STATE BOARD OF ELECTIONS

ELECTION NEWS ELECTION NEWS ELECTION NEWS

100 W. Randolph Street
Suite 14-100
Chicago, Illinois 60601
312-814-6440

2329 S. MacArthur Blvd.
Springfield, Illinois 62704
217-782-4141
www.elections.il.gov

FOR IMMEDIATE RELEASE

CONTACT: MATT DIETRICH
(217) 558-1955 mdietrich@elections.il.gov

SBE TO HOLD PUBLIC HEARING ON CYBER NAVIGATOR PROGRAM

SPRINGFIELD, IL – July 27, 2018 – The Illinois State Board of Elections will hold a public hearing on August 1, 2018, to accept comments on the implementation of the Cyber Navigator Program. Financed by a $13.2 million grant from the U.S. Election Assistance Commission, the Cyber Navigator Program is a major initiative aimed at ensuring that all 108 local election authorities in Illinois employ best cybersecurity practices in the handling of Illinois voter data.

The meeting will begin at **10:00 a.m.** at the Board's principal office located at 2329 S. MacArthur Boulevard, Springfield, IL and via video conference in Suite 14-100 of the James R. Thompson Center, 100 W. Randolph Street, Chicago, IL. Admittance to the 14th floor of the Thompson Center requires security screening and production of a government issued identification.

Information about the Cyber Navigator Program and the proposed rules to be discussed at the Aug. 1 hearing are below.

STATE BOARD OF ELECTIONS
MEMORANDUM

From the desk of:
Amy Kelly, Assistant to the Executive Director

TO: **Steve Sandvoss & Members of the Board**
SUBJECT: **Amended tentative 5-year budget for HAVA grant**
DATE: **June 6, 2018**

Governor Rauner signed into law Public Act 100-0587 effective June 4, 2018 which requires the SBE to implement a Cyber Navigator Program for local election authorities. This legislative mandate requires an amendment to the Board's tentative 5-year budget plan for allocating HAVA grant funds, which was approved at the May 21, 2018 meeting.

Public Act 100-0587 (10 ILCS 5/1A-55 new)

Sec. 1A-55. Cyber security efforts. The State Board of Elections shall provide by rule, after at least 2 public hearings of the Board and in consultation with the election authorities, a Cyber Navigator Program to support the efforts of election authorities to defend against cyber breaches and detect and recover from cyber-attacks. The rules shall include the Board's plan to allocate any resources received in accordance with the Help America Vote Act and provide that no less than half of any such funds received shall be allocated to the Cyber Navigator Program. The Cyber Navigator Program should be designed to provide equal support to all election authorities, with allowable modifications based on need. The remaining half of the Help America Vote Act funds shall be distributed as the State Board of Elections may determine, but no grants may be made to election authorities that do not participate in the Cyber Navigator Program.

The purpose of this memo is to provide an outline of the possible considerations, both short and long term, for use of the 2018 Election Cyber-Security HAVA Funding, as it will pertain to the creation and implementation of the "Cyber Navigator Program".

Proposed Components of the Cyber Navigator Program

As required under Public Act 100-0587 no less than half of any such funds received shall be allocated to the "Cyber Navigator Program" to support the efforts of election authorities to defend against cyber breaches and detect and recover from cyber-attacks. The HAVA grant award of $13,232,290.00 plus the 5% required state match of $ 661,615.00 provides for a total of $13, 893,905.00. Under PA100-0587, **$6,946,952.50**, must be used to provide equal support to all election authorities, with allowable modifications based on need. In order to provide equal support to all election authorities, the SBE is proposing the following components:

1. **Illinois Century Network (ICN) Expansion Project.** The ICN is a state-managed network delivering network and internet services to government agencies in Illinois. The network allows DoIT to provide centralized monitoring, mitigation, and security services to participating agencies. The goal of the ICN is to provide agencies with a "cleaner, safer internet" .Currently, 25-30 counties are already or in the process of utilizing the ICN for their internet connectivity. The SBE plan would bring all network traffic to and from election authorities in to an internal "10 dot IP" internal network system and "whitelisting" IP addresses for access to the IVRS website. Currently, we are unable to whitelist connectivity to IVRS because many of the election authorities do not receive their internet connection via a static IP. The Department of Innovation and Technology (DoIT), through inter-agency agreement would perform the on-site construction and "build out" to the network. DoIT will also provide to each election authority on the ICN: (Currently provided only to state agencies)

- A firewall for the purpose of protecting local election authorities.
- Distributed Denial of Service Attack (DDoS) protection

- Security Operation Center (SOC) 24/7 monitoring
- Albert sensor intrusion detection

The cost of implementation and fees is estimated at $1,500 per month per site over three years. These costs (~$2,000,000) would be paid for with a portion of the $6,946,952.50. The cost to maintain ICN service following the initial three years (monthly bandwidth, etc.) would be an expense allowable each fiscal year with funds from the IVRS Lump Sum Grant. Implementation is expected to take 2-3 years. Participation would be required to maintain a secure connection to IVRS. Cost: $2,000,000 over 3 years

2. **Create an Outreach/Awareness Program.** In partnership with the Illinois State Police's division of Statewide Terrorism and Intelligence Center (STIC) through inter-agency agreement, the SBE will assist in overseeing the "Cyber Security Information Sharing Program" through the appointment of a "Program Manager". The program manager will preferably have an IT background, will assist in coordinating efforts with DoIt's Risk Assessments Team (Cyber Navigators), will be introduced to the local election authorities by the SBE and will begin an outreach effort to educate the local election authorities on the necessity of working with and cooperating with the Program Manager. The Program Manager will offer the following services:

Cyber Security Information Sharing for Election Officials

- Assigned to the Statewide Terrorism & Intelligence Center as the coordinator for conducting outreach to county election officials and election boards in the State of Illinois.
- Contact or meet each county election official and election board commission staff. Use already established professional associations and networks to facilitate the communication.
- Identifies the election official and person in charge of IT in each county. Also identifies the city election board commissioners 'person in charge of IT.
- Processes applications for those who have a 'need to know' to receive information classified as For Official Use Only. Maintains a database of members.
- Disseminates information on "best practices" identified by DoIT to each county election official and election board commission staff.
- Shares cyber-related information to the county election officials, election boards, and those in charge of their IT. This information will come from a variety of sources, including, but not limited to: FBI, DHS, MS-ISAC, STIC, etc.) Will identify their information needs, and ensure these requirements are being met.
- On a daily basis, research and gather information pertinent to cyber-attacks and cyber resiliency. Disseminate information daily by e-mail to vetted partners. Produce intelligence notes based on information received from program participants by researching, validating, and analyzing the data.
- Serves as a resource to assist county election officials and election boards with information on who to contact (STIC, FBI, DHS, MS-ISAC, DoIT, and ING) regarding response to cyber-attacks. STIC already has relationships with these entities.
- Facilitate training webinars and conferences for information sharing.
- Provides routine administrative updates to the Illinois State Board of Elections and produces an annual report assessing the effectiveness of the program.
- Responsible for maturing the program.

Estimated cost for salary for a one year contract with option for a second year: $105,000 per year.

3. **Create a team known as Cyber Navigators/Advisors**. The Cyber Navigator/Advisor would assist the local election authorities by performing onsite risk assessments and providing resources to ensure the Election Security Posture for the upcoming November 2018 mid-term election and continuing into the 2020 Election cycle. The SBE would enter into an interagency agreement with DoIT to provide the staff necessary to perform the duties of the Cyber Navigator/Advisor. The Cyber Navigator/Advisor will ensure that the following resources are utilized based on recommendations of the Center for Internet Security:

- Security Awareness Training (CIS 17)

- DoIT and STIC ($0.00) - Will provide online training or participate in regional trainings to address security awareness training on common areas of vulnerabilities including spear-phishing and phishing assessments.

- Accurate systems and network documentation is available for analysis (CIS 1,2)
  - Per election official performed by internal staffing ($0.00)

- Software updates and patches are regularly applied to information systems (CIS 3)
  - Per election official performed by internal staffing ($0.00)

- Information systems security logs are regularly monitored (CIS 6)
  - ICN – SOC Monitoring ($0.00)

- E-mail accounts for elections officials are secured against phishing attacks (CIS 7)
  - Per election official per account using O365 ($12.50 per month)

- Anti-malware tools are deployed on servers and workstations (CIS 8)
  - Per election official performed by internal staffing ($0.00)

- A stateful firewall is being used to protect elections information systems (CIS 9)
  - ICN – Possible ($0.00)

- Elections systems are protected by an Intrusion Detection Device (IDS/IPS) (CIS 12)
  - ICN – Albert ($0.00)

- IT systems are protected from Distributed Denial of Service (DDoS) attacks (CIS 12)
  - ICN – Monitoring and Mitigation ($0.00)
    - We suggest both

- Vulnerability scans are performed against publicly available servers (CIS 20)
  - Per election official (DHS Cyber Hygiene - $0.00)

The most critical role of the Cyber Navigator/Advisor would be to perform Risk Assessments for each local election authority.

a. Risk Assessment- DoIT, through interagency agreement would provide 8 individuals on a personal services contract basis for the initial 6 month "startup" phase, and then reduce to 4-6 individuals for a 12 month period after that (coverage for 18 months in total). The agreement would consist of the SBE agreeing to pay (with HAVA grant funds) the associated costs (payroll, travel, etc.). The duties of these individuals would be defined as providing "risk assessment" to the local election authorities and provide cyber related training at the SBE's direction. DoIT's procurement and legal team are currently working with SBE staff to provide further details. Cost: TBD

4. **Providing additional cyber security resources for local election authorities.** Currently, SBE staff is in discussions with officials of the Illinois National Guard to secure any available resources regarding cyber security matters. As those discussions continue, a more detailed report of services will be supplied to the Board.

5. **Participation in the Cyber Navigator Program.** If the local election authorities participate in the ICN Expansion Project and Risk Assessment provided by the Cyber Navigators/Advisors, and there are additional grant funds still available, the local election authorities will be able to apply for grants offered by the SBE with any remaining HAVA funds. However, no grants may be made to election authorities that do not participate in the Cyber Navigator Program.

Proposed Components of the Internal SBE Use of HAVA Grant Funds

We propose the amount of $1.2 million be retained by the SBE in the Help Illinois Vote fund for the following uses: consulting contracts that would include services such as cyber security consultants, audit firms, or additional IT consultants for new application development. After additional assessments are completed on the Board's overall cyber security posture, it is anticipated that additional hardware and/or software will be needed to further strengthen the Board's overall network security. Since it is no longer anticipated that local election authorities will utilize a significant portion of their funding allocation for the purchase of new equipment, which will no longer require staff to travel to various election authority offices to perform "audits" (or site visits), the amount of travel was reduced and reallocated into consulting contracts.

Year 1 through year 3:	
Consulting contracts	$185,000/year
IT Hardware/Software	$100,000/year
Travel	$ 15,000/year
Year 4 and year 5:	
Consulting contracts	$90,000/year
IT Hardware/Software	$50,000/year
Travel	$10,000/year
Total 5-year estimate	$1,200,000

Additionally, staff are in the process of drafting rules that will be presented at the July 10, 2018 SBE monthly board meeting. The first required public hearing will also be held during the July meeting.

Emergency Rules- Cyber Navigator Program

Public Act 100-0587 (10 ILCS 5/1A-55 new)

Sec. 1A-55. Cyber security efforts. The State Board of Elections shall provide by rule, after at least 2 public hearings of the Board and in consultation with the election authorities, a Cyber Navigator Program to support the efforts of election authorities to defend against cyber breaches and detect and recover from cyber-attacks. The rules shall include the Board's plan to allocate any resources received in accordance with the Help America Vote Act and provide that no less than half of any such funds received shall be allocated to the Cyber Navigator Program. The Cyber Navigator Program should be designed to provide equal support to all election authorities, with allowable modifications based on need. The remaining half of the Help America Vote Act funds shall be distributed as the State Board of Elections may determine, but no grants may be made to election authorities that do not participate in the Cyber Navigator Program.

Definitions-

Compromised – The state wherein a computer system, network, or data has had its integrity, availability, or confidentiality undermined by an attacker

Cyber- Of, relating to, or involving computers or computer networks (such as the Internet)

Cybersecurity- The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Cybersecurity posture-Overall cyber security strength, particularly as it relates to the internet and vulnerability to outside threats.

Department of Innovation and Technology (DoIT)- The State Agency with responsibility for the information technology functions of agencies under the jurisdiction of the Governor. The agency tasked with managing the Illinois Century Network.

Illinois Century Network (ICN) - 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.

The State Board of Elections shall use no less than half of the funds from the 2018 HAVA Election Security Grant to implement the following provisions of the Cyber Navigator Program

Infrastructure-Illinois Century Network (ICN) Connectivity

1. The Illinois State Board of Elections shall modify the statewide voter registration database, including the electronic canvas transmissions, to allow for connection from local election jurisdictions via an ICN established internal network.
    a. The State Board of Elections shall make a reasonable effort for all direct connectivity to the statewide registration database to be from known “whitelisted” IP addresses.

b. Once all jurisdictions are connected via the ICN, traffic between the election jurisdictions and the State Board of Elections will be configured to use private IP addressing.

2. Each election jurisdiction participating in the Cyber Navigator Program shall connect to the statewide voter registration system via the ICN or have entered into an agreement to connect via the ICN as soon as practicable.
3. The State Board of Elections shall establish a Memorandum of Agreement with DoIT to provide the election jurisdictions access to a reliable ICN connection, for the purposes outlined in this section.
4. DoIT shall provide "protective services" to each election authority's connection on the ICN.
    a. A firewall shall be configured such that it provides protections for the election authority's connection through the ICN.
    b. Software shall be installed to provide protection against attempted Distributed Denial of Service Attacks (DDoS).
    c. Election jurisdictions connections on the ICN shall be eligible to receive DoIT's Security Operation Center (SOC) 24/7 monitoring.
    d. Election jurisdiction connections shall have Albert Sensor, or comparable device, intrusion detection

<u>Outreach-Cyber Security Information Sharing</u>

The State Board of Elections shall establish a Memorandum of Agreement with the Illinois State Police's Statewide Terrorism and Intelligence Center (STIC) to develop a cyber security outreach and/or awareness program.

a. At least one individual shall be hired as the Program Manager and he/she shall;
    i. Work with the Cyber Navigators to compile relative information for distribution to all affected parties.
    ii. Be assigned to the Statewide Terrorism & Intelligence Center as the coordinator for conducting outreach to county election officials and election boards in the State of Illinois.
    iii. Contact or meet each county election official and election board commission staff. The Program Manager shall use already established professional associations and networks to facilitate the communication.
    iv. Identify the election official and person in charge of IT in each county and shall also identify the city election board commissioners 'person in charge of IT.
    v. Process applications for those who have a 'need to know', to receive information classified as For Official Use Only. The Program Manager shall maintain a database of these persons.
    vi. Disseminate information on "best practices" identified by DoIT or the Cyber Navigators to each county election official and election board commission staff.
    vii. Share cyber-related information to the county election officials, election boards, and those in charge of their IT. This information will come from a variety of sources, including, but not limited to: The FBI, DHS, MS-ISAC, STIC, etc. The Program Manager shall will identify

their information needs, and ensure these requirements are being met.

viii. On a daily basis, research and gather information pertinent to cyber-attacks and cyber resiliency. The Program Manager shall disseminate information daily by e-mail to vetted partners and produce intelligence notes based on information received from program participants by researching, validating, and analyzing the data.

ix. Serve as a resource to assist county election officials and election boards with information on who to contact (STIC, FBI, DHS, MS-ISAC, DoIT, and ING) regarding response to cyber-attacks. STIC already has relationships with these entities.

x. Facilitate training webinars and conferences for information sharing.

xi. Provide routine administrative updates to the Illinois State Board of Elections and produces an annual report assessing the effectiveness of the program.

xii. Be responsible for maturing the program.

xiii. Oversee security awareness training for election authorities and their staff

1. Participants shall at least once per calendar year complete an online security awareness training on common areas of vulnerabilities including spear-phishing and phishing assessments;

b. Data sharing related to a known compromise of an election system

i. Election authorities shall notify the State Board of Election as soon as reasonably possible in the event of a security compromise related to any of their election systems.

ii. The State Board of Elections shall notify all election authorities as soon as reasonably possible in the event of a security compromise related to the statewide registration database.

<u>Personnel-Cyber Navigators</u>

1. The State Board of Elections shall enter into an interagency agreement with the Department of Innovation and Technology (DoIT) to provide cyber-security personnel resources for an election jurisdiction cyber assistance program. These personnel will be known as Cyber Navigator/Advisors and they;
    a. Shall work to increase election jurisdictions' cybersecurity posture;
    b. Analyze system and network documentation for accuracy.
    c. Recommend software updates and patches are regularly applied to information systems;
    d. Make recommendations for secure e-mail accounts and best practices regarding same;
    e. Provide guidance for anti-malware tools and their deployment on both serves and workstations;
    f. Perform Risk Assessments for each election jurisdiction;
    g. Assist jurisdictions and/or their IT department with assessing their systems against the Center for Internet Security's recommended procedures.
2. DoIT shall provide 9 individuals on a personal services contract basis for an initial 12 month "startup" phase. The ongoing need will be evaluated as the program matures.

The State Board of Elections shall pay the associated costs (payroll, travel, etc.) using 2018 HAVA Election Security Grant funds, if available. The duties of these individuals is outlined above.

Participation in Cyber Navigator Program

In order for an election authority to be eligible for funds from the 2018 HAVA Election Security Grant, the jurisdiction must participate in the Cyber Navigator Program.

1. Election Authority minimum requirements;
    a. The election authority must utilize the ICN for connectivity to the State Board of Elections as outlined above or have entered into an agreement to do so as soon as practicable.
    b. The election authority must participate in the Outreach portion of the program including:
        i. Register with at least the EI-ISAC
        ii. Work with the Program Manager to establish two-way data sharing
        iii. At least one representative of the election authority shall complete the security awareness training as outlined above.
    c. The election authority shall allow the Cyber Navigators to complete a Risk Assessment and an analysis against the Center for Internet Security's recommended procedures.
2. Program Manager/Cyber Navigator requirements
    a. The Program Manager shall provide in writing to the State Board of Elections, verification for each election authority that has met their requirements as outlined above.
        i. The Cyber Navigator shall provide in writing to the Program Manager verification for each election authority under their review that has met the requirements as outlined in c. above