Illinois State Board of Elections

Submission for the U.S. Election Assistance Commission (EAC) Clearinghouse Award "Outstanding Innovation in Election Cybersecurity and Technology"

The Illinois State Board of Elections built the Cyber Navigator Program (CNP) in response to the Russian attack against election infrastructure in 2016. The program took an innovative approach to cybersecurity by splitting the state up into geographic zones and placing two Cyber Navigators in each zone. Cyber Navigators have a technical background, often in network infrastructure or security, and visit the individual election authorities from their zones. A key aspect of the program is building trust and rapport with election authorities to help make sense of the complicated nature of cybersecurity.

The Cyber Navigator Program (CNP) seeks to train the end users in election authority offices to help guard against phishing, malware, and other security breaches. The educational aspect of the program provides sustainable, long term benefits through continued support and training. The CNP allocated funding to connect offices to the Illinois Century Network (ICN) for any election authority that volunteered to do so. The ICN is similar to an office intranet but it connects government offices across the entire state without need to send data through the world wide web. The ICN has provided all 108 offices with 24/7 monitoring, protection against DDoS attacks, strong firewalls, and an Albert Sensor.

The Cybersecurity Information Sharing Program Managers (CISPM), a position under the CNP, aid in public engagement around cybersecurity best practices by participating in public events. They also host workshops, create table top exercises, and disseminate information to election authorities and their staff in a way that is palatable for individuals who may not have a strong background in security or technology. These outreach efforts resulted in trainings and resources shared in new partnerships with state and federal agencies that had never existed before. The program brought Public Information Officers from Illinois' State Police, Emergency Management Agency, Army and Air National Guard, Department of Innovation and Technology, Statewide Terrorism & Intelligence Center, Office of the Governor, and State Board of Elections in to coordinate messages to counter misinformation during the 2020 election cycle.

Before the Cyber Navigator Program was established, many election authorities were operating outdated election related systems with negligible security. Since then, all 108 election authority offices in Illinois have had cybersecurity risk assessments performed. The results from these assessments have guided each office's HAVA related purchases to improve their security. The CISPMs and CNP manager review spending requests from election authorities to ensure the purchases paid for with HAVA dollars produce positive security related improvements in the election space. Purchases have included upgrading entire offices to Windows 10, installing modern firewalls, providing offsite digital storage backups, and many other projects. Recently over 2,500 copies of CloudStrike have been installed in 74 election authority offices throughout Illinois. These upgrades have caught hundreds of malicious attacks, some of which would surely have been successful without the improved remediation.

Illinois does not require election authorities to participate in the Cyber Navigator Program, it is 100% volunteer based. Between the outreach efforts of the CISPMs and CNs all 108 election authorities chose to join the program. The program has been so successful that Illinois has been approached to, and has been happy to, share the details and lessons learned with other states. Illinois is in a far stronger position now to defend its elections from security concerns specifically because of the Cyber Navigator Program.

Thank you for considering the Illinois State Board of Elections Cyber Navigator Program for the Clearies.

Neil Herron | Illinois State Board of Elections
Cybersecurity Information Sharing Program Manager
(217) 558-1755 | NHerron@elections.il.gov

Cyber Navigator Program Inception

Election infrastructure has become a focal point for foreign cyberattacks. The United States Department of Homeland Security (DHS) designated the United States election systems as critical infrastructure for the country on January 6, 2017. In March 2018, the federal government appropriated $380 million in grants to the states to improve election security.

In response, the General Assembly tasked the Illinois State Board of Elections with creating a cybersecurity program to help every Election Authority in the state improve their cybersecurity posture. In 2018, the Illinois legislature passed Public Act 100-587 (specifically 10 ILCS 5/1A-55) and the State Board established the Cyber Navigator Program (CNP) through Administrative Rule (Title 26, Chapter I, Part 213).

Cybersecurity Information Sharing Program Manager (CISPM)

In order to administer parts of the CNP, the State Board of Elections hired two experts to Cybersecurity Information Sharing Program Manager (CISPM) positions. This position is tasked with building a relationship with election authorities to facilitate the sharing of cybersecurity related information. This includes increasing defensive knowledge through distribution of resources and training but also providing guidance when a cyberattack does occur. There are currently two CISPM employees, one stationed at the ISBE and one at the Statewide Terrorism & Intelligence Center (STIC).

Collectively they oversee outreach and documentation of four geographic Election Authority zones made up of 108 total agencies. This includes tracking cybersecurity related incidents reported to STIC, reviewing them for indicators relevant to Election Authorities, and sharing them with all necessary parties including the Federal Bureau of Investigations (FBI), Department of Homeland Security (DHS), Multi-State Information Sharing & Analysis Cent (MS-ISAC), Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC), Illinois Department of Innovation & Technology (DoIT), and others when needed. Cybersecurity incidents were not tracked before the development of the cyber navigator program that started in August of 2018.

Throughout the year, CISPMs coordinate special webinars to partners based on the information needs of the group, such as how to use the Homeland Security Information Network (HSIN).

An Election Dashboard is maintained by the CISPM in conjunction with the STIC. The CISPMs developed surveys to collect information from each jurisdiction to populate into the election dashboard. In the event of an incident, the program manager would have the ability to query election vendors, IT hardware, polling locations, election equipment, social media accounts, e-

pollbooks, and other data points. The dashboard can help identify patterns in attacks by seeing if multiple attacks have something specific in common.

To promote the CISP, managers have attended various meetings, conferences, and exercises to develop the program. This is a select list of meetings that the program managers have presented information on projects and threats attendees may be facing throughout the election cycle:

AECOI conference	IACCR conference	Zone meetings	Jurisdiction meetings
DHS TT Exercise	CSG conference	Cyber Shield 2019	MS-ISAC conference

The CISPMs maintain multiple distribution lists for our partners. The creation of the distribution lists has assisted in providing targeted information to each partner in the program.

- The election cybersecurity distribution list provides technical cyber bulletins to IT professionals throughout Illinois.
- The election authority distribution list provides election specific information.
- The OS distribution list provides information to election authorities that do not have secure email addresses. The content is limited to only open source information.

The CISP Managers work to develop relationships with county clerks, election authorities, and IT professionals throughout Illinois.

Cyber Navigator Program (CNP) Participation Requirements

1. The election authority must utilize the Illinois Century Network (ICN) for connectivity to the State Board of Elections or have entered into an agreement to do so as soon as practicable.
2. The election authority must participate in the Outreach portion of the program including:
    - Register with EI-ISAC
    - Work with CISPM to establish two-way data sharing
    - Have at least one representative of the election authority complete the security awareness training on at least a yearly basis.
3. The election authority must allow the Cyber Navigators to complete a Risk Assessment and an analysis against the Center for Internet Security's recommended procedure

1. Illinois Century Network (ICN)

The ICN is the equivalent of an office intranet that connects the entire state of Illinois. When one ICN user sends a file to another ICN user, that file remains inside the network and therefor never makes it to the World Wide Web. The service also provides 24/7 monitoring, protection from Distributed Denial of Service Attacks (DDoS), strong firewalls, and an Albert Sensor.

The ISBE is using Help America Vote Act (HAVA) funds to connect every election authority office to the ICN. Eventually, the Illinois Voter Registration System (IVRS) will never have to send data over the general internet, which provides added security to the transmission of voter registration information. The ICN provides safer internet usage for all connected agencies.

2. Outreach Program

- **Register with EI-ISAC**
  Illinois is dedicated to ensuring that all election authorities have the resources and knowledge to prepare and prevent an incident. The Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC) is a resource for election authorities to receive election specific information on the national level. The CNP team has been working with EI-ISAC to certify that all agencies in Illinois have a representative signed up to receive alerts. As of July 29, 2019, Illinois has 100% membership within the EI-ISAC.

- **Establish Two-Way Data Sharing**
  The Election Authority agrees to receive information from the program and, importantly, share any cybersecurity related issues they come across directly with program managers. For more detail to this practice, please see the CISPM section above.

- **Annual Security Awareness Training**
  Each Election Authority office is required to take a cybersecurity-based training. At least one member from the office must take a short test based on the training. All other members of the office can, and should, take the training, but are not required to be tested. The training covers basic cyber hygiene and awareness

3. Cyber Navigators (CN)

The CNP calls for eight CNs, two for each of the four geographical Election Authority zones, and one Lead Navigator. They all work under DoIT and coordinate operations with the ISBE.

CNs are IT professionals with a background in security. They must travel to the offices of Election Authorities to conduct risk assessments and make recommendations on how to improve security, both cyber and physical. CNs also review documentation and general practices of each office so they may recommend updates, configuration changes, and best practices that are tailored to each individual office's needs.

The program plans to grow the CN role to offer new services as the program matures.

Participation Grant

All Election Authorities that participate in the volunteer Cyber Navigator Program are eligible for grant money to spend on physical and cybersecurity.

There is a base $10,000 grant with additional money allocated based on the voting age population for the area each Election Authority covers. Participants must submit an itemized list of what they intend to purchase with the grant money, this ensures it is used on security related equipment, services, or staff. Voting equipment does not qualify as security related equipment for the purposes of this cybersecurity grant.

Addendums

Acronym and Initialism Index

(CIS) Center for Internet Security

(CISPM) Cybersecurity Information Sharing Program Manager

(CN) Cyber Navigator

(CNP) Cyber Navigator Program

(DDoS) Distributed Denial of Service Attacks

(DHS) Department of Homeland Security

(DoIT) Department of Innovation and Technology − the State agency with responsibility for the information technology (IT) functions of agencies under the jurisdiction of the Governor. This term also includes the agency tasked with managing the Illinois Century Network.

(EI-ISAC) The Elections Infrastructure Information Sharing and Analysis Center

(HAVA) Help America Vote Act

(HSIN) Homeland Security Information Network

(ICN) Illinois Century Network − A service that creates and maintains high speed telecommunications networks providing communication links to and among Illinois schools, institutions of higher education, libraries, museums, research institutions, State agencies, units of local government, and other local entities providing services to Illinois citizens.

(ISBE) Illinois State Board of Elections

(IVRS) Illinois Voter Registration System

(MS-ISAC) The Multi-State Information Sharing and Analysis Center

(STIC) The Statewide Terrorism and Intelligence Center

Elections Resources

To enable the elections that define democracy, we must protect the security and reliability of elections infrastructure. Through a best practices approach, we aim to help organizations involved in elections better understand what to focus on, know how to prioritize and parse the enormous amount of guidance available on protecting IT-related systems, and engage in additional collaboration to address common threats to this critical aspect of democracy.

A Handbook for Elections Infrastructure Security

Protect your election's infrastructure with this free best practices handbook and other resources from CIS and our elections partners. Read the Handbook and ready to implement? Download the Best Practices Excel spreadsheet to start securing your elections infrastructure.

https://www.cisecurity.org/elections-resources/

A Guide for Ensuring Security in Election Technology Procurements

Computer hardware, software, and services are essential for an election organization to execute its mission. You can view the guidebook online and use the Searchable Best Practices Database to filter and export the components that are essential to your organization.

https://www.cisecurity.org/elections-resources/

Election Security Self-assessments

Assess and understand the gaps in your security using Election Security Self-assessments

https://www.cisecurity.org/elections-resources/

Join the EI-ISAC – Free for U.S. Elections Organizations

Membership in the Elections Infrastructure ISAC is open to all state, local, tribal, and territorial government organizations that support the elections officials of the United States of America, and associations thereof. This is always a free and voluntary membership for these eligible organizations.

If you are affiliated with an eligible organization, please fill out this form and an EI-ISAC representative will reach out to you as soon as possible to complete the membership enrollment process.

EI-ISAC Services and Benefits Provided to Members:

- 24/7 Security Operations Center
- Incident response and remediation
- Weekly Elections Security News Alerts
- Elections Sector Quarterly Report
- Election-specific threat intelligence
- Threat and vulnerability monitoring
- Training sessions and webinars
- Promote security best practices
- Automated Indicator Sharing
- Access to a Members-Only Discussion Board
- Malicious Code Analysis Platform (MCAP)
- Digital forensics and log analysis

Individuals who do not support the Elections Critical Infrastructure of the United States but are employees of any other public non-federal entity are eligible and strongly encouraged to take full advantage of the services and benefits offered through the Multi-State Information Sharing Analysis Center by enrolling at https://learn.cisecurity.org/ms-isac-registration.

Employees of for-profit companies or non-profits, consultants, or private citizens that are unaffiliated with an eligible entity are strongly encouraged to take advantage of our free advisories on known vulnerabilities, national webcasts, and end-user focused cybersecurity newsletters by enrolling https://learn.cisecurity.org/ms-isac-subscription.

Who can join the MS-ISAC?
Membership is open to all U.S. SLTT government entities.

What does it cost to join the MS-ISAC?
There is no cost to join the MS-ISAC. It is primarily supported by the DHS to serve as the central cybersecurity resource for the nation's SLTT governments.

Can the MS-ISAC help me with a cyber-incident?
Yes. The MS-ISAC Computer Emergency Response Team (MS-ISAC CERT) comprises highly trained staff who are able to assist you with a cybersecurity incident. MS-ISAC CERT can provide malware analysis, reverse engineering, log analysis, forensics analysis and vulnerability assessments. The Incident Response service is available to all SLTT entities.

Are there any requirements to join?
The only requirement is the acceptance of terms and conditions, which set forth the responsibilities of members to protect information that is shared.

What are the benefits of MS-ISAC membership?
Membership benefits include direct access to cybersecurity advisories and alerts, vulnerability assessments and incident response for entities experiencing a cyber-threat, secure information sharing through the Homeland Security Information Network (HISN) portal, tabletop exercises, a weekly malicious domains/IP report, multiple DHS initiatives, CIS SecureSuite Membership, MS-ISAC National Webinar, and more.

Are there any educational or training resources available?
Yes. In addition to advisories and information bulletins regarding the latest cyber threats and vulnerabilities, the MS-ISAC provides a variety of educational, awareness, and training resources and opportunities.

Does MS-ISAC work with federal agencies, private sector groups, and the other ISACs?
Yes. The MS-ISAC works closely with federal partners at DHS, along with Federal Bureau of Investigation, U.S. Secret Service and others to better share information on emerging threats. The MS-ISAC also has strong relationships with major internet service providers, cybersecurity firms, researchers, and software developers.

How do I join?
Register for MS-ISAC Membership at https://learn.cisecurity.org/ms-isac-registration or contact us at info@msisac.org.

Not an SLTT entity? You can still benefit from our publicly-available MS-ISAC Daily Tips, white papers, and other resources.

Homeland Security

The Department of Homeland Security maintains an Election Security Resource Library at https://www.dhs.gov/publication/election-security-resource-library
It includes a number of resources, such as:

Election Security Resources Guide
A compilation of CISA contacts and resources for support state and local election officials.

Incident Handling Overview for Election Officials
A summary of CISA's cyber incident response team services for election officials as well as one page guidance on incident response planning considerations, a checklist for requesting assistance, the incident response process and common mistakes to avoid.

Ransomware Executive One Pager and Technical Document
An interagency guide that provides an aggregate of Federal government and private industry best practices and mitigation strategies focused on the prevention and response to ransomware incidents.

Securing Voter Registration Data
An overview of threats to voter registration websites and databases along with recommendations on how election officials and network administrators can protect and prevent the threats.

Multi-Factor Authentication
Multi-factor authentication (MFA) is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identify for login. MFA increases security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space, computing device, network, or database.

Vote with Confidence
A joint flyer produced by the U.S. Election Assistance Commission, the National Association of Secretaries of State, the National Association of State Election Directors, and the Department of Homeland Security to help voters cast their ballots with confidence.

Best Practices for Continuity of Operations
A paper providing organizations recommended guidance and considerations as part of their network architecture, security baseline, continuous monitoring, and Incident Response practices in order to actively prepare for and respond to a disruptive event such as destructive malware.

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

Directed by Eric Rosenbach and featuring the former campaign managers for Hillary Clinton and Mitt Romney along with experts from the national security and technology communities—including Facebook, Google, and Microsoft—Defending Digital Democracy (D3P) Project aims to identify and recommend strategies, tools, and technology to protect democratic processes and systems from cyber and information attacks. By creating a unique and bipartisan team comprised of top-notch political operatives and leaders in the cyber and national security world, D3P intends to offer concrete solutions to an urgent problem.

Foreign nations and non-state actors are not backing down in their efforts to hack, alter the outcome and undermine confidence in our elections. The Defending Digital Democracy Project will help institutions fortify themselves against these attacks by:

- Developing solutions to share important threat information with technology providers, governments, and political organizations;
- Providing election administrators, election infrastructure providers, and campaign organizations with practical "playbooks" to improve their cybersecurity;
- Developing strategies for how the United States and other democracies can credibly deter hostile actors from engaging in cyber and information operations;
- Assessing emerging technologies, such as blockchain, that may improve the integrity of systems and processes vital to elections and democracy;
- Convening civic, technology, and media leaders to develop best practices that can shield our public discourse from adversarial information operations.

The Belfer Center has created especially helpful resources for campaigns and election authorities such as:

- Cybersecurity Campaign Playbook
- The State and Local Election Cybersecurity Playbook
- Election Cyber Incident Communications Coordination Guide
- Election Cyber Incident Communications Plan Template

Find them at: https://www.belfercenter.org/project/defending-digital-democracy#!playbooks

PHISHING

Protect yourself and your team

Anyone can be the target of a phishing scam. This information will help you know what to look out for. If you do think an email is suspicious, use **Forward as Attachment** to send it to your IT team. **Forward as Attachment** can be found by clicking "More" next to "Forward" in a fully open Outlook email window. It is important that you forward as attachment rather than simply forwarding the email, it reduces the risk of spreading an infection.

What is phishing?

The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

What do phishing emails ask me to do?

- ! Open an attachment
- ! Click on a link
- ! Send personal information
- ! Provide confidential agency information

How can I spot phishing emails?

Looks similar to a professional email but may have grammar, spelling, or formatting errors.

Message conveys a high sense of urgency.
Example: "Your account will be closed and your funds will be inaccessible unless you change your password at this link."

Emphasizes personal, confidential or potentially embarrassing information.

Attempts to get you to interact via threat or reward.

Mentions recent transaction or says you won a contest you have no knowledge of.

WHAT ARE YOU REALLY CLICKING?

Phishing emails frequently include hyperlinks that can giveaway their malicious intent. Hover your mouse over the hyperlink to see a small pop up window, this shows where the link will actually take you.

Look for suspicious addresses in the pop up that:

- ! Have multiple top level domains in the link (.gov, .com, .org, .net, etc.)
- ! Use URL encoding (http:%4B%2T%Fi)
- ! Subtle misspellings (apple.suport.com)
- ! Odd naming (microsoft.helpunlocking.com)

Illinois Election Officials Incident Reporting Aid

Provided by the Illinois State Board of Elections Cybersecurity Information Sharing Program

Does something seem suspicious?

Unknown person in your area with questionable behavior.	1. Ask them to explain what they are doing. 2. Do not provide them with sensitive info. **Reason:** They may be trying to gain unauthorized access to sensitive information.
Documents or devices containing PII have been lost or accessed by unauthorized people.	1. Follow the **Personally Identifiable Information Breach** steps. 2. Catalog what was lost, stolen or improperly accessed. Make available to the police.
Email asking you to update or validate information via a hyperlink.	1. Do you recognize the sender? 2. If no, follow the **Phishing Attempt** steps. 3. If yes, call them (do not use any unrecognized phone numbers in the email) to ask for details. **Reason:** This is a common phishing tactic. The most successful attacks try to make the email look like it comes from a trusted company or person.
Roaming cursor, black box with streaming text, or strange pop-ups.	Follow the **Computer Virus** steps. **Reason:** Someone may have unauthorized remote access to your computer.
Website asks for personal information.	1. If it seems suspicious, check the URL by copying it to https://safeweb.norton.com/ **Reason:** It could be a targeted phishing page.
Browser pop up saying computer has a virus or data has been stolen.	1. Do not click anything. Close browser. 2. Contact IT, request a pop up blocker. **Reason:** False virus prompts are used to scare people into installing malicious Scare Ware.
Email with a Virus Warning.	1. Do not forward, do not open any attachments or click links. 2. Inform your IT Support and STIC.

Election Day

Electioneering within Campaign Free Zone.	Contact Election Authority.
Security threat at polls.	Contact local law enforcement, EA, & STIC.
Weather causing issues at the polling location.	Contact EA, they can notify voters and request a court order to extend hours (if necessary).
Loss of power.	Contact EA and power company to report outage.
Election related webpage or social media accounts become compromised.	Contact EA and STIC. Attempt to regain control of account login through the hosting company or vendor.
Run out of ballots.	Contact EA, they can contact SBoE (if necessary).
Voting equipment or data is missing or stolen.	If it is missing, contact EA. If you saw it being stolen then also contact local law enforcement.

Contact Information

STIC Watch Center:	
State Board of Elections:	
Election Authority:	
Power Company:	
Tech Support:	
Other:	

Computer Virus

STEP 1	Disconnect the network cable of the affected device.
STEP 2	Leave the system powered on.
STEP 3	Write down any messages that appear.
STEP 4	Report Immediately by contacting your IT support and STIC.

Personally Identifiable Information (PII) Breach

Loss of control or compromise via unauthorized disclosure/acquisition/access to PII data.

STEP 1	Take actions to mitigate further loss.
STEP 2	Report the incident to STIC.
STEP 3	If theft related, report to local police.

Phishing Attempt

Phishing is an attempt to obtain information through fraudulent emails that appear legitimate.

STEP 1	Do not download attachments, reply, or click any links.
STEP 2	Forward it to your IT Support and note why you believe it is suspicious.
STEP 3	Block the sender and delete the email.

Social Media Incident Reporting Form

Please email the completed form and attach a screenshot of the incident to STIC@illinois.gov

Reporting Contact Information

First Name

Last Name

Email address

Phone number

Agency

Incident Information

Date of original post

Date post was reported

Social Media Platform

Provide Link to the post

Preferred way to contact you? ◯ E-mail ◯ Phone

Please describe the incident in detail and include any other relevant information

CYBER INCIDENT CHECKLIST

Investigate | Remediate | Communicate

Establish Reliable Facts

- **Who** is reporting the problem? How did they become aware?
- **What** do we know so far about what happened?
  - What network/systems are affected?
  - What data/information was compromised? (e.g., stolen, deleted, altered)?
- **When** did the breach occur?
  - When did we find out about it?
  - When did we begin to do something about it?
  - When will we know the full scope of the problem?
  - When do we estimate that the problem will be remediated?
- **Where** did the breach occur? (what office, activity, locale, etc.)?
- **How** much do we know, with certainty, about how the breach occurred? Do we know the source of the attack?
- **How** will we stay informed of efforts to remediate the breach and restore normal service?

Connect Resources

- **Who** should lead operational response efforts? What role will your office play?
- **Are** experts on hand to work the problem? What additional help do you need? Who will provide it?
- **What** measures are needed to secure the networks/systems from further exploitation?
- **What** additional steps are needed to secure data?
- **How** will the remediation efforts to limit or repair the damage and restore normal services be prioritized?
- **What** actions do your PII (Personally Identifiable Information) laws require? Is there a maximum length of time before victims must be notified?
- **What** are the legal implications of the incident?
- **Have** you contacted your cyber insurance provider?
- **Is** the incident of a nature that the cyber navigators can assist you?

Relay the Facts

- **Avoid** making definitive statements about anything you cannot positively confirm as fact but keep in mind that waiting to release bad news tends backfires.
- **Release** your first public statement as soon as you have an understanding of the problem and are able to explain how you are working to correct the situation.
- **Describe** what you currently know about the incident and what is being done to improve the situation.
- **Be prepared** to explain the pre-existing cybersecurity posture, your work before the attack to mitigate issues, and the training that was in place to prevent events of this kind.
- **Be honest** about the breakdown and what has been learned from it to prevent future issues.
- **Establish** a regular cadence of updates for victims, media, and other stakeholders—including your own workforce.

Illinois State Board of Elections | Statewide Terrorism & Intelligence Center | Illinois Elections Cyber Navigators

Currently experiencing an incident?
Contact STIC at or STIC@illinois.gov

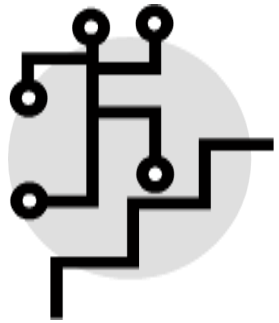
Social Media

SAFE WAYS TO SHARE

Being able to share updates and photos with friends and family is a great way to keep in touch but what is oversharing?

PRIVACY SETTINGS TO DISABLE

- ! Location sharing
- ! Linked Apps posting for you
- ! Search engines linking to your profile
- ! "Apps Others Use" from using your info



THINGS TO AVOID SHARING

- ! Vacation dates: don't post about an upcoming vacation or while you are away. Wait until you are back home before uploading vacation photos.
- ! Your regular schedule: don't let the world know you go to a specific location every Wednesday for X hours.
- ! Don't "like" pages for your bank, insurance, employer, phone company, or any other company that a hacker could use for social engineering to obtain your personal information.

Open Source Sites

Open Source Sites are webpages that crawl various online open source repositories to compile your information. You can request to opt out, but must do so at each individual webpage. While your information is still available from the original locations, opting out of these pages makes gathering your information harder for hackers.

CHECK THE BOX ONCE YOU'VE OPTED OUT

- ☐ anywho.com/help/privacy
- ☐ familytreenow.com/optout
- ☐ intelius.com/optout
- ☐ isapps.acxiom.com/optout
- ☐ risk.lexisnexis.com/consumer-and-data-access-policies
- ☐ spokeo.com/optout
- ☐ thatsthem.com/optout
- ☐ whitepages.com/suppression_requests

HAS YOUR EMAIL BEEN COMPROMISED?

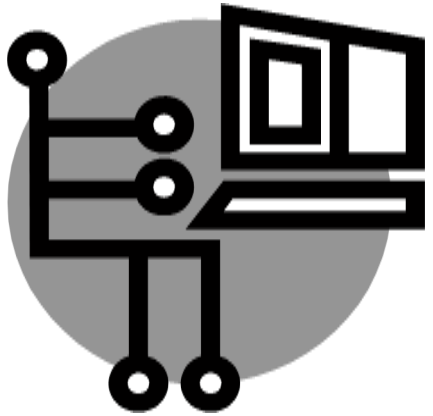
Many large companies have had their users personal data compromised. Search for your email at **haveibeenpwned.com** to find out if your information was a part of one of those hacks.

Have more questions? Contact the
Cybersecurity Information Sharing Program
cisp@elections.il.gov

ILLINOIS STATE BOARD OF ELECTIONS

Cybersecurity Information Sharing Program

Ways to Protect Your Digital Identity



TOUGH PASSWORDS

BASIC PRECAUTIONS TO TAKE

- Have separate passwords for every account. This way, if one account is compromised, the others may not be.
- Use a password manager so you only need to memorize one password.
- Password strength is increased by length and number of unique characters.

MIX IT UP - HACKERS KNOW OUR TRICKS

- Don't capitalize the first or last letters.
- Don't use common or real words.
- Don't use leetspeak (a = @, e =3, etc.).
- Don't use birthdays or phone numbers, even of other family members.
- Don't use successive characters like 345678 or qwerty.

HOW LONG TO CRACK YOUR CODE?

Hackers use dictionary software to quickly go through every possible combination to find your password. They can hasten their search by using your personal information (birthdate, pet's name, phone, etc.).

Fluffyismydog—17 hours
fLuffyisdog— 3 days
fLuffy17mydog—7 days
fLuffy17my^dog—4 years
fL*ffy17my^dOg—17 million years
fL*ffy17mi^dOg—30 million years
fL*fFy17mi^d5g— 80 billion years

WAYS TO STAY SAFE

TWO-FACTOR AUTHENTICATION

Use two of the three means of identification to log into an account. Something you know (password), something you have (phone), or something you are (fingerprint). Enabling two-factor authentication makes it much harder for hackers to gain access to your accounts. This is one of the strongest and easiest ways to protect yourself.

MOBILE DEVICES

- Turn Bluetooth off when not being used.
- Disable Location Services such as GPS on photos.
- Update your device software when prompted.
- Restore device to factory default before selling.
- Avoid apps that request odd permissions, like access to your contacts for a Solitaire app.

HOME DEVICES

- Set a unique username and password for your Wifi router. Many people never change it. To a hacker, that is the same as leaving your front door wide open.
- Create an Admin and Standard account on your home computer. Use the Standard account most of the time and only use the Admin account when necessary. This makes it difficult for malicious software to be installed.
- Always upgrade your Windows/iOS operating systems when new official patches are released.

PHISHING

WHAT IS PHISHING?

The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

WHAT DO PHISHING EMAILS ASK FOR?

- Open an attachment.
- Click on a link.
- Send personal information.
- Provide confidential agency information.

HOW CAN I SPOT THEM?

- Looks similar to a professional email but may have grammar, spelling, or formatting errors.
- Conveys a high sense of urgency.
  Example: "Your account will be closed and your funds will be inaccessible unless you change your password at this link."
- Emphasizes personal, confidential, or potentially embarrassing information.
- Attempts to get you to interact via threat or reward.
- Mentions a recent transaction or says you won a contest that you have no knowledge of.

Statewide Terrorism & Intelligence Center
Election Briefing
April 10, 2020

UNCLASSIFIED *

(U) STIC is providing this information to our partner agencies for situational awareness. This document contains information obtained from open source information. While STIC has gone to great lengths to verify the information found in open source documents on the internet, this information may not be accurate.

Microsoft Expands Security Offerings to Election Officials

Microsoft announced Thursday it is expanding its cybersecurity offerings to state and local election officials, including access to a free service that offers threat detection on email or other accounts, and specialized services from the company's incident-response group. The announcement is part of Microsoft's two-year-old Defending Democracy Program, a suite of election-security products that the company has been providing to campaigns and officials in both the United States and abroad. The first offering announced Thursday gives state and local officials — as well as members of Congress and their staffs — access to AccountGuard, a service that alerts users of Microsoft's Outlook and Hotmail email platforms or its Office 365 suite of productivity applications if their accounts are threatened or compromised by hackers known to be associated with a foreign government. Previously, AccountGuard, which was introduced in 2018, was only available to campaigns, political parties and some nonprofit organizations. Microsoft also said it will make members of its Detection and Response Team, or DART, its incident-response group, available to election officials at discounted rates through a program the company's calling "Election Security Advisors." Cybersecurity, including functions like incident response and forensics, accounted for more than half of states' expenditures with the $380 million that the U.S. Election Assistance Commission awarded in 2018. More spending is expected following another $425 million grant round approved in a federal spending package approved last December, and $400 million that was included in last week's emergency relief act.

https://statescoop.com/microsoft-expands-security-offerings-election-officials/

Implementing Safety Practices for Critical Infrastructure Workers Who May Have Had. Exposure to a Person with Suspected or Confirmed COVID-19

To ensure continuity of operations of essential functions, CDC advises that critical infrastructure workers may be permitted to continue work following potential exposure to COVID-19, provided they remain asymptomatic and additional precautions are implemented to protect them and the community. A potential exposure means being a household contact or having close contact within 6 feet of an individual with confirmed or suspected COVID-19. The timeframe for having contact with an individual includes the period of time of 48 hours before the individual became symptomatic. Critical Infrastructure workers who have had an exposure but remain asymptomatic should adhere to the following practices prior to and during their work shift:

- **Pre-Screen:** Employers should measure the employee's temperature and assess symptoms prior to them starting work. Ideally, temperature checks should happen before the individual enters the facility.
- **Regular Monitoring:** As long as the employee doesn't have a temperature or symptoms, they should self-monitor under the supervision of their employer's occupational health program.
- **Wear a Mask:** The employee should wear a face mask at all times while in the workplace for 14 days after last exposure. Employers can issue facemasks or can approve employees' supplied cloth face coverings in the event of shortages.
- **Social Distance:** The employee should maintain 6 feet and practice social distancing as work duties permit in the workplace.

- **Disinfect and Clean work spaces:** Clean and disinfect all areas such as offices, bathrooms, common areas, shared electronic equipment routinely.

Analyst Note: The second link provides a printable flyer that election officials can use in their office.

https://www.cdc.gov/coronavirus/2019-ncov/community/critical-workers/implementing-safety-practices.html

https://www.cdc.gov/coronavirus/2019-ncov/downloads/Essential-Critical-Workers_Dos-and-Donts.pdf

Voting By Mail/Absentee Voting

More voters are using mail ballots across the country and the COVID-19 pandemic has increased the need to explore options to increase vote by mail opportunities. Voting by Mail/Absentee Voting is also essential part of the elections process for citizens away from home, such as our military and overseas voters. The Election Assistance Commission (EAC), the Federal Voting Assistance Program (FVAP) and the United States Postal Service (USPS) continue to work together to ensure the entire voting by mail/absentee voting process works smoothly and efficiently. Below are COVID-19 specific resources and other resources to help election officials identify procedures, strategies, and policies for ensuring mail ballots get cast and counted, and all election-related materials that help citizens cast these ballots are delivered in a timely manner.

https://www.eac.gov/election-officials/voting-by-mail-absentee-voting

National Association of State Election Directors COVID-19 Resources

The below resources may be helpful for election officials as they contemplate changes to their election processes in light of the COVID-19 health emergency.

https://www.nased.org/covid19

COVID-19 & Elections

Across the Nation, thousands of election officials are working to manage the consequences of the COVID-19 pandemic on election operations and administration. As the Nation's risk advisor, CISA is coordinating with government and industry partners to ensure upcoming elections are accessible and secure, and that voters are safe. This list is composed to provide awareness of the latest resources and up-to-date information on the ongoing efforts by government and industry organizations to assist election officials and voters prepare for possible impacts to election security and voter registration practices and procedures. Please note that this list will be updated as more information becomes available.

https://www.cisa.gov/covid-19-and-elections

Illinois State Board of Elections

Navigator News

May 2019

Allowable HAVA Expenditures

- Hardware: firewalls, backups, new PCs
- Software: New operating system, Endpoint security, Intrusion detection/ prevention, Email or Web browsing protection, Backup, Multi-factor authentication, Network monitoring or inventory, Log monitoring, Security incident & event management
- Services: Penetration test, Cybersecurity training, Phishing training, Managed Security Services
- Personnel: Cybersecurity staff or consulting
- Other: physical security upgrades or any other costs not outlined above (please submit request for approval before purchasing)

The required **Annual Training** has been sent out. Complete it soon!

Contact Neil if you have any questions: NHerron@elections.il.gov

The Work Goes On: Procurement Security

The Illinois State Board of Elections Cyber Team went to the MS-ISAC 2019 Annual Conference to present and learn about elections related cybersecurity. They brought back information to help improve the Cyber Navigator Program. Other conference attendees said they were impressed by what Illinois has accomplished so far and requested more information so they could implement similar programs in their states. Among the topics at MS-ISAC was *A Guide for Ensuring Security in Election Technology Procurements.* On 5/6/2019 Amy Kelly sent out the CIS Elections Procurement pdf that was presented at MS-ISAC 2019. Getting procurement language right is always a challenge, this document is designed to help ease that challenge. The right language will help protect your county from cyber threats that target vendors and shield you from liability. The guide provides helpful context for procurement decisions and 33 best practices that cover the people, process, and technology. Each one has suggested Request for Proposal language, ideas on how to recognize good and bad responses, as well as helpful tips and other resources. If you need the email resent please reach out to AKelly@elections.il.gov

Illinois State Board of Elections
Program Manager
Amy Kelly

CISPMs
Neil Herron
Alana Sorrentino

DoIT Zone Navigators
Lead Navigator
Jim Patterson

Zone 1—South
Josh Clark
Terry Harger

Zone 2—West
Ryan Cook
Sean Sowers

Zone 3—East
Jason King
Brian Rudnicke

Zone 4—North
Andrew Dyke
Jeff Jasica

Where to Report a Security Incident

STIC Watch Center
877-455-7842
NOTE: NEW EMAIL
STIC@illinois.gov

Cyber Navigators Ongoing Support

Liked the Navigators? Sign up to see them again! The team would like to offer the following services as part of the Cyber Navigator Programs continuing efforts:

- Interactive phishing email training—your office will receive practice versions of phishing emails as a way to learn what is and is not safe to click on
- Physical security walk through and suggestions
- External scanning of the office network to identify and recommend ways to strengthen your defenses
- Customized cybersecurity best practices for your office
- Explanations of advanced firewall services, log monitoring, and albert sensor defenses on the ICN

Regional Table Top Conferences

SBE, STIC, and DoIT are all creating relatable, useful content to share with you at these events starting in July.

Vendor Spoofing

The Mueller report revealed a previously publicly unknown attempt by the Russian military intelligence agency GRU to send a phishing email to 120 election officials throughout Florida. The email was disguised as a message from an election equipment vendor and had a coded attachment that could give Russian agents access to election systems. At least one county was infiltrated.

Navigator Spotlight

Josh Clark originally became interested in IT at the age of 4, when he became inseparable from his father's Commodore 64 computer. That spark eventually led to work as a web developer, several service roles for private corporations in the Effingham area, and experience with risk analysis, support of patch management systems, network administration, and response to cybersecurity incidents impacting the private healthcare sector.
When he's not assisting with the Navigator program in southern Illinois, Josh works to refine his sound as a semi-professional Blues musician, and carries a minimum of one custom-tuned harmonica on his person at all times.

Illinois State Board of Elections

Navigator News

October 2020

Location Changes?

Worried about last minute changes for polling locations? The Illinois State Board of Elections is getting software that will allow voters, based on their voting area, to receive an email and text message about emergency polling location changes.

Starting 10/30/2020, Please call Neil at 217-558-1755 if you have an emergency change to report.

Social Patrol: Free Social Media Monitoring

Have you responded to Alana's Social Media Survey? Are your accounts eligible to be Blue Check/ Badge Verified? If so, the State Board of Elections can provide you even more social media protection!

An email invite to ProofPoint Social Patrol went out to those who responded to our social media survey. If you did not receive one but would like to know more, please contact nherron@elections.il.gov

What does Social Patrol do?

- Detect impostor attacks, malicious content that uses trusted lookalike email domains, web domains, and social media
- Find social media security threats (phishing, malware, spam and personal threats)
- Monitor hashtags related to election authorities that opt into this program and notify those EAs of any suspicious activity
- Scan for potential sensitive data exposure on the dark web
- Base search result alerts on locations, thus the sooner we can get a list of your polling places from you the better
- Find spoofed social media accounts

CISA Election Risk Profile Tool

This is a free user-friendly assessment tool for state and local election officials to

- Used to develop a high-level risk profile across a jurisdiction's specific infrastructure
- Provides election officials a method to gain insights into their cybersecurity risk and prioritize mitigations
- Accepts inputs of a jurisdiction's specific election infrastructure configuration
- Outputs a tailored risk profile for jurisdictions, which identifies specific areas of highest risk and recommends associated mitigation measures that the jurisdiction could implement to address the risk areas.

Find it at: http://www.eac.gov/app/esa/
If you would like help using this tool, please contact your Cyber Navigator to setup a time to go over it together.

October is Cyber Awareness Month

Deepfakes at the Local Level

Deepfakes use computer learning to simulate a persons face to create footage that looks real but is not. Any deepfake of a national level candidate would draw large attention and be quickly debunked.

Experts warn deepfakes targeting local elections could cause substantial damage due to low visibility causing them to spread longer before being debunked. If you suspect a video or audio file is a deepfake, alert STIC.

Illinois State Board of Elections
Program Manager
Amy Kelly

CISPMs
Neil Herron
Alana (Sorrentino) Mundhenke

Department of Innovation and Technology
Lead Navigator
Jim Patterson

Zone 1—South
Josh Clark
Terry Harger

Zone 2—West
Ryan Cook
Sean Sowers

Zone 3—East
Jason King
Alex Carrell

Zone 4—North
Jerry Joel
Caelin Banks

Where to Report a Security Incident

STIC Watch Center
877-455-7842 | STIC@illinois.gov

Who to Contact

Sign up for HSIN, MS/EI-ISAC, report a cyber incident to STIC—
Alana Mundhenke | 217-558-3739 | Alana.Sorrentino@illinois.gov

ICN Connection Questions—
Email Lead Navigator Jim Patterson James.L.Patterson@illinois.gov

Public inquiry, physical and cyber security training, and messaging—
Contact Neil Herron | 217-558-1755 | NHerron@elections.il.gov

HAVA Grant or Procurement Questions - Call or email Amy Kelly | 217-782-1536 | AKelly@elections.il.gov

#BECYBERSMART

DHS is raising awareness on how to recognize cyber vulnerabilities

Free Security with CrowdStrike

This software has already helped protect multiple counties and aided another with recovery after a successful phishing email resulted in ransomware shutting down their office.

In collaboration with the Department of Information and Technology the Illinois State Board of Elections is providing CrowdStrike protective software free of charge to all election authorities who request it. It is a fully managed endpoint service made to help protect against ransomware.

- 24/7 service endpoint protection
- Gain efficiency by reducing time to remediation
- Avoid the cost of having to hire specialized employees
- Reduce the risk from Ransomware

Please send your request to have a cyber navigator contact you to Jim Patterson at james.l.patterson@illinois.gov

Navigator Spotlight—Jerry Joel

Very Cliché, but I have a strong passion for computers. I am fascinated by the new technology and I keep myself up to date with any new gadget on the market. I live in Chicago's northern suburbs and cover northern Illinois counties for the CN program. I was lucky enough to be offered a seat in a cybersecurity bootcamp in City Colleges of Chicago which helped me pass my cybersecurity certifications and land this job. I love this job! I have an immense interest in US politics and cybersecurity and this job is showing me a lot about both. Learning about local, state, federal United States government structure and a lot of new and exciting cyber security tools is exciting. In my free time, I play tennis and read books. I am planning to get more cybersecurity certifications. Much more to achieve in this land of opportunities.