FBI & CISA Warn American Voters: You Won't Get 2024 Election Results!

The FBI & CISA are telling you that “bad actors” will attack our voting systems — and these attacks will be successful.

EMERALD ROBINSON
AUG 02, 2024

♡ 345 41 Share

The Right Way **is the #1 conservative blog on Substack — recommended by over 274 other Substack authors!**

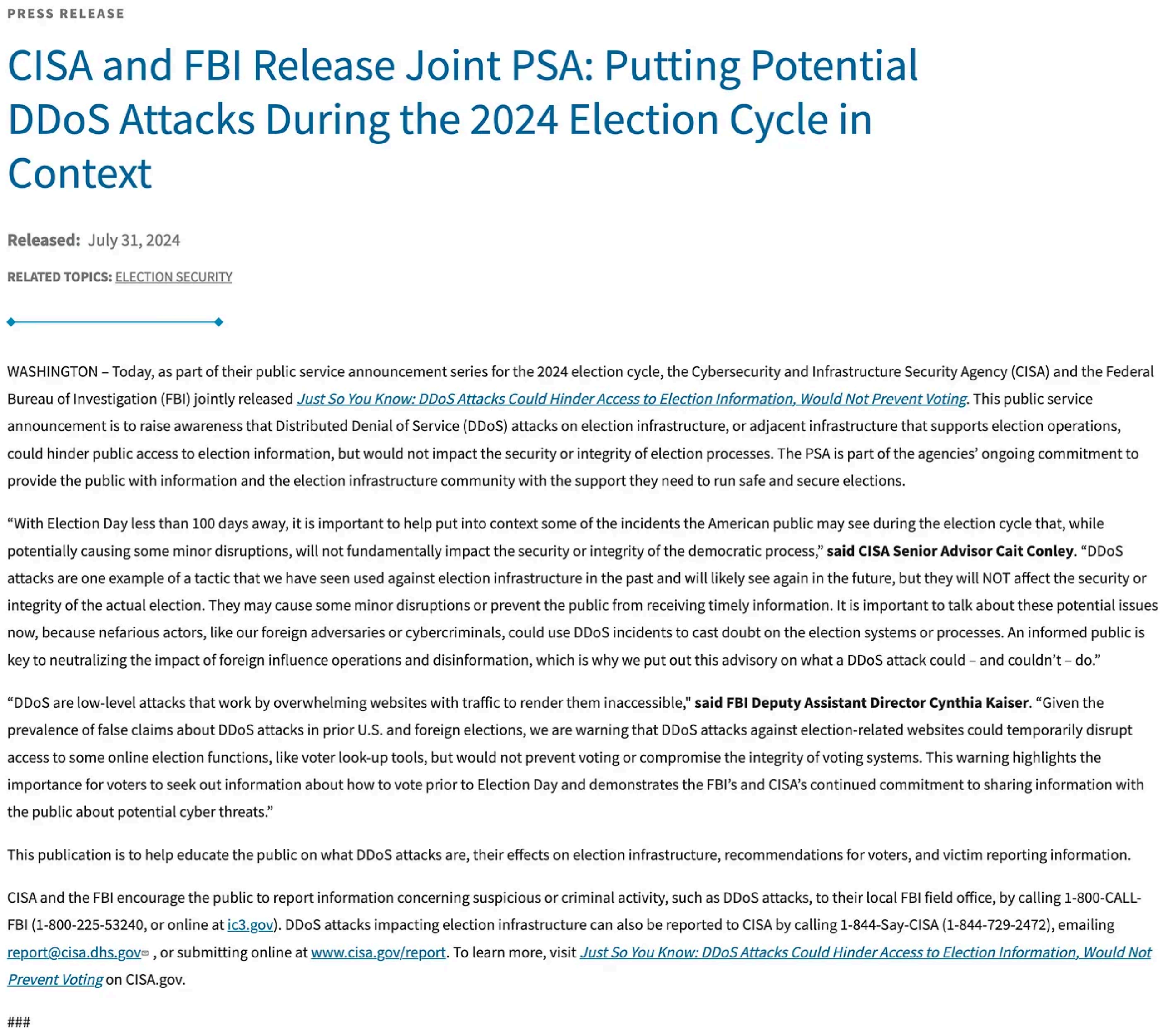
The FBI and CISA (the cybersecurity unit inside DHS) have issued a joint statement just 94 days before the 2024 election.

Are they telling you that America’s voting systems are secure and ready for the 2024 election?

No.

Are they telling you that America’s voting systems are *vulnerable* and *not secure* before the 2024 election?

Yes.



PRESS RELEASE

CISA and FBI Release Joint PSA: Putting Potential DDoS Attacks During the 2024 Election Cycle in Context

Released: July 31, 2024

RELATED TOPICS: ELECTION SECURITY

WASHINGTON – Today, as part of their public service announcement series for the 2024 election cycle, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) jointly released *Just So You Know: DDoS Attacks Could Hinder Access to Election Information, Would Not Prevent Voting*. This public service announcement is to raise awareness that Distributed Denial of Service (DDoS) attacks on election infrastructure, or adjacent infrastructure that supports election operations, could hinder public access to election information, but would not impact the security or integrity of election processes. The PSA is part of the agencies' ongoing commitment to provide the public with information and the election infrastructure community with the support they need to run safe and secure elections.

"With Election Day less than 100 days away, it is important to help put into context some of the incidents the American public may see during the election cycle that, while potentially causing some minor disruptions, will not fundamentally impact the security or integrity of the democratic process," **said CISA Senior Advisor Cait Conley**. "DDoS attacks are one example of a tactic that we have seen used against election infrastructure in the past and will likely see again in the future, but they will NOT affect the security or integrity of the actual election. They may cause some minor disruptions or prevent the public from receiving timely information. It is important to talk about these potential issues now, because nefarious actors, like our foreign adversaries or cybercriminals, could use DDoS incidents to cast doubt on the election systems or processes. An informed public is key to neutralizing the impact of foreign influence operations and disinformation, which is why we put out this advisory on what a DDoS attack could – and couldn't – do."

"DDoS are low-level attacks that work by overwhelming websites with traffic to render them inaccessible," **said FBI Deputy Assistant Director Cynthia Kaiser**. "Given the prevalence of false claims about DDoS attacks in prior U.S. and foreign elections, we are warning that DDoS attacks against election-related websites could temporarily disrupt access to some online election functions, like voter look-up tools, but would not prevent voting or compromise the integrity of voting systems. This warning highlights the importance for voters to seek out information about how to vote prior to Election Day and demonstrates the FBI's and CISA's continued commitment to sharing information with the public about potential cyber threats."

This publication is to help educate the public on what DDoS attacks are, their effects on election infrastructure, recommendations for voters, and victim reporting information.

CISA and the FBI encourage the public to report information concerning suspicious or criminal activity, such as DDoS attacks, to their local FBI field office, by calling 1-800-CALL-FBI (1-800-225-53240, or online at ic3.gov). DDoS attacks impacting election infrastructure can also be reported to CISA by calling 1-844-Say-CISA (1-844-729-2472), emailing report@cisa.dhs.gov , or submitting online at www.cisa.gov/report. To learn more, visit *Just So You Know: DDoS Attacks Could Hinder Access to Election Information, Would Not Prevent Voting* on CISA.gov.

###

Here's the key point:

This public service announcement is to raise awareness that Distributed Denial of Service (DDoS) attacks on election infrastructure, or adjacent infrastructure that supports election operations, could hinder public access to election information, but would not impact the security or integrity of election processes.

The FBI and CISA are telling you that "bad actors" will attack our voting systems —and these attacks will be successful!

How? Well, the American public will not have "public access to election information."

Allow me to translate the language of *bureaucratese* into plain English: you won't get election results on time.

This is the moment when I remind you: CISA's role is supposedly to safeguard our election systems so that the American public has *access to election results.*

Instead, CISA is sending out bulletins that it has already failed.

CISA cannot safeguard our election systems.

This bulletin is simply an admission that CISA won't be able to do its job — but the American public should not be too worried or upset about it.

You see: you won't get election results on time in the coming election (94 days away!) but that doesn't "impact the security or integrity of election processes."

Failure is actually success at CISA!

Get a load of the next paragraph:

They may cause some minor disruptions or prevent the public from receiving timely information. It is important to talk about these potential issues now, because nefarious actors, like our foreign adversaries or cybercriminals, could use DDoS incidents to cast doubt on the election systems or processes. An informed public is key to neutralizing the impact of foreign influence operations and disinformation, which is why we put out this advisory on what a DDoS attack could – and couldn't – do."

Is preventing the public from receiving timely information during the 2024 election considered to be a *minor disruption* by CISA?

Because I've got news for you: *that's the mother of all major disruptions.*

A link in this bulletin leads the reader to an additional page (image below).

Public Service Announcement

FBI & CISA

Alert Number: I-073124-PSA

July 31, 2024

Just So You Know: DDoS Attacks Could Hinder Access to Election Information, Would Not Prevent Voting

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are issuing this announcement to raise awareness that Distributed Denial of Service (DDoS) attacks on election infrastructure, or adjacent infrastructure that support election operations, could hinder public access to election information but would not impact the security or integrity of election processes.

These low-level attacks, which are expected to continue as we approach the 2024 U.S. general election, could disrupt the availability of some election-related functions, like voter look-up tools or unofficial election night reporting, during the election cycle but will not impact voting itself. Threat actors may falsely claim that DDoS attacks are indicative of a compromise related to the elections process as they seek to undermine confidence in U.S. elections. In recent years, DDoS attacks have been a popular tactic used by hacktivists and cyber criminals seeking to advance a social, political, or ideological cause.

DDoS attacks occur when malicious cyber actors flood a public-facing, internet-accessible server with requests, rendering the targeted server slow or inaccessible. This temporarily prevents legitimate users from accessing online information or resources, such as web pages and online services, and may disrupt business activities for a period of time. Specific to elections, DDoS attacks targeting election infrastructure could prevent a voter from accessing websites containing information about where and how to vote, online election services like voter registration, or unofficial election results.

In the event that foreign actors or cyber criminals conduct DDoS attacks against election infrastructure or other infrastructure supporting election administration, the underlying data and internal systems would remain uncompromised, and anyone eligible to vote would still be able to cast a ballot. In the past, cyber actors have falsely claimed DDoS attacks have compromised the integrity of voting systems to mislead the public that their attack would prevent a voter from casting a ballot or change votes already cast. The FBI and CISA have no reporting to suggest a DDoS attack has ever prevented an eligible voter from casting a ballot, compromised the integrity of any ballots cast, or disrupted the ability to tabulate votes or transmit election results in a timely manner.

In addition to direct communication channels such as official websites, election offices across the country have identified alternative channels to disseminate information to voters, such as traditional news outlets, direct messaging to voters, and other backup resources. Election officials have multiple safeguards, backup processes, and incident response plans to limit the impact of and recover from a DDoS incident with minimal disruption to election operations.

Since you lived through the rigged 2020 election, you know exactly what's happening.

The Biden regime is *pre-seeding the narrative* that a disrupted 2024 election is "no big deal" because they're going to steal it from President Trump.

Again.

Support My Substack Sponsors!

Get *10% off* a box of limited edition Trump 2024 Victory cigars by using this coupon code at checkout: **emerald2024**

My favorite skin care products are called: Organic Body Essentials. I love the Extreme Day & Night Face Cream and the Flawless Face Serum and all the rest of the items in the Luxury Face Package. You will get a 5% discount if you use my link.

If you got vaccinated with the mRNA gene therapies, then you programmed your immune system to produce spike proteins. The problem is that spike proteins are toxic — so *you want to degrade* those spike proteins in your body.

The Wellness Company has formulated a supplement that contains nattokinase and it's called: Spike Support. Use coupon code **EMERALD** at checkout for the discount.

345 Likes · 72 Restacks

41 Comments

Write a comment...

Daniel R. Street Daniel R. Street's Fake News Ex... Aug 2

Everyone on planet earth knows the FBI is corrupt, but few people in the USA are even aware of CISA. CISA was a major part of the misinformation and propaganda campaigns surrounding the 2020 election. It literally originated the MASSIVE LIE that the 2020 election was the "most secure in history" in a press release on November 12, 2020. Despite the fact this statement was absolute BS when it was made, multiple security warnings from CISA about various 2020 election hardware and software system vulnerabilities (including vulnerabilities involving Dominion Voting Systems) since the election have not caused these hacks to walk back that false statement.

Yeah, the FBI and CISA "safeguarding" our elections is the "fox guarding the hen house." Make no mistake.

♡ LIKE (47) REPLY SHARE ...

1 reply

BTeboe Aug 2

Time to ditch the machines. If they are so vulnerable perhaps they should not use them. Paper ballots, sequentially numbered (like money), filled out in ink and counted by hand. Secure election! Not hard to do. Maybe even dip the finger in purple ink so people aren't tempted to do it again.

♡ LIKE (40) REPLY SHARE ...

2 replies

39 more comments...