

Supreme Court of Pennsylvania

Court of Common Pleas Civil Cover Sheet

Delaware County

County

For Prothonotary Use Only:

Docket No:

CV-24-18838-9.25

The information collected on this form is used solely for court administration purposes. This form does not supplement or replace the filing and service of pleadings or other papers as required by law or rules of court.

SECTION A

Commencement of Action:

- Complaint Writ of Summons Petition
 Transfer from Another Jurisdiction Declaration of Taking

Lead Plaintiff's Name:

ROBERT MANCINI

Lead Defendant's Name:

Delaware COUNTY

Are money damages requested? Yes No

Dollar Amount Requested: within arbitration limits
(check one) outside arbitration limits

Is this a *Class Action Suit*? Yes No

Is this an *MDJ Appeal*? Yes No

Name of Plaintiff/Appellant's Attorney:

Check here if you have no attorney and are self-represented (Pro Se) (Lingua)

SECTION B

Nature of the Case: Place an "X" to the left of the **ONE** case category that most accurately describes your **PRIMARY CASE**. If you are making more than one type of claim, check the one that you consider most important.

TORT (do not include Mass Tort)

- Intentional
 Malicious Prosecution
 Motor Vehicle
 Nuisance
 Premises Liability
 Product Liability (does not include mass tort)
 Slander/Libel/ Defamation
 Other: _____

CONTRACT (do not include Judgments)

- Buyer Plaintiff
 Debt Collection: Credit Card
 Debt Collection: Other _____
 Employment Dispute: Discrimination
 Employment Dispute: Other _____
 Other: _____

CIVIL APPEALS

- Administrative Agencies
 Board of Assessment
 Board of Elections
 Dept. of Transportation
 Statutory Appeal: Other _____
 Zoning Board
 Other: _____

MASS TORT

- Asbestos
 Tobacco
 Toxic Tort - DES
 Toxic Tort - Implant
 Toxic Waste
 Other: _____

REAL PROPERTY

- Ejectment
 Eminent Domain/Condemnation
 Ground Rent
 Landlord/Tenant Dispute
 Mortgage Foreclosure: Residential
 Mortgage Foreclosure: Commercial
 Partition
 Quiet Title
 Other: _____

MISCELLANEOUS

- Common Law/Statutory Arbitration
 Declaratory Judgment
 Mandamus
 Non-Domestic Relations Restraining Order
 Quo Warranto
 Replevin
 Other: INJUNCTION

PROFESSIONAL LIABILITY

- Dental
 Legal
 Medical
 Other Professional: _____

NOTICE

Pennsylvania Rule of Civil Procedure 205.5. (Cover Sheet) provides, in part:

Rule 205.5. Cover Sheet

(a)(1) This rule shall apply to all actions governed by the rules of civil procedure except the following:

- (i) actions pursuant to the Protection from Abuse Act, Rules 1901 et seq.
- (ii) actions for support, Rules 1910.1 et seq.
- (iii) actions for custody, partial custody and visitation of minor children, Rules 1915.1 et seq.
- (iv) actions for divorce or annulment of marriage, Rules 1920.1 et seq.
- (v) actions in domestic relations generally, including paternity actions, Rules 1930.1 et seq.
- (vi) voluntary mediation in custody actions, Rules 1940.1 et seq.

(2) At the commencement of any action, the party initiating the action shall complete the cover sheet set forth in subdivision (e) and file it with the prothonotary.

(b) The prothonotary shall not accept a filing commencing an action without a completed cover sheet.

(c) The prothonotary shall assist a party appearing pro se in the completion of the form.

(d) A judicial district which has implemented an electronic filing system pursuant to Rule 205.4 and has promulgated those procedures pursuant to Rule 239.9 shall be exempt from the provisions of this rule.

(e) The Court Administrator of Pennsylvania, in conjunction with the Civil Procedural Rules Committee, shall design and publish the cover sheet. The latest version of the form shall be published on the website of the Administrative Office of Pennsylvania Courts at www.pacourts.us.

Robert Mancini
4 Guernsey Lane
Media PA 19063
Phone 610-506-9827

Fax- None

Email Delcocyber@gmail.com

Representing Self

Alfeia Goodwin
117 Abbey Ter. | 19065
Drexel Hill, PA 19026
267-977-0757

None

Alfeia@mail.com

Representing Self as Candidate

**IN THE CIVIL COURT OF DELAWARE COUNTY,
PENNSYLVANIA**

Alfeia Goodwin, Candidate 5 th District,	:	Preliminary Injunction
Of the United States House of Representatives	:	
Robert Mancini, Delaware County resident	:	
Registered Voter of Pennsylvania	:	
Individually	:	
Petitioners Pro Se,	:	CV-2024 - 8838
v.	:	
Delaware County, PA	:	
Respondent	:	

**APPLICATION FOR EMERGENCY RELIEF AND SEEKING A
PRELIMINARY INJUNCTION**

Petitioners, Pro Se, pursuant to PA. R.A.P. 123, PA R.A.P. 1532(a) and PA R.C.P. submit the following Application for Emergency Relief Seeking a Preliminary Injunction and aver as follows:

INTRODUCTION

1. Petitioner Alfeia Goodwin is a resident and candidate for the 5th District of Pennsylvania in the United States House of Representatives, with the address of 117 Abbey Terrace, Drexel Hill, PA 19026.
2. Petitioner Robert Mancini is a resident, taxpayer, and registered voter in the 5th District of Pennsylvania of the United States House of Representatives, with the address of 4 Guernsey Lane, Media PA 19063
3. The Respondent, Delaware County (heretofore, the “County”), is a jurisdiction and government agency with a business address of 201 West Front Street, Media, PA 19063.
4. The Election Assistance Commission, or EAC, is a federal agency located at 633 Third Street, NW, Suite 200; Washington, DC 20001.
5. The Election Assistance Commission is a federal agency responsible for overseeing the testing and approval of all Electronic Voting Systems in the United States of America.
6. The Department of State of Pennsylvania is a government agency with a business address of 401 North Street; Harrisburg, PA 17120.
7. The Department of State (or Commonwealth) of Pennsylvania is responsible for certifying all Electronic Voting Systems for use in Pennsylvania, having adopted EAC certification standards, and given the EAC has also certified any voting system that would be used by any jurisdiction in Pennsylvania.
8. The November 5, 2024 election is a federal election and all votes in Pennsylvania count equally toward the determination of the Pennsylvania Electoral College votes, and numerous state-wide races, including the Pennsylvania senatorial race.
9. On January 12, 2023, the Acting Secretary of the Commonwealth of Pennsylvania certified the use of the Hart Intercivic’s proprietary election software upgrade known as the Hart Verity Voting Software Version 2.7.
10. In February of 2023, Delaware County Bureau of Elections installed the Hart Verity Voting Software Version 2.7 as an upgrade to its Hart Verity electronic voting system.
11. The Pennsylvania Department of State’s Voting Machine Certification Department, itemizes the various components of the Hart Verity 2.7 proprietary software used in the Hart Verity Voting System, as seen below in Attachment A, page 11:

Proprietary Software

System Component	Software or Firmware Version	Comments
Verity Data	2.7.1	Data management software
Verity Build	2.7.1	Election definition software
Verity Central	2.7.1	High speed digital scanning software
Verity Count	2.7.1	Tabulation and reporting software
Verity Relay Receiving Station	2.7.1	Data transmission software (receiving station)
Verity Transmit	2.7.1	Data transmission software
Verity Transmit Receiving Station	2.7.1	Data transmission software (receiving station)
Verity Print	2.7.1	On-demand ballot printing device firmware
Verity Scan	2.7.1	Digital scanning device firmware
Verity Scan with Relay	2.7.1	Digital scanning device firmware with optional Relay functionality
Verity Touch Writer	2.7.1	Ballot marking device
Verity Touch Writer Duo	2.7.1	Ballot marking device, with internal COTS ballot summary printer and optional audio tactile interface
Verity Touch Writer Duo Standalone	2.7.1	Ballot marking device, with internal COTS ballot summary printer and optional audio tactile interface
Verity Controller	2.7.1	Polling place management device

11 | Page

Figure 1 Hart Proprietary Software¹

12. The Pennsylvania Department of State Certification lists the commercial-off-the-shelf, or COTS, Software and Firmware, authorized for use in the Hart Verity 2.7 system, as follows in Attachment A, page 12 :

¹

<https://www.pa.gov/content/dam/copapwp-pagov/en/dos/programs/voting-and-elections/voting-systems/certification/Hart-Verity-Voting-2.7-Final-for-web.pdf> P11

COTS Software and Firmware

Description	Version
Verity Data, Build, Count, Relay Receiving Station, Transmit Receiving Station	
Microsoft Windows 10 Enterprise 2019 LTSC	10.0.17763
Microsoft SQL Server Standard 2019	15.0.4153.1
McAfee Application Control for Devices (McAfee Solidifier)	8.2.1-143
Verity Central – Central Count Paper Ballot Scanner	
Microsoft Windows 10 Enterprise 2019 LTSC	10.0.17763
Microsoft SQL Server Standard 2019	15.0.4153.1
McAfee Application Control for Devices (McAfee Solidifier)	8.2.1-143
Nuance Western OCR, Desktop, OEM	V20
Verity Print, Touch Writer – Electronic BMD Device, Touch Writer Duo – Electronic BMD Device, Touch Writer Duo Standalone – Electronic BMD Device, Controller, Transmit	
Microsoft Windows 10 Enterprise 2019 LTSC	10.0.17763
Microsoft SQLite	3.36.0
McAfee Application Control for Devices (McAfee Solidifier)	8.2.1-143
Verity Scan – Precinct Paper Ballot Scanner	
Microsoft Windows 10 Enterprise 2019 LTSC	10.0.17763
Microsoft SQLite	3.36.0
McAfee Application Control for Devices (McAfee Solidifier)	8.2.1-143
Nuance Western OCR, Desktop, OEM	V20

Hardware

Figure 2 Figure 1 COTS Software and Firmware²

13. The Election Assistance Commission (EAC) sets national standards for the testing and certification of election machines and software. The EAC standards call for the testing of all software used in elections, before and after an election. The EAC defines software testing, sometimes known as “hash testing”, as a “trusted build”. (Exhibit A).

“Trusted Build – A software build is the process whereby a source code is converted to machine readable binary instructions (executable code) for the computer. A trusted build is a build performed with adequate security measures implemented to give confidence that the executable code is a verifiable and faithful representation of the source code. The primary function of a trusted build is to create a chain of evidence that allows stakeholders to have an approved model to use for verification of a voting system.”

²

<https://www.pa.gov/content/dam/copapwp-pagov/en/dos/programs/voting-and-elections/voting-systems/certification/Hart-Verity-Voting-2.7-Final-for-web.pdf> P12

14. On Monday, September 23, Delaware County Bureau of Elections performed a “trusted build” on a small sample, less than 3%, of the Hart Verity 2.7 voting machines the county intends to use in the November 5, 2024 General Election. Despite the requirement for all software on all machines to be tested with a trusted build validation, only 9 out of 428 voting precincts, or 18 out of 856 machines were tested in Delaware County. (There are two machines per precinct.) Listed below are the URLs published by the county, claiming to show the results of that testing.

15. https://delcopa.gov/vote/hash_test_results.html

16. The results for Marple 3-1 is on the next page

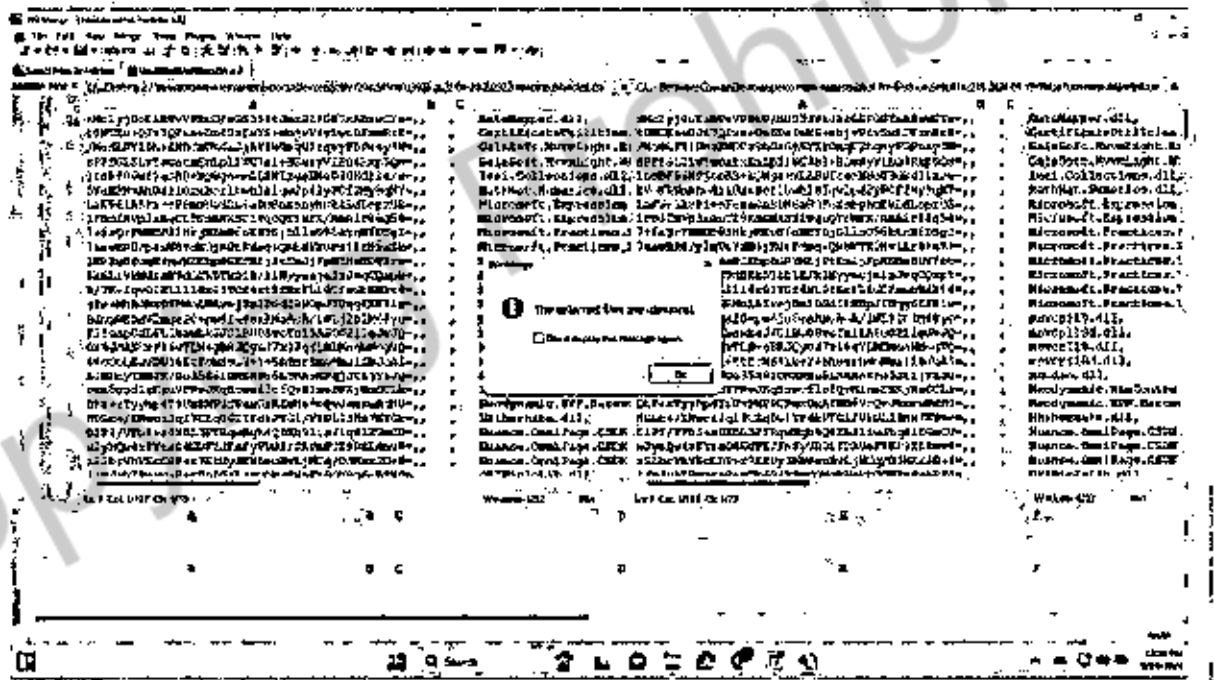


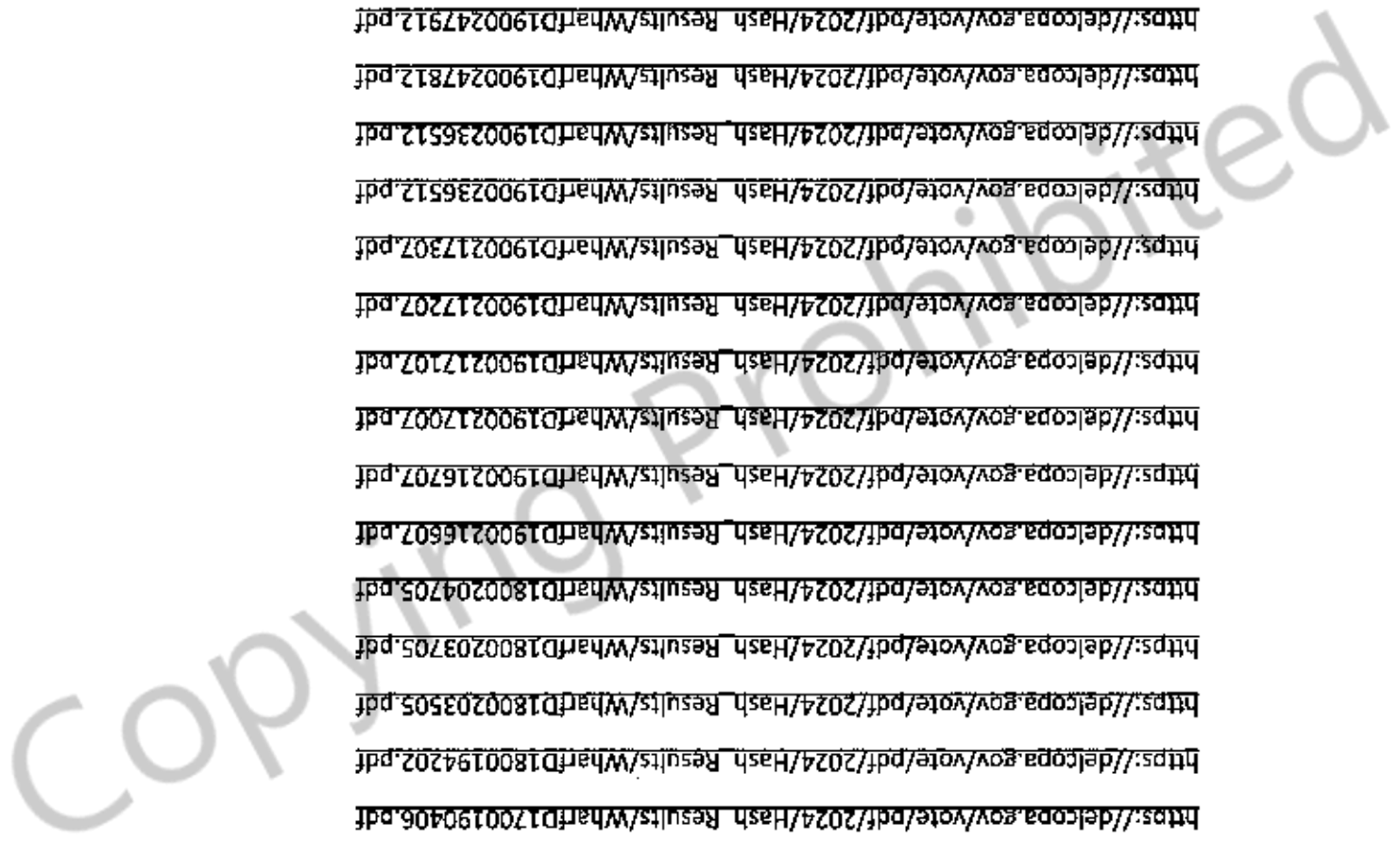
Figure 3 Marple 3-1

17. Below is the list of URLs for the testing results from the remainder of precincts tested:

https://delcopa.gov/vote/pdf/2024/Hash_Results/Aldan_West_S1903222110.pdf

https://delcopa.gov/vote/pdf/2024/Hash_Results/Aldan_West_W1913451711.pdf

- https://delcopa.gov/vote/pdf/2024/Hash_Results/Maple_3_1_51903182210.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Maple_3_1_W1913440511.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Upper_Darby_3_551903215910.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Upper_Darby_3_5W1913442711.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Upper_Darby_7_751903176810.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Upper_Darby_7_ZW1913461211.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Wharfedale1700189706.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Wharfedale1700190406.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Wharfedale1800194202.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Wharfedale1800203505.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Wharfedale1800203705.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Wharfedale1800204705.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Wharfedale1900216607.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Wharfedale1900216707.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Wharfedale1900217007.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Wharfedale1900217107.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Wharfedale1900217207.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Wharfedale1900217307.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Wharfedale1900236512.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Wharfedale1900236512.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Wharfedale1900247812.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Wharfedale1900247912.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Haverford_7_451903185710.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Haverford_7_4W1913438711.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Radnor_6_251903219010.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Radnor_6_ZW2013635001.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Upper_Darby_4_551913562312.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Upper_Darby_4_5W19134427311.pdf
- https://delcopa.gov/vote/pdf/2024/Hash_Results/Upper_Darby_7_851903204310.pdf



on Delaware County's voting machines, invalidates the certification of those machines granted by the Pennsylvania Department of State,

21. Delaware County is in violation of EAC authorization standards and of the Pennsylvania Department of State certification, and is therefore cannot legally run an election using the Hart Verity 2.7 software, that is not identical to the software the Pennsylvania Department of State has certified⁵. It is illegal for Delaware County to proceed with the use of the Hart Verity 2.7 voting system in the November 5, 2024 general election. (Emphasis added).

POTENTIAL HARMS

22. Moreover, and more importantly, the use of machines containing MathNet.Numerics puts at risk the security and accuracy of the election. The potential harm in the use of uncertified machines, loaded with software that has the capability to use algorithms to manipulate election data, is self-evident, as candidates and the general public will be unable to trust the results of the election, be sure that their vote was not diluted, or that election data was not corrupted, altered, or even fabricated.
23. Furthermore, this situation begs the questions of WHY MathNet.Numerics has been installed in Delaware County's voting machines, and BY WHOM?

EVIDENCE OF ELECTION INTERFERENCE

24. The "why" question is self-evident, since the purpose of the unauthorized software is for manipulation of data, in this case election data. Unauthorized software does not install itself. Somebody with access to Delaware County's election machines has deliberately installed MathNet.Numerics in an attempt to INTERFERE with elections.
25. The "by whom" question is unclear, but there are only 3 possibilities as to who would benefit or have the means, motive, and opportunity to do so:
26. There are 3 possibilities: 1 - The manufacturer, Hart InterCivic. 2 - A malignant insider with access to the election system. 3 - An outsider with remote access to Delaware County's voting machines conducting election interference.

5

<https://www.pa.gov/content/dam/copaowp-pagov/en/dos/programs/voting-and-elections/voting-systems/certification/Hart-Verity-Voting-2.7-Final-for-web.pdf> P28

27. The person(s) who installed MathNet.Numerics on Delaware County's voting machines must be investigated for election interference and violating the civil rights of the people of Delaware County to have their votes counted accurately in a secure election process.
28. Regardless of who chose to corrupt the votes of the people of Delaware County, the fact remains that Delaware County cannot legally use the Hart Verity 2.7 machines in the upcoming election on November 5, and therefore the county must immediately prepare for hand counted tabulation, as specified in the Pennsylvania Election Code.

PREREQUISITE FOR A PRELIMINARY INJUNCTION

29. In Pennsylvania, a party must establish the following six prerequisites to obtain a preliminary injunction.
- a. [The] injunction is necessary to prevent immediate and irreparable harm that cannot be adequately compensated by damages;
 - a. [G]reater injury would result from refusing an injunction than from granting it, and concomitantly, that issuance of an injunction will not substantially harm other interested parties in the proceeding;
 - b. [A] preliminary injunction will properly restore the parties to their status as it existed immediately prior to alleged wrongful conduct;
 - c. [The] activity it seeks to restrain is actionable, that its right to relief is clear, and that the wrong is manifest or, in other words, must show that it is likely to prevail on its merits;
 - d. [The] injunction it seeks is reasonably suited to abate the offending activity; and
 - e. [A] preliminary injunction will not adversely affect the public interest.

Warehime v. Warehime, 860 A.2d 41, 46-47) (Pa. 2004) (internal quotations and citations omitted); see also ALL-PAK, Inc v. Johnston, 694, A.2d 347,350 (Pa Super Ct. 1997) (the purpose of a preliminary injunction is "the avoidance of irreparable injury or gross injustice until the legality of the challenged action can be determined.")

30. Here, Petitioner can ably meet all six prerequisites.

THE PRELIMINARY INJUNCTION IS NECESSARY TO PREVENT
IMMEDIATE AND IRREPARABLE HARM

31. In the absence of a preliminary injunction, Delaware County will conduct a Federal Election with Hart Verity Voting 2.7 that has **Unauthorized Software** (emphasis added) on its system. Delaware County will conduct and complete a Federal Election on a system that is not compliant with the PA Department of State's Certification. There will **NOT** be [emphasis added] confidence in the results of the election if Delaware County uses the system as is.
32. A preliminary injunction is necessary to avoid immediate and irreparable injury that cannot be remedied. All candidates, residents, taxpayers of Delaware County, residents of PA, citizens and candidates of the United States of America deserve to have a fair election.

GREATER INJURY WOULD RESULT IN NOT GRANTING INJUNCTION RELIEF

33. Greater injury will result to the Petitioner, Voters of Delaware County, Taxpayers of Delaware County, Residents of Delaware County, Residents of PA, and Citizens of the USA will be injured by Respondent if the requested injunctive relief is not granted.
34. Specifically, if an injunction is not granted, a foreign entity or malicious insider (emphasis added) will have manipulated the results in a swing county, in a swing state and can probably determine the winner of the 2024 Presidential race.
35. By Contrast, the Respondent will suffer no harm by the granting of the injunction and will ensure that the votes cast in the Federal Election will be **ACCURATELY** (emphasis added) tabulated as an error in any one county can swing the results of the state and of the country. Furthermore, the results of the state, and the 19 Electoral votes to either candidate for the Office of the President, which could mean the Office of Presidency for the next four years.

A PRELIMINARY INJUNCTION WILL MAINTAIN THE STATUS QUO

FOR ALL PARTIES

36. Granting the injunction will restore the status quo with respect to the Petitioner's constitutional and statutory rights as they existed prior to the discovery of the illegal software.

37. If the injunction is granted, all the Respondent would have to do is conduct the election results by a hand count, a tried and true method which was used for over 200 years.

PETITIONERS ARE LIKELY TO PREVAIL ON THE MERITS

38. The Petitioners' right to relief is clear, and there is a reasonable likelihood of success on the merit, as set forth in more detail in the Petition.

AN INJUNCTION IS REASONABLY SUITED TO THE OFFENDING ACTIVITY

39. As the offending activity here, the existence of **unauthorized software** (emphasis added) is evidence of illegal activity to interfere with the results of the 2024 Election.

THE PUBLIC WILL NOT BE ADVERSELY AFFECTED BY THE INJUNCTION

40. The Respondent has control over all election activities in Delaware County. In execution of every election, the Respondent is required to follow federal law, state law, and Pennsylvania Department of State requirements. There is no adverse effect of hand-counting the ballots

41. Moreover, the requested relief enables the Respondent to comply with the Pennsylvania Election Law. **WHEREFORE**, Petitioner respectfully asks this Honorable Court to grant a Preliminary Injunction;

42. We ask this Honorable Court to stay the use of the Hart Intercivic Electronic Voting Systems until the issues raised herein have been adjudicated.

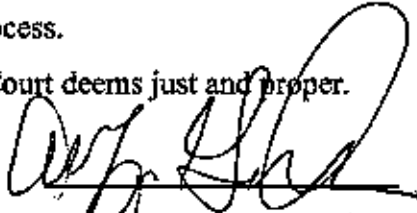
43. We ask this Honorable Court to stay the use of the Electronic Voting Systems that have been tested, quarantining them until the evidence can be analyzed by the FBI and DHS, because it is apparent that a either a foreign agent or a malicious insider has violated the Chain of Custody of the Electronic Voting System in accordance with Exhibit A.

44. We ask this Honorable Court for the performing of a proper Trusted Build Validation on the remaining Electronic Voting machines to determine if that unauthorized software is present on the machines that did not undergo hash testing.

45. We ask this Honorable Court to Direct the Respondent to take all reasonable steps possible to notify the public, candidates, voters, taxpayers, residents, and the Pennsylvania Department of State of the existence of this litigation, and the deficiency of the Respondent in the Election Process.

46. Entering such other relief as this Court deems just and proper.

Date: 10/09/2024



Alfeia Goodwin, Pro Se

117 Abbey Terrace

Drexel Hill, PA 19026

Alfeia@mail.com

267-977-0757



Robert Mancini, Pro Se

4 Guernsey Lane


Media PA 19063

Delcocyber@gmail.com

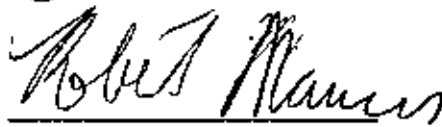
610-506-9827

CERTIFICATE OF COMPLIANCE

I certify that this filing conforms with the provisions of the Public Access Policy of the Unified Judicial System of Pennsylvania case records of the Appellate and Trial Courts that require the filing of confidential information and documents differently than non-confidential information and documents.



Alfeia Goodwin



Robert Mancini

Copying Prohibited

VERIFICATION

Robert Mancini states is making this verification. I verify that the statements are true and correct to the best of my knowledge, information, and belief. I understand that false statements made herein are subject to the penalties of 18 PA. C.S,Subsection 4904, relating to unsworn falsification to authorities

Date : 09 September 2024



Robert Mancini

Alfeia Goodwin states is making this verification. I verify that the statements are true and correct to the best of my knowledge, information, and belief. I understand that false statements made herein are subject to the penalties of 18 PA. C.S,Subsection 4904, relating to unsworn falsification to authorities

Date : 9 September 2024



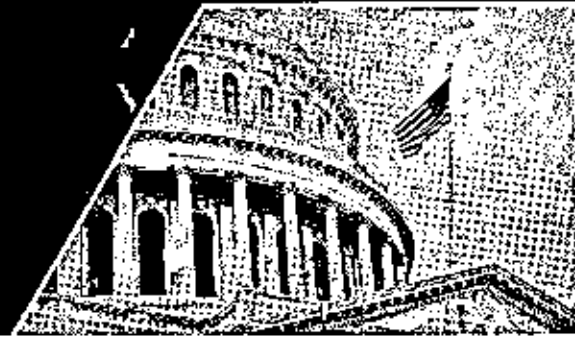
Alfeia Goodwin

Exhibit A

Copying Prohibited



2024 U.S. Federal Elections: The Insider Threat



The Federal Bureau of Investigation (FBI), in coordination with the Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A), the Cybersecurity and Infrastructure Security Agency (CISA), and the U.S. Election Assistance Commission (EAC) prepared this overview to help partners defend against insider threat concerns that could materialize during the 2024 election cycle. For years, federal, state, local, and private sector partners nationwide have worked closely together to support state and local officials in safeguarding election infrastructure from cyber, physical, and insider threats. Because of these efforts, there is no evidence that malicious actors changed, altered, or deleted votes or had any impact on the outcome of elections. Over the past several years, the election infrastructure community has experienced multiple instances of election system access control compromises conducted by insider threats. While there is no evidence that malicious actors impacted election outcomes, it is important that election stakeholders at all levels are aware of the risks posed by insider threats and the steps that they can take to identify and mitigate these threats.

This document outlines several recent examples of election security-related insider threats, discusses potential scenarios that could arise during the 2024 election cycle, and provides recommendations for how to mitigate the risk posed by insider threats.¹

Insider Threats to Elections

In the United States, elections are administered at the state and local levels of government, which has resulted in a diverse landscape of election systems and technologies across the country. Throughout the election cycle, many people are involved in administering or carrying out responsibilities that support elections, including election workers, officials from other divisions of government, vendors, contractors, temporary workers, and volunteers. Understanding what constitutes insider status and how insiders can present risks to an organization are important components of developing a comprehensive Insider threat mitigation program.

An insider threat can be an individual or group who uses their authorized access or special knowledge to cause harm to an organization or entity. This harm can include malicious acts that impact the security and integrity of election systems and information. Insider threats could manifest as current or former employees, temporary workers, volunteers, contractors, or any other individuals with privileged access to election systems and information. This could include individuals who work outside of the immediate election office in roles that support or interact with infrastructure that the election office relies upon.

Recent Examples of Election Infrastructure-related Insider Threats

- A temporary election worker inserted an unauthorized personal flash drive into an electronic poll book containing voter registration data, including confidential information barred from release under state law. The temporary election worker extracted the data because they wanted to compare it against documents they would acquire after the election through the Freedom of Information Act. The breached election equipment was decommissioned after this incident was identified.

¹ The FBI and CISA encourage the public to report information concerning suspicious or criminal activity to their local FBI field office (www.fbi.gov/contact-us/field).

- A State identified a series of digital images of a voting system from one of its counties and related confidential passwords published on the Internet without authorization. Further review determined a county clerk and their subordinate allegedly granted an unauthorized person access to the county's voting machines. The clerk and the subordinate also allegedly disabled the security cameras and gave false identifying credentials to the unauthorized individual.
- A county official reported an attempt to gain unauthorized access to the county's election network during the state's spring primary election. According to the official, someone was granted access into a government office where they were able to plug an unauthorized laptop into a government network. Data from that election network later appeared at a public gathering discussing perceived election fraud issues.
- Two county officials allowed unauthorized users access to their election systems during an audit process, resulting in the state's chief election official subsequently decertifying the machines and prohibiting them from being used in future elections.

Potential for Foreign Adversary Exploitation of Insider Threats

To date, the examples of insider threat activity related to the elections process have been domestic in nature, both in terms of the actor and the motivations. However, since at least 2016, a growing number of foreign adversaries have continued to monitor election networks and attempted to influence or interfere in U.S. elections. While we assess that the threat of a foreign adversary gaining access to election infrastructure through a witting insider is minimal, the perceived normalization (or steady-state) of election influence or interference might help drive some adversaries to push the boundaries of U.S. "red lines," such as targeting and exploiting U.S. persons or election workers to interfere in U.S. elections. One way this foreign derived threat could manifest is via attempts to exploit insider access to interfere with election infrastructure or processes. Foreign adversaries, as well as other malicious actors such as criminal networks, could attempt to gain insider access through a variety of methods.

- Adversaries may seek to gain insider access by exploiting a targeted insider's ideological views, providing financial incentives, or using proxy organizations or diplomatic presence to establish contact with an individual either already in a position of trust or would be willing to seek out and acquire a position on behalf of the foreign actor.
- Adversaries may attempt to blackmail or coerce an insider to leverage the insider's access, collect insights on election security efforts and vulnerabilities, or direct the insider to perform malicious activity. Prior to initiating contact, the foreign adversaries likely would collect information on the target to uncover anything they could use for blackmail or coercion. The type of information could include financial debts, and potentially embarrassing or illegal activity.

In the event an adversary was to gain access to election infrastructure via an insider, they could potentially use that access to disrupt processes and/or spread false information in an attempt to discredit the electoral process and undermine confidence in U.S. democratic institutions.

- If an adversary gained access through an insider to election systems in a particular jurisdiction, such activity could expose voters' personal information, hinder voters' ability to access accurate information on election day or render these systems temporarily inaccessible to the public or election workers, all of which could slow, but would not prevent, voting or the reporting of results.
- In addition, adversaries could also employ insiders to assist with their malign influence operations to undermine American confidence in the security and integrity of the elections process. An insider could provide an adversary with material to develop or amplify messaging challenging election system security, results, or operations. This

includes through coordinated data leaks or the publication of information alleging an adversary's compromise of election infrastructure.

Potential Indicators of Insider Threat Activity

Individuals at risk of becoming insider threats often exhibit warning signs, or indicators.² The following list is not all inclusive, but contains potential flags that election officials should be alert to and seek further review by authorities:

- Attempting to alter or destroy ballots, mail-in ballot envelopes, administrative documentation, or allowing others to access these materials without prior approval.
- Without need or authorization, accessing systems, equipment and/or facilities they have no need to access or providing unauthorized personnel access.
- Turning off security cameras or access control systems or disregarding two-person rule requirements.
- Without need or authorization, taking proprietary or other material home via documents, thumb drives, computer disks, or e-mail. Unnecessarily copying material, especially if it is proprietary or sensitive.
- Remotely accessing the computer network at odd or unexpected times atypical for normal operations.
- Disregarding agency computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information.
- Intimidating or threatening other staff.

Securing Your Organization: Building an Insider Threat Mitigation Program

Election workers and their private sector partners regularly employ practices designed to deter, detect, or prevent harmful acts by insiders, whether or not they use the term "insider threat" or have articulated their approach and practices in a documented program. From handling ballots in teams of two (often bipartisan), to robust chain-of-custody procedures, to the presence of observers during voting and ballot counting, many longstanding core election practices have been designed with insider threat mitigation in mind. Nevertheless, election infrastructure stakeholders may benefit from documenting their approach and establishing a more formalized insider threat mitigation program. Such actions can help identify gaps in current practices and inform the organization's broader approach to risk management.

Organizational culture should also reinforce proactive reporting of employee concerns and security issues as a core component of securing the environment. From this foundation, a successful insider threat mitigation program should implement practices, strategies, and systems that limit and track access across organizational functions. Provided they receive the necessary oversight to ensure they are being applied appropriately, preventative measures against insider threats also contribute to detecting threats by establishing transparent, auditable election systems and processes and then identifying outliers or anomalies for investigation. Key elements of election infrastructure insider threat mitigation programs include:

- **Standard Operating Procedures (SOPs)** describe the sequence of steps or requirements to complete a task. Examples can include requiring visual signs to identify authorized personnel in specific areas or requiring the "buddy system" or a two-person minimum for handling sensitive tasks. Checklists are helpful tools for promoting adherence to SOPs.

² (U) The Insider Threat: An Introduction to Detecting and Detering an Insider Spy | FBI | 21 May 2016 | <https://www.fbi.gov/file-repository/insider-threat-brochure.pdf/view>

- Physical and Digital Access Control** systems can detect and prevent insider threats. Access control systems should apply the principle of least-privilege, giving individuals access only to systems required to perform their essential functions. Access privileges may change leading up to an election or other key dates. Physical access controls may include limiting access to facilities, equipment, devices, tamper-evident seals and bags, and other assets as well as providing video surveillance of physical assets. Digital access controls grant access only to necessary systems, assets, data, or applications related to an individual's job or function. In both cases, access logs, control forms, and surveillance video provide auditable records of who accessed a physical or digital asset, as well as when it was accessed. Overall, access control systems prevent any one individual from gaining entry to all assets within an organization and reduce potential harm to physical or digital systems. If an incident is suspected, access logs and control forms can help with post-incident investigations and even serve as evidence.
- A key challenge around access control for election workers is access to the state voter registration database system. The state may not always know who has access within each local election office, so it is important for jurisdictions and state offices to work together to regularly confirm and update a list of authorized users and associated privileges.
- Chain of Custody Procedures** track the movement and control of physical and digital assets by documenting each time an asset is handled or transferred and who was responsible for it. This can help prevent unauthorized access to sensitive systems, detect the presence of an insider threat, provide evidence, and improve remediation time if an incident occurs. It produces an auditable record of an asset's transfers and transactions, enabling detection of a potential threat if there is a gap in the chain.
 - Zero Trust Security** is based on the principle of "always verify." Instead of assuming that everything that happens on an organization's networks and systems is safe, the zero trust approach assumes that a breach has or will occur and verifies each request as though it is unauthorized. A zero trust approach explicitly verifies every request for access, regardless of where it originates or what resource it accesses. Many digital systems now include zero trust security features that can be turned on, such as always requiring users to enter their password rather than storing it in the device's memory. Election infrastructure stakeholders may also consider procedures like implementing the "two-person rule" (require at least one observer to be present) or working in bipartisan teams when accessing sensitive resources.
 - Continuous Monitoring** is a key practice for detecting anomalous behavior, to include potential insider threats. It involves a combination of the human and digital tools—such as access logs, video surveillance, endpoint detection and response software—underpinned by a strong organizational culture of proactive reporting.
 - Auditing** of all election and business processes should be a routine part of election administration before, during, and after an election. Audits validate whether measures such as access control and chain of custody are functioning properly, collecting and maintaining necessary data, and being used appropriately by staff. They also provide the opportunity to review records (access logs, security footage, chain of custody forms, etc.) and identify any potential gaps or areas for improvement. It is recommended to build audits into an organization's SOPs.
 - Follow Cybersecurity Best Practices** for systems and networks to implement a defense-in-depth approach that prevents single points of failure from being enough for a system compromise. These security best practices are also designed with the expectation that a malicious actor has already obtained access to a like system or software to try and identify vulnerabilities. Cybersecurity best practices like multi-factor authentication, patching and updating, and network segmentation all help minimize the potential security impact if an incident, like an insider threat, were to occur.

- Reporting all incidents to the appropriate authorities so they can be investigated and documented can prevent or reduce the likelihood of similar incidents occurring in the future.

Establishing and maintaining necessary standard operating procedures, access controls, zero trust security, and chain of custody procedures are necessary facets of election administration. Further, they must be reviewed, tested, and audited before, during, and after elections. Altogether, these measures support the integrity, reliability, and security of an election, providing the evidence to build public confidence in the process. To assist stakeholders with their insider threat mitigation efforts, CISA developed an "Insider Threat Reporting Template" and an "Insider Threat Investigation Template" as tools for organizations to download, review, and incorporate into their insider threat mitigation programs. These templates and "Insider Threat Reporting Templates User Guide" are annexes to this guide and can be found on the CISA #PROTECT2024 website and are linked below.

Additional Election Security Resources and Contacts

The FBI and CISA encourage the public to report information concerning suspicious or criminal activity to their local FBI field office (www.fbi.gov/contact-us/field).

For additional assistance, best practices, and common terms, please visit the following websites:

- [Protected Voices – FBI](#)
- [#Protect2024 - CISA](#)
- [Election Security – U.S. Election Assistance Commission \(eac.gov\)](#)
- [Election Security - Dept of Homeland Security](#)
- [Election Crimes and Security – FBI](#)

Copying Prohibited



Insider Threat Reporting Templates

The Cybersecurity and Infrastructure Security Agency (CISA) created these reporting templates as a tool for stakeholder organizations to download, review, and incorporate into their insider threat mitigation programs. The **Reporting Form** and the **Investigative Form** are fillable PDFs that can be used with any insider threat program. Like other templates CISA has developed, stakeholders can utilize the forms in their current format or use them as an example in developing their own products internally.

The **Reporting Form** allows individuals to submit concerns related to a potential insider threat to the appropriate point of contact within their organization. This form features a "submit" button that organizations can edit to auto-generate an email to the appropriate mailing address within the organization. An organization intending to use the Reporting Form will need to edit the "submit" button as outlined in this document before making the form available for employee use. This helps ensure that all reports are collected centrally by the appropriate selected recipient(s) or inbox.

The **Investigative Form** is designed to help organizations document incidents and determine appropriate next steps, including, but not limited to, review by an organization's Threat Management Team, referral to law enforcement, or other follow-on actions as necessary to protect the organization and its employees. This will assist stakeholders as they keep a record of organizational actions related to an insider threat incident, promote accountability of necessary steps to protect assets, and to identify vulnerabilities in the effort of mitigating future insider threats.



The forms are downloadable and the data collected is controlled and managed by the policies and protocols of the stakeholder organizations.



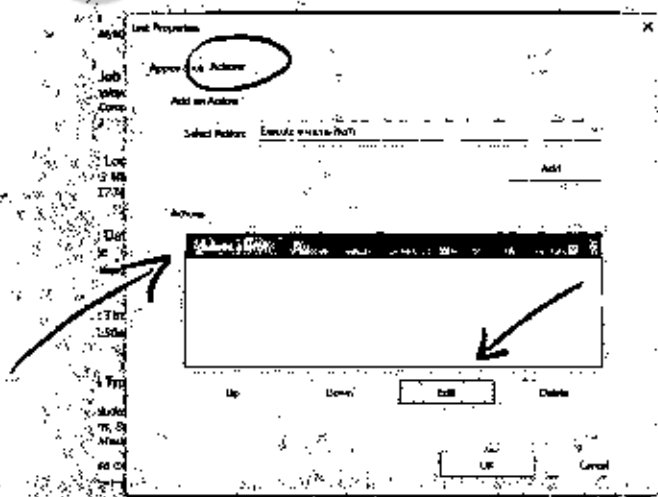
If you have a concern about an immediate threat in the workplace, contact your local law enforcement. The reporting and investigative templates are not intended to provide any organization with the authority to perform activities that they are otherwise not able to perform under applicable law, regulation, and policy. Consult with your legal counsel before implementing these forms in your organization.

EDITING THE REPORTING FORM FOR YOUR SPECIFIC ORGANIZATION:

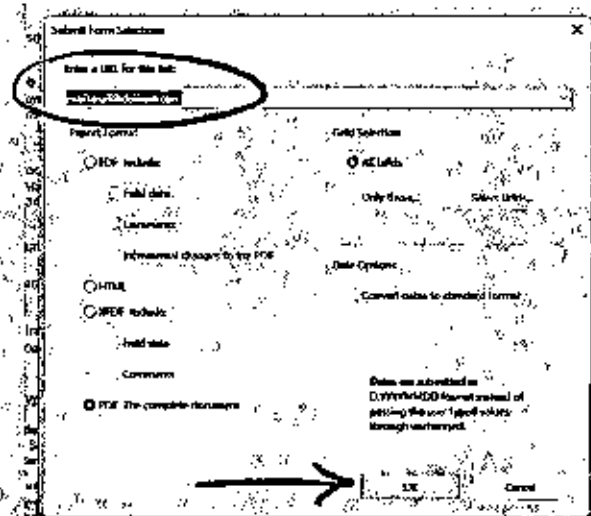
1. Right-click **SUBMIT** button and click "Edit Link..."



2. Navigate to "Actions" tab and edit the "Submit a form" action



3. Edit the "mailto:uri@domain.com" line to your preferred email address and click OK



Insider Threat Reporting Template

WORKPLACE REPORTING FORM

The reporting and investigative templates are not intended to provide any organization with the authority to perform activities that they are otherwise not able to perform under applicable law, regulation, and policy. Consult with your legal counsel before implementing these forms in your organization.

Please use this section to report any suspicious activity in the workplace, focusing on documenting the incident and providing relevant details about the observed behavior/incident:

1 | Description of Incident

Provide as many details as you can regarding the incident and your observations.

2 | Incident Location

Example: 123 Main Street, Anytown, ST 12345

3 | Incident Date or Date Range

4 | Incident Time(s)

Example: 11:30 A.M.

5 | Concern Type

Examples include: Verbal/Written Threats; Terrorism/Violent Extremism; Personal Conduct; Financial Considerations; Substance Abuse; Behavioral Considerations; Criminal Conduct; Mishandling Protected Information; Misuse of Information Technology; Cyber Crime; Espionage; Financial/Intellectual Property Theft; Workplace Violence

Please share details about the individual(s) associated with the suspicious activity in the following section:

6 | Name (or Description if Unknown)

Example: John Doe

7 | Job Title

Example: Analyst, Sales Rep, Software Engineer

8 | Role or Job Type

Example: Employee, Contractor, Consultant, Vendor, etc.

This reporting template is intended to document activities and behaviors that are suspicious or indicative of criminal activity. Such activities or behaviors should be reported only when there are articulable facts to support a rational conclusion that the behavior is suspicious or suggests criminal activity. Do not report based on constitutionally protected activities or on the basis of race, ethnicity, religion, gender, sexual orientation, disability, or other such characteristics, and do not report based on a combination of only such factors. If you have a concern about an immediate threat in the workplace, contact your local law enforcement.

SUBMIT

Insider Threat Reporting Template

WORKPLACE INVESTIGATIVE FORM

REPORT NUMBER

The reporting and investigative templates are not intended to provide any organization with the authority to perform activities that they are otherwise not able to perform under applicable law, regulation, and policy. Consult with your legal counsel before implementing these forms in your organization.

INCIDENT DETAILS

- 1 | **Incident Description** | *Outline incident in further detail (i.e. witness statement, etc.). What IT systems were compromised? What technology identified the breach (if applicable)?*
- 2 | **Concern Type** | *Examples include: Verbal/Written Threats; Terrorism/Violent Extremism; Personal Conduct; Financial Considerations; Substance Abuse; Behavioral Considerations; Criminal Conduct; Mishandling Protected Information; Misuse of Information Technology; Espionage; Financial/Intellectual Property Theft; Other*
- 3 | **Has the appropriate security professional been notified?** | Yes No N/A
- 4 | **Has the Insider Threat Management Team been notified?** | Yes No N/A

INFORMATION ON THE PERSON OF INTEREST

- 5 | Name
- 6 | Job Title
- 7 | Labor Category
- 8 | Clearance Level / Special Access
- 9 | Network Privileges
- 10 | Equipment Used in Incident
- 11 | Office Location
- 12 | Incident Date or Date Range
- 13 | Incident Time(s)

INVESTIGATOR/INTAKE OFFICIAL'S INFORMATION

- 14 | Name
- 15 | Contact Information
- 16 | Position

ADDITIONAL INFORMATION

17 **Initial Recommendations** *Does law enforcement need to be involved? What action needs to occur to keep individuals safe?*

18 **How was the suspicious activity detected?** *What activity occurred? What was the individual's main motivation (if known)? Were any organizational policies violated? How were the security policies/procedures evaded if possible? What action did the organization take to mitigate and prevent an incident?*

19 **Next Steps, Follow-up, and Conclusion** *What actions did the organization take? Were consequences for the individual recommended to HR such as a formal warning, suggested counseling, or termination? Was the matter sent to law enforcement for further investigation? Were witness interviews conducted? What action must come next in this particular instance?*

20 **Recommendations / Updates / Changes to Make** *What security considerations should the organization address? What changes need to be made to protect the organization's high-value assets? Did the reporting pathway lead to a successful mitigation or prevention? If not, what security gap needs to be addressed? Is increased monitoring of the individual needed?*

REPORT REVIEWED BY

Name

Title

Law Enforcement Investigation Number (if applicable)

Investigating Office (if applicable)

Date

Robert Mancini
4 Guernsey Lane
Media PA 19063
Phone 610-506-9827
Fax- None
Email

Alfeia Goodwin
117 Abbey Terrace
Drexel Hill, PA 19026
267-977-0757
None

Represent Self

IN THE CIVIL COURT OF DELAWARE COUNTY OF PENNSYLVANIA

Robert Mancini, resident : Petition and Preliminary Injunction
Alfeia Goodwin, Candidate 5th District :
Of PA, US Congress :
Jointly Plaintiffs, :
v. :
Delaware County, PA : CV-2024- 8838
Defendant :

CERTIFICATE OF SERVICE

I hereby certify that on 11 October 2024 a true copy of the Complaint and Preliminary Injunction will be served upon the following in the following in the manner indicated:

VIA the Sheriff

Sharon Scattolino, County Clerk,
Office of Open Records Officer
201 West Front Street, Room 206
Media PA 19063


Robert Mancini