INSTITUTE FOR

CYBER CIVICS

Cyber Security Handbook for Poll Watchers and Election Observers

Supplemental Training Material

v1.4 October 2024

Introduction and Glossary of Terms

Purpose of this Handbook

The purpose of this Handbook is to provide Poll Watchers and Election Observers with non-partisan insight into how to spot potential cybersecurity issues during the US election season. In accordance with each state law, Observers will receive official guidelines and/or training in their state's rules and protocols for the Observer role. This Handbook is intended as *voluntary* and *supplemental* to official training and is designed for educational purposes. It will be of support for any Poll Watcher/Observer stationed in a voting location or in final tabulation or recount areas.

The Institute for Cyber Civics' intent with this Handbook is to educate the Election Observer on what to be aware of while he/she is carrying out their poll watching duties. While some of the items are somewhat "techy", we've provided a Glossary on Page 4 and have also focused on providing observable "symptoms" of Potential Issues, so that Poll Watchers can more easily spot a potential issue before it escalates, even if that individual is non-technical. This is not intended as a deeply technical document; for greater technical specifications, please refer to other publications by our Institute or links available on the Institute's website.

To the Poll Watcher:

The Poll Watcher role is critical in election process, as it provides a great service to validate the integrity, resilience, and fairness of the election. Thank you for your service to the country and to your fellow citizens!

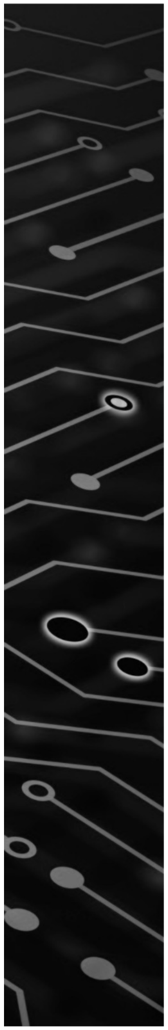
The adage is true: If you see something, say something! Being vigilant about subtle issues or abnormalities can help you spot potential cyber security issues. At all times, be aware of and adhere to your State's rules and protocols. Also:

Step 1: Familiarize yourself with the Potential Cyber Issues scenarios contained in this Handbook

Step 2: On Election Day, be ready to capture notes about any suspected issue you spot. If allowed in your state, capture photo/video evidence, too

Our Institute recommends you use the ImageProof app when capturing photo and video evidence. Download the app (for iPhone and Android) at https://imageproof.io/. Instructions are available on the website and in the app. Note: no personally identifiable information or device data is captured when you use the ImageProof app, and the media you capture in the app is tamper proof!

Step 3: Report any abnormality right away, per your training, to the appropriate election official on site and to your Team Coordinator!



Glossary of Terms

You do NOT need to be a tech expert to spot a potential cybersecurity issue! Familiarize yourself with the below Glossary of Terms. This will help you as you learn about Potential Cyber Issues to be on the lookout for.

Access: Your ability to get to something, in the physical sense – like walking up to an actual computer and touching it – or in the digital sense – like using a keyboard to type in a digital ID and password to log into a computer.

Code: A set of instructions written in a language that a computer can understand to perform specific tasks. Think of it like a *recipe* for a machine:

- **The instructions (code)** tell the computer what to do, step by step.
- **The computer (chef)** follows the code exactly to get the desired result—whether that's displaying a webpage, running a video game, or calculating numbers.

Insider: An individual who has an authentic and valid physical or digital ID with which to access systems or data. An Insider can also be a threat, if he/she uses that access for nefarious purposes

Logs: Records or "diaries" that track what's happening in a computer system, network, or software. Think of them as **detailed journals** that document every important event—like actions, errors, or changes—so people can go back and review what happened. Imagine it like a **flight control tower**. The controllers write down every plane's arrival, departure, and issue in a logbook. If something goes wrong (like a delayed flight), they can look at the log to find out what happened. It's the same way in systems and software, but the actual system creates its own logbook that can be inspected when something goes wrong.

Network: A group of devices (like computers, phones, and servers) connected so they can communicate and share information with each other. The biggest network is the global **internet**! A smaller network can be like what you have at **home** or an **office**, where your phone connects to your smart TV, or your work laptop connects to a work printer. A **wireless** network (Wi-Fi) requires no cables for devices to connect to each other through radio signals. An **unsecure network** is where anyone with any device can jump on a network – no password or ID needed – and access the internet. *Using unsecure networks is not a safe practice.*

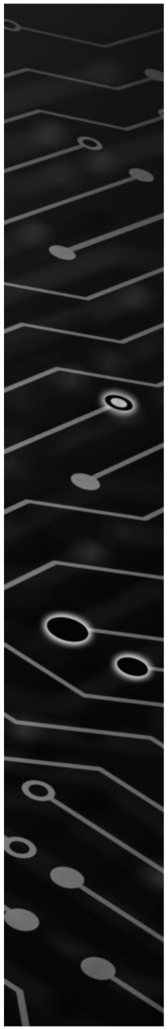
Server: a powerful computer that provides services, data, or resources to other devices (like a laptop, tablet or phone), over a network (like the internet). Think of this in terms of how a restaurant kitchen works:

- **The kitchen (a server)** stores ingredients (data) and recipes (software for using data in certain ways)
- **The customers (devices)** make requests of the kitchen (the server), like ordering a pizza
- **The kitchen (a server)** prepares the food using ingredients and recipes (data and software) and sends the appropriate order to the table (your device).

Server room: A dedicated, access-controlled space that houses servers and other important computer equipment needed to run websites, apps, databases, and networks. It's like the brain center of digital operations.

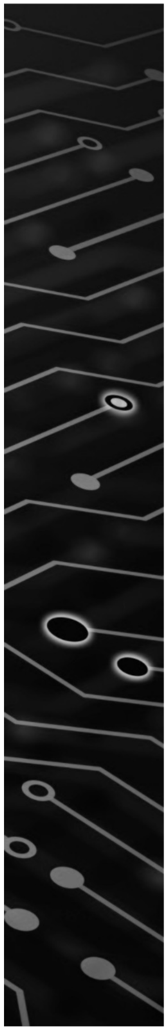
"**Voting systems**" or "**Election Systems**" or "**Voting Machines**":
Any technology, or string of technologies, by which the elections are conducted. These systems and machines can range from:

- Voter registration software and data created when a citizen registers to vote
- Voting day check-in stations, e-books or laptops, and the software on them
- Machines where voters cast their ballots, and the software on them, as well as the data they produce (the vote)
- Tabulation machines and the software on them (to count the votes)
- Servers that support the above, and the network(s) they are connected to.



Potential Cyber Issues, and How to Spot Them

Potential Issue 1: Unauthorized Access to Voting Systems



What do I look for?

Be on the lookout for **unusual individuals or persons with suspicious credentials** trying to access *areas* where voting machines are being stored or trying to access the systems themselves.

- Proper credentials may include a visible, official badge with an accompanying photo that matches their likeness
- If in doubt, and the individual is accessing storage areas or attempting to access the voting machines, follow your Election Observer guidance (varies by state) on who to immediately raise this issue to
- See also "Potential Issue 2" – the red flag of software updates or patches of systems on Election Day.

Why is this Important?

Unauthorized individuals could potentially load malicious software or inject malicious code into an election system, which could impact the integrity election results.

Potential Issue 2: Software Updates on Election Day

What do I look for?

Any **attempts to update, patch or service** voting machines or election systems on Election Day should be a red flag.

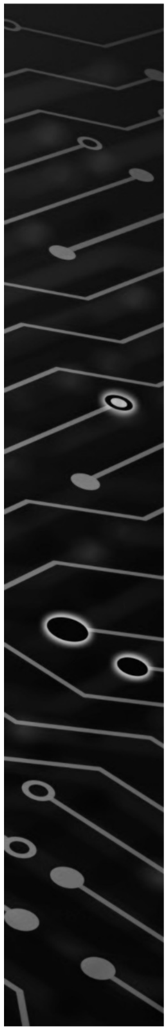
- Best practices in IT and Cybersecurity are that changes to software and maintenance of machines need to have been completed well before voting begins, with full testing by appropriate IT staff, and then validation by election officials.
- During an election, there should be no maintenance of voting systems, patches to the system, or updates to the software. This is what is called a “Change Freeze Window”.

Regardless of the reasoning, rationale, or person conducting the work, any attempts at maintenance, patches or system updates on Election Day should be immediately reported in alignment with your Observer protocols (varies by state) and to your Team Coordinator.

Why is this Important?

System updates or software patches implemented while the election systems are in active use for voting could interfere with the integrity of the voting data already collected and/or could inject nefarious code into system software which could interfere with the integrity of election results.

Potential Issue 3: External Devices Attached to Election Systems



What do I look for?

Keep a keen eye out for clues that the election systems might have **physical tampering**. The voting machines should have seals over any open port (so that a USB drive or cable cannot be inserted) and potentially over the seams of the machine itself. Remember to follow your state's official Observer protocols when it comes to inspecting systems.

- Be suspicious of any external USB drives, memory cards, or other devices plugged into voting machines or election systems
- Be alert for any broken seal, or a seal that appears it may have been tampered with (e.g., a lifted edge or serration across it)
- If your state permits it, conduct regular, periodic visual inspection of voting systems, in accordance with your Observer protocols, to ensure all seals remain intact and untampered with, and that there are no devices or cables attached to the voting system.

Why is this Important?

Insertable devices (like a thumb drive) could be used to introduce malicious software (malware) into the election system which could extract or manipulate sensitive voting data.

Potential Issue 4: Unexplained Machine Behavior

What do I look for?

Pay attention to any malfunctioning or unusual behavior of voting machines or voter check-in stations. Malfunctioning could look like:

- Delays in system processing
- Auto restarts
- Frequent requirement for restarts
- Freezing of the screen (BSOD or “blue screen of death”).

Any of these could appear as an impact to *one* system, could look like *multiple* machines experiencing outages simultaneously, or could appear as an outage of an end-to-end voting infrastructure.

Why is this Important?

Any of the above unexplained machine behaviors could be signs of underlying hardware failures, software crashes, malware infections or attempts at system hacking, any of which can interrupt or interfere with the elections and/or undermine integrity of elections.

Potential Issue 5: Unapproved Wireless Capabilities, and Unsecure Networks

What do I look for?

Depending on your state, **voting machines may be *prohibited*** from having wireless capabilities activated. In certain jurisdictions, *a portion or all* of the election infrastructure **may be permitted** to be connected to a secure network. Know the rules in your state/county.

While you won’t inspect election systems as an Observer, you can check in the vicinity of voting for Wi-Fi networks and for any systems which are trying to ping to the internet:

- In an area you are allowed to use your phone, open “Settings>Wi-Fi” to see if there are any device or network names. Look especially for any that are not secure (they won’t have a lock icon next to them). Device names may also be visible (with or without a lock next to them), and might have a name similar to a voting machine brand
- Note also any publicly available internet, and look around, in areas you are permitted, to see if a password is posted for the public to see (this often happens in libraries)
- Take a screen shot of these wireless networks and devices you see on your phone
- If you suspect there might be an issue, follow up according to your state’s Observer protocols and with your Team Coordinator
- Check several times through your duty day to be vigilant to spot anything new that may pop up.

Why is this Important?

Machines which are connecting to a network when they are not supposed to be able to at all, or which are connecting to an old or unapproved network, may create an opportunity for a threat actor to gain malicious access to the election systems or to the voting data itself.

Potential Issue 6: Unsecured or Unmonitored Voting Machines, Equipment or Cables

What do I look for?

Voting machines and electronic systems should be properly secured, and there should be no unattended/unmonitored machines, or systems that are not properly locked down or locked away. Always follow your state’s Observer protocols, and look for good practices such as:

- Server rooms, network cables, and connections used for the election process, as well as unused voting machines, should be properly secured in a room, which is monitored at all times (e.g., via CCTV camera)
- All access to election equipment rooms should be meticulously documented (sign-in, sign-out)
- All in-use voting machines and check-in systems used on Election Day should be visible to election officials, and therefore to Observers. No in-use systems should be obscured from sight (e.g., under a desk)
- Any laptop or e-check-in used in the voting process should have its screen locked when the authorized user is not sitting in front of it

Why is this Important?

Unattended devices can be tampered with, and potentially used to access and tamper with election infrastructure and/or voting data, which could undermine the integrity of the election.

Potential Issue 7: Network Abnormalities (two parts)

7.1 What do I look for?

In certain jurisdictions, a portion of the election infrastructure may be securely connected to the internet. Be aware of any sudden or **unexplained disconnections** of an election system from the network (e.g., a laptop suddenly going off-line).

Why is this Important?

Sudden disconnections of elections systems could be a result of a cyber attack attempting to isolate a system and disrupt the voting process.

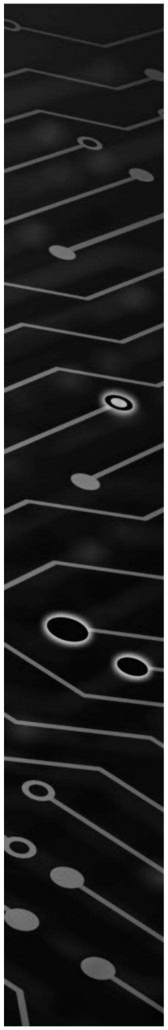
7.2 What do I look for?

In certain jurisdictions, a portion of the election infrastructure may be securely connected to the internet. You may observe an election worker experiencing **unusual delays in their connection speed**. These delays could happen during the normal work of a voting system or it could be during an especially critical phase such as tabulation or transmission of vote totals. This might look like an election worker being especially frustrated with the slow speed of their connection.

Why is this Important?

Unexplained network congestion or slowness could suggest a system is under some form of cyber attack such as an attempt to manipulate its data transmission.

Potential Issue 8: Voting Data Leak or Breach



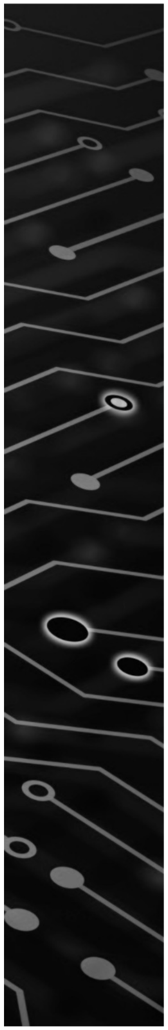
What do I look for?

Take very seriously any **news about a data leak** or data breach. Furthermore, pay special attention to any **suspicious access to data**, whether in physical or digital form, like mis-handling paper ballots or individuals digitally accessing systems or servers outside of protocol (*see also Potential Issue 1*).

Why is this Important?

With access into voting data, or to the software that processes the data, data sets could be "poisoned", or the analytics models used to count the votes could be tampered with. Any malicious access to or leakage of voter information could also compromise the privacy or safety of voters.

Potential Issue 9: No Backup Plan for an Outage or Incident



What do I look for?

Research ahead of your duty day what your state/county's **"Plan B" or contingency plan** is should there be a systems outage during Election Day.

Poll Workers should have a documented process they will follow on which they have also been trained. Backup processes (such as using paper ballots if the systems go down) should be well understood by Poll Workers, and the supplies to conduct their backup plan need to be readily available.

If an incident happens where the contingency plan must be invoked, look for things like:

- Speedy switchover to the backup plan, to ensure least disruption possible to the voters
- Election officials may use a secure, paper copy of the official Registered Voter List
- Officials should have the ability to issue paper ballots to voters right away, especially if the site is usually fully tech driven
- Election Officials should have secure mechanism to collect and store those paper ballots once completed by each voter, and the end of day, a way to tabulate the same (in addition to votes collected before the outage or incident occurred).

Why is this Important?

An extended interruption of IT systems on Election Day without an appropriate Backup Plan could deny citizens their right to vote, undermining the integrity fairness of the election.

Potential Issue 10: Phishing Attempts on Election Staff

What do I look for?

Be on the alert for Poll Workers **receiving suspicious emails or text messages**. Phishes (email) and Smishes (text message) could be being sent to a Poll Worker's personal email or phone, or even to the messaging capabilities on an election system (e.g., an e-polling station or laptop) if that system is enabled with access to the internet.

Why is this Important?

Phishing and SMSishing are tools threat actors use to easily trick people with enticing, real-sounding messages which may result in a person entering their login credentials into a fake website or sending sensitive voting information to a malicious site.

Potential Issue 11: Voting Discrepancies, and Ballot Count to Voter Count Irregularities

What do I look for?

Be especially sensitive to any **voter who claims their vote is not being accurately captured**. For example, a voter could complain that the selection they made in their voting machine session *is not accurately reflected* on the paper print out (their ballot) which they are supposed to validate before inserting into the final balloting machine.

Be also on the lookout at the end of voting day for any **discrepancies between electronic vote tallies** and the paper backups and/or other count of the voter numbers of the day. Any mismatch in number could indicate a tampering with the data or a system malfunction. At the end of the voting day, the number of people who walked through the door to vote should match exactly the number of ballots and tallies in the systems at that location.

Why is this Important?

Election software could have a code issue, whether inadvertent or malicious, which digitally misinterprets what a voter enters on the system screen to the vote record. This issue could interfere with the integrity of the election.

Any discrepancy between the number of physical people who walked in the door versus the final tally of votes in the machines could indicate tampering, either with individual votes or with the full voting data that day.

Potential Issue 12: Insider Threats

What do I look for?

Watch for any **suspicious behavior by authorized individuals** in and around voting systems, including IT providers, Poll Workers, or other Third-Party Suppliers… even building maintenance staff. Always be mindful to follow your Observer protocols as prescribed by your state, and remain respectful *and* vigilant. Suspicious behavior could include things we have covered elsewhere in this Handbook, as well as:

- An individual attempting to override security protocols of the systems
- Odd timing of access to a system or room in which systems are securely stored
- Insistence on logging into a system that their role does not usually have access to
- Discouraging or blocking the lawful activity of Poll Watchers or Election Observers.

Why is this Important?

Even “verified” individuals can use their influence and position to conduct activities outside of the scope of their role or which undermine good cybersecurity protocols. Through their behavior, trusted individuals may impact the integrity of the election.

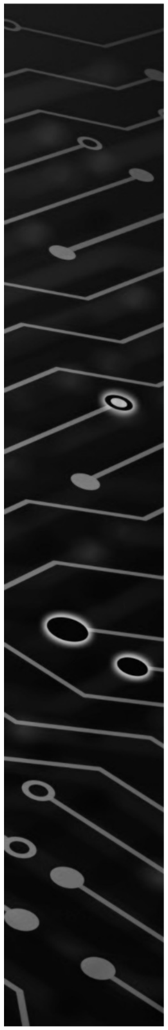
Bonus Information: System Logs

Bonus Information

While you won’t have direct access to the systems which are part of the election infrastructure, it’s good for you to understand, especially if you are a Challenger, that **every technical system writes a digital record** of everything it “does”. This is called the System Logs. Logs include every activity of the system and the software from power on and off, to legitimate access by an Election Official or Poll Worker, to the full operations of the software, to collecting of data (votes). Election systems should be **logging *all* activity**.

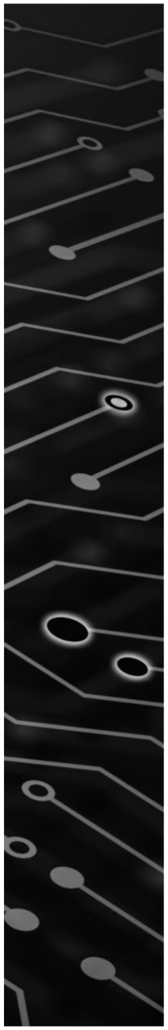
Why is this Important?

Logs will show authorized ***and*** unauthorized activity and can later be inspected should something be challenged or if there is a suspected issue. The absence of logs or skips in logging activity are a red flag and may result in security incidents going unnoticed or unable to be investigated.



About The Institute

The Institute for Cyber Civics



Our Passion
Bringing the best of Fortune 500 cybersecurity knowledge, skills and practices into everyday civic life and people’s interactions with the digital universe.

Our Mission
We are a non-profit organization with a Mission to advance the safety, security, privacy, and digital integrity of experiences citizens have while using technology, AI, and digital data in their everyday lives. To support the rights and responsibilities of citizens in the digital universe, the Institute develops and delivers cutting-edge cybersecurity education, research, and advocacy based on Fortune 500 cybersecurity best practices, tailored to citizens and their everyday digital experiences.

Our Initiatives
Our inaugural focus is to equip state and county election officials, poll watchers, cybersecurity leaders, and technology providers of voting systems with the knowledge and tools necessary to protect the electoral process from cyber threats. We are currently focusing on the 2024 US Elections, aiming to eventually expand our efforts to provide guidance for democratic elections everywhere. As part of our Mission, we will also tackle topics like safe cyber practices for youth on social media, effective use of cybersecurity and AI to combat human trafficking, and tips for the safety and security of citizens' online footprint.

Visit us at: https://InstituteforCyberCivics.org

INSTITUTE FOR

CYBER CIVICS

We welcome your feedback on this Handbook!

Visit us at: https://InstituteforCyberCivics.org

v1.4 October 2024