STATE BOARD OF ELECTIONS

STATE OF ILLINOIS

2329 S. MacArthur Blvd.
Springfield, Illinois 62704-4503
217/782-4141
Fax: 217/782-5959

James R. Thompson Center
100 W. Randolph St., Ste. 14-100
Chicago, Illinois 60601-3232
312/814-6440
Fax: 312/814-6485

EXECUTIVE DIRECTOR
Steven S. Sandvoss

PUBLIC NOTICE

OF

PUBLIC HEARING

Pursuant to Public Act 100-0587, a Public Hearing will be conducted on **August 1, 2018,** to accept comments on the implementation of the Cyber Navigator Program.

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.

Public Act 100-0587 may be viewed on the General Assembly's website at http://www.ilga.gov/legislation/publicacts/100/PDF/100-0587.pdf. Written comments may be submitted via e-mail to Amy Kelly at akelly@elections.il.gov or mailed to the Board's Springfield office. The proposed Rules are also attached to this Notice.

DATED: July 26, 2018

Steven S. Sandvoss, Executive Director

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