**Section 213.30 Outreach − Cyber Security Information Sharing**

The Board shall establish an Interagency Agreement with the Illinois State Police's Statewide Terrorism and Intelligence Center (STIC) to develop a cyber security outreach and/or awareness program. The Interagency Agreement shall include the following:

a) The Board shall hire at least one individual as the Program Manager and he/she shall:

1) Work with the Cyber Navigators to compile relative information for distribution to all affected parties.

2) Be assigned to STIC as the coordinator for conducting outreach to county election officials and election boards in the State of Illinois.

3) 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.

4) Identify the election official and person in charge of IT in each county and shall also identify the election board commissioners' person in charge of IT.

5) 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.

6) Disseminate information on "best practices" identified by DoIT or the Cyber Navigators to each county election official and election board or commission staff.

7) Share cyber-related information with the county election officials, election boards, and those in charge of the IT of those officials/boards/commissions. This information will come from a variety of sources, including, but not limited to: FBI, Department of Homeland Security, MS-ISAC, STIC. The Program Manager shall identify the official's/board's/commission's information needs and ensure these requirements are being met.

8) 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.

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

10) Facilitate training webinars and conferences for information sharing.

11) Provide routine administrative updates to the Board and produce an annual report assessing the effectiveness of the program.

12) Be responsible for maturing the program.

13) Oversee security awareness training for election authorities and their staff.

b) Participants in the Cyber Navigator Program shall at least once per calendar year complete an online security awareness training on common areas of vulnerabilities, including spear-phishing and phishing assessments.

c) Data Sharing Related to a Known Compromise of an Election System

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

2) The Board shall notify all election authorities as soon as reasonably possible in the event of a security compromise related to the Board's statewide registration database.