EXHIBIT E

SPECKIN FORENSICS, LLC REPORT,

SEPTEMBER 15, 2022

Speckin Forensics, LLC

120 N. Washington Square, Suite 300
PMB 5068
Lansing, Michigan 48933
517-349-3528 • Fax 954-839-8219

Please Direct Correspondence & Payment Here:
2450 Hollywood Boulevard, Suite 700
Hollywood, Florida 33020
954-763-6134 • Fax 954-839-8219

www.4N6.com

Leonard A. Speckin
Retired Document Analyst

Michael J. Sinke
Retired Latent Print Specialist
Retired Crime Scene Reconstruction
Retired Forensic Document Analyst

Dr. George F. Jackson Ph.D.
Forensic Toxicologist

Erich J. Speckin
Forensic Document Analyst
Ink Dating Specialist

Phillip Matusiak
Computer & Graphics Specialist

Thomas K. Huard Ph.D.
DNA Analyst & Consultant

Marshaun Blake
Arson & Fire Specialist

Anthony A. Milone
Computer & Graphics Specialist
Forensic Document Specialist

Dr. Julie Howenstine
Serologist
DNA Analyst & Consultant
Crime Scene Reconstruction

September 15, 2022

Speckin Forensics was retained to acquire forensic Images of hard drives in Fulton County, Pennsylvania. The images of the drives that are the subject of this report were created on July 13-14, 2022.

A total of six hard drives were tendered for copying and analysis. The hard drives were in the corresponding device and were removed for copying and analysis. The record of the drive and the corresponding machine was recorded. One of the hard drives was not operable at the time of our imaging and therefore was not copied. This can be attempted at a later time with a more time-consuming procedure but has not yet been attempted. The remaining five drives were copied during the time onsite in Pennsylvania. The forensic image of each drive was saved on its own new unused Western Digital 4TB USB hard drive. This allowed for later duplication and examination of the evidence.

Using forensically sound procedures we documented the service tag numbers for all machines and the serial numbers of the corresponding hard drives contained within. Photographs were taken to record this. The drives copied are labeled as follows:

	Service Tag	Computer Name	Serial Number	Machine Model
1	3095PY2	EMSSERVER	59PUPSi1T/ 59PUPSi0T	Dell Precision 3430
3	1FPLNY2	Adjudication01	59OUPRS2T	Dell OptiPlex 3050
4	1FNPHY2	Failed drive	59OUPRRRT	Dell OptiPlex 3050
5	30C4PY2	EMSCLIENT02	59PUPSHNT	Dell Precision 3430
6	30B4PY2	EMSCLIENT01	59PUPSI5T	Dell Precision 3430

The key findings are summarized below:

1. The security measures necessary to harden and secure the machines was not completed. The last update or security patch to the devices shows to be April 10, 2019, and no patches or updates were performed after this date.

2. External USB drives have been inserted on several occasions. We are unaware of any current list of approved external drives that could have been used. Therefore, there is no way to determine if any of the inserted USB drives was from an unauthorized source or if the USB drive further comprised the data or the system.
3. There have been substantial changes to the drives as seen with the inclusion of over 900 .dll files and links created since the date of installation of the Dominion software. This .dll additional pathway is a security breach because of the introduction of an unauthorized script.
4. There have also been no updates to the usernames or passwords as the passwords use default settings like "admin" and "guest". The group policies of the devices remain at default settings which in simple terms allows the username "admin" with password "admin"; complete access to the device.
5. The Adjudication01 workstation has a python script installed after the certification date of the system. This should not be added to the drive after a system has already been certified. This python script can exploit and create any number of vulnerabilities including, external access to the system, data export of the tabulations, or introduction of other metrics not part of or allowed by the certification process.
6. As expected and normal, each of the drives are interconnected in a system to one another. This would be required to provide sharing of data and counts between devices. Because of this networking, unauthorized access any one device, allows unauthorized access to any device connected to the network of devices.
7. An external IP address that is associated with Canada is found on the Adjudication 01. This shows that at least one of the network devices has connected to an external device on an external network. This is the same device that the post certification python script is found.

Procedure:

The hard drives from the computers were removed and connected them to a Forensic workstation. The hard drives were mounted as READ ONLY. Using FTK Imager a bit for bit copy was created using the Expert Witness file format. This is an industry standard format for storing forensic images. During the image creation process a hash value was computed to ensure the integrity of evidence. One of the main uses of hash values is to determine the integrity of data.

The copied data was analyzed using standard computer forensic software generally accepted in the field to search for the elements contained in this report.

Results:

Windows defender was found on the machines which dates to July 2016. No updates have been made since this time. Simply stated this means that viruses or malicious software components created after that date would not be combatted by this protection without the updates.

Further, Dominion published hardening procedures in 2019 that would reduce the chance of the system being compromised and provide additional security measures for the integrity of the system.

Below is a chart that shows external drives that have been connected to the devices examined.

The Dominion voting Systems software was installed on the devices on 04/10/19, 8/16/19 and 8/23/19. This last install date is consistent with the drives Generic, Canyon, and ScanDisk listed below. However, the 2021 drives do not fit this pattern and are unexplained at this point.

Computer Name	Device	Last Connection Date	Connection Time
3095PY2	PNY USB 2.0 Drive	2019-07-31	16:11
3095PY2	Generic USB Flash Drive	2019-08-23	16:54
3095PY2	Canyon USB Drive	2019-08-23	18:07
3095PY2	ScanDisk Cruzer FIT	2019-08-23	18:15
3095PY2	Samsung Flash Drive	2021-04-22	13:49
3095PY2	Kingston Data Traveler	2021-05-03	20:27
1FPLNY2	Samsung Flash Drive	2021-04-30	19:27
1FPLNY2	Kingston Data Traveler	2021-05-05	13:22

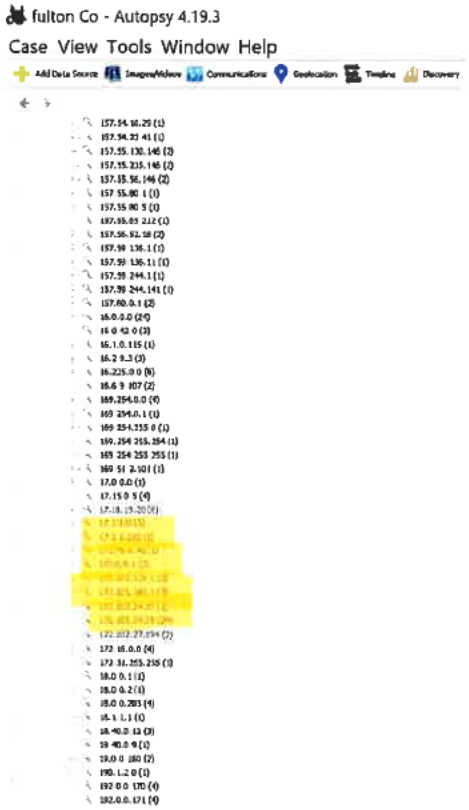
The following chart shows a small sample of .dll activity after the installation date of the voting software.

Name	Deleted	Last Accessed	File Created	Last Written	Entry Modified
UIAutomationTypes.ni.dll	•	08/29/19 08:02:12AM	08/29/19 08:02:12AM	08/29/19 08:02:12AM	10/02/19 04:44:27AM
System.Management.ni.dll		08/29/19 08:02:13AM	08/29/19 08:02:13AM	08/29/19 08:02:13AM	05/18/20 06:50:50AM
UIAutomationProvider.ni.dll	•	08/29/19 08:02:13AM	08/29/19 08:02:13AM	08/29/19 08:02:13AM	10/02/19 04:44:27AM
System.Drawing.ni.dll		08/29/19 08:02:15AM	08/29/19 08:02:15AM	08/29/19 08:02:15AM	10/02/19 04:44:24AM
System.Windows.Forms.ni.dll		08/29/19 08:02:19AM	08/29/19 08:02:19AM	08/29/19 08:02:19AM	10/02/19 04:44:26AM
System.Web.ni.dll		08/29/19 08:02:31AM	08/29/19 08:02:31AM	08/29/19 08:02:32AM	10/17/19 05:55:54AM
System.Messaging.ni.dll		08/29/19 08:02:33AM	08/29/19 08:02:33AM	08/29/19 08:02:33AM	10/17/19 05:55:53AM
System.EnterpriseServices.ni.dll		08/29/19 08:02:34AM	08/29/19 08:02:34AM	08/29/19 08:02:34AM	10/17/19 05:55:52AM

At least six different user and administrator accounts on the devices still have the password "Dvscorp2018!!!". This is the default password for the software at the time of installation. It has never been updated nor was it set to expire as should be the case. This is a glaring issue as this is specifically addressed by the Pennsylvania Secretary of State and referencing NIST.

"All jurisdictions implementing the Democracy Suite 5.5x must ensure that no default passwords are used on any devices and that all passwords are complex and secured. Counties must implement an audit process to review and ensure that no default passwords are used upon equipment install/reinstall and routinely change passwords to avoid any password compromise. The passwords and permissions management must at a minimum comply to the password requirements outlined in NIST 800-63".

The log files for the Adjudication device shows an IP address, 172.102.16.22. This IP address comes back to a location in Quebec, Canada, this is a serious issue to be connected remotely to a Canadian system. We cannot determine when this connection occurred or what data was transmitted, but an external connection was made at some point.



Donald A. Smith

Computer Data Specialist