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

BOARD MEMBERS
William J. Cadigan, Chairman
John R. Keith, Vice Chairman
Andrew K. Carruthers
Ian K. Linnabary
William M. McGuffage
Katherine S. O'Brien
Charles W. Scholz
Casandra B. Watson

EXECUTIVE DIRECTOR
Steven S. Sandvoss

FOR IMMEDIATE RELEASE

CONTACT: MATT DIETRICH
(217) 558-1955
MDIETRICH@ELECTIONS.IL.GOV

STATE, FEDERAL AND LOCAL OFFICIALS TO DISCUSS ELECTION CYBERSECURITY, VOTING SYSTEM INTEGRITY

SPRINGFIELD – Officials from the Illinois State Board of Elections will hold a press conference at 2 p.m. Tuesday, Oct. 16, in Room 2-025 of the James R. Thompson Center in Chicago to discuss election cybersecurity and the integrity of the Illinois election system in the 2018 elections. Joining Board of Elections officials will be representatives from federal and state agencies and local election authorities who have worked together to bolster all aspects of election security ahead of the Nov. 6 general election.

State Board of Elections Executive Director Steve Sandvoss and directors from the Board's Information Technology and Voting & Registration Systems divisions will be present to answer questions on election security. They will be joined by officials from the Illinois Department of Innovation and Technology, Illinois National Guard and U.S. Department of Homeland Security and local election officials.

The conference will be live-streamed at https://multimedia.illinois.gov/balance/doit-live.html and archived video will be posted there after the event.

Satellite coordinates are as follows:
HD Satellite Coordinates:
Slug: BOE Election Security
Date: October 16, 2018
Time: 4:00 PM (CT) 4:15 PM (CT)
Satellite: Echo105k
Transponder: 11
Slot: D9
Downlink Frequency: 11933.5000
Downlink Polarization: Vertical
Bandwidth: 9 MHz
Symbol Rate: 7.5
FEC: 5 / 6
Data Rate: 18.589212
Video: MPEG-4 4:2:0
Modulation Scheme: 8PSK

For technical assistance please call IOCI Media Services at 217-785-5499.

Oct. 16, 2018

2016 VOTER DATA BREACH LEADS TO ENHANCED SECURITY MEASURES

SPRINGFIELD, Ill. – In July 2016, the electronic voter registration database maintained by the Illinois State Board of Elections was breached in a cyberattack. The breach was detected and closed by SBE information technology staff, who later notified some 76,000 voters whose data may have been viewed in the intrusion.

What follows is a report filed in August 2016 detailing the data breach and an addendum listing steps that have been taken in its aftermath to avoid another such incident.

Illinois Voter Registration System
Database Breach Report
August 26, 2016

The Illinois State Board of Elections was the victim of a malicious cyber -attack of unknown origin against the Illinois Voter Registration System database (IVRS) beginning June 23, 2016. SBE staff became aware of a breach on July 12 and immediately took measures to stop the intrusion. In the following weeks, SBE staff has worked to determine the scope of the intrusion, secure databases and web applications, comply with state law regarding personal information loss, and assist law enforcement in their investigation of the attack.

Timeline

July 12, 2016

- State Board of Elections IT staff was made aware of performance issues with the IVRS database server.
- Processor usage had spiked to 100% with no explanation.
- Analysis of server logs revealed that the heavy load was a result of rapidly repeated database queries on the application status page of the Paperless Online Voter Application (POVA) web site.
- Additionally, the server logs showed the database queries were malicious in nature – a form of cyber-attack known as SQL Injection. SQL Injections are essentially unauthorized, malicious database queries entered in a data field in a web application.
- SBE programmers immediately introduced code changes to eliminate the vulnerability.

July 13, 2016

- SBE IT took the web site and IVRS database offline to protect against further attack.
- Analysis of the web server logs showed that malicious SQL queries began on June 23, 2016.
- SBE staff maintained the ability to log and view all site access attempts.

- Malicious traffic from the IP addresses continued, though it was blocked at the firewall level.
- Firewall monitoring indicated that the attackers were hitting SBE IP addresses 5 times per second, 24 hours per day.
- SBE staff began working on determining the extent of the breach, analyzing the integrity of the IVRS database, and introducing security enhancements to the IVRS web servers and database.

July 19, 2016
- We notified the Illinois General Assembly of the security breach in accordance with the Personal
- Information Protection Act (PIPA).
- In addition, we notified the Illinois Attorney General's office.

July 21, 2016
- SBE IT completed security enhancements and began bringing IVRS back online.

ADDENDUM, October 2018

In the aftermath of the 2016 cyberattack, SBE has taken numerous steps to bolster the security of its electronic database. These include:

- Since October 2016, the U.S. Department of Homeland Security has performed weekly "hygiene scans" to detect potential vulnerabilities in our systems. None have been identified to date.
- Immediately after the breach, SBE installed new hardware and software and implemented new security procedures to enhance cybersecurity
- Executive Director Steve Sandvoss obtained security clearance to attend national briefing with DHS in Washington, D.C., on cybersecurity and election integrity efforts in February 2018
- In May 2018, SBE completed an on-site "Risk and Vulnerability Assessment" with DHS, the most stringent cybersecurity analysis the agency offers
- Created the Illinois Cyber Navigator Program in conjunction with the Illinois Department of Innovation and Technology and Illinois State Police to bring uniform cybersecurity standards to all local election authorities statewide (please see attached document for details on the program)
- Participated in numerous groups and associations dedicated to sharing cybersecurity intelligence and analysis, including the Multi-State Information Sharing & Analysis Center (MS-ISAC) and Election Infrastructure Information Sharing and Analysis Center.
- Worked with state and federal law enforcement and intelligence agencies to facilitate information sharing from the federal level all the way down to the local level
- Created an agreement with the Illinois National Guard to assist in case of election cybersecurity incidents in 2018 midterm election
- In summer 2018, SBE added three cybersecurity specialists to its IT staff, one of whom is stationed at the Illinois State Police State Terrorism Intelligence Center.

###

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

BOARD MEMBERS
William J. Cadigan, Chairman
John R. Keith, Vice Chairman
Andrew K. Carruthers
Ian K. Linnabary
William M. McGuffage
Katherine S. O'Brien
Charles W. Scholz
Casandra B. Watson

EXECUTIVE DIRECTOR
Steven S. Sandvoss

2018 HAVA Election Security Grants
Program Narrative and Budget Submission

The State of Illinois was awarded **$13, 232, 290.00** as authorized under Section 101 of the Help America Vote Act of 2002 (P.L. 107-252) (HAVA) and provided for in the Consolidated Appropriations Act, 2018 (Public Law 115-141), the purpose of this award is to "improve the administration of elections for Federal office, including to enhance "election technology and make election security improvements" to the systems, equipment and processes used in federal elections. The State of Illinois is required to provide a 5% state match of $661,615.00 prior to March 23, 2020. The entire 5% state match of **$661,615.00** will be vouchered from the general revenue fund to the Help Illinois Vote fund by July 20, 2018. The physical transfer of funds could take an additional 3-4 months based on current pay cycles.

Illinois Governor, Bruce 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. Due to this legislation, the SBE is working with stakeholders to implement a cyber navigator program to provide direction to the election officials in the state for both short and long term use of the funding.

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.

As required by law, no less than half of any such funds received shall be allocated to the "Cyber Navigator Program" to support efforts of election authorities to defend against cyber breaches and detect and recover from cyber-attacks. Under PA100-0587, **$6,946,952.50**, must be used to provide equal support to all Illinois 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.   **Infrastructure- 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 (Department of Innovation and Technology) 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". 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 statewide voter registration database (IVRS). 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. Implementation is expected to take 2-3 years. Participation would be required to maintain a secure connection to IVRS. Cost: $2,000,000 for initial connection, which is reflected as part of the sub-grants to local voting jurisdictions.

2.   **Outreach- Cyber Security Information Sharing 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 hiring of a "Program Manager".   The program manager 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. While the salary for the program manager will be funded from GRF funds, the hardware, software and training services used to create support for the Cyber Security Information Sharing Program will be supported with HAVA funds.

3.   **Personnel-Cyber Navigator/Advisor**. 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 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 9 individuals on a personal services contract basis for the initial 12 month "startup" phase. The ongoing need will be evaluated as the program matures. The agreement will propose 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 drafting the agreement.   Cost: $1,420,312.32 for 2-month period and projected 5 staff for 12 months at $813, 980 (total of 2 years).

4.   **Providing additional cyber security resources for local election authorities.**   SBE staff is in discussions with officials from other local, state and federal agencies to secure any available resources regarding cyber security matters.   These discussions will continue to evolve to increase the cyber security posture through 2020.

5.   **Participation in the Cyber Navigator Program.**   If the local election authorities meet participation requirements outlined in the Cyber Navigator Program Rules, they will be eligible to apply

for sub-grants offered by the SBE. The sub-grants will be funded with any remaining HAVA funds that are not utilized for the operational costs associated with administering the Program. Since participation in the Cyber Navigator Program is mandated, and the timeframe projected for creation and implementation is not fully known, $8,747,998.00 has been budgeted for sub-grants over the 5 year grant period. The sub-grants could include direct grants offered to local election authorities after Program participation has been verified. Non-operational costs (i.e. sub-grants, etc.) could include direct contracts with vendors to address vulnerabilities discovered during the on-site risk assessments.

The SBE is required to hold public hearings in consult with local election officials while developing this program. The first hearing was held July 10, 2018 and the second hearing was held August 1, 2018.

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.

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

STATE BOARD OF ELECTIONS

| **WILLIAM J. CADIGAN** | **JOHN R. KEITH** | **STEVEN S. SANDVOSS** |
| *Chairman* | *Vice Chairman* | *Executive Director* |

ELECTION NEWS   ELECTION NEWS   ELECTION NEWS

FOR IMMEDIATE RELEASE

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

Oct. 15, 2018

ELABORATE TESTING PROCESS PROTECTS VOTING SYSTEM INTEGRITY, ACCURACY

SPRINGFIELD, IL – Voters concerned about the safety of their votes and the accuracy of vote tabulation in the 2018 primary and general elections should be aware of the extensive testing to which all voting equipment in Illinois is subject. In addition, voting equipment used in early voting and at polling places on Election Day are never connected to the Internet.

After extensive testing of voting equipment before Election Day, the Illinois State Board of Elections randomly selects 5% of precincts and early voting equipment in all election jurisdictions to retabulate ballots to check for accuracy.

Here is summary of the process for testing voting equipment before, on and after Election Day.

Before Election Day

- By law, all equipment must be rigorously and successfully tested and approved by both an independent voting system testing laboratory (VSTL) and by the State Board of Elections' team of election specialists
- Automatic tabulating equipment programmed only using unique office and candidate ID numbers which are assigned by the State Board of Elections and provided to the election authority
- All election authorities must conduct a pre-test to ensure 100% accuracy in detecting ballots that are overvoted (more votes marked on the ballot than are allowed), undervoted (fewer votes marked on the ballot than are allowed) or cannot be read by the system.
- Not less than five days before the election, a "public test" is held. Public notice of the time and place of the public test must be given at least 48 hours prior to the test by publishing notice in one or more newspapers within the election jurisdiction. The test is required to be open to representatives of the political parties, the press, representatives of the State Board and the public.
- After an errorless public test, all materials used in the test must be SEALED AND REMAIN SEALED
- State Board also conducts random tests up to two days before the public test.

On Election Day

- Election judges oversee voting at every polling place

- Election judges are citizen volunteers who are trained by the county governments to work at polling places
- Depending on the county, there will be three to five election judges present at every precinct polling place
- Judges must represent both Democratic and Republican parties
- In addition to election judges, authorized poll watchers may be present
- Poll watchers can be representatives of established political parties, candidates, qualified organizations of citizens, State nonpartisan civic organizations, or organized proponents or opponents of ballot propositions
- They are permitted to closely observe election judges and periodically inspect the equipment when not in use by voters

After Election Day

- Immediately after polls close, judges open the ballot box and count ballots to make sure the number agrees with number of voters voting according to both scan equipment and by applications for ballots
- "In-precinct totals report" must be generated and posted in a conspicuous area inside the polling place
- Bipartisan team of 2 judges immediately returns the paper ballots and all other election materials to the election authority in a sealed container
- After election day, the State Board randomly selects 5% of precincts and early voting equipment in all election jurisdictions to retabulate ballots to check for accuracy
  - In those precincts or on the early voting equipment selected for retabulations, the election authority conducts a post-election test similar to the pre-test and public test
  - Representatives of both parties, the local state's attorney, local law enforcement agencies and qualified civic organizations are notified of its time and place and can be present for the retabulation

The outcome of the election is not official until this process is complete. This can take up to three weeks.

###

STATE BOARD OF ELECTIONS
STATE OF ILLINOIS

EXECUTIVE DIRECTOR
Steven S. Sandvoss

The following officials participated in the Illinois State Board of Elections security press conference on Oct. 16, 2018:

Steve Sandvoss, executive director, Illinois State Board of Elections

William J. Cadigan, chairman, Illinois State Board of Elections

Maj. Gen. Richard J. Hayes Jr., adjutant general, Illinois National Guard

Sally Turner, Logan County Clerk

Noah Praetz, director of elections, Office of Cook County Clerk David Orr

Chris Hill, deputy chief information security officer, Illinois Department of Innovation and Technology

Alexander S. Joves, regional director, U.S. Department of Homeland Security

Matt Emmons, director of information technology, Illinois State Board of Elections

Kyle Thomas, director of voter registration and systems, Illinois State Board of Elections