ELECTION RESEARCH INSTITUTE

Failure of the Weaponized Department of Justice to Protect the US Election System

The Breach

Hackers gained access to Alaska's voter registration system between September 19 and 28, 2020, and began posting about their successful breach of the system in late September. Despite the fact that the breach was real and that members of a designated Foreign Terrorist Organization[i], the Iranian Republican Guard Corp (IRGC), had gained access to sensitive, non-public voter registration data from Alaska, the FBI initially denied that the breach occurred. On September 28, 2020, the FBI and CISA issued a joint public announcement[ii] titled "False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections" which characterized the breach as "attempts to spread disinformation regarding cyberattacks on U.S. voter registration databases or voting systems."

Similar to actions of the FBI to quash reports of Hunter Biden's laptop and mislead the American people, the FBI announcement falsely claimed that the reports of the voter registration system breach were simply disinformation:

> "During the 2020 election season, foreign actors and cyber criminals are spreading false and inconsistent information through various online platforms in an attempt to manipulate public opinion, discredit the electoral process, and undermine confidence in U.S. democratic institutions. These malicious actors could use these forums to also spread disinformation suggesting successful cyber operations have compromised election infrastructure and facilitated the "hacking" and "leaking" of U.S. voter registration data."[iii] —*FBI and CISA Joint Announcement September 28, 2024*

The malicious actors' claims of a successful breach were true – not simply disinformation. Alaska's system administrators subsequently confirmed the breach, but the voter registration system vulnerability was not corrected until October 26, 2020. Then, on October 30, 2020, the FBI finally acknowledged that a voter registration system had been hacked.[iv] The Advisory did not warn of the potential for targeting of UOCAVA voting system vulnerabilities but instead suggested that the threat was limited to voter intimidation and disinformation.

> "CISA and the FBI are aware of an Iranian advanced persistent threat (APT) actor targeting U.S. state websites—to include election websites. CISA and the FBI assess this actor is responsible for the mass dissemination of voter intimidation emails to U.S. citizens and the dissemination of U.S. election-related disinformation in mid-

> October 2020. This disinformation (hereinafter, "the propaganda video") was in the form of a video purporting to misattribute the activity to a U.S. domestic actor and implies that individuals could cast fraudulent ballots, even from overseas."

Buried on page two of that Advisory was the acknowledgement that "the actor successfully obtained voter registration data in at least one state."[v] After the election, on December 3, 2020, Alaska's Lieutenant Governor Kevin Meyer, confirmed the breach but issued a statement[vi] echoing the DOJ, minimizing the seriousness of the breach and misleading the public about the potential impact.

> "Although some voters' personal information was exposed, the division has determined that no other election systems or data were affected. The division's ballot tabulation systems, the 2020 general election results and the state's voter database remain secure."

Exposure of voters' sensitive PII most certainly can affect "other election systems." The voter registration system is the foundation for the administration of elections. The primary security measure for absentee and mail ballot requests is verification of identity by matching driver's license numbers or Social Security numbers from ballot applications with the official government records. Many states do some version of signature comparison,[vii] but Alaska does not do signature verification on absentee ballots therefore the only barrier to accessing a ballot is having a valid ID number on the application. If the IRGC had submitted fraudulent applications or ballots to election officials in Alaska using the data from the breach—the Social Security or Driver's License numbers would have been verified as correct in the matching process.

The Video

The Iranian hackers successfully accessed data including the names, addresses, dates of birth, social security numbers and driver's license numbers of at least 113,000 Alaskans. They produced and disseminated a video[viii] demonstrating how they could use the breach data to complete Federal Write-In Absentee Ballots (FWAB) or Federal Post Card Applications (FPCA). The IRGC attempted to falsely attribute the video to the Proud Boys but that was quickly dispelled.

The video included confirmed valid voter information that was copied and pasted into the fields used to create PDFs for at least three FWABs which can be used as emergency back up ballots by individuals who are eligible to vote under the Uniformed Overseas Citizens Absentee Voting Act (UOCAVA). This group of voters includes members of the military and their family members and non-military US citizens who are outside of the US at the time of

the election. In 2024, only 30% of UOCAVA voters were members of the military or their family members. The majority, more than 70%, were non-military individuals including students who were studying abroad, people who have permanently moved out of the US and many who have never resided in the US but indicate that they are US citizens.

As shown in a screenshot from the video, (Figure 1) after the FWAB is completed online, the applicant is instructed to print and sign the form and then return it to the local election jurisdiction. Many states allow the FWAB and other UOCAVA ballots to be submitted by email or fax.

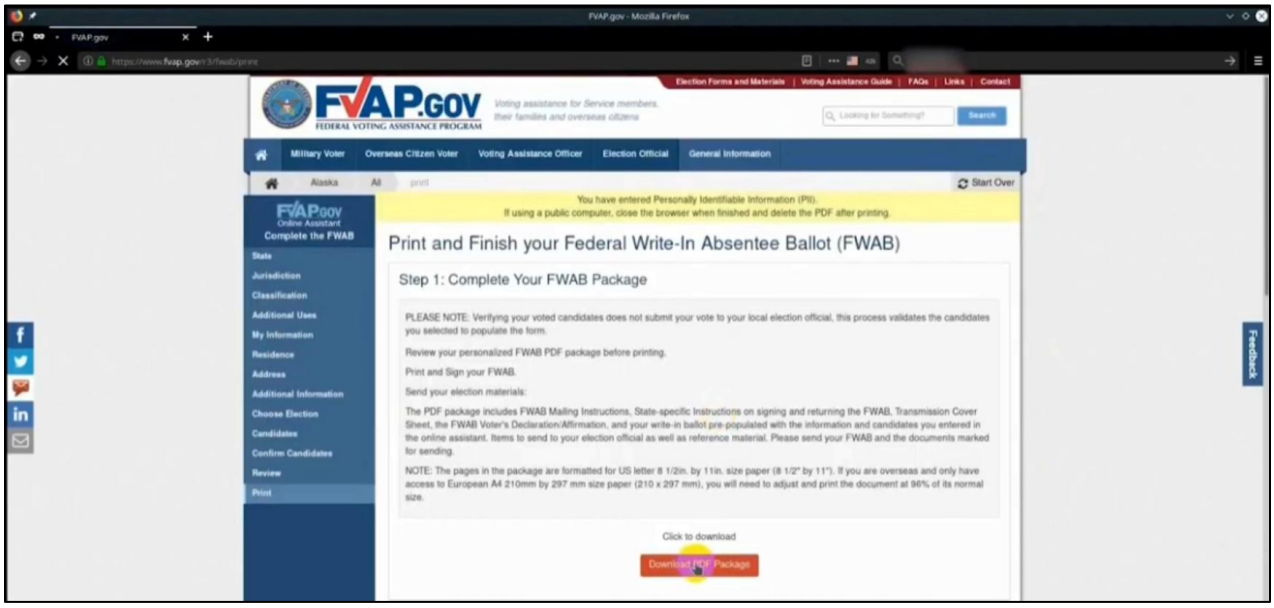

Figure 1: Screenshot from the IRGC video

The IRGC video included a view of computer files for 40 states and a demonstration that at least some of those state folders contained multiple PDF documents of UOCAVA FWAB ballots or FPCA ballot applications. (See Figure 2) While there is no evidence that the FWABs created in the video were submitted to states, there is ample evidence that the vulnerabilities exist.

The September 2020 breach and the IRGC video should have prompted the distribution of an alert to all states with guidance for elevated scrutiny of all absentee ballot applications and returned absentee ballots. Instead, officials minimized the true risk and exposure and misled the public by claiming that the breach was nothing more than an effort to "spread propaganda and shake voter confidence—not to impact the election results."[ix]

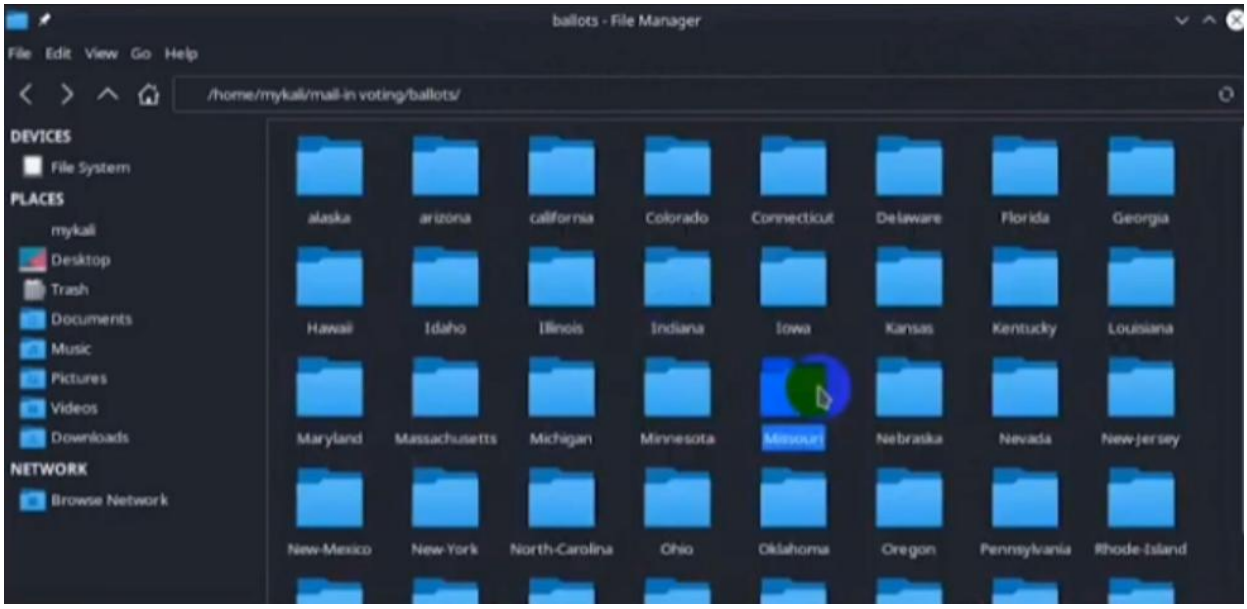

Figure 2: Screenshot from the IRGC video showing 40 state folders

Consistent with the FBI's narrative, CISA later falsely claimed that election offices have "security measures in place" to detect fraudulent FWABs and Federal Post Card Applications for UOCAVA ballots. [x] (See Figure 3)

✔Reality: Safeguards are in place to protect against fraudulent voting using the Federal Write-In Absentee Ballot (FWAB).

✘ Rumor: A malicious actor can easily defraud an election using the Federal Write-In Absentee Ballot (FWAB).

Get the Facts: Changing an election using fraudulently submitted FWABs would be highly difficult to do. This is because election offices have security measures in place to detect such activity.

The FWAB is primarily used as a backup ballot for military and overseas voters who requested but did not yet receive their absentee ballot. FWAB users must provide their signature and meet varying state voter registration and absentee ballot request requirements, which can include provision of full or partial social security number, state identification number, proof of identification, and/or witness signature.

Since only military and overseas voters are eligible to use the FWAB, relatively few of them are submitted each election. In 2016, states reported that only 23,291 total FWABs were submitted nationwide, with all but six states receiving less than 1,000 FWABs statewide. Since use is relatively rare, spikes in FWAB usage would be detected as anomalous.

Figure 3: Screenshot from CISA's website labeling the IRGC video as disinformation

CISA's "Rumor Control" post is not accurate and does not reflect the reality of UOCAVA administration in states. They note that relatively few FWABs are submitted and that "spikes in FWAB usage would be detected". However, states reported receiving 41% more FWABs in 2020 than in 2016. Nationally, 33,027 FWABs were submitted to election offices for the 2020 General Election[xi]. That was an increase of nearly 10,000 more FWABs submitted in 2020 when there were travel restrictions and far fewer US citizens abroad.

The Vulnerability

Election officials reported that Alaska had a 60% increase in UOCAVA ballots from 2016 to 2020. The increase alone was significant enough to warrant further review. Statewide, Alaska issued 16,466 online delivery ballots in the 2020 election.[xii] Nationally, the number of FPCAs received for the 2020 Election was 764,691 which was nearly double the 420,861 FPCAs that states reported receiving ahead of the 2016 general election. The 2020 election occurred during a global pandemic which significantly reduced the number of US citizens traveling, studying or working abroad but the significant increase in UOCAVA ballots was not investigated by the DOJ.

The federal government routinely issues alerts for owners and operators of critical infrastructure regarding threats that include actionable guidance and recommendations for mitigation strategies to harden defenses. In this case, election officials should have been warned of the potential threat involving UOCAVA ballots. The FBI and CISA should have notified states to be vigilant and to ensure that they were taking steps to prevent malicious actors from exploiting the vulnerabilities in state UOCAVA voting systems. Instead, the vulnerabilities exposed by the IRGC video were dismissed as mere propaganda.

In addition to the threat in Alaska described above, there are serious, well-documented vulnerabilities in UOCAVA voting in multiple other states. In some states, a voter registration database breach would not be necessary to submit fraudulent UOCAVA ballots. Several states have policies and procedures that would allow a bad actor to complete an FWAB or FPCA online using a fictitious name and fictitious driver's license or SSN4. Absent verification, the submission could result in the delivery of a ballot by email[xiii] to the bad actor who could then vote and return that ballot which would be accepted and counted in the election.

Without attempting to verify the identity or eligibility of UOCAVA applicants, there was and is nothing to prevent the IRGC or other bad actors from influencing elections in states like Wisconsin and Pennsylvania where the chief election officials are failing to follow even the minimum requirements of the Help America Vote Act (HAVA).

Wisconsin's Legislative Audit Bureau[xiv] confirmed that WEC does not even attempt to verify personally identifiable information provided by some UOCAVA voters. The auditors reported that "WEC's staff indicated that no attempts were made to match the personally identifiable information provided" by applicants who indicate on the application that they are members of the military or family members of the military. Therefore, any bad actor who submitted an FPCA or FWAB in Wisconsin could receive a ballot by email and have that ballot counted because there are no safeguards in place to prevent such an exploitation.

In fact, in 2022, a Milwaukee election official was prosecuted for using made up names to request UOCAVA ballots. Each of the three WI jurisdictions that received the fraudulent FPCAs with the fake information, approved the applications and mailed a ballot to the fake applicant. WI State Representative Janel Brandtjen received three ballots by mail at her home and notified law enforcement of the issue.[xv] However, bad actors intent on interfering in the election, could receive and return fraudulent ballots and be undetected by the current system in WI. The election official admitted that she submitted the fraudulent FPCAs but said that she did so to expose the problem with WEC's guidance and to demonstrate the vulnerability of the system.

Pennsylvania has a similar policy to not even attempt to verify information on UOCAVA applications. Pennsylvania doesn't even register UOCAVA applicants or verify any information if they check the box on the FPCA indicating that they may not intend to return to the United States[xvi]. In Pennsylvania, bad actors would not need to breach the voter registration system to submit fraudulent FWABs or FPCAs as there are no protections. Notably, Pennsylvania counties rejected zero FWABs in the 2024 election[xvii]. Six members of Congress attempted to challenge the PA DOS' illegal non-verification policy in 2024, but the case was dismissed for lack of standing.[xviii]

The Indictment

In 2021, the DOJ indicted two Iranians for their involvement in the Alaska breach which was described as a "cyber-enabled campaign to intimidate and influence American voters, and otherwise undermine voter confidence and sow discord, in connection with the 2020 U.S. Presidential election." They were charged with successfully breaching at least one statewide voter registration database and attempting to breach voter registration systems in eleven other states. The exposure of the vulnerability in the UOCAVA system was described in the indictment as a "False Election Video" and the DOJ claimed that "FVAP could not be leveraged in the manner implied in the False Election Video."[xix] That is a verifiably false statement by the DOJ as described above.

The DOJ issued a press release regarding the indictment which trivialized and covered up the real issues associated with the actions of the IRGC. "As part of this campaign, the conspirators obtained confidential United States voter information from **at least one state election website**, sent threatening email messages to intimidate voters, created and **disseminated a video containing disinformation pertaining to purported but non-existent voting vulnerabilities**."[xx] (emphasis added)

The video, created by individuals associated with a designated Foreign Terrorist Organization, demonstrated a knowledge of the UOCAVA vulnerabilities and a willingness to violate the law to interfere in US elections. Claiming that the vulnerabilities are "non-existent" is a flagrant untruth. Either the FBI was completely unfamiliar with the procedures associated with UOCAVA voting or they intentionally misled the public.

Threats by the IRGC remain. As recently as June 30, 2025, the FBI issued a warning regarding escalating threats from Iran, particularly in response to the bombing of Iran's nuclear facilities.[xxi] Efforts by the IRGC continued in 2024 and, absent meaningful investigations and prosecutions, will likely continue in 2026 and beyond. The existing vulnerabilities in the UOCAVA voting system must be addressed to prevent the IRGC and other foreign adversaries from interfering in future elections.

There is an urgent need for the FBI to fully investigate the potential exploitation of vulnerabilities in UOCAVA voting. Further, the DOJ should ensure compliance with the federal requirements for verification of voter registration information for individuals who apply to register to vote in federal elections.

The Election Research Institute is a non-partisan think tank dedicated to identifying vulnerabilities in the election system, making recommendations for mitigation and improving efficiency and transparency in election administration.

---

[i] https://2017-2021.state.gov/designation-of-the-islamic-revolutionary-guard-corps/

[ii] https://www.ic3.gov/PSA/2020/PSA200928

[iii] Id.

[iv] https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-304a

[v] Id.

[vi] https://ltgov.alaska.gov/newsroom/2020/12/state-of-alaskas-online-voter-registration-system-victim-of-data-exposure/

[vii] Voter registration databases typically include images of voters' signatures that are used for signature verification purposes. Hackers could potentially obtain the signature images and use those images to apply matching signatures to ballot envelopes to defeat the signature verification security measure for states that employ this method.

[viii] The video, available here, has been redacted to remove the visible sensitive PII which was visible and in the video that was circulated. https://archive.org/details/irgc-video-2020-fvap

[ix] https://ltgov.alaska.gov/newsroom/2020/12/state-of-alaskas-online-voter-registration-system-victim-of-data-exposure/

[x] https://web.archive.org/web/20201030170859/https://www.cisa.gov/rumorcontrol#rumor8

[xi] https://www.eac.gov/sites/default/files/document_library/files/2020_EAVS_Report_Final_508c.pdf

[xii] https://www.elections.alaska.gov/research/statistics/#aeqstats

[xiii] In the case of an FWAB, the ballot could be accepted and counted if no subsequent ballot is returned by the UOCAVA applicant.

[xiv] https://legis.wisconsin.gov/lab/media/rz1nj2dh/21-19full.pdf

[xv] https://www.wpr.org/news/jury-former-milwaukee-election-official-guilty-election-fraud-zapata

[xvi] https://www.pa.gov/content/dam/copapwp-pagov/en/dos/resources/voting-and-elections/directives-and-guidance/2023-UOCAVA-Federal-Voters-Guidance-2.1.pdf

[xvii] https://www.eac.gov/sites/default/files/2025-06/2024_EAVS_Report_508c.pdf

[xviii] Reschenthaler, et al. v. Schmidt - https://ecf.pamd.uscourts.gov/doc1/15519099414

[xx] https://www.justice.gov/usao-sdny/pr/us-attorney-announces-charges-against-two-iranian-nationals-cyber-enabled

[xxi] https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran