election officials were restored. The security and resilience of election systems were improved by phasing out the use of voting machines that did not leave an auditable paper trail. Federal agencies collaborated better and faster with each other and with their state and local counterparts.

   Defensive Strategy
   Securing the systems for U.S. elections in 2020 was a multi-layered defensive strategy. Those layers included pre-election testing, risk-limited audits, certification of voting equipment, ballot handling procedures and election process control. States had ballot processing and tabulation safeguards designed to ensure that each ballot cast in the election could be correctly counted, with robust chain-of-custody procedures, auditable logging requirements, and canvass processes.

   Security Measures Used
   These security measures were available and used by election officials to check and verify that votes are accurately accounted for during processing and counting. CISA's **Official Rumor Control Website**, **#Protect2020 Rumor v. Reality** at 1/15, https://www.cisa.gov/rumorcontrol.
   As noted above, the focus of efforts on the part of governmental and private sector collaborators was on countering or repelling disinformation and

cyberattacks. CISA undertook massive efforts to protect the U.S. election infrastructure, making securing the presidential elections in 2020 a priority. There was high motivation to avoid a repeat of the cybersecurity problems that beset the 2016 elections and to an extent the 2018 elections with the threat of foreign malign interference.

Lines of Communication Established
Good lines of communication were established well before election day among the federal government, state and local election officials, technology companies, and other players in the private sector, leading to effective collaboration.

Planning, Practice and Implementation
The key to successfully safeguarding the 2020 election from a cybersecurity standpoint was very effective planning, practice, and implementation. CISA's 24/7 **Virtual War Room,**
https://www.washingtonpost.com/nation/2020/10/30/dhs-is-planning-largest-ever-operation-secure-us-election-against-hacking/
enabled election officials to rapidly report and address potential cybersecurity threats in real time. Beyond our borders, U.S. Cybercommand officials sent teams across the globe to identify and undermine foreign hacking groups ahead of the election, following a strategy of "defending forward" and persistent engagement.

Joint Working Group of GCC and SCC
A Joint Working Group of The Election Infrastructure Subsector's Government Coordinating Council (GCC) and the Sector Coordinating Council (SCC) includes voluntary tools for state and local election officials to assess risk, secure their systems, and respond to any cyber-related incidents involving their election systems.

Available Tools for Risk Assessment, Security and Response
Some of those tools CISA made available include: (a) estimating the number of ballot drop boxes, which are deployed in support of increased mail voting and vote-by-mail, that would be needed, and establishing norms for security and chain of custody for these drop boxes; (b) providing election education and outreach for increased absentee or mail voting to educate legislators, policymakers, parties, campaigns, and advocacy groups on absentee voting or voting by mail; and (c) establishing standards for electronic ballot delivery and marking to help jurisdictions determine whether expanded election ballot delivery and marking options were appropriate for them. Other measures and assistance provided by the Joint Working Group included helping voters request mail-in ballots and apprising them of the application process for requesting same, emphasizing the importance of accurate voter

data when expanding absentee or mail ballot voting and risks associated with inaccurate voter records and secure voter registration data, , and processing of increased volume of inbound mail ballots, managing an increase in outbound ballots, working with vendors, the USPS, and others to handle an increased volume of outgoing mail ballots, signature verification and cure process to remedy rejected mail ballots, vote-by-mail, and establishing absentee voting timelines, with lead times required for states to consider when implementing processes to support significant increases in mail-in voting.

2. **Voting Systems Not Compromised**: The Election Infrastructure Government Coordinating Council and its Executive Committees in a Joint Statement released November 12, 2020 confirmed that "the November 3rd election was the most secure in American history" and that "there is no evidence that any voting system deleted or lost votes, changed votes or was in any way compromised."

   Testing and Certification
   Voting systems undergo hardware and software testing to assure consistency with state and federal requirements, including certification testing by a state- or federally certified testing laboratory. Logic and accuracy testing before the systems are deployed that entail a review of a system's source code along with environmental, security, and functional testing, and these are backed by post-election audits that ensured the proper functioning of the voting equipment.

   Enhanced Public Communication
   From a transparency and public communication standpoint, CISA significantly enhanced its communication links before and after the November 3, 2020 election to spread awareness of potential threats, suspicious activity, and election disinformation, a task that was made all the more difficult in light of the main purveyor of that disinformation being the President of the United States and his enablers. Amazingly, no voter fraud, massive or otherwise, and no significant voting irregularities that would have altered the outcome of the election were witnessed by international election observers from the Organization of American States or by international election monitors from the OSCE. The OAS sent 28 international election observers to witness the 2020 U.S. general election, and the observers reported on November 6, 2020 that they witnessed no instances of fraud or voting irregularities. http://www.oas.org/documents/eng/press/Preliminary-Report-of-the-OAS-EOM-USA-2020.pdf

   The OAS report contradicts claims from Donald John Trump and his enablers pushing baseless allegations of widespread election fraud. Trump enablers

nonetheless launched dozes of legal challenges while Trump has refused to concede. The OAS report followed another report from the Organization for Security and Co-operation in Europe that the U.S. election was "well managed" and that Trump's baseless claims "harm public trust in democratic institutions." https://www.businessinsider.com/international-observers-say-no-voter-fraud-us-election-oas-2020-11

With respect to audits done by state officials, which entails officials taking part of their paper ballots and matching them against electronic machine voting results to detect errors or potential instances of fraud or irregularities, Trump and his Republican enablers called for post-election audits in states where Trump was the loser, despite having the results of audits already completed. This is a sampling of the completed post-election audits.

Arizona: In Arizona, the state Republican Party asked for a new hand count of a sample of ballots in Maricopa County, where most of the state population lives, for the avowed purpose of seeing if voting machines were hacked, despite no evidence of fraud or hacking of voting machines in Arizona. Maricopa County had already completed its own audit, finding no problems following a hand-count.

Georgia: Georgia election officials conducted a high-profile audit of the Presidential race as required by state law that mandated an audit of any once race after every election. The audit was not in response to any suspected problems, and a hand tally of 5 million votes was conducted and revealed so significant problems or irregularities. Georgia Secretary of State Brad Raffensperger chose to audit the Presidential race because of its significance and because of the tight margin between Trump and the winner, Joe Biden.

Michigan: In Michigan, when two Republican election board members of the district that includes Detroit voted to block a routine certification of the votes, citing discrepancies between the number of votes cast and the number of ballots given to voters who voted by mail or in person, their claim drew complaints of racism from Democrats and others. The Republican board members later reversed themselves following assurances that there would be an audit, which Secretary of State Jocelyn Benson said would be done in Wayne County and any other community with significant clerical errors.

Alaska: In Alaska, the Lt. Governor said he planned to seek an audit of votes cast on a statewide ballot initiative to eliminate party primaries. Without any evidence of serious irregularities and even though the voting machines had proved to be accurate during the primary, the Lt. Governor said he was seeking an audit because “so many people think our Dominion machines are faulty, and I think a lot of this is misinformation that’s coming from the

national level." Without factual substantiation, Trump and his enablers sought to cast doubt on the vote tabulation technology involving Dominion Voting Systems, amidst assertions about vote-switching and software issues. The hand audit did not change the outcome. It was done after the results were certified, and revealed that the state's new election system was more than 99% accurate in counting the votes for the ballot initiative. https://apnews.com/article/election-2020-donald-trump-technology-elections-voting-f42170f9ca455058049bf9854c99e60b

3. **Technologically Secure Election**: As attested in an Open Letter on Election Security signed November 16, 2020 by 59 election security experts, the 2020 Presidential Election was technologically secure. https://www.mattblaze.org/papers/election2020.pdf

   Safeguards to Ensure Accuracy
   Many safeguards help election officials ensure the accuracy of election results through measures that help ensure tabulation systems function as intended , as well as verification of vote tallies before results are officially certified, using auditable logs, canvass processes, and certification procedures that are generally conducted in the public eye with political party representatives and other observers allowed to be present, including a bipartisan hand count of paper ballots.

   Coordination of Federal Efforts
   CISA's federal election protection efforts were coordinated with state and local election officials responsible to the operation and administration of over 8000 election jurisdictions across America. As CISA spearheaded those efforts, it facilitated planning and identification of potential vulnerabilities to election infrastructure before and during the election. CISA's efforts went beyond engaging election officials and included engaging political campaigns, political parties, and political committees at the national level.

   CISA's #Protect2020 Resources
   CISA also developed an extraordinary tool, **#Protect2020 Resources,** https://www.cisa.gov/nrmc-resources,
   to combat disinformation by equipping election officials, stakeholders and voters with information on mail-in voting, and election and post-election result processes for each state and jurisdiction. This included the following array of resources: (a) a weekly updated mail-in voting process factors map that provided a visual of the staus of each state's mail-in ballot processing; (b) a mail-in voting 2020 policy changes map that provided a visual of election-related changes established in each state as a result of COVID-19; (c) a mail-in voting election integrity safeguards infographic that provided the

description and in-person equivalent for procedural and physical ballot safeguards; (d) a post-election process mapping infographic that provides a timeline of post-election processes for the presidential election from the close of the polls on election day, November 3, to Inauguration Day on January 20, 2021; (e) an election-result reporting risk and mitigation infographic that provides an overview of the risks associated with results reporting systems and how they are managed through mitigating measures.

4. **No Evidence of Systemic Fraud that would Change Outcome**: As then-Attorney General William Barr stated on December 1, 2020 "to date, we have not seen fraud on a scale that could have affected a different outcome in the election."

   No Substantiation of Systemic Fraud Claims
   Barr added that "there's been one assertion that would be systemic fraud and that would be the claim that machines were programmed essentially to skew the election results. And the DHS and DOJ have looked into that, and so far, we haven't seen anything to substantiate that." Specifically, state and federal laws prohibit voter impersonation and casting a ballot on behalf of a deceased person, and election integrity safeguards such as signature matching and information checks protect against voting by ineligible persons. Variations in vote totals for different contests on the same ballot occur in every election and by themselves do not indicate issues with voting technology of integrity of the election process.
   Ballot Security Measures
   Ballot security measures can include signature matching, information checks, barcodes, watermarks, and precise paper weights. While CISA had funded an independent third party to develop an open-source election auditing tool for voluntary use by state and local election officials, it does not audit elections and does not have access to the tool as states use it. Moreover, DHS and CISA operate in support of and assist states and local governments and election officials with securing election infrastructure, but they do not design, print, or audit ballots.

   CISA's Operation Rumor Control Website
   As the former Director of CISA noted in a December 15, 2020 CNN Op Ed, CISA developed an **Official Rumor Control Website, #Protect2020 Rumor v. Reality,** https://www.cisa.gov/protect2020**,**
   to counter perception hacks and to provide facts to help American voters make their own decisions by preempting disinformation campaigns and to protect the public from misleading disinformation before it could take root and become perceived as true. These measures were designed to counter

disinformation and at least partially succeeded in maintaining voter confidence and squelching false information.

Battlefield of Disinformation
Indeed, the 2020 election and post-election struggles right up to and beyond the Electoral College vote on December 8 were fought on the battlefield of disinformation. CISA joined forces with the FBI and through regional and centralized interagency cooperation, helped keep the American election system resilient against increasingly aggressive threats from foreign state actors and private domestic interests.

5. **Most Secure Election in American History**: Shortly before President Trump terminated Chris Krebs as Director of the Cybersecurity and Infrastructure Security Agency, Krebs repeatedly contradicted Trump and rejected Trump's multiple statements that the president was robbed of re-election by glitches in voting machines that changed votes from Trump to Biden and that there were millions of fraudulently cast votes. Krebs called those claims unfounded and asserted that "the November 3rd election was the most secure in American history," that all votes are counted in the U.S. and that no tabulation or accumulation of votes happens outside the U.S.

   A Different Election in 2020
   In this year of the COVID-19 pandemic, elections looked different, and ballot processing in some states took longer than in past years due to increases in mail-in ballot usage and process adaptations to make voting safer during the pandemic without impacting the accuracy of the counting process.

   Election Security Community Statement
   CISA joined an election security community statement on November 12, 2020 assuring Americans that there is no evidence that any voting system deleted or lost voted, changed votes, or was in any way compromised. Chris Krebs echoed this assessment (before and after he was fired by a Trump tweet), and emphasized that there was no evidence that states require that official results be certified on election night, and that election results reported on election night are always unofficial and are provided solely for voters' convenience.

   December 16 Testimony Before Senate Homeland Security and Governmental Affairs Committee
   As Krebs noted in his testimony before the Senate Homeland Security and Governmental Affairs Committee on December 16, 2020, continued unsupported assaults on democracy and the November 3 election outcome only serve to undermine confidence in the process and are corrosive to the institutions that support elections. During and after election night there can

be fluctuations in the reporting of official results as more ballots are processed and counted, often including military and overseas ballots and validated provisional ballots. Depending on variations in state processes, ballots cast through early in-person voting, mail-in voting, and election day voting may be counted and unofficially reported in different orders.

Persistent Onslaught of False Information

None of this indicates that there was a problem with the counting process or the trustworthiness of results, or that the process has been hacked or compromised. Nonetheless, the Trump campaign continued its onslaught of false information alleging systems interference where none occurred, ignoring the fact that 59 election and cybersecurity experts agreed in a public statement that the Trump campaign's claims of a "rigged" election either have been unsubstantiated or are technically incoherent. As Krebs concluded in his Senate committee testimony, "the trick about elections is that you're not so much trying to convince the winner that they won, it's the loser that they lost."

CISA Guidance

CISA provided a number of guides, announcements, toolkits and resources to address some of these problems: (a) a general guide, *Physical Security of Voting Locations and Election Facilities*, with four actionable steps – to connect, plan, train, and report – that election officials should consider to improve the physical security posture and enhance resilience of election operations in their jurisdictions; (b) an *Election Disinformation Toolkit* for election officials to emphasize their role as "trusted voices" for election information, and to spread the importance of "we're all in this together" in reducing the impacts of disinformation campaigns on the 2020 election; (c) *Spoofed Internet Domains Pose Cyber and Disinformation Risks to Voters*, a CISA and FBI announcement to help the public recognize and avoid spoofed election-related internet domains during the 2020 election; (d) *Foreign Actors Likely to Use Online Journals to Spread Disinformation Regarding 2020 Election*, an announcement by CISA to raise awareness of the potential threat posed by foreign-backed online journals that spread disinformation regarding the 2020 elections; (e) *DDoS Attacks on Election Infrastructure Can Hinder Access to Voting But Would Not Hinder Voting,* an announcement by CISA and the FBI to raise awareness that Distributed Denial of Service (DDoS) attacks on election infrastructure can hinder access to voting information but would not prevent voting; (f) *False Claims of Hacked Voter Information Likely Intended to Cast Doubt on the Legitimacy of U.S. Elections*, an announcement by CISA and the FBI to raise awareness of the potential threat posted by attempts to spread disinformation regarding cyberattacks on U.S. voter registrations databases or voting systems; (g) *Cyber Threats to Voting Processes Could Slow But Not Prevent Voting*, an

announcement by CISA and the FBI to inform the public that attempts by cyber actors to compromise election infrastructure could slow by not prevent voting; (h) A public service announcement by CISA and the FBI, *Foreign Actors and Cybercriminals likely to spread Disinformation Regarding the 2020 Election Results*, to raise awareness of the potential threat posed by attempts to spread disinformation regarding the results of the 2020 election; (i) *Cyber Incident Detection and Notification Planning Guide for Election Security*, made available by CISA as a voluntary tool to help jurisdictions effectively recognize and respond to potential cyber incidents; (j) *Foreign interference taxonomy infographic*, provided by CISA to describe the methodology and goals of foreign interference operations; (k) Disinformation Stops With You, an infographic provided by CISA with the following steps on how to lessen the impact of foreign influence operations:

i. *Think Before You Link*, which urges everyone to take a moment to investigate the source and content of provocative content before sharing it with others;
ii. *Talk to your Circle*, which helps people talk with their social circle about the risks of spreading disinformation;
iii. *Recognize the Risk*, which helps people understand how adversaries try to influence behavior;
iv. *Question the Source*, which helps people check for a diversity of credible sources, consider who produced the content, and question their intent;
v. *Investigate the Issue*, which highlights the importance of searching reliable sources before sharing a controversial or emotionally charged article, post, tweet, or meme, such as taking a few moments to investigate the issue to assure it is not amplifying disinformation.

6. **Absence of Successsful Cyberthreats or State-Sponsored Hackers**: In sharp contrast to the 2016 presidential election when the Russian government's "active measures" were unleashed in waves aimed at helping President Trump win office and at hurting his opponent, Hillary Clinton, four years of aggressive attention to cyber security made a difference.

Election Infrastructure Resilience

While the cyberattacks per se have never stopped, since 2016 CISA, DHS, the FBI and other agencies have worked to build new relationships and invent new practices to defend U.S. election infrastructure and make it more resilient. In this connection, there are three main ways in which the federal government has supported state and local efforts to enhance election infrastructure resiliency: sharing information about vulnerabilities and threats to election systems, providing technical assistance, playbooks, and exercises, and assisting state and local election officials in responding to cyber-related incidents targeting their election systems.

Iranian Spoof-Mail Intimidation Tactics

As a recent example, authorities took about 27 hours from the point at which they learned about Iranian spoof-email intimidation attacks to attributing them to announcing them in an unusual news conference with Director of National Intelligence John Ratcliffe and FBI Director Christopher Wray. That followed earlier declarations by Wray about the speed with which authorities now move in disrupting cyber-interference. The goal was to deny foreign spreaders of disinformation, removing their ability to try to gain credibility by building up a body of work on social networks or their own websites. When the FBI detected such a scheme that involved Facebook, the bureau acted as swiftly as possible to try to snuff it out.

No Major Disruption of Election by Cyberattacks

In 2020, our nation was able to go through the voting season without major disruption by cyberattacks or other malign activity. For example, problems with electronic pollbooks in a small number of places were quickly resolved when county leaders had paper records on which to fall back and they were able to keep voting underway. Preparedness was rewarded.

"Hunt Forward" Capability

American operatives went on the offense, with the cyber-troopers of U.S. Cyber Command, a division of the Defense Department, having the capability to "hunt forward" and surveil the work of Russian and other foreign cyber-operatives. That strategy helped American authorities identify the targets they had selected within the United States, take note of their practices and even study the malware they use to help bolster cyber-defenses at home.

Transparency and Disclosure

For reasons of national security, Cyber Command cannot disclose its efforts against Russian, Iranian, North Korean and other counterparts that were undertaken in the week ahead of Election Day and thereafter, but today, the new arrows in the quiver of American officials are transparency and disclosure. This is in sharp contrast to earlier stages in the cyber-game at a time when even local or state entities that had been victims of attacks were not necessarily plugged in and knowledgeable about what Washington knew.

Trust, Expertise, and Relationships

The much-anticipated cyber threats from Russia or other state-sponsored hackers never materialized. Despite unfounded claims the election machines provided by Colorado- and Canada-based Dominion Voting Systems switched hundreds of thousands of Trump voters to Biden and deleted large numbers

of Trump votes, despite a Trump retweet that Dominion Voting Systems was a "national security threat," and despite thoroughly debunked claims that Dominion is owned by Hugo Chavez, the long-deceased president of Venezuela, and that those machines were originally created to falsify election results in Venezuela for Chavez and then later for Nicolas Maduro, no evidence of these allegations or, indeed, any foreign interference was ever presented.

CISA defines Foreign Influence as malign actions taken by foreign governments to spread disinformation designed to manipulate the public, sow discord and ill will, discredit the electoral process, disrupt markets and undermine the interests of the American people. Through CISA's #Protect2020 outreach, CISA built on the trust, expertise, and relationships it developed to broaden its state and local cybersecurity risk management efforts. Some examples of efforts to include:

i.Spoofing Email Sender Addresses Cyber actors can forge or "spoof" email sender addresses to look like they came from someone else, as where attackers send an email pretending to be from a specific domain or organization in an attempt to harvest personally identifiable information, spread malware or ransomware, or disseminate false or inflammatory information;

ii. Trusted Source Communications

These are often detectable as out-of-the-ordinary emails, and while realistic looking, the better practice is to look to trusted source such as an organization's website for verification. Any suspicious election-related email should be reported to local election officials or the local FBI field office. One resource provided by CISA can be helpful in this regard, a *Social Media Bots Overview*, an infographic that examines the various types, uses and risks of social media bots;

iii.False Claims of Hacked Voter Information

A recent FBI and CISA public alert reported that cyber actors may make false claims of "hacked" voter information in order to undermine confidence in U.S. domestic institutions. If an online voter registration website experiences an outage, it may be and is most likely for non-malicious reasons, including configuration errors, hardware issues, natural disasters, communications infrastructure issues, and distributed denial of service (DDoS) attacks.

Compromise of Election-Related System and Vote Integrity

That said, some voter registration information is in the public domain and as public information it is available to political campaigns, researchers, and members of the public. While hacks of state and local IT systems should not

be minimized, a compromised local IT system does not mean an election-related system is involved, and even if an election-related system is compromised, it does not necessarily mean the integrity of the vote has been affected.

Multiple Safeguards

Election officials have multiple safeguards and contingencies in place to address these concerns and to limit impact from a cyber incident with minimal disruption to voting, including provisional ballots, backup paper poll books, and an auditable paper record that ensures the vote count can be verified and validated. Similarly, if voter registration data were to be manipulated, states have safeguards in place to enable voters to vote, including offline backups of registration data, provisional ballots, and in several states, same-day registration.

Solid Election Administration Based on Comprehensive and Coordinated Election Security

Given the extensive, thorough and meticulous implementation of a proactive strategy to avoid a repeat of the 2016 election problems, it is clear that many things were done correctly in 2020. While the election may not have been perfect in every respect, it was a secure one, both from the standpoint of a resilient system capable of withstanding foreign attack and an election system that could stand up to the demons of misinformation and disinformation flowing from the Administration. We close these remarks with observations by some of the federal and state court judges who confronted and correctly decided dozens of claims between the November 3 election day and the January 20 swearing in of Joe Biden as President of the United States. These judicial observations demonstrate how inseparable election administration really is from election security. They are opposite sides of the same coin.

Cases and Controversies

Federal courts under Article III of the Constitution may adjudicate only actual, ongoing cases or controversies. But when the issues presented are no longer live, the parties lack a legally cognizable interest in the outcome, or the court lacks the ability to give meaningful relief, it cannot go forward.

Trump's' "elite strike force team" was the 2020 version of the emperor who had no clothes. In its fanciful and almost universally failed election challenges, it had no evidentiary basis - no provable, supporting facts - the grist of any civil lawsuit.

Over 60 federal and state lawsuits later, including an original action filed by the State of Texas in the U.S. Supreme Court against four other states and summarily dismissed by the Court on December 11, 2020, all but one of the lawsuits have been dismissed for lack of evidence, laches, standing, mootness, or fatally defective pleadings. Sidney Powell's Kraken has been tamed, and its tentacles have been severed in Pennsylvania, Georgia, Wisconsin, Michigan, Arizona, Nevada and other jurisdictions in which Trump's "elite strike force team" filed and litigated their conspiratorial claims that thousands of voting systems had deleted or lost votes, changed votes or were compromised, and that foreign-sourced election machines from the late Venezuelan dictator Hugo Chavez switched hundreds of thousands, possibly millions, of votes from Trump to Biden.

Of the over 90 judges who handed down rulings, opinions, findings and decisions in over 60 lawsuits, let us take a quick look at what some of the judges in the battleground states had to say about the beehive of election challenges confronting them:

Michigan: As one U.S. District Court judge noted in assessing the thin proof offered in one of the Michigan challenges and why it was barred by mootness, "this ship has sailed." The plaintiffs in most instances were asking the courts to ignore the orderly statutory scheme established under state law to challenge elections. In this instance, the time had passed to provide most of the relief plaintiffs requested in their pleadings, and the remaining relief was beyond the power of any court. *King v. Whitmer*, 2020 U.S. Dist. LEXIS 228621, at *13 (E.D. Mich. 2020).

U.S. District Judge Linda V. Parker, in declining to grant relief in a suit seeking to throw out Michigan's election results, described the suit as "stunning in its scope and breathtaking in its reach," and found that "if granted, the relief would disenfranchise the votes of more than 5.5. million Michigan citizens who, with dignity, hope, and a promise of a voice, participated in the 2020 General Election." She noted "the right to vote is among the most sacred rights of our democracy and, in turn, uniquely defines us as Americans." She concluded that the task of selecting political leaders, especially the President of the United States, should fall to the voters, not judges, and in this case "the people have spoken." *King v. Whitmer*, 2020 U.S. Dist. LEXIS 228621 (E.D. Mich. 2020)

Pennsylvania: Several challenges filed in the keystone state were dismissed with pleadings that judges condemned as mere speculation and conjecture that votes for President Trump were destroyed, discarded, or switched to votes for Joe Biden. In dismissing one of the lawsuits in Pennsylvania that targeted a 2019 law allowing no-excuse absentee ballots in the state, the

court said the plaintiffs should have challenged the law well before the 2020 election rather than after millions of such votes had been cast.

U.S. District Judge Matthew Brann, in dismissing a challenge that sought to invalidate Pennsylvania's election results said the lawyers presented "strained legal arguments without merit and speculative accusations un-pled in the operative complaint and unsupported by evidence. In the United States of America, this cannot justify disenfranchisement of a single voters, let along all of the voters in its sixth most populated state. Our people, laws and institutions demand more." Judge Brann compared the Trump campaign's stitched-together legal theories as "Frankenstein's monster." *Trump v. Boockvar,* 2020 WL 6821992 (M.D. Pa. 2020).

Third Circuit Judge Stephanos Bibas, a Trump appointee, pointedly reminded members of the Trump elite strike force team that "voters, not lawyers, choose the president" and that "free, fair elections are the lifeblood of our democracy. Charges of unfairness are serious. But calling an election unfair does not make it so. Charges require specific allegations and then proof. We have neither here." *Trump v. Boockvar,* https://electioncases.osu.edu/wp-content/uploads/2020/11/Donald-J.-Trump-for-President-v-Boockvar-3rd-Cir-Doc6.pdf
(3rd Cir. Nov. 27, 2020)

Wisconsin: Wisconsin Supreme Court Judge Brian Hagedorn rejected a voters' group's request to invalidate the entire election as "unprecedented in American history" and said that the pleadings fell "far short of the kind of compelling evidence and legal support we would undoubtedly need to countenance the court-ordered disenfranchisement of every Wisconsin voter." Judge Hagedorn declined a challenge to overturn election results, stating that "something far more fundamental than the winner of Wisconsin's electoral votes is implicated in this case, and that "at stake, in some measure, is faith in our system of free and fair elections, a feature central to the enduring strength of our constitutional republic." He concluded that "once the door is opened to judicial invalidation of presidential election results, it will be awful hard to close that door again. This is a dangerous path we are being asked to tread." *Trump v. Biden*, 2020 Wi. 91 9 (Wi. 2020).

U.S. District Judge Pamela Pepper noted "Federal judges do not appoint the president in this country. One wonders why the plaintiffs came to federal court and asked a federal judge to do so." *Feehan v. Wisconsin Election Commission, https://www.courtlistener.com/docket/18702085/feehan-v-wisconsin-elections-commission/*
(E.D. Wi. 2020).

U.S. District Judge Brett H. Ludwig, a Trump appointee who took the bench in September 2020, dismissed a Trump challenge that sought to throw out the election results in Wisconsin, calling the request "extraordinary" and concluding that "[a] sitting president who did not prevail in his bid for reelection has asked for federal court help in setting aside this popular vote based on disputed issues of election administration, issues he plainly could have raised before the vote occurred." Judge Ludwig ruled "This court has allowed the plaintiff the chance to make his case and he has lost on the merits." He added that Trump asked for the rule of law to be followed, and "it has been." *Trump v. Wisconsin Election Commission,* *https://www.courtlistener.com/docket/18710035/trump-v-the-wisconsin-elections-commission/*
(E.D. Wi. 12-12-20).

Georgia: U.S. District Judge Steven D. Grimberg, a recent Trump appointee, turned away Trump's attempt to block certification of Joe Biden's win in Georgia, noting that it "would breed confusion and potentially disenfranchisement that I find has no basis in fact or in law." *Wood v. Raffensperger, https://www.courtlistener.com/docket/18760576/wood-v-raffensperger/*
(N.D. Ga. 11-20-20).

Nevada: First Judicial District Court Judge James T. Russell ruled that the Trump campaign "did not prove under any standard of proof that illegal votes were cast and counted, or legal votes were not counted at all, due to voter fraud, nor in an amount equal to or greater" that Joe Biden margin in Nevada. Witness statements submitted by the Trump campaign were "self-serving statements of little or no evidentiary value", its proposed expert testimony "was of little to no value," and a claim of ballot-stuffing in broad daylight asserted by an anonymous witness with no corroboration was "not credible." *Law v. Whitmer,* *https://www.leagle.com/decision/innvco20201209323*
(1st Jud. Dist. Ct. of State of Nevada, Carson City 12-4-20)

Arizona: U.S. District Judge Diane J. Humetewa evaluated voter fraud complaints from Sidney Powell and concluded "allegations that find favor in the public sphere of gossip and innuendo cannot be a substitute for earnest pleadings and procedure in federal court. Plaintiffs have not moved the needle for their fraud theory from conceivable to plausible, which they must do to state a claim under Federal pleading standards." *Bowyer v. Ducey*, https://electioncases.osu.edu/wp-content/uploads/2020/12/Bowyer-v-Ducey-Doc84.pdf#:~:text=In%20that%20case%2C%20on%20December%208%2C%202020%2C%20the,evidence%20of%20fraud%20or%20misconduct%20in%20Arizona%E2%80%99s%20election

(D. Az. 12-9-20).

CONCLUSION

Election security is inextricably linked to election administration. Those thousands of state and local election officials who devoted their best efforts to assure that the electoral process was efficiently, correctly, and properly conducted did their jobs and did what they were trained to do. They got it right in 2020.

---

[1] The Kraken had a taste for human flesh and would start swimming in circles around a ship, creating a fierce maelstrom to drag the vessel down as it swallowed the entire crew. Alfred Lord Tennyson introduced us to the Kraken as a mythological sea monster closely linked to sailors' ability to tell tall tales:

Below the thunders of the upper deep,
Far, far beneath in the abysmal sea,
His ancient, dreamless, uninvaded sleep
The Kraken sleepeth: faintest sunlights flee
About his shadowy sides; above him swell
Huge sponges of millenial growth and height;
And far away into the sickly light,
From many a wondrous grot and secret cell
Unnumber'd and enormous polypi
Winnow with giant arms the slumbering green.
There hath he lain for ages, and will lie
Battening upon huge sea-worms in his sleep,
Until the latter fire shall heat the deep;
Then once by man and angels to be seen,
In roaring he shall rise and on the surface die.