



Recognizing and Addressing Threats to Statewide Voter Registration Databases

July, 2026

VOTE



EXECUTIVE SUMMARY

Recently declassified records revealed that China breached multiple state voter registration systems prior to the 2020 election. Unfortunately, this is not a new phenomenon. Unclassified reports from the last decade reveal that Statewide Voter Registration Databases (VRDB) are attractive targets for foreign adversaries.¹ Hackers have attempted to breach voter registration systems in all 50 states, with confirmed successes in at least 20 states. However, experts have routinely minimized the significance of successful voter registration breaches and the exposure of sensitive personal data used for voter verification. This failure to identify and accurately describe the potential threats makes U.S. elections less secure.

State and local election officials must prioritize enhanced defenses to protect voter registration databases, and to limit the ways that compromised data can be exploited. Steps should be taken to prevent bad actors from using stolen data to successfully obtain absentee ballots, alter voter registration information, or add and delete registrants. Implementing and maintaining safeguards is essential to protecting the electoral process and sustaining public confidence in elections.

It is imperative to be realistic about the threats posed by foreign adversaries to our critical systems, including election infrastructure. Accurately assessing and communicating the potential for serious consequences is fundamental to effective preparedness and risk management. While candid acknowledgment of these threats may cause concern, it enables critical infrastructure owners to make informed decisions about security measures and mitigation strategies, thereby reducing vulnerability to worst case scenarios. Ignoring or minimizing risks undermines the ability to implement robust controls and leaves critical systems exposed. Transparent recognition of the threat landscape is essential for developing resilient defenses and ensuring the integrity and security of our election systems.

This product provides an unclassified overview of the threats to statewide voter registration databases from both foreign and domestic actors. It relies on reporting from the intelligence community, law enforcement, and state election officials. This report is intended to inform state and local election officials of the associated threats and the need to implement recommended mitigating controls.

HISTORY OF VOTER REGISTRATION SYSTEM BREACHES

Below are examples of unclassified reports of breaches of voter registration databases in the last ten years.

- Russian government cyber actors attempted to identify and exploit SQL database vulnerabilities in web servers and databases. The FBI reported that they lacked insight into the extent to which the attempts were successful. However, in at least two separate instances, Russian actors accessed voter registration files from a US county website.² (June 2016)
- The District Attorney in Riverside County, California revealed that a bad actor used the state's voter registration website to change the party affiliation of a large number of registered voters. The individual made the changes by leveraging access to voters' personal information (name, date of birth, driver's license, or Social Security number) to make the change without the voters' knowledge or consent.³ (July 2016)
- Russian actors hacked the website of a state board of elections and stole information related to approximately 500,000 voters, including names, addresses, partial social security numbers, dates of birth, and driver's license numbers.⁴ (July 2016)
- Russian actors hacked into the computers of a U.S. vendor that supplied software used to verify voter registration information.⁵ (August 2016)
- DHS and FBI confirmed that Russian actors conducted election system reconnaissance to identify vulnerable databases, usernames, and passwords in webpages of state and local governments and probed voter registration database in **all 50 states**. They could not confirm how many of the probes resulted in successful breaches.⁶ In January 2017, WH officials reported that the federal assessment was that networks in at least seven states were compromised.⁷ (2016)
- Arizona experienced a breach and the Illinois State Board of Elections announced that attackers gained access to voter registration data, including names, addresses, birth dates, and partial Social Security numbers.⁸ (2016)
- Kennesaw State University, which was responsible for supporting Georgia's voter registration database, was found to expose nearly 7 million voter records including driver's license and Social Security numbers of registered voters. The data may have been exposed for as long as seven months.⁹ (March 2017)

- Chinese state-sponsored cyber actors aggressively targeted U.S. critical infrastructure to steal sensitive data and personally identifiable information (PII).¹⁰ (August 2021)
- CISA and the FBI reported that members of the Iranian Republic Guard Corp attempted to exploit websites to obtain voter registration data. They confirm that the actor successfully obtained voter registration data in at least one state. They could not determine if the attempts were successful in the other 11 states targeted.¹¹ (September 2020)
- Pro-Russian hackers claimed to have conducted a Distributed Denial of Service (DDoS) attack that resulted in temporarily restricted access to a public-facing US state election office website.¹² (2022)
- Suspected Chinese cyber actors scanned both election-related and non-election state government websites. Other suspected PRC cyber actors also collected publicly available U.S. voter information.¹³ (2022)
- New Hampshire election officials discovered that a vendor selected to replace the state's aging voter registration database had offshored part of the project. The software had been configured to connect to servers in Russia, and a programmer had hard-coded the Ukrainian national anthem into the database. The issues were corrected prior to deployment.¹⁴ (2023)

State and local election officials must prioritize enhanced defenses to protect voter registration databases and to limit the ways that compromised data can be exploited. Implementing and maintaining safeguards to prevent bad actors from using stolen data to successfully obtain absentee ballots, alter voter registration information, or add and delete registrants are essential for protection of the electoral process.

While the potential impact of voter registration database breaches is often minimized, these exploitations could have serious consequences for the administration of elections. The impact of the breaches is not limited to “undermining confidence” or “spreading false claims” but the data itself could be used months or years after the breach to alter voter registration information or request absentee ballots. **The real threat is what can be done with the stolen data.**

POTENTIAL AVENUES FOR EXPLOITATION

WHY IT MATTERS

OBTAINING ABSENTEE BALLOTS

In nearly every election jurisdiction, the information required to apply for and receive an absentee ballot is stored in the voter registration database. A breach can allow bad actors to access public information such as name, date of birth, and address but also sensitive information like driver's license numbers, full or partial social security numbers, and voter signatures on file. That information could enable bad actors to request absentee ballots at scale for low-propensity voters. Data obtained in a breach from 2021, for example, could be used to request a ballot for an election in 2028 because the data does not get stale.

ALTERING VOTER REGISTRATION INFORMATION OR DELETING REGISTRANTS

A malicious actor could use data from a breach to alter voter registration records to change addresses and therefore their polling place or change party affiliation to impede voting in an election. Perpetrated at scale, this type of exploitation could disenfranchise a significant number of voters, and if carefully distributed, such an attack might go unnoticed even if the scope was significant. This type of malicious alteration of voter data could be done over time using data obtained from a breach to log into official online state systems that enable voters to update their voter registration after passing identity checks using personal data like date of birth, portions of social security numbers, or driver's license number. Deletion of voter registration files could cause disruptions in the administration of elections if done at scale or, if executed in a distributed manner.

PREPAREDNESS IS THE BEST DEFENSE

DEVELOP A PLAN

Preparedness, built on a realistic threat assessment, is the foundation of effective election security measures. With a sober acknowledgment of the threat, state and local election officials can take steps to enhance the security of voter registration databases and absentee and mail ballots.

BACK UP DATABASE FILES REGULARLY

A commitment to good cybersecurity and best practices is critical to protecting voter registration data. States should schedule frequent, routine back-ups of the voter registration database files and store them securely offline. States should also test the ability to revert to back-up during an incident.

For jurisdictions that utilize electronic pollbooks, producing paper pollbooks as back-ups will limit the potential for disruptions on Election Day.

ENGAGE YOUR PLAN

If you detect unauthorized access to your voter registration database, immediately implement your security incident response plan. It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. In the meantime, you should take steps to maintain your organization's essential functions according to your election resiliency and continuity plan.

PREPARE FOR POTENTIAL CYBERSECURITY INCIDENTS

Network infrastructure and internet-facing applications, including voter registration databases, underpin and enable a variety of functions in the conduct of elections. These may include election infrastructure networks that store, host, or process voter registration information, as well as public-facing election websites that support functions like polling place lookup. Local election officials have the power to prevent most security incidents using basic security measures. Take steps now so that even if an incident occurs, critical election operations can continue.

Protect and Respond: Phishing Attempts Targeting Your Email

- Enable Multifactor Authentication on all accounts.
 - Ensure each account has its own unique credentials and do not allow credential sharing.
 - Apply the principle of least privilege by separating admin accounts and user accounts.
 - Ensure everyone changes their default passwords and require strong passwords for all accounts.
- Enable Domain-based Message Authentication Reporting and Conformance for all email accounts to make it easier for email senders and receivers to determine whether an email legitimately originated from the identified sender and provides the user with instructions for handling the email if it is fraudulent.
- Implement flagging external emails to alert users to use due care when opening.
- Train staff so they know to only use their official email accounts, which often include enhanced security features, for official business.
- Train staff to spot and report phishing or other suspicious emails.
 - Malicious actors are improving their techniques all the time, so training should be provided at regular intervals to educate staff about the latest tactics and how to respond to suspicious communications. Regularly review common signs of phishing so staff are familiar with what to look out for and how to report.

Protect and Respond: Distributed Denial of Service Targeting Your Websites

- Review existing contracts and coordinate with both website service providers and internet service providers before an incident occurs.
 - Identify what additional Distributed Denial of Service (DDoS) mitigation and redundancy measures are available. Most major service providers have protections available, which may be offered at no cost for basic services, or at additional cost for advanced services.
 - Ensure you know who to contact in the event of an incident.
-

- Share information about important election dates and locations, requesting that ample troubleshooting is available during key periods, and ensuring mutual awareness of any planned maintenance that could impact election operations.
- Ensure network traffic monitoring and analysis is enabled via a firewall or intrusion detection system and that the logs are being reviewed.
- Have an alternate plan for information dissemination in case your website does go down. Make sure to test that plan.

Protect and Respond: Ransomware Targeting Your Network

- While not binding on non-Federal entities, CISA's Binding Operational Directives are indicative of best practices and network owners should consider following them.
- Develop a patch management plan that makes reducing the significant risk of known exploited vulnerabilities a top priority for remediation and requires critical vulnerabilities to be re-mediated within 15 calendar days of initial detection.
- Implement and enforce network segmentation. Proper network segmentation is an effective security mechanism to prevent an intruder from propagating exploits or moving laterally within an internal network. This includes not transferring election results on the business network.
- Implement endpoint detection and response software on endpoint devices to monitor for malicious traffic. Verify alerts are being created and response processes are followed.
- If not already being used, government entities should use .gov domains.
- Implement Malicious Domain Blocking and Reporting (MDBR) across your network devices to prevent IT systems from connecting to harmful web domains. MDBR can block the vast majority of ransomware infections just by preventing the initial outreach to a ransomware delivery domain.
- Develop and maintain incident response plans that specifically detail how to operate mission-critical processes in the event of a cybersecurity incident.
- Test your incident response plans with all key players who would be involved in implementing the response.
- Maintain backups that allow you to recover data at a minimum of up to 30 days prior.
 - Encrypt backup files and ensure credentials for accessing the backups are not stored in the targeted environment. Ransomware actors often hunt for and collect credentials stored in the targeted environment and use those credentials to attempt to access backup solutions; they also use publicly available exploits to target unpatched backup solutions.
 - Ensure backups are maintained offline, as most ransomware actors attempt to find and subsequently delete or encrypt accessible backups to make restoration impossible unless the ransom is paid.
 - Test the availability and integrity of backups in a disaster recovery scenario.

DATA BREACHES GENERALLY

Over the last decade, millions of Americans have had their personally identifiable information (PII) leaked in data breaches that are not related to voter registration but compromise election security, nonetheless. Cybercriminals have gained access to databases belonging to financial institutions, healthcare providers, and other government agencies, obtaining PII including Social Security numbers, addresses, full names, dates of birth, and driver's license numbers. In many cases, this information is sold on the dark web, where it is easily accessible to malicious actors. Because much of this same data is used to verify voter eligibility, maintain voter rolls, and verify identity for absentee ballot requests, large-scale PII exposure of data held by private companies has implications not only for privacy and financial fraud, but also for the integrity of U.S. elections.

- In July 2017, a credit reporting firm discovered a data breach that affected a potential 143 million United States citizens, almost half of the population. The breach reportedly began in May 2017 and was announced nearly four months later. By exploiting an unpatched vulnerability in web application software, cyber attackers were able to steal an unprecedented amount of PII including Social Security numbers, dates of birth, home addresses, driver's license numbers, and full names.
- On February 10, 2020, the Department of Justice (DOJ) indicted four members of China's People's Liberation Army on counts of economic espionage, wire fraud and computer fraud. In a statement following the indictment, Attorney General William Barr said the hack fits "a disturbing and unacceptable pattern of state-sponsored computer intrusions and thefts by China and its citizens that have targeted personally identifiable information, trade secrets, and other confidential information."
- In April 2024, a background check firm that stored troves of records including full names, current and past addresses, Social Security numbers, dates of birth, and telephone numbers suffered a colossal data breach of 2.9 billion records containing PII of 170 million individuals. The information was reportedly found on the Dark Web being offered for \$3.5 million.
- One of the largest supplemental insurance providers in the United States suffered a data breach in June 2025 that affected 22.65 million individuals. Information accessed by hackers included PII such as Social Security numbers, dates of birth, driver's license numbers and full names. Hackers gained access to the provider's systems via social engineering tactics e.g. phishing, whaling, and impersonation.
- A report from the University of Oxford found that Russia and China ranked first and third, respectively, as nations that pose the highest threat level of cybercrime. Moreover, the PII available to these adversaries is not limited to that accessed through their own cyber operations but can be readily purchased or accessed on the dark web.

The cases mentioned above involve breaches that contained the information typically needed for voter registration and absentee ballot applications. The threat this exposed data poses to the integrity of U.S. elections is significant and ongoing, underscoring the need to recognize and mitigate the direct risk it poses to critical election infrastructure.

CONCLUSION

Voter registration databases are the foundation of our voting system. State and local election officials must prioritize system security and implement safeguards to prevent the exploitation of data that may have already been exposed. Adopting modern security enhancements such as smart network monitoring and multi-factor authentication can limit the risks of fraud and election disruptions. The Department of Homeland Security is charged with protecting the nation's critical infrastructure, including election infrastructure, and all state election officials are encouraged to collaborate with DHS on this important mission.

For more information about election security and resources to protect elections, visit the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Toolkit and Resources to Protect Elections page: [https:// www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections](https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections)

REFERENCES

¹ <https://www.justice.gov/archives/sco/file/1080281/dl?inline>

² <https://www.justice.gov/archives/sco/file/1080281/dl?inline>

³ [RIVERSIDE COUNTY: District attorney claims voters' party affiliations purposely changed without consent - Press Enterprise](#) ⁴
<https://www.justice.gov/archives/sco/file/1080281/dl?inline>

⁵ <https://www.justice.gov/archives/sco/file/1080281/dl?inline>

⁶ <https://www.intelligence.senate.gov/2020/08/18/publications-report-select-committee-intelligence-unitedstates-senate-russian-active-measures/>

⁷ [U.S. intel: Russia compromised seven states prior to 2016 election](#)

⁸ [Voter Databases in Arizona and Illinois Breached, FBI Says](#)

⁹ [GEORGIA VOTING HACK: FBI investigating alleged breach of Georgia elections center at Kennesaw State University - WSB-TV Channel 2 - Atlanta](#)

¹⁰ https://media.defense.gov/2021/Jul/19/2002805003/-1/-1/1/CSA_CHINESE_STATE-SPONSORED_CYBER_TTPS.PDF

¹¹ <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-304a>

¹² [Key Findings and Recommendations: Foreign Interference Related to the 2022 US Federal Elections | Homeland Security](#)

¹³ https://www.dhs.gov/sites/default/files/2023-12/1_b_%20Memo%20DOJ%20and%20DHS%20Approved_508c.pdf

¹⁴ [Hacking Blind Spot: States Struggle to Vet Coders of Election Software - HSToday](#)



PREVENTING ALIEN VOTING

NATIONAL SECURITY INVESTIGATIONS: The Department of Homeland Security has initiated multiple investigations related to allegations of non-citizen voting and registration. Review of the first set of public voter files from states that have not utilized the SAVE system revealed:

**OVER 250,000 NON-CITIZENS ARE ILLEGALLY REGISTERED TO VOTE
IN JUST THE FOUR STATES FOR WHICH PUBLIC DATA FILES HAVE BEEN REVIEWED.**

State election officials in California, Pennsylvania, New Jersey and Nevada have been notified of this serious threat to national security and DHS stands ready to support their efforts to identify and remove ineligible registrants. The investigation is expanding to include multiple additional states. In addition, DHS will support the Department of Justice's review of voter files obtained pursuant to their enforcement authority under the National Voter Registration Act of 1993 and the Help America Vote Act of 2002.

STATES THAT PROTECT FEDERAL ELECTIONS: Numerous proactive, conscientious state officials have successfully utilized free services offered by the Department of Homeland Security to assist election officials in identifying non-citizens who have registered and/or voted in their states.

In the short time that the enhanced SAVE system has been available to states, 10 have states processed their full voter lists. As of June 22, 2026, a total of 25 different states processed more than 68 million registration records through the SAVE system. DHS has enabled those states to identify over **400,000** deceased registrants and over **28,000** non-citizens who illegally registered to vote.

As demonstrated by the sample data to the right, these states are serious about ensuring that only US citizens vote in US elections. DHS applauds their efforts to prevent non-citizens from registering and to remove ineligible registrants who unlawfully register.

Proactive SAVE User States		
State	Deceased	Non-Citizen
Georgia	42,776	2,549
Ohio	59,774	769
Tennessee	37,850	1,009
Texas	111,573	2,296
North Carolina	34,622	1,599
Idaho	4,328	49
Alabama	33,165	465
Missouri	10,660	1,112
Louisiana	15,231	419
Kansas	10,197	449

Several other proactive state officials have also signed Memoranda of Agreement with USCIS to utilize the SAVE system and have processed portions of their state voter rolls. Unfortunately, due to the actions of the activist Judge Sparkle Sooknanan, many of the enhancements to this service of USCIS have been suspended pending appeal. As a result, US citizens are at risk of having their votes diluted by ineligible alien voters.

UNAMBIGUOUS CONTRAST: There is an undeniable pattern emerging as DHS begins to unravel the horrific damage done by the open border policies of the Biden administration. States that have adopted alien-first policies instead of American-first policies have a disproportionate number of non-citizens on their voter rolls.



FEDERAL BUREAU OF INVESTIGATION

Date of entry 12/20/2023

[REDACTED] date of birth [REDACTED] phone number [REDACTED]
Social Security account number [REDACTED] home address [REDACTED]
[REDACTED] was interviewed over the phone. After
being advised of the identity of the interviewing Agents and the nature of
the interview, [REDACTED] provided the following information:

[REDACTED] initially, could not recall working for a company that was involved
in the 2020 election. He finally remembered his employment when he was
reminded of the location he applied for the job. He applied for the job on
[REDACTED] near the Dollar General. He remembered wearing bright neon colored
shirts. He worked for only a couple of weeks in the Fall.

[REDACTED] understood his job as collecting signatures for voter registration.
He was paid based on how many signatures he collected. He was expected to
get a certain amount of signatures every day. If he did not collect any
signatures, he would not get paid. He did not recall how many signatures he
was required to get every day.

[REDACTED] could not specifically remember if he forged signatures but advised
that he probably did at some point during the employment. He believed people
would fake signatures.

[Agent Note. Agent sent photo of the canvasser contract to his cell phone
number [REDACTED]. The canvasser contract will be maintained in the
attached 1A.]

[REDACTED] confirmed the canvasser contract contained his handwriting and his
signature.

Investigation on 12/14/2023 at Muskegon, Michigan, United States (Phone)File # 56D-DE-3407960Date drafted 12/18/2023by [REDACTED]

UNCLASSIFIED//~~FOUO~~**FEDERAL BUREAU OF INVESTIGATION**
Electronic Communication

Title: (U) Alleged fraudulent voter registrations
being submitted to the Muskegon City
Clerk's Office.

Date: 10/29/2020

From: DETROIT

Contact: [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: 56-DE-3249380-
Muskegon

(U//~~FOUO~~) Michigan Election Crimes; Type
III Assessment; Assessment Began
03/10/2020; SENSITIVE INVESTIGATIVE MATTER

Synopsis: (U) This EC serves to summarize allegations of fraudulent
voter registrations being submitted to the Muskegon City Clerk's Office.

Enclosure(s): Enclosed are the following items:

1. (U) Muskegon Police Department

Details:

Detroit Field Office was informed the Michigan State Police (MSP), Michigan Attorney General (MAG), and Muskegon Police Department (MCPD) were investigating allegations of fraudulent voter registrations being submitted to the Muskegon City Clerk's Office (MCCO). The matter was referred to law enforcement by the MCCO. Since on or about 10/5/2020, MCCO received six packages via U.S. Mail containing voter registration applications. MCCO determined some of the applications were fraudulent based on non-existent addresses, invalid telephone numbers, and signatures on applications not matching Michigan Secretary of State voting or DMV records. In addition, many applications appeared to have the same hand writing. MCCO determined the bulk applications were sent by

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

Title: (U) Alleged fraudulent voter registrations being submitted to the Muskegon City Clerk's Office.

Re: 56-DE-3249380-Muskegon, 10/29/2020

[REDACTED] a resident of [REDACTED] as [REDACTED] also hand delivered numerous applications with similar red flags. MCPD estimates [REDACTED] submitted approximately 8 to 10 thousand applications of which an undetermined number appeared fraudulent. [REDACTED] informed investigators she works for [REDACTED] and [REDACTED] [REDACTED] and was paid for voter registration work. She was involved in similar registration drives in Detroit, Ypsilanti, Southfield, Flint, and Lansing. Open source search revealed a candidate in the 2018 Georgia District 7 congressional election paid [REDACTED] \$52 thousand for "field consulting and canvasser payments." A Sentinel search revealed positive results for [REDACTED] related to restricted cases, 56E-BA-2140100 and 56D-AT-3310478. The local and state law enforcement agencies will continue their active investigation and will likely take overt action by search warrant this week.

On 10/05/2020, the MCCO, Muskegon, Michigan, began receiving State Of Michigan Voter Registration Applications (applications) via mail, in total six packages. The applications appeared to be fraudulent based on non-existent addresses, invalid telephone numbers, mismatched signatures when compared to Michigan Secretary of State Records, and multiple applications appeared to have the same handwriting/signatures. The packages were marked [REDACTED] and had two return addresses, [REDACTED] [REDACTED] The [REDACTED] address is a Staybridge Street and the [REDACTED] address is a single family residence.

On 10/8/2020, [REDACTED] turned in multiple voter applications at the MCCO. An employee at the MCCO, aware of the suspicious applications received via mail, questioned [REDACTED] who advised she worked for [REDACTED] [REDACTED] also advised she works for [REDACTED] [REDACTED] and was aware applications were mailed.

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

Title: (U) Alleged fraudulent voter registrations being submitted to the Muskegon City Clerk's Office.

Re: 56-DE-3249380-Muskegon, 10/29/2020

On 10/16/2020, the MCPD initiated an investigation into allegations of Voter Registration Fraud.

On 10/20/2020, [REDACTED] returned to MCCO with a box of approximately 2,500 applications. An MCCO clerk contacted MCPD who then interviewed [REDACTED]

[REDACTED]
[REDACTED]
office in [REDACTED]. She is paid \$1,150/week. Her job is to locate unregistered voters and provide them with a form to register/obtain their ballot. [REDACTED] advised [REDACTED] has similar campaigns ongoing in Muskegon, Detroit, Ypsilanti, Southfield, Flint, and Lansing which began on 08/06/2020. [REDACTED] claimed all the registrations were legitimate and cross-checked by [REDACTED] with the fraudulent registrations removed at their office. During the interview, [REDACTED] raised red flags by providing an inaccurate DOB, initially claiming her workers were paid by the application then said they were paid hourly, and had trouble recalling [REDACTED] last name after initially providing it.

After the interview, [REDACTED] drove away in a Volkswagen Jetta, registered to EAN Holdings (Enterprise Rent-A-Car), and last rented by [REDACTED]

In total, the MCCO received approximately 8,000-10,000 forms in person or via mail associated with [REDACTED]

On 10/22/2020, MSP initiated an investigation to assist the MCPD. The investigation is being prosecuted by AG's office.

On 10/23/2020, the MSP obtained a 48 hour GPS warrant which has since been renewed. [REDACTED] was last pinged at the Best Western Hotel in Grand Haven, Michigan.

On 10/26/2020, an evening email to the PC SSA indicated MSP's intention to brief the FBI Detroit Election Team (DET) the next day about an

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

Title: (U) Alleged fraudulent voter registrations being submitted to the Muskegon City Clerk's Office.

Re: 56-DE-3249380-Muskegon, 10/29/2020

allegation of voter fraud.

On 10/27/2020, MSP briefed the DET regarding allegations related to [REDACTED]

On 10/27/2020, Detroit PCOR discussed investigation with lead MSP F/LT. [REDACTED] MSP could use assistance and have a general willingness to work jointly with the FBI on the condition the USAO and AG discuss and agree.

On 10/27/2020, Detroit notified the U.S. Attorneys of EDMT and WDMT and had conversations with the DOE the following day.

MSP anticipates executing search warrants on Thursday, 10/29/2020 at the [REDACTED] location and Best Western Grand Haven hotel room. [REDACTED] as scheduled to checkout of the hotel on 10/29/2020.

Detroit will discuss matter with MSP, MAG, MCPD as well as the U.S. Attorney's Offices for the Eastern District of Michigan and Western District of Michigan after the conclusion of the election to determine potential investigative steps.

On 10/27/2020, MCPD Captain [REDACTED] provided the FBI with a copy of police report 2020-19124, which is attached hereto.

◆◆

UNCLASSIFIED//~~FOUO~~

From: [REDACTED] (DE) (FBI)
Sent: Tuesday, November 16, 2021 4:22 PM
To: [REDACTED] (DE) (FBI)
Subject: Fwd: [REDACTED]

Just so you're aware, I sent the below message to [REDACTED] last week. I haven't yet gotten a response. I'm not really comfortable closing the case at this point without raising these issues. I'm also not thrilled with the wording from [REDACTED] stating that the PIN concurs with our decision not to pursue it as opposed to the PIN directing us not to pursue it.

From: [REDACTED] (DE) (FBI)
Sent: Thursday, November 11, 2021 1:31:01 PM
To: [REDACTED] (USAMIW) <[REDACTED]>
Subject: FW: [REDACTED]

In our initial meeting regarding this case, I was somewhat unprepared, having not previously been involved in election-related investigations. I recall from that meeting, you had concerns regarding proving how the fraudulent voter registration applications could impact the election as well as showing that it was done "willfully". I was recently provided with "Federal Prosecution of Election Offenses", put out by the DOJ's Public Integrity Section, December 2017. After reading through it, I have some concerns regarding whether closing the matter is appropriate. Some of the relevant portions of the manual include:

- Under the heading, "What is election fraud?"
 - "Simply put, then, election fraud is conduct intended to corrupt... the process by which voters are registered." (pg. 22)
- Under the heading, "Conduct that Constitutes Federal Election Fraud"
 - "Submitting fictitious names to election officers for inclusion on voter registration rolls, thereby qualifying the ostensible voters to vote in federal elections (52 U.S.C. §§ 10307(c), 20511(2))." (pg. 24)
 - "Providing false information concerning a person's name, address, or period of residence in a voting district to establish that person's eligibility to register or to vote in a federal election (52 U.S.C. §§ 10307(c), 20511(2)). (pg. 25)
 - "Causing the production of voter registrations that qualify alleged voters to vote for federal candidates, or the production of ballots in federal elections, that the actor knows are materially defective under applicable state law (52 U.S.C. § 20511(2)). (pg. 25)
- Under the heading, "False Information in, and Payments for, Registering and Voting: 52 U.S.C. § 10307(c)"
 - "Section 10307(c) is particularly useful for two reasons: (1) it eliminates the unresolved issue of the scope of the constitutional right to vote in matters not involving racial discrimination, and (2) it eliminates the need to prove that a given pattern of corrupt conduct had an actual impact on a federal election. It is sufficient under Section 10307(c) that a pattern of corrupt conduct took place during a mixed election; in that situation it is presumed that the fraud will expose the federal race to potential harm. *Slone* 411 F.3d at 647 (collecting cases)." (pg. 39 – 40)
- Under the heading, "False information to an election official"

- “The “false information” provision of Section 10307(c) prohibits any person from furnishing certain false data to an election official to establish eligibility to register or to vote in a federal election. The statute applies to three types of information: name, address, and period of residence in the voting district.” (pg. 40)
- “Some, but not all, states permit a practice commonly known as “bounty-hunting,” that is, paying people to collect voter registrations on a per-registration basis. Where it is allowed, it is not unusual to find that this method of remuneration provides a motive for the unscrupulous to forge voter registrations and to enhance the piecework payments they can receive. While this situation usually does not result in fraudulent votes actually being cast, it does cause voter registration offices to become overloaded with the task of processing large numbers of bogus registrations immediately prior to an election, when the resources of those offices should be directed at preparing ballots and staffing polling sites. It also risks overloading voter rolls with “deadwood” names , which in turn undermines public confidence in the election process. Thus, even when no fraudulent votes result from bounty-hunting, the fraudulent registrations that arise from this conduct are not victimless offenses. Federal prosecutors should be cognizant of these circumstances and, when evidence of fraudulent registrations inspired by bounty-hunting is discovered, should consider prosecuting the individuals submitting the false registrations, as well as, in appropriate circumstances, the organizations that employ and pay them, under Section 10307(c).” (pg. 42 - 43)

Although, it doesn't appear [REDACTED] was paying on a per-registration basis, it is reasonable for the canvassers to believe they would not keep the job if they weren't somewhat productive, and regardless of what they believed, they still submitted fraudulent voter registration applications. I understand that proving this was done “willfully” would still be difficult, but I wanted to raise my concerns before closing the case.

From: [REDACTED] (DE) (FBI) <[REDACTED]>
Sent: Wednesday, November 3, 2021 9:40 AM
To: [REDACTED] (DE) (FBI) <[REDACTED]>
Subject: Fwd: [REDACTED]
FYSA

From: [REDACTED] (CRM) <[REDACTED]>
Sent: Wednesday, November 3, 2021, 9:35 AM
To: [REDACTED] (DE) (FBI)
Subject: [EXTERNAL EMAIL] - RE: [REDACTED]

[REDACTED]
Sorry I missed your calls. I'll send an email today memorializing PIN's agreement with the decisions of the USAO and FBI to not seek prosecution here. I'll also copy [REDACTED] of USAO-W.D. Mich.

From: [REDACTED] <[REDACTED]>
Sent: Wednesday, October 20, 2021 10:28 AM
To: [REDACTED] (CRM) <[REDACTED]>
Subject: [REDACTED]
Hello [REDACTED]

We previously discussed the current state of the [REDACTED] investigation, the results of our financial review, and the content of the Michigan Attorney General's Office casefile that was provided to

us. Would you be able to provide an undated letter regarding DOJ/PIN's view on concurrence/nonconcurrence?

Please don't hesitate to call with any questions or if you need additional information.

Thanks,

A small black rectangular redaction mark covering the signature.



UNCLASSIFIED//~~FOUO~~
FEDERAL BUREAU OF INVESTIGATION

Date of entry 12/18/2023

[REDACTED] date of birth (DOB) [REDACTED] cellular telephone [REDACTED]

[REDACTED] the identities of the interviewing Agents and the nature of the interview, [REDACTED] provided the following information:

In 2020, [REDACTED] worked as a canvasser for an organization that registered people to vote. [REDACTED] did not sound familiar. [REDACTED] heard about the canvassing job through her uncle. For each shift, [REDACTED] wore a green and blue shirt and reported to an office on [REDACTED]. The office used to be an eye care center. [REDACTED] would then canvass for voter registrations outside the Walmart. At the end of each shift, [REDACTED] would return to the office on [REDACTED] to turn in the voter registration applications she collected. [REDACTED] was paid \$400 every two weeks. [REDACTED] was paid via direct deposit or prepaid debit card. There wasn't an incentive or bonus to turn in voter registration applications. [REDACTED] was never directed to make up information on the voter registration applications. [REDACTED] was never told she might have an opportunity to work in other offices.

[REDACTED] knew of other canvassers who would trade marijuana and/or money for voter registration applications. Other canvassers were "probably" submitting voter registration applications with fictitious names. [REDACTED] never submitted voter registration applications with fictitious information. [REDACTED] met her baby's father, [REDACTED] while she was canvassing. [REDACTED] likely filled out fictitious information on his voter registration application. [REDACTED] is now in prison for an unrelated issue.

[Agent Note: [REDACTED] provided a screenshot from Facebook of [REDACTED]. The screenshot has been digitally attached to this report as a 1A.]

[REDACTED] and [REDACTED] brother, First Name Unknown (FNU) Last Name Unknown (LNU), were supervisors at the organization. [REDACTED] and FNU LNU were from [REDACTED].

[Agent Note: [REDACTED] did not have contact information for either [REDACTED] or [REDACTED].

UNCLASSIFIED//~~FOUO~~

Investigation on 12/12/2023 at [REDACTED] (In Person)

File # 56D-DE-3407960Date drafted 12/15/2023by [REDACTED]

UNCLASSIFIED//~~FOUO~~

56D-DE-3407960

Continuation of FD-302 of (U) Interview of [REDACTED], On 12/12/2023, Page 2 of 2

FNU LNU but provided screenshots from Facebook of both individuals. The two screenshots have been digitally attached to this report as 1As.]

[Agent Note: At this point in the interview, Agents showed [REDACTED] two canvassing contracts. [REDACTED] confirmed that it was her handwriting and her signature on both contracts. The contracts shown to [REDACTED] have been digitally attached to this report as 1As.]

UNCLASSIFIED//~~FOUO~~

From: [REDACTED] (CRM) [REDACTED]
Sent: Thursday, February 2, 2023 3:14 PM
To: [REDACTED] (USAMIW); [REDACTED] (DE) (FBI)
Subject: [EXTERNAL EMAIL] - Election Consult re. Voter Registrations (W.D. Mich.)

[REDACTED]

Thank you for the call today. Subject to our discussion, PIN concurs in the full GJ investigation into the alleged voter registration fraud matter referenced and summarized in part below. Specifically, PIN concurs in investigating only those voter registration applications in which (1) the purported applicant does not exist and/or appears to be fabricated (i.e., "unable to locate" with incorrect associated information); and (2) signatures of the purported applicants are the same or substantially similar to signatures on other applications (thereby suggesting that one person, and not the actual purported applicants, signed multiple applications). This concurrence does not extend to applications featuring the names of actual persons in which the application includes a unique signature. Please let me know if there is any confusion or questions about the scope of this concurrence. Please consult if and when your offices seek to pursue criminal charges or lacks venue for any criminal conduct. No federal public statement should be made about this matter without conferring with PIN.

Please do not hesitate to contact me if we can help or you want to discuss further.

[REDACTED]

[REDACTED]
Director of Enforcement & Litigation | Election Crimes Branch
U.S. Department of Justice | Criminal Division | Public Integrity Section
1301 New York Ave., NW | Washington, D.C. 20530
[REDACTED] (office) | [REDACTED] (cell)

We've completed our database checks on 20 randomly selected voter registration applications with apparently different handwriting from those identified by the Muskegon Clerk as potentially fraudulent. We compared the names, last four of SS#, MI DL number, DOB, gender, address, and phone number listed on the applications to those found in available databases. We've found the following:

- #1 – Name located. Address, DOB, SS# don't match. Phone number matches.
- #2 – Unable to locate anyone by that name. Address does not exist. Phone number does not return to anyone.
- #3 – Name located. DOB matches. Middle name is different than initial provided. No indication individual ever lived at the listed address or had the listed phone number.
- #4 – Name located. All information matches.
- #5 – Unable to locate anyone by that name and DOB. Address exists, but residents do not match.
- #6 – Name located. All information matches.
- #7 – Unable to locate anyone by that name and DOB. Address exists, residents do not match.
- #8 – Name located. DOB matches. SS# does not match. Address matches.

#9 – Unable to locate anyone by that name. Address does not exist. Phone is inactive, but returns to a different name.

#10 – Name located. DOB matches. SS# does not match. Address does not match.

#11 – Name located. DOB and SS# match. Address doesn't exist. Doesn't appear to have ever lived in Muskegon.

#12 – Name located. All information matches except phone number is inactive.

#13 – Name located. All information matches except phone number is inactive.

#14 – Name located. Deceased, but was alive at the time of registration. All information matched except address.

#15 – Unable to locate anyone by that name and DOB. Address does not exist. Phone is inactive.

#16 – Unable to locate anyone by that name and DOB. Address does not exist. Phone is inactive.

#17 – Name located. DOB matches. Formerly lived at the address. Driver's license number is wrong.

#18 – Name located. DOB, SS#, and address match. Phone number is inactive.

#19 – Unable to locate anyone by that name and DOB. Address is a park. Unable to locate phone number.

#20 – Name located. DOB, SS#, and address match. Phone number is inactive.

Based on these results, it appears as though:

- seven of the applications contain completely fabricated information.
- four of the applications contain a real name, but DOB, driver's license, and/or SS# don't match.
- one of the applications contain a real name, but middle name doesn't match.
- one of the applications is for someone who does not appear to have ever lived in Muskegon and has a fabricated address.
- seven of the applications contain all correct or nearly all correct information.

FEDERAL BUREAU OF INVESTIGATION

Date of entry 12/15/2023

[REDACTED] date of birth (DOB) [REDACTED] Social Security account number (SSAN) [REDACTED] telephone number [REDACTED] was interviewed telephonically. After being advised of the identity of the interviewing Agent and the nature of the interview, [REDACTED] provided the following information:

In 2020, [REDACTED] was employed by an organization who assisted in registering people to vote. The organization provided her with a T-shirt to wear, and gave them a paper to have people sign to vote. [REDACTED] could not remember the name of the organization. She was referred to the organization by a friend, and was told she would be paid to get people to vote. Her job was to get people to sign. She would then bring the signed papers back to the employer, and then be paid. [REDACTED] walked around and asked people to register to vote for OBAMA approximately 3-4 years ago.

[REDACTED] did not work in one specific location. When the voter registration applications were completed, [REDACTED] brought them back to the employer. She was paid \$300.00 once, almost \$400.00 once and then \$200.00. [REDACTED] was paid based on how many signatures she received. [REDACTED] was given a "card" and money was placed on it.

[Agent Note: [REDACTED] did not recall exactly how much she was paid. The dollar amount provided in the paragraph above are approximations.]

[REDACTED] of the supervisor. [REDACTED] recalled the supervisors as a black male, and a black female. The black female was "running things" at the Muskegon location located on Broadway and Hoyt.

[REDACTED] was required to submit a certain number of voter registrations. She was required to submit 2-3 applications in order to get paid. She was not offered any bonuses. There were no incentives or opportunities to work in other cities or states. She was not aware of anyone giving anything to people they approached in return for completing a voter registration application. Most of the employees submitted voter registrations with false

Investigation on 12/12/2023 at Muskegon, Michigan, United States (Phone)File # 56D-DE-3407960Date drafted 12/14/2023by [REDACTED]

56D-DE-3407960

Continuation of FD-302 of (U) Interview of [REDACTED], On 12/12/2023, Page 2 of 2

information because it was "easy money." She was not directed to make up information to complete the forms. She never made up information to complete any forms. She never submitted any applications with fake signatures. She only heard about people submitting falsified forms.

[REDACTED] believed people would submit falsified applications so they could get as many applications as possible. She did not maintain contact with anyone else who worked for the organization. She completed a canvasser contract for the organization. She has not discussed this investigation with anyone else.

The unknown black male supervisor was described as follows:

Name: FNU, LNU

Gender: Male

Race: Black

Height: Medium

Build: Average

UNCLASSIFIED//~~FOUO~~



FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) Searches on [REDACTED]

Date: 05/12/2022

CC: [REDACTED]

From: DETROIT

DE-I21

Contact: [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: 56D-DE-3407960

(U) [REDACTED]

STATE OF MICHIGAN;
CDPO - ELECTION LAWS
SENSITIVE INVESTIGATIVE MATTER

Synopsis: (U) Searches on [REDACTED]

Details:

(U) On 5 May 2022, writer conducted searches in Clear, Accurint and through the Secretary of State on [REDACTED] to determine if the information on her voter registration form is fraudulent. The returns are included below:

- (U) There were no results for [REDACTED] (writer also tried [REDACTED] with the date of birth listed on the form.
- (U) There were no results for [REDACTED] (writer also tried [REDACTED] in Michigan.
- (U) The address listed on the voter registration form does not exist.

♦♦

UNCLASSIFIED//~~FOUO~~

From: [REDACTED] (CRM) [REDACTED]
Sent: Tuesday, January 4, 2022 11:51 AM
To: [REDACTED] (DE) (FBI)
Cc: [REDACTED] (D)
Subject: [EXTERNAL EMAIL] - Re [REDACTED]

[REDACTED]

Happy to discuss. Are you available this afternoon between 1:30-3:00 pm, ET? Otherwise, I can talk later this week.

[REDACTED]

On Jan 3, 2022, at 11:46 AM, [REDACTED] > wrote:

[REDACTED]

I've been unable to reach you by phone, so I thought it might be best to reach out to you via email. I am one of the agents assigned to the [REDACTED] investigation out of FBI Detroit. We are preparing to close the investigation. Before we do so, I was hoping to discuss with you the limited scope that PIN approved into the investigation of the fraudulent voter registration applications. After reviewing "Federal Prosecution of Election Offenses" (December 2017), put out by the DOJ's Public Integrity Section, it appears as though this type of fraud would result in a full field investigation. Specifically –

- Under the heading, "Conduct that Constitutes Federal Election Fraud"
 - o "Submitting fictitious names to election officers for inclusion on voter registration rolls, thereby qualifying the ostensible voters to vote in federal elections (52 U.S.C. §§ 1037(c), 20511(2))." (pg. 24)
 - o "Providing false information concerning a person's name, address, or period of residence in a voting district to establish that person's eligibility to register or to vote in a federal election (52 U.S.C. §§ 1037(c), 20511(2)). (pg. 25)
 - o "Causing the production of voter registrations that qualify alleged voters to vote for federal candidates, or the production of ballots in federal elections, that the actor knows are materially defective under applicable state law (52 U.S.C. § 20511(2)). (pg. 25)
- Under the heading, "False Information in, and Payments for, Registering and Voting: 52 U.S.C. § 10307(c)"
 - o "Section 10307(c) is particularly useful for two reasons: (1) it eliminates the unresolved issue of the scope of the constitutional right to vote in matters not involving racial discrimination, and (2) it eliminates the need to prove that a given pattern of corrupt conduct had an actual impact on a federal election. It is sufficient under Section 10307(c) that a pattern of corrupt conduct took place during a mixed election; in that situation it is presumed that the fraud will expose the federal race to potential harm. *Slone* 411 F.3d at 647 (collecting cases)." (pg. 39 – 40)
- Under the heading, "False information to an election official"

- “The “false information” provision of Section 10307(c) prohibits any person from furnishing certain false data to an election official to establish eligibility to register or to vote in a federal election. The statute applies to three types of information: name, address, and period of residence in the voting district.” (pg. 40)
- “Some, but not all, states permit a practice commonly known as “bounty-hunting,” that is, paying people to collect voter registrations on a per-registration basis. Where it is allowed, it is not unusual to find that this method of remuneration provides a motive for the unscrupulous to forge voter registrations and to enhance the piecework payments they can receive. While this situation usually does not result in fraudulent votes actually being cast, it does cause voter registration offices to become overloaded with the task of processing large numbers of bogus registrations immediately prior to an election, when the resources of those offices should be directed at preparing ballots and staffing polling sites. It also risks overloading voter rolls with “deadwood” names , which in turn undermines public confidence in the election process. Thus, even when no fraudulent votes result from bounty-hunting, the fraudulent registrations that arise from this conduct are not victimless offenses. Federal prosecutors should be cognizant of these circumstances and, when evidence of fraudulent registrations inspired by bounty-hunting is discovered, should consider prosecuting the individuals submitting the false registrations, as well as, in appropriate circumstances, the organizations that employ and pay them, under Section 10307(c).” (pg. 42 - 43)

Although, it doesn't appear [REDACTED] as paying on a per-registration basis, it is reasonable for the canvassers to believe they would not keep the job if they weren't somewhat productive, and regardless of what they believed, they still submitted fraudulent voter registration applications. I understand that proving this was done “willfully” would still be difficult, but I wanted to raise my concerns before closing the case and was hoping to better understand the reasoning behind not approving a full investigation.

Thanks,

[REDACTED]

S [REDACTED]
FBI Detroit

[REDACTED]

FEDERAL BUREAU OF INVESTIGATION

Date of entry 12/18/2023

[REDACTED] date of birth (DOB) [REDACTED] telephone number [REDACTED] was interviewed telephonically. After being advised of the identity of the interviewing Agents and the nature of the interview, [REDACTED] provided the following information:

In 2020, [REDACTED] was employed by an organization that registered people to vote. The name of that organization could have been [REDACTED] heard about the job through a friend. A regular shift at that job was for four hours. Before each shift, [REDACTED] would go to an office building on [REDACTED] where she would be instructed where she would solicit voter registrations that day. [REDACTED] spent most of her shifts outside gas stations. At the end of each shift, [REDACTED] would go back to the office on [REDACTED] with the voter registrations she collected during the shift and turn them into management. [REDACTED] could not recall the names of the two managers she dealt with; however, one manager was a man and one was a woman. The manager would then put the voter registrations in an envelope. [REDACTED] did not know what happened with the envelopes after that.

[REDACTED] was paid hourly. [REDACTED] could not recall how she was paid. [REDACTED] knew other people who worked at the organization because they were all "locals". There were no incentives for submitting voter registrations. Canvassers were told that there were other offices they could work at. [REDACTED] recalled that there was another office in [REDACTED] [REDACTED] was instructed by management to make up phone numbers and date of births on voter registration applications.

Investigation on 12/13/2023 at Muskegon, Michigan, United States (Phone)File # 56D-DE-3407960Date drafted 12/14/2023by [REDACTED]

UNCLASSIFIED



FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) Database Checks Spreadsheet

Date: 05/19/2023

From: DETROIT

Contact: [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: 56D-DE-3407960-
1B1_REVIEW

(U) [REDACTED]

1B1 Review Subfile;

Synopsis: (U) Database Checks Spreadsheet

Enclosure(s): Enclosed are the following items:

1. (U) Database Checks Spreadsheet

Details:

Database searches were conducted on the 107 voter registration applications from item 1B1 (Box containing voter registration forms. MUPD PR# 94333) in an attempt to identify voter registration applications with potentially fraudulent signatures or listing non-existent individuals. The database searches revealed the following:

- Ninety-one individuals returned no results in database checks.
- Sixteen individuals were confirmed to be existing people but only four had signatures on file that matched the signatures provided on the associated voter registration application.

A spreadsheet summarizing the findings is attached in the 1A portion of the file.

◆◆

UNCLASSIFIED

UNCLASSIFIED//~~FOUO~~

U. S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No. 56D-DE-3407960

Grand Rapids, Michigan
September 25, 2025

(U)

**STATE OF MICHIGAN;
CDPO - ELECTION LAWS
SENSITIVE INVESTIGATIVE MATTER**

FBI Detroit, Grand Rapids Resident Agency closed the captioned
n [REDACTED]
af [REDACTED]
o further investigation is warranted because logical
investigation and/or leads have been exhausted, and the investigation
to date did not identify a criminal violation or a priority threat to
national security. [REDACTED]
[REDACTED] allegedly subm
for the purpose of establishing the ability to vote.
[REDACTED] found no evidence that [REDACTED]
[REDACTED] submitted false voter r
the purpose of establishing the ability to vote. Further, GBI Detroit
found no evidence that anyone [REDACTED] submit false voter
registrations. Interviews of [REDACTED] employee, and several
canvassers were conducted whi [REDACTED] t canvassers were not
instructed to falsify voter registration information.

No further investigation is warranted because logical
investigation and/or leads have been exhausted, and the investigation
to date did not identify a criminal violation. AUSA [REDACTED]
concurred with the closing of the captioned investigation.

The point of contact for this investigation is Special Agent [REDACTED]
[REDACTED], telephone number [REDACTED]

This document contains neither recommendations nor conclusions of the FBI. It is the property of
the FBI and is loaned to your agency; it and its contents are not to be distributed outside your
agency.

UNCLASSIFIED//~~FOUO~~

FEDERAL BUREAU OF INVESTIGATION

Date of entry 12/15/2023

On December 13, 2023, Special Agents [REDACTED] and [REDACTED]

[REDACTED]
identity of the interviewing Agent, and the nature of the interview,
[REDACTED] provided the following:

[Agent Note: On December 12, 2023, SA [REDACTED] spoke with MDOC Parole Officer [REDACTED] at [REDACTED] to obtain current information about [REDACTED].]

[REDACTED] has never heard of [REDACTED] does not know anyone who works there, and has never worked in any job trying to get people to register to vote. [REDACTED] has had issues with identity theft in the past and thinks that perhaps someone who has his information got a job with those companies.

[Agent Note: SA [REDACTED] explained to [REDACTED] that the FBI was investigating the company based on allegations that [REDACTED] violated the law and were not specifically investigating [REDACTED]. Information from the Canvasser Contract was read to [REDACTED]. SA [REDACTED] initially misread one digit in the SSAN, then when corrected was confirmed to be the correct information.]

[REDACTED] is trying to get his life back together and is currently on parole. He has made mistakes in the past and knows everyone is responsible for what they do. [REDACTED] was released from prison in March of 2020. He has never done any work like what the FBI is investigating. The 2020 election was the first time [REDACTED] registered to vote and voted.

On December 15, 2023, [REDACTED] called SA [REDACTED] and said he remembered working for a company for about one week in 2020 where he was tasked with finding people to register to vote. He could not remember the name of the company, nor anyone who worked there. [REDACTED] spoke with his girlfriend who reminded him about the job. [REDACTED]'s friend, [REDACTED] worked for the company and told [REDACTED] he should join him. [REDACTED] said you can just make up names on the form and get paid. [REDACTED] was paid by the hour, not by the signature; he could not remember how he got paid. After about one week, [REDACTED] quit the job. [REDACTED] never collected any names; he would

Investigation on 12/13/2023 at Muskegon, Michigan, United States (Phone)File # 56D-DE-3407960Date drafted 12/14/2023by [REDACTED]

56D-DE-3407960

Continuation of FD-302 of (U) Interview of [REDACTED], On 12/13/2023, Page 2 of 2

just sit in his car the whole shift and would put down a name of a friend or relative in order to have something to turn in with his clipboard.

FEDERAL BUREAU OF INVESTIGATION

Date of entry 12/13/2023

[REDACTED]

Agent and the nature of the interview, [REDACTED] provided the following information:

In Fall 2020, [REDACTED] who was not married at the time and went by [REDACTED] went to [REDACTED] on [REDACTED] in [REDACTED]. People were standing outside an office next door and asked [REDACTED] if she wanted a job. The office was previously an eyeglass store. [REDACTED] went into the office and applied for a job registering people to vote. [REDACTED] was hired the following day. The office was run by a tall thin white male with [REDACTED] in the office. [REDACTED] previously lived at [REDACTED] and [REDACTED] later worked in the office, but were not working there when [REDACTED] was hired.

[REDACTED] job was to stand outside of businesses asking people if they wanted to register to vote. There were over 100 people doing the same job in the Muskegon area. These employees were paid based upon how many completed registrations they submitted each day, but [REDACTED] couldn't recall how much she was paid per registration. The white male told employees that the organization was huge and had operations in other states. He also said employees who did the best, meaning turned in the most voter registration applications, could travel to other states to work. [REDACTED] and [REDACTED] also drove employees to their locations and collected registration applications themselves. Once the police executed the search warrant at the office, the employees were told their job assignment was over.

[REDACTED] was shown two canvasser contracts (attached as "[REDACTED] 1A13_1_6" and "[REDACTED] 1A13_2_114.") [REDACTED] confirmed she had filled out both of these forms.

[REDACTED] was shown 22 completed voter registration applications (attached

Investigation on 12/12/2023 at [REDACTED] (In Person)File # 56D-DE-3407960Date drafted 12/13/2023by [REDACTED]

56D-DE-3407960

Continuation of FD-302 of (U) Interview of [REDACTED], On 12/12/2023, Page 2 of 3

as "Similar Hand A.") [REDACTED] initially stated that she remembered all the people on the pages. After being told that these applications appeared to be fabricated, [REDACTED] then stated that [REDACTED] or [REDACTED] told all of the employees that if they couldn't get enough applications, they should just fill them in. This occurred at a meeting with over 100 employees present. One of the employees asked what this person meant. [REDACTED] couldn't recall if it was [REDACTED] or [REDACTED] in front of the group, but whichever it was picked up a blank application and filled it out with made-up information and said, "this is what I mean." This person, either [REDACTED] or [REDACTED] then told them to make sure the information was filled out correctly or they wouldn't get credit for the application. [REDACTED] was told she needed to submit seven to eight applications per shift if working alone and ten per shift per person if working with another employee.

[REDACTED] was paid approximately \$800 each payday. The company gave employees debit cards and loaded their pay on the cards each week. [REDACTED] didn't recall if she turned in the same number of applications each time or why she would have received the same pay for different numbers of applications.

[REDACTED] was told by [REDACTED] or [REDACTED] to put any number she could think of for the social security number, but not to use her own social security number or date of birth. [REDACTED] was told by [REDACTED] or [REDACTED] she could make up names or use anyone else's name. [REDACTED] would return to the office at the end of her shift and fill in enough blank sheets with made-up people so that she reached her daily quota. [REDACTED] confirmed that she filled out all of the "Michigan-issued driver's license/Michigan-issued state ID card #" and "personal information" sections of the 22 reviewed voter registration applications, except for "[REDACTED]" and "[REDACTED]". [REDACTED] signed all of the remaining 20 reviewed voter registration applications except [REDACTED]

[REDACTED] can't write in cursive. These would have been signed by someone at the office for [REDACTED] before she turned them in. [REDACTED] often helped [REDACTED] fill in the fabricated applications. [REDACTED] told [REDACTED] the forms were sent to the main office and then shredded, so it didn't matter that the names were fabricated.

If there were forms that were rejected because they weren't signed sitting around the office, some employees would pick them up, sign them, and turn them in for credit. There were long lines of people at the end of each shift turning in their completed voter registration applications.

The white male who ran the office left before the office closed. He never

56D-DE-3407960

Continuation of FD-302 of (U) Interview of [REDACTED], On 12/12/2023, Page 3 of 3

said he was leaving. After he left, [REDACTED] and [REDACTED] ran the office. The white male was around when people were instructed to fill out fake applications and was aware it was occurring. Everyone working there was aware it was occurring. [REDACTED] doesn't know if the group was trying to impact the election or were just personally trying to make money at a job. Others employed by the group were [REDACTED] and [REDACTED]. There were a couple of black males that were friends of [REDACTED] whom [REDACTED] hired. One was approximately 5'5" and the other was approximately 5'6" and 120 pounds. They always worked together and seemed "fishy". They were always whispering to each other and didn't really interact with anyone else.

[REDACTED] worked for this organization for almost a month. [REDACTED] collected legitimate voter registration applications during this time. [REDACTED] did not fill out any of the sections on the legitimate voter registration applications. The people registering to vote always completed those sections. [REDACTED] estimated she submitted 100 fake voter registration applications to the group. [REDACTED] told [REDACTED] personally to make up information on the forms. [REDACTED] heard [REDACTED] tell the same thing to lots of people. It would not surprise [REDACTED] if there were thousands of fake voter registration applications submitted. [REDACTED] would blame [REDACTED] and the white male for the fake voter registration applications. If those people claimed they told employees not to turn in fake applications, they are lying. There was no posters or anything else telling employees not to turn in fake applications. The employees were just doing what they were told. [REDACTED] knew what was going on was fraud, but these people were forcing the employees to do it so they could make a living. [REDACTED] doesn't have contact information for any of the people she discussed during the interview.

FEDERAL BUREAU OF INVESTIGATION

Date of entry 07/10/2025

(U) On 07 July 2025, [REDACTED] date of birth [REDACTED] [REDACTED] cellular telephone number [REDACTED] was interviewed at her residence located at [REDACTED] [REDACTED] by FBI Special Agents (SA) [REDACTED]. After being advised of the identities of the interviewing Agents and the nature of the interview, [REDACTED] provided the following information:

(U) [REDACTED] currently works as a certified nursing assistant (CNA) for [REDACTED] [REDACTED] also works for [REDACTED] as a medical transportation driver. [REDACTED] typically works from 11:00 AM to 7:00 PM at [REDACTED] [REDACTED] works for [REDACTED] on Monday and Wednesday from approximately 4:30 AM to 2:00 PM. [REDACTED] works for [REDACTED] as a driver in the [REDACTED] area, but the [REDACTED] company is based in the [REDACTED] area.

(U) Around mid-2020, [REDACTED] responded to an online advertisement for an office clerk job at a company called [REDACTED] in Michigan. The job paid approximately \$500-600 USD per week, and [REDACTED] worked as an office clerk at [REDACTED] from August 2020 until the end of the election season around October 2020. [REDACTED] worked for [REDACTED] while she was employed at [REDACTED] as an office clerk, [REDACTED] was responsible for redacting voter forms. The forms typically included an individual's name, date of birth, address, and telephone number. The forms did not include Social Security Account numbers. Employees, called canvassers, went door-to-door in the local area to register individuals to vote. The canvassers then provided the collected forms to [REDACTED] and [REDACTED] would make the necessary redactions. [REDACTED] was only able to make redactions on forms that were filled out correctly and were completed. [REDACTED] recalled one occasion when she stayed late at [REDACTED] to complete redactions and she was paid a bonus. [REDACTED] initially worked in the [REDACTED] office located in [REDACTED] around August 2020 and she later worked in the office located in [REDACTED] around September 2020. [REDACTED] did not recall the cellular telephone number she used between August and October 2020, but thought her number could possibly have been [REDACTED]

Investigation on 07/07/2025 at [REDACTED] In Person)File # 56D-DE-3407960Date drafted 07/07/2025by [REDACTED]

56D-DE-3407960

Continuation of FD-302 of (U) Interview of [REDACTED], On 07/07/2025, Page 2 of 3

(U) [REDACTED] met [REDACTED] while working at [REDACTED] during 2020. [REDACTED] believed [REDACTED] was originally from the [REDACTED] area and moved up to [REDACTED]. [REDACTED] met [REDACTED] as a result of her application to the job at [REDACTED] but only met [REDACTED] toward the end of her employment with [REDACTED]. [REDACTED] felt working for [REDACTED] was like working for a mobster. [REDACTED] owned [REDACTED] but [REDACTED] did not communicate with [REDACTED] often. [REDACTED] only saw [REDACTED] during remote morning meetings via Zoom or teleconference. During the meetings, [REDACTED] directed canvassers to fill out forms completely and correctly because incomplete forms could not be redacted. [REDACTED] also provided instructions to [REDACTED] for redactions, and directed [REDACTED] not to redact incomplete forms. [REDACTED] was never given contact information for [REDACTED] and [REDACTED] was not aware of a telephone number for [REDACTED]. [REDACTED] last spoke to [REDACTED] at the end of the season around October 2020. [REDACTED] had two female office employees that helped run the business, and the last time [REDACTED] spoke with either of the two female employees was around October 2020. [REDACTED] was aware [REDACTED] had other offices, to include an office in [REDACTED]. [REDACTED] never visited other [REDACTED] locations outside of [REDACTED]. [REDACTED] heard [REDACTED] was involved in selling Social Security numbers, but could not provide additional information.

(U) [REDACTED] recalled one particular female [REDACTED] employee (referred to as VP or vice president) that helped [REDACTED]. [REDACTED] dealt with VP when she was hired at [REDACTED] but [REDACTED] could not remember her name. VP operated like a vice-president and helped with on-boarding employees, handled problems with rooms, and seemed to handle the more serious company issues. [REDACTED] described VP as a light-skinned, black female, who often wore her hair wrapped. [REDACTED] spoke with VP and a second female employee in-person at the office and communicated with both of them by telephone, email, and Skype or video call. [REDACTED] could not remember the name of the second female employee, but described the second female employee as a dark-skinned, black female who handled other financial matters for [REDACTED]. VP and the second female employee ran the [REDACTED] office, which operated as a headquarters for [REDACTED]. [REDACTED] would likely have worked at the [REDACTED] office, but never went to the [REDACTED] office. [REDACTED] remembers that there was a room, which she presume [REDACTED] s office, that she was not allowed into and had never seen.

(U) [REDACTED] knew [REDACTED] and advised [REDACTED] was from the [REDACTED] area and had a daughter. [REDACTED] did redactions for [REDACTED]. [REDACTED] was responsible for running canvassers and checking paperwork for completeness. [REDACTED] last spoke to [REDACTED] during August 2021. [REDACTED] could not recall contact information for [REDACTED] but believed [REDACTED] may have a social media page on Instagram.

56D-DE-3407960

Continuation of FD-302 of (U) Interview of [REDACTED], On 07/07/2025, Page 3 of 3

(U) [REDACTED] was familiar with the name [REDACTED] and [REDACTED] believed [REDACTED] could have been employed at [REDACTED]. [REDACTED] did not recall [REDACTED]'s last name, but advised she might recognize a photograph of [REDACTED].

(U) [REDACTED] did not know how canvassers were recruited but felt the people hired as canvassers would not be individuals she would hire herself. [REDACTED] believed several may have been hired off the street. Canvassers were paid approximately \$10 USD per hour and were also paid \$50 USD as a bonus for collecting a certain amount of application forms. [REDACTED] did not remember how many forms a canvasser was required to collect to receive a bonus. Canvassers were paid with funds loaded to debit cards. The cards frequently had problems and needed to be fixed in the office. The canvassers were required to provide an identification card and their Social Security account number to activate the cards and resolve any issues. [REDACTED] would usually only see or interact with the canvassers during the morning meetings, which were held daily around 9:00 AM or 9:30 AM. [REDACTED] was not aware of canvassers receiving any specific training, but [REDACTED] knew [REDACTED] instructed canvassers to collect the full first and last name, address, date of birth, and telephone [REDACTED] ion forms. Canvassers collected forms for the [REDACTED] office, and later more locations were added to include [REDACTED] and others.

(U) [REDACTED] did not know if anyone at [REDACTED] submitted false applications. [REDACTED] did not work with or conspire with anyone to submit false applications. [REDACTED] was never paid by anyone to submit false applications. [REDACTED] never paid or offered compensation to anyone to submit false applications. After her time at [REDACTED], [REDACTED] stated she felt like [REDACTED] was possibly trying to suppress or prevent people from voting for President Trump. [REDACTED] advised she was willing to speak with interviewing agents again in the future.

56D-DE-3407960

Timeline

10/27/2020 – MSP briefed FBI DE Election Team

2/11/2021 – SA [REDACTED] emailed [REDACTED] for concurrence to open investigation

3/11/2021 – PIN authorized FFI into prepaid cards. Investigation into voter fraud not authorized

3/16/2021 – FFI opened

4/1/2021 – PIN concurred with contacting election and law enforcement authorities to gather more information regarding voter fraud

5/6/2021 – SA [REDACTED] added as case manager with SA [REDACTED] and SA [REDACTED]

5/27/2021 – Interview of [REDACTED]

7/1/2021 – Case synopsis provided to AUSA [REDACTED]

7/7/2021 – SA [REDACTED] met with AUSA [REDACTED] and A/USA [REDACTED]

8/12/2021 – AUSA [REDACTED] advised that PIN did not approve further action in the Western District

11/2/2021 – AUSA [REDACTED] advised that the Western District portion of the investigation could be closed

11/11/2021 – SA [REDACTED] emailed AUSA [REDACTED] with concerns about closing investigation

1/4/2022 – Discussion with PIN

3/10/2022 – PIN advised that previous guidance allows DE to review applications and run database checks

3/14/2022 – SA [REDACTED] copied 20 applications from MPD

3/31/2022 – SA [REDACTED] provided results of database checks on these 20 to PIN and USAO

4/22/2022 – SA [REDACTED] copied 100 applications reportedly not processed by the clerk from MPD

8/1/2022 – SA [REDACTED] provided results of database checks on these 100 to PIN and USAO

11/10/2022 – SA [REDACTED] again requested PIN guidance

1/31/2023 – PIN arranged call with SA [REDACTED] and AUSA [REDACTED]

2/2/2023 – PIN authorized full field investigation

2/3/2023 – SA [REDACTED] obtained evidence from MPD

5/2/2023 – SA [REDACTED] provided results of database checks on 107 applications

5/8-6/22/2023 – SA [REDACTED] interviewed eight canvassers and attempted interviews of eight additional canvassers

8/8/2023 – SA [REDACTED] interviewed [REDACTED] and [REDACTED]

9/13/2023 – SA [REDACTED] sent a lead to the FBI Laboratory to have examinations conducted of voter registration applications associated with [REDACTED]

9/21/2023 – [REDACTED] completed searches of the canvassers identified from 1A13.

9/27/2023 – SA [REDACTED] requested funding from FBIHQ for 20 agents to conduct canvasser interviews. Approval provided by the Public Corruption Unit on the same date.

10/3/2023 – SA [REDACTED] canvassed FBI DE agents for volunteers to conduct canvasser interviews the week of 11/5/2023.

10/3/2023 – SA [REDACTED] spoke with [REDACTED] Director, Election Crimes Branch, Deputy Chief, Public Integrity Section, Department of Justice, who advised interviews could not be conducted the week of 11/5/2023 due to Michigan elections scheduled for 11/7/2023.

10/3/2023 – SA [REDACTED] sent an updated request for volunteers to FBI DE agents to conduct canvasser interviews the week of 12/10/2023.

12/11/2023 – Briefing conducted with interviewing agents at the Kent County SO

12/12/2023 – 12/15/2023 – Mass interviews of canvassers conducted

1/6/2024 – SA [REDACTED] canvassed interviewers for any outstanding FD-302s. Was advised one was still outstanding.

1/8/2024 – SA [REDACTED] emailed [REDACTED] FBI Laboratory, to request an update on the status of the examination of voter registration applications submitted 9/13/2023

1/9/2024 – [REDACTED] replied that examinations would be completed in approximately 60 days

~1/15/2024 – Copies of FD-302's given to AUSA [REDACTED]

~1/29/2024 – Copies of FD-302's given to AUSA [REDACTED]

2/11/2024 – SA [REDACTED] received email from ASAC [REDACTED] which was a forwarded email from SAC Chey Gibson. Attached to email was a letter to Director Wray from Michigan State Representatives [REDACTED] and [REDACTED]

2/12/2024 – Met with ASAC [REDACTED] and SSA [REDACTED] to brief on status of case. Advised waiting on results of handwriting analysis from Lab Division.

2/12/2024 – SA [REDACTED] sent ASAC [REDACTED] a link to the outstanding lead to Lab Division

2/12/2024 – SA [REDACTED] Cc'ed on email from ASAC [REDACTED] to [REDACTED] at lab Division requesting assistance on getting the lead completed soon.

~2/13/2024 – SA [REDACTED] spoke on Lync call with ASAC [REDACTED] and [REDACTED] at Lab Division about getting handwriting analysis complete. ASAC [REDACTED] explained the lead had attained a higher priority

3/11/2024 – SA [REDACTED] spoke with AUSA [REDACTED] who advised he did not expect this case was going to lead to prosecution. SA [REDACTED] requested a written declination from the USAO

3/20/2024 – ASAC [REDACTED] emailed SA [REDACTED] to ask if Lab Division ever got back with the exam results. SA [REDACTED] responded “no”

3/20/2024 – ASAC [REDACTED] emailed [REDACTED] asking for an update

3/20/2024 – [REDACTED] responded that she has completed handwriting analysis, but the indented writing exams were still in progress. [REDACTED] advised she could issue two separate reports, one for the handwriting and one for the indented writing.

3/21/2024 – SA [REDACTED] responded that one report was preferred as the USAO could not make a final determination until testing was complete.

5/15/2024 – [REDACTED] advised SA [REDACTED] via email that the Questioned Documents Laboratory Report was complete and provided a copy. Also uploaded to Sentinel on the same date.

5/15/2024 – SA [REDACTED] forwarded [REDACTED] email to AUSA [REDACTED] and requested a charging decision.

7/17/2024 – SA [REDACTED] attended a meeting with USA [REDACTED] ASAC [REDACTED] ASAC [REDACTED] AUSA [REDACTED] AUSA [REDACTED] AUSA [REDACTED] AUSA [REDACTED] PCU Section Chief Devin Kowalski, SSA [REDACTED] SSA [REDACTED] SA [REDACTED] members of PIN, and other FBI and DOJ employees. USA [REDACTED] advised that there would be no prosecution in the [REDACTED] case.

7/30/2024 – SA [REDACTED] called AUSA [REDACTED] and requested an update on the written declination. [REDACTED] advised he would send a message up his chain and get back.

8/1/2024 – SA [REDACTED] advised [REDACTED] and [REDACTED] via email that the case was no longer actively being investigated and that there had been prior FOIA requests. [REDACTED] responded that she would leave a note in the case should the requester come back.

8/19/2024 – SSA [REDACTED] emailed AUSA [REDACTED] and AUSA [REDACTED] asking whether additional action from PIN was needed to obtain a declination. AUSA [REDACTED] advised he anticipated having guidance from PIN between 9/3 and 9/13.

9/26/2024 – SA [REDACTED] emailed AUSA [REDACTED] requesting an update. AUSA [REDACTED] advised that his office had received a response from PIN which prompted follow-on discussions and there was not yet an official position for next steps in the case.

10/8/2024 – ASAC [REDACTED] advised that USA [REDACTED] stated he was reconsidering prosecution.

10/8/2024 – SA [REDACTED] emailed [REDACTED] and [REDACTED] that the USAO was considering prosecution and that in the event any FOIA requests were received, the case agent should be contacted.

10/25/2024 – AUSA [REDACTED] called SA [REDACTED] and stated that a PIN attorney would like to review the FD-302s from the investigation. On the same date, AUSA [REDACTED] emailed SA [REDACTED] requesting copies of the 302s be provided to his office.

FEDERAL BUREAU OF INVESTIGATION

Date of entry 12/20/2023[REDACTED] date of birth [REDACTED] phone number [REDACTED]
[REDACTED]
[REDACTED]

identity of the interviewing Agents and the nature of the interview,
[REDACTED] provided the following information:

[REDACTED] worked for [REDACTED] some time between September and October. She worked Monday through Friday from 8:00 am to 12:00 pm. At the time, she was taking care of an elderly person and was contacted by someone about the job with [REDACTED]. She went to an eyewear store near Dollar General and provided her drivers license and was given a W2 form and other paperwork. [REDACTED] was paid by a visa card every two weeks. She did not recall how much she was paid but it was based on the amount of hours she worked. She did not file taxes on the money she made working for the company.

[REDACTED] was dropped off at different stores like Save A lot, Family Dollar, and liquor stores and would ask people as they entered the store whether they were registered to vote. A van would drop off people at the stores. The employees had a goal for each day with regards to how many voter registration forms were completed. There were no incentives for producing a certain amount of forms.

[REDACTED] thought people might be forging signatures because the younger employees would return with a lot of signed registration forms and she would only have three or four for the entire week. [REDACTED] did not forge signatures on the voter registration forms. The supervisors told [REDACTED] what they were doing was cleared with the Secretary of State.

The employees would return signed voter registration forms to the main office and there would be a paper with their names on it and they would tally how many forms they turned in. [REDACTED] never heard about incentives for producing more registration forms from the supervisors. [REDACTED] confirmed it was her handwriting and her signature on the Canvasser Contract attached as a 1A.

Investigation on 12/12/2023 at [REDACTED] (In Person)File # 56D-DE-3407960Date drafted 12/18/2023by [REDACTED]

From: [REDACTED] (CRM) [REDACTED]
Sent: Tuesday, October 3, 2023 3:38 PM
To: [REDACTED] (DE) (FBI)
Subject: [EXTERNAL EMAIL] - RE: Call

[REDACTED]

Thanks for reaching out and for taking the time to discuss this matter today. I understand that FBI/DE is currently investigating a potential voter registration fraud scheme involving canvassers for [REDACTED] in Michigan's 2020 election. As part of that investigation, you have proposed conducting interviews of approximately 100 individuals who served as [REDACTED] canvassers in 2020 to determine whether those canvassers submitted falsified voter registration applications in 2020, possibly in order to meet quotas for the submission of voter registration applications as part of their employment. Michigan has an election for local offices throughout the state scheduled for November 7, 2023.

As we discussed, this matter implicates the Department's election non-interference policy, JM § 9-85.300, and its election-year sensitivities policy, JM § 9-85.500. This is because voter registration in Michigan is unitary, meaning that voter registration involves registering to vote both in federal and state elections. In addition, interviews of numerous current or former canvassers close in time to the November 7, 2023, election may create a public perception of the Department and FBI acting with a purpose of affecting the outcome of that upcoming election.

Accordingly, PIN concurs in the proposed interviews of the canvassers only after the November 7, 2023, election is concluded, certified, and uncontested. We discussed conducting these potential interviews in December 2023, and PIN would concur in conducting those interviews at that time. PIN also concurs in any appropriate coordination with state and local law enforcement and election administration authorities, and any other appropriate covert investigative activity, even prior to the November 7, 2023, election.

Please consult with us again prior to engaging in any other potentially overt investigative activity close in time to another election, to include Michigan's presidential primary election on February 27, 2024, or Michigan's state primary election on August 6, 2024. Please also consult again before bringing any charges or making any public statement regarding this matter.

Please let me know if there is anything else we can do to assist.

Best,

[REDACTED]
[REDACTED]
Director | Election Crimes Branch
Deputy Chief | Public Integrity Section
Criminal Division | United States Department of Justice
1301 New York Avenue NW | Washington, D.C. 20005
Office: [REDACTED] | Cell: [REDACTED]

From: [REDACTED]
Sent: Tuesday, October 3, 2023 11:03 AM
To: [REDACTED] (CRM) [REDACTED]
Subject: RE: Call

Thanks. Not an emergency, but something I'd like to resolve today. 2:30 is great.

[REDACTED]

From: [REDACTED] (CRM) [REDACTED]
Sent: Tuesday, October 3, 2023 11:01 AM
To: [REDACTED] (DE) (FBI) [REDACTED]
Subject: [EXTERNAL EMAIL] - RE: Call

Thanks, [REDACTED] In that case I'll schedule a call for 2:30 p.m. today. If it is an emergency let me know and I'll leave my meeting now.

From: [REDACTED]
Sent: Tuesday, October 3, 2023 10:59 AM
To: [REDACTED] (CRM) [REDACTED]
Subject: RE: Call

I'm available any time and would like to speak as soon as you are available after your meetings.

Thanks,

[REDACTED]

From: [REDACTED] (CRM) [REDACTED]
Sent: Tuesday, October 3, 2023 10:56 AM
To: [REDACTED] (DE) (FBI) [REDACTED]
Subject: [EXTERNAL EMAIL] - RE: Call

Hi [REDACTED]

I'm moving [REDACTED] to bcc as he is now on detail to another office.

Please let me know when you are available to talk today. I have meetings until about 2:30 p.m. but will be available after that.

Best,

[REDACTED]

From: [REDACTED] (CRM) [REDACTED]
Sent: Tuesday, October 3, 2023 10:48 AM
To: [REDACTED] (DE) (FBI) [REDACTED]
Cc: [REDACTED] (CRM) [REDACTED]
Subject: Fwd: Call

[REDACTED]

I'm currently on detail. I've copied my PIN colleague [REDACTED] who will be able to help you.

[REDACTED]

Begin forwarded message:

From: [REDACTED]

Date: October 3, 2023 at 10:41:08 AM EDT

To: [REDACTED] (CRM) [REDACTED]

Subject: Call

[REDACTED]
Could you please give me a call on my cell [REDACTED] when you have a chance?

Thanks,

[REDACTED]
SA [REDACTED]
FBI Detroit
Grand Rapids RA
[REDACTED]

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION****Import Form****Form Type:** FD-71A - Guardian Complaint Form**Date:** 10/05/2021**Title:** U NTOC2020 343jaj02 Possible Election Fraud in Southfield, MI (DE)**Approved By:** [REDACTED]**Drafted By:** [REDACTED]**Case ID #:** 56-DE-0

(U) ZERO FILE FOR ELECTION LAW MATTERS

Synopsis: U DOCUMENT SYNOPSIS CREATED ON 10-05-2021 09:13 AM--SEE GUARDIAN 694326_DE FOR CURRENT ASSESSMENT DATA.

On 12/08/2020, at 1:01 p.m. Eastern Time, [REDACTED] date of birth

[REDACTED] Center (NTOC) and reported possible election fraud.

[REDACTED] provided the following information:

On 11/03/2020, an unknown subject (UNSUB) wearing a Biden shirt came to [REDACTED] home. The UNSUB addressed [REDACTED] by name and offered to collect her absentee ballot. [REDACTED] told the UNSUB she was not registered to vote. The UNSUB had a tablet with him and offered to register her to vote. [REDACTED] declined and told the UNSUB she did not want to register. [REDACTED] did not provide any of her personal information to the UNSUB.

Recently, [REDACTED] received a voter's registration ID card in the mail. [REDACTED] did not register to vote and did not request to be registered to vote.

[REDACTED] contacted her county and city clerk's offices who won't tell her any information.

[REDACTED] also noted that a few weeks prior to Halloween, she received what she believes was an absentee ballot in the mail. [REDACTED] shredded the ballot. [REDACTED] said she is 100% certain she was never registered to vote

UNCLASSIFIED

UNCLASSIFIED

Title: U NTOC2020 343jaj02 Possible Election Fraud in Southfield, MI
(DE)

Re: 56-DE-0, 10/05/2021

and she has never voted in an election.

Database Queries:

An open source query of mvic.sos.state.mi.us revealed [REDACTED] as a registered voter (see attached).

A Guardian query for [REDACTED] AND [REDACTED] revealed zero results.

A Sentinel query for [REDACTED] AND [REDACTED] revealed one restricted result in the JK Div (zero in the DE Division).

A DIVS query for [REDACTED] with date of birth [REDACTED] revealed zero results.

Enclosure(s): Enclosed are the following items:

1. U Capture1.PNG
2. U Contents of Submission

◆◆

UNCLASSIFIED

From: [REDACTED] (DE) (FBI)
Sent: Friday, April 28, 2023 11:47 AM
To: [REDACTED] (DE) (FBI)
Subject: Voter Fraud Spreadsheet --- UNCLASSIFIED
Attachments: Person Checks_2023.xlsx

RMtFRUserProp: Short-Term Use Email (Transitory)
SentinelCaseld: Short-Term Use Email (Transitory)

Classification: UNCLASSIFIED

=====
Transitory

Hi [REDACTED]

See attached the voter fraud spreadsheet which details all information and outcome of persons search. On other spreadsheet named 'Stats', I've provided some percentage breakdowns per your request. Let me know if there are any specific stats you'd like in addition to those.

Thanks,

[REDACTED]
GR-1/I-21
FBI Detroit – Grand Rapids
c: [REDACTED]
d: [REDACTED]

=====
Classification: UNCLASSIFIED

UNCLASSIFIED

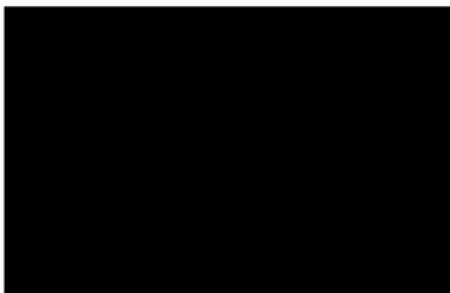


FEDERAL BUREAU OF INVESTIGATION
Electronic Communication

Title: (U) Opening EC

Date: 03/16/2021

CC:



From: DETROIT

DE-C3

Contact:



Approved By: SSA



Drafted By:



Case ID #: 56D-DE-3407960

(U)



STATE OF MICHIGAN;
CDPO - ELECTION LAWS
SENSITIVE INVESTIGATIVE MATTER

Synopsis: (U) To open a full investigation and notify the Public Corruption Unit of the case opening.

Administrative Notes: (U) Consultation with DOJ Public Integrity Section was completed on March 11, 2021.

Enclosure(s): Enclosed are the following items:

1. (U) PIN consultation letter
2. (U) LHM

Details:

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Opening EC
Re: 56D-DE-3407960, 03/16/2021

I. Sensitive Investigative Matter

The above captioned matter is not a "Sensitive Investigative Matter"

II. A brief, general summary of the PC allegation.

The FBI Detroit Field Office (FBI Detroit) was informed that the Michigan State Police (MSP), Michigan Attorney General (MAG), and Muskegon Police Department (MCPD) were investigating allegations of fraudulent voter registrations being submitted to the Muskegon City Clerk's Office (MCCO). MCCO determined the bulk of applications were sent by [REDACTED] from [REDACTED] MCPD estimated [REDACTED] delivered between 8,000 to 10,000 registrations. [REDACTED] informed MCPD investigators that she worked for [REDACTED] under its owner [REDACTED] and [REDACTED] [REDACTED] and that she was paid for voter registration work. The matter was referred to law enforcement by the MCCO. A subsequent investigation by the MSP found a number of prepay debit cards located at [REDACTED] office based in [REDACTED] raising concerns that [REDACTED] as paying people to register.

III. An in-depth summary of the predication setting forth the relevant facts and circumstances, including witness allegations.

Since on or about October 5, 2020, MCCO has received six packages, marked [REDACTED] via U.S. Mail containing voter registration applications. MCCO determined some of the applications were fraudulent based on a number of factors. MCCO determined the bulk of applications were sent by [REDACTED] as [REDACTED] also hand delivered numerous applications with indicators of potential fraud. MCPD estimated [REDACTED] and [REDACTED] had delivered between 8,000 to 10,000 registrations.

MCPD conducted a non-custodial interview of [REDACTED] on October 8, 2020, where she informed MCPD investigators that she worked for [REDACTED]

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Opening EC

Re: 56D-DE-3407960, 03/16/2021

[REDACTED] under its owner [REDACTED] and [REDACTED] and that she was paid for voter registration work. MSP investigators subsequently conducted an interview of [REDACTED] on October 20, 2020, where she stated she was a first level supervisor overseeing "canvassers" with canvassing being conducted in Muskegon, Detroit, Ypsilanti, Southfield, Flint, and Lansing. [REDACTED] told MSP investigators that canvassers were paid through a reloadable "pay card" and that canvassers were paid for each completed form, but later changed her statement and indicated they were paid hourly. [REDACTED] later told MSP investigators that she could not recall her boss' name despite earlier identifying [REDACTED] as her employer. MSP discovered the vehicle [REDACTED] was driving was a rental vehicle rented by [REDACTED]

On October 22, 2020, MSP investigators received authorization to track [REDACTED] movements via a cellphone GPS ping. The information received from [REDACTED] cellphone subsequently showed [REDACTED] had traveled to [REDACTED] on October 23, 2020. An open source search for information associated with that address identified it as an office location for [REDACTED]

MSP subsequently received authorization to search [REDACTED] office located at [REDACTED] for among other things, employee lists, payroll information, and any information on the purchase and distribution of reloadable pay cards. MSP executed the search on October 29, 2020. SAs [REDACTED] and [REDACTED] were dispatched to the search scene due to concerns about weapons located at the scene and SA [REDACTED] saw a quantity of reloadable [REDACTED] pay cards.

IV. A statement that the requisite level of predication exists.

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Opening EC
Re: 56D-DE-3407960, 03/16/2021

There is information or an allegation the subject, and others yet unknown, were engaging in and/or are currently engaged in possible federal criminal activity.

V. The identification of all known SIMS or significant issues involved in the investigation.

The allegations involve potential payments for registrations for the 2020 national election and concern matters which require the concurrence of DOJ Public Integrity Section Election Crimes Unit and the FBI PCU as documented in Section X below.

VI. The identities of the subjects, including all reasonably available descriptive data to be indexed within FBI databases.

Name: [REDACTED]
Date of Birth: [REDACTED]
Sex: [REDACTED]
Race: [REDACTED]
Social Security Number: [REDACTED]
Address: [REDACTED]
Telephone: [REDACTED]
Driver License Number: [REDACTED]

Name: [REDACTED]
Date of Birth: [REDACTED]

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Opening EC
Re: 56D-DE-3407960, 03/16/2021

Sex:

Race:

Social Security Number:

Address:

Telephone:

VII. A citation of the federal criminal statutes that may have been violated/AUSA opinion.

On March 16, 2021, United States Attorney (USA) for the Western District of Michigan [REDACTED] was fully informed of the facts of this case. USA [REDACTED] advised that his office would prosecute [REDACTED] and/or [REDACTED] for violations of 18 U.S.C. 1343 (Wire Fraud) or any other federal criminal laws that could be proven.

VIII. Investigative Strategy.

The investigative strategy may include, but will not necessarily be limited to, obtaining publicly available information, recovering records/information via subpoena, interviews, and consensual recordings.

IX. CDC Review.

CDC review is not required because the above captioned matter is not a "Sensitive Investigative Matter".

X. Notification to PCU and DOJ PIN

Per PCU Program Guide 23.10.1.2 (2), on March 11, 2021, DOJ Attorney [REDACTED] [REDACTED] as advised of the above captioned matter and provided written approval. On March 16, 2021, PCU SSA [REDACTED] was apprised of the same

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Opening EC

Re: 56D-DE-3407960, 03/16/2021

by verbal notification and concurred with the opening.

◆◆

UNCLASSIFIED