# FEDERAL BUREAU OF INVESTIGATION

**Electronic Communication**

**Title:** (U//[redacted]) Opening Document **Date:** 11/03/2020

**From:** PHOENIX
PX-CY-1
**Contact:** [redacted]

**Approved By:** SSA [redacted]

**Drafted By:** [redacted]

**Case ID #:** 288A-PX-3341832 (U//[redacted]) Unknown Subject; Maricopa County Recorder's Office; Cyber Intrusion Data Exfiltration

**Synopsis:** (U//[redacted]) To document the opening of a full investigation.

**Enclosure(s):** Enclosed are the following items:
1. (U//[redacted]) P3 Tip

**Details:**

(U//[redacted])On November 2, 2020, [redacted], [redacted] with the Maricopa County Recorder's Office, phone number [redacted], provided a tip through the Arizona Counter Terrorism Intelligence Center (ACTIC) documenting an attempt to scrape voter registration information. A follow up phone conversation with [redacted] provided the following information:

(U//[redacted])Since October 21, 2020, an intruder was able to obtain voter registration data from, "recorder.maricopa.gov/pollingplace". [redacted] stated an intruder set up a PowerShell script that resulted in the exfiltration of approximately 633,000 voter registration records. [redacted] determined that the voter information was accessed by logging GET requests through the website from October 21, 2020 - November 2, 2020.

Title: (U//[redacted]) Opening Document
Re: 288A-PX-3341832, 11/03/2020

Approximately 930 of the records obtained were sensitive voter information including domestic violence victims, Judges, and law enforcement officers. [redacted] stated that there were no special markings or indicators that would alert to the fact certain voter information was sensitive. The information obtained included: full name, voter ID, party affiliation. [redacted] noted that the information did not include social security numbers.

(U//[redacted])[redacted] stated that the website was "poorly written" and the intruder was able to inject an ID number into the URL. Doing this allowed the intruder to bypass authentication and access the registered voter's information. Normally, a user would enter a known last name, date of birth, and street address along with either the last four of their social security number or a driver's license number; before accessing that voter's information. The website then would provide an ID number attached in the URL after the voter's information was verified. The intruder was able create a PowerShell script where ID numbers were automated and included to the URL in sequential order. [redacted] explained that the voter registration of approximately 633,000 voters was exfiltrated to the IP address [redacted].

On 11/2/20, at around 4:50 PM, the Maricopa County Recorder's Office was made aware that their polling website was not accessible. [redacted] commented that he observed a spike in traffic occurring around 4:17 PM. [redacted] eventually configured a firewall to filter traffic through Cloudflare. This helped to mitigate and enforce traffic rate limits to the website.

[Agent note: [redacted] could not state for certain whether the data exfiltration and increase in traffice were related].

[Agent note: the initial tip sent by [redacted] was included in the 1a file.]

Title: (U//[redacted]) Opening Document
Re: 288A-PX-3341832, 11/03/2020

♦♦