APPROVED CYBERSECURITY PLAN- 2020

Background

The New York State Board of Elections (NYSBOE) has been closely monitoring the ever-growing threat posed to information and elections systems by nation-states, terrorist organizations and independent criminal actors. In 2018, NYSBOE received federal funding available through the 2018 HAVA (Help America Vote Act) Election Security Grant, which allocated $19,483,647 dollars to the State of New York "to improve the administration of elections for Federal office, including to enhance election technology and make security improvements."[1] In order to be eligible for the 2018 allocated federal cybersecurity funds, New York State provided matching funds in the amount of $974,182.35, for a total of $20,457,829.35.

In furtherance of that same purpose, the 2020 HAVA Election Security Grant has allocated $21,838,990 to New York State. In order to receive those funds, New York State will again match with its own funds, in the amount of 20%, or $4,367,798, to be used for voting equipment, staffing, and Online Voter Registration system development and security. In total between federal and state matching funds, NYS anticipates receiving $26,206,788 to further protect secure elections for the people of New York State.

To fulfill the purpose of the grant, NYSBOE previously initiated, and intends to continue, the **ARMOR** plan, designed to:
Assess the risk to the State and County election systems;
Remediate the vulnerabilities;
Monitor ongoing **O**perations; and
Respond to incidents.

Key elements of that plan which have already been executed include:

- a thorough risk assessment of each County Board of Elections (CBOE);
- Intrusion Detection System (IDS) protections at each CBOE;
- Managed Security Services (MSS) as an option for each CBOE;
- cyber hygiene user training, provided by industry-recognized Secure Awareness Network (SANS);
- creation of a Secure Elections Center;
- conducting Table-Top Exercises across the State;
- daily pre-election operation center statewide calls; and
- a Cybersecurity newsletter distributed to CBOEs.

Further details on these programs, and their continuation in the new program, are outlined below.

[1] 2018 Help America Vote Act Elections Security Grants Award Packet, April 17, 2018, page 1.

Collaboration and Consultation

Over the last several years, NYSBOE has established and cultivated relationships to form a trusted network of partners in NYS. These collaborative and interdependent relationships are a necessity to address complex, cross-government, and multi-dimensional cybersecurity events. NYSBOE has invested significant resources in fostering these relationships and works closely with many organizations including the NYS DHSES, NYS ITS, and the Governor's Cyber Advisory Board, the MS-ISAC, and many others (see listing). NYSBOE recognizes the value of each partner organization and continues to leverage the strengths of each. Over the past two years, two new relationships were established with the Center for Technology in Government at the University at Albany, State University of New York (CTG UAlbany) and New York State Local Government Information Technology Directors Association (NYSLGITDA). Both organizations bring a wealth of expertise in New York state and local government IT, and have provided insights in day-to-day operational tactics and long term cybersecurity planning that is essential to protecting NYS elections.

To develop a comprehensive plan to ensure the security of New York State's elections infrastructure. NYSBOE has worked, and continues to work, extensively with federal, state, local and other important partners, including:

- Elections Assistance Commission (EAC),
- United States Department of Homeland Security (DHS),
- Federal Bureau of Investigation (FBI),
- United States General Services Administration (GSA),
- National Association of State Election Directors (NASED),
- National Association of Secretaries of State (NASS),
- Center for Internet Security (CIS),
- Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC),
- NYS Department of Homeland Security and Emergency Services (DHSES),
- NYS Association of Counties (NYSAC),
- NYS Local Government IT Directors Association (NYSGLITDA)
- NYS Office for Information Technology Services (OITS),
- Governor's NYS Cybersecurity Advisory Board (CSAB),
- NYS Intelligence Center (NYSIC),
- New York State Police,
- Belfer Center for Science and International Affairs at Harvard University, and
- The Center for Technology in Government at Albany, State University of New York (CTG UAlbany)

The Plan

Continuing the work already begun with previous funding, NYSBOE will both advance existing ARMOR initiatives, and provide for additional, expanded activity. The details, in relation to the ARMOR outline, are expounded upon below.

Assess the Risk

Comprehensive Risk Assessment for the New York State Board of Elections

Utilizing one of several key strategic partnerships, the New York State Board of Elections engaged the federal Department of Homeland Security to conduct a free comprehensive Risk and Vulnerability Assessment conducted on the State's elections infrastructure. This one-on-one engagement combined national level threat and vulnerability information with data collected and discovered through the assessment. From this, DHS provided NYSBOE with specific risk analysis reports and strategic remediation recommendations prioritized by risk. The process of addressing the recommendations provided by DHS is well underway at NYSBOE, and NYSBOE seeks to utilize the additional 2020 HAVA funding to continue these remediation efforts through the update of software/hardware, additional segmentation, enhanced logging and monitoring, increased website protections, and enhanced staffing. NYSBOE further intends to again utilize this service from DHS in the future, and subsequently to use a portion of 2020 HAVA funds for possible remediation recommendations resulting from that assessment.

Comprehensive Risk Assessment for all County Board of Elections

Beginning in 2018, NYSBOE contracted with a third-party vendor for professional services to conduct a comprehensive, uniform and verified risk assessment at every County Board of Elections (CBOE). This was in addition to a previously-conducted CBOE elections risk survey to gain an understanding of the security posture of each county board. County Boards are responsible for procuring, inventorying, securing and training staff on elections infrastructure and technologies. A uniform and verified third party risk assessment was deemed critical in ascertaining a security baseline for our statewide elections infrastructure. Individual reports were created for each CBOE, for distribution to the corresponding county IT unit and Board of Elections. In addition, an overarching report on statewide trends observed at CBOEs was also generated by the third-party vendor, and augmented with analysis by in-house NYSBOE staff from the Secure Elections Center (SEC).

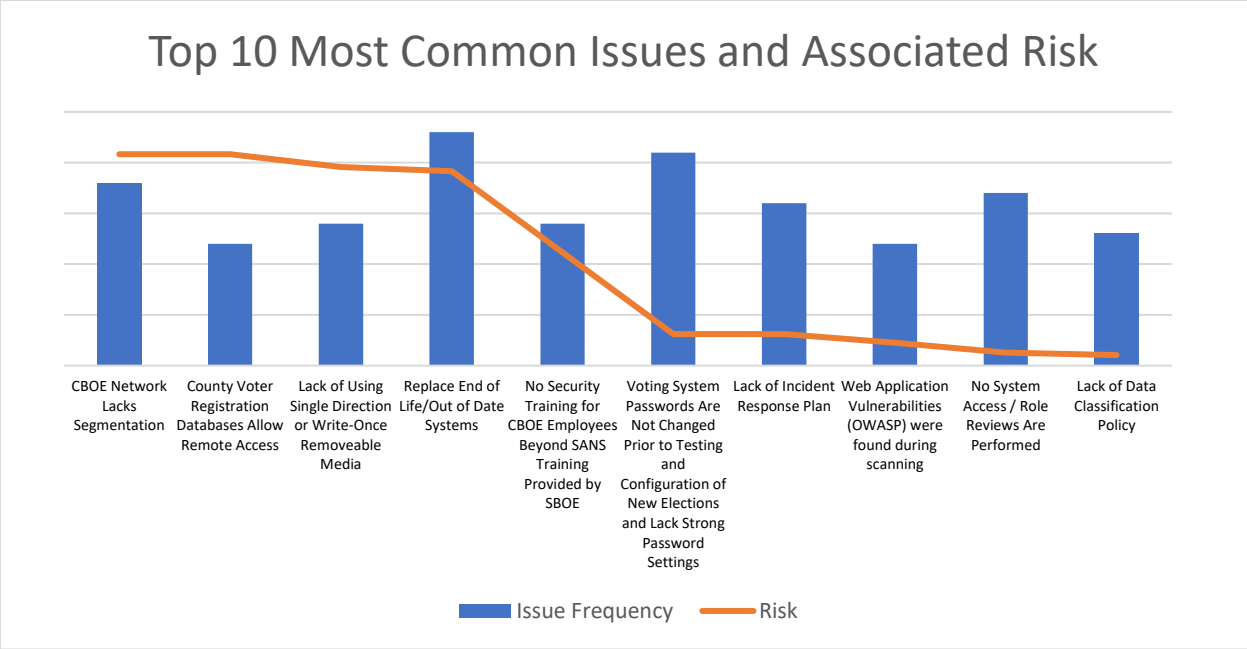

Figure 1: Top trend analysis from CBOE Risk Assessment reports.

Remediate Vulnerabilities

NYSBOE Remediation

Based on the Risk Assessment performed by DHS, NYSBOE has identified several areas of remediation to implement. These remediations include updated hardware/software, additional segmentation, improved malware protections, website protections, and enhanced backup and recovery provisions.

County Board Remediation

CBOE risk assessment findings identified potential vulnerabilities in county elections infrastructure. These vulnerabilities require remediation to ensure the security of CBOE infrastructure and systems. The Secure Elections Center has begun the process to receive, analyze and evaluate, and set priorities to address identified vulnerabilities.

Areas of remediation identified to this point include:

1. **Information Security Officer (ISO) on-demand advisory services** – NYSBOE will contract for the services to fully analyze each CBOE risk assessment report, meet with appropriate county BOE and IT personnel for each county, and develop individualized mitigation recommendations for the short term and long term.
2. **Temporary staff assistance** – This would be hourly or project based supplemental staff to assist "hands on" for mitigation.
3. **Purchasing and/or acquisition assistance** – This could take the form of a "navigator type" service to help guide through the procurement process. Alternatively, or in addition, NYSBOE could implement a reimbursement type of service, allowing for reimbursement of approved

county infrastructure/hardware to be purchased, as determined through the ISO on-demand advisory service plan.

Monitor Operations

Cybersecurity Regulation

As part of monitoring ongoing operations, NYSBOE will develop cybersecurity regulations designed to promote uniform regulatory standards. To do this, NYSBOE will procure information advisory services to assist in the development of cybersecurity regulations, setting minimum cybersecurity standards for state and county boards. Regulations and standards will be in accordance and complementary to standards already recommended for government entities. The regulation will require each Board to assess risk and show evidence of a cybersecurity program that addresses their risk profile. While all counties have cybersecurity measures in place, this regulation will set forth a focus of a program that includes both technical and policy considerations. SBOE has started developing the regulation by collaborating with relevant state partners and will soon engage county BOE and IT partners for their feedback.

NYSBOE Secure Elections Center

Created with funding from the 2018 HAVA grant, the NYSBOE Secure Elections Center is tasked with assisting all Counties with the formulation, implementation and evaluation of security measures, regulations and policies relative to elections infrastructure. The Center is responsible for collecting, reviewing, consulting and evaluating all elections security policies and regulations and ensure continuity of election administration and operations. The Secure Elections Center works closely with the existing executive management of the Board. Overseeing the SEC, and created at the same time, is the position of NYSBOE Elections Chief Information Security Officer (CISO). Reporting directly to the NYSBOE Chief Information Officer, the CISO has responsibility to oversee the State Board's cybersecurity policy, patching, internal log review, incident management, security software management, and cybersecurity activity of the SEC personnel. To properly expand and support the mission of the Secure Elections Center would require additional staff, including:

- two (2) additional **Elections Security Specialists** to act as liaisons and coordinate with CBOEs relative to policy implementations, improved audits of elections results, risk analysis coordination and connection support;
- one (1) additional **Website Secure Access Specialist** to manage the Board's website and ensure the accessibility of documents; and
- two (2) additional **Cybersecurity Election Analysts**, to assist the State Board to monitor and rapidly respond to election-related social media mis/disinformation.

Network Monitoring at CBOEs

Federal, State and other stakeholders recommended that network monitoring be immediately implemented at each County Board of Elections, if not already in place. Monitoring, Distributed Denial of Service (DDOS) protection and site scanning provide a baseline of security for elections systems and

infrastructure. County Board of Elections infrastructure may be networked with County infrastructure which increases the scope and cost of network monitoring. Through 2018 HAVA Grant funds, NYSBOE undertook two significant efforts to provide this monitoring:

- **Intrusion Detection System (IDS)** – each CBOE was required, at no cost to themselves, to implement IDS protection, or alternatively to substantively demonstrate pre-existing IDS protection of an equivalent level. All CBOEs in New York now have this protection, either through this program, through the federal DHS program, or through their own procurement. (See Figure 2.)
- **Managed Security Services (MSS)** –each CBOE was also given the option to participate, again at no cost to themselves, in log monitoring services to detect and report anomalies and potential threats. In total, thirty-four (34) CBOEs took advantage of this program. (See Figure 3.)

Through the 2020 HAVA Grant funding, NYSBOE intends to continue, and expand where possible, each of these two programs for an additional two (2) years of monitoring and protection.

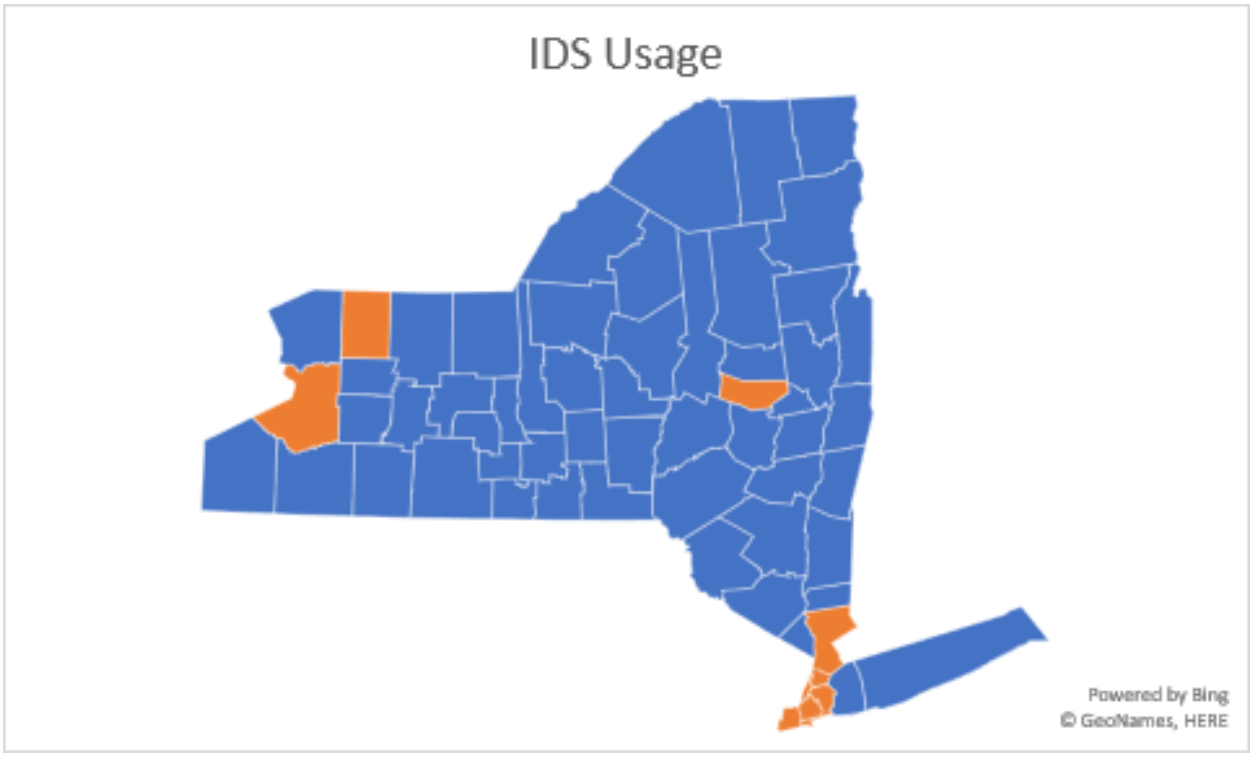

Figure 2: Counties participating in the NYSBOE IDS program are represented in blue. Counties represented in orange have functionally equivalent solutions, which were not procured through this program.

County Cybersecurity Training and Toolkit

The NYSBOE established a series of training tools for CBOEs, based on recognized industry standards, in relation to cyber hygiene best practices, access management protocols and recommendations for incident handling. This was largely accomplished through the procurement of industry-recognized online SANS cybersecurity awareness training courses. Comprehensive cybersecurity training will be provided to all CBOEs, county IT support, and election system vendors on a continuous basis. This is required to ensure a consistent level of cyber hygiene and combat vulnerabilities raised by staff turnover as well as to stay current with the latest trends and developments in cybersecurity. Through the additional 2020 HAVA Grant fund, NYSBOE intends to continue this training for an additional three years.

Research and Analysis

In New York, both state and county Boards of Elections carry out a series of error detection processes on Voter Registration data to ensure the accuracy and completeness of those records. While these processes have produced value, NYSBOE continues to look for more advanced approaches to statewide pattern detection. The prototype project, led by CTG UAlbany, and in collaboration with the University at Albany's College of Engineering and Applied Sciences (CEAS), and the College of Homeland Security and Emergency Preparedness and Cybersecurity (CEHC), focused on conducting data forensics on NYS Voter Registration data (NYSVoter), applying statistical and machine learning modeling to identify anomalies and patterns in the data, and developing a range of visualizations for both state and county leaders.

In May of 2018, NYSBOE met with key stakeholders in a first-of-its-kind series of tabletop exercises to consider threats to the state's elections infrastructure. The exercises included technical components such as networks and platforms, applications, processes, and data. Several recommendations for action resulted from that exercise, one of which specifically directed re-envisioning of the State's elections infrastructure that would provide a roadmap for SBOE and its partners across the state to continue to deliver secure and resilient elections systems in an increasingly complex and threat-rich environment. Working again with CTG UAlbany, phase one of this project includes gaining a more in depth understanding of how current state-local data processes are carried out, gathering input from county (BOE and IT) leaders on different shared infrastructure models, and documenting election infrastructure efforts in other bottom up and hybrid states across the nation.

Respond to Incidents

NYSBOE has established the Secure Elections Center to increase the cybersecurity of the State and County Boards of Elections. The SEC's focus on training and preparedness will prevent some incidents from occurring. The SEC, in collaboration with the consulting and advisory services of NYSTEC, will also develop both a continuity of operations plan (COOP) and a comprehensive incident response plan, for the State and County Boards to triage, coordinate and respond to incidents. The response plan requires:

- the development of a comprehensive cyber incident plan which includes the review and updating of State and County Board of Elections current emergency security and response plans;
- procedures for incident identification, containment, eradication, recovery and post-response assessment will be fully developed;
- personnel to staff and respond to cyber incidents; and
- technology to facilitate the intake, coordination and tracking response to cyber incidents

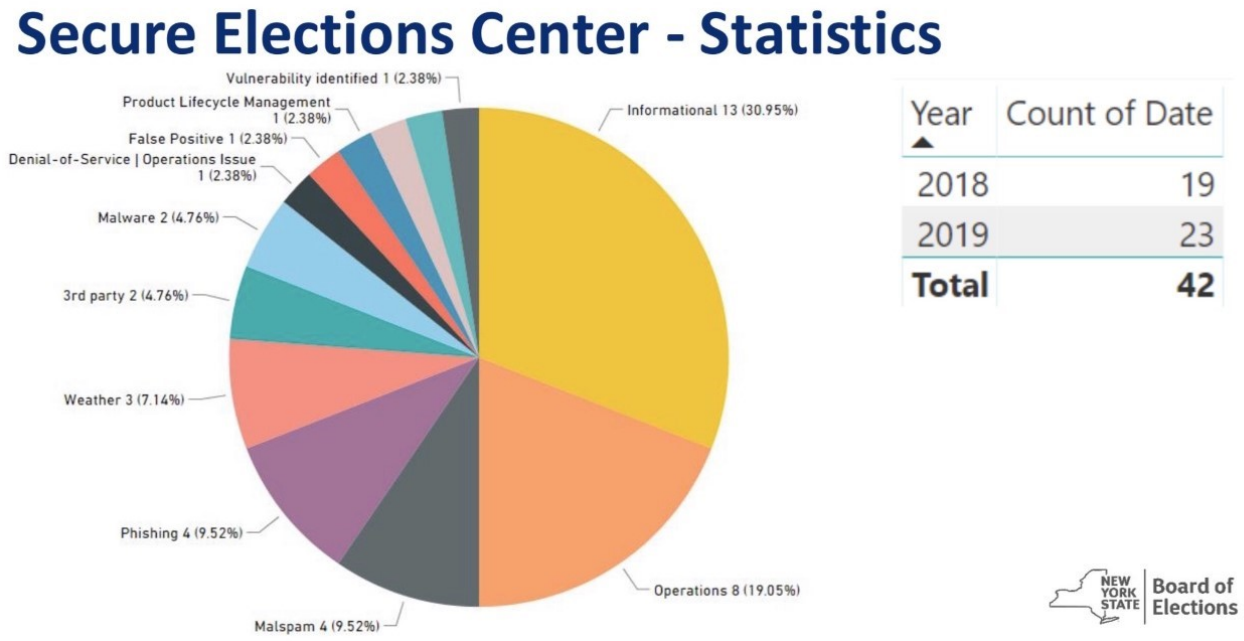

Figure 4: Incidents responded to by NYSBOE SEC in calendar years 2018 – 2019.

To further support the mission of the NYSBOE SEC, and in addition to the Center working with other state and federal partners, the Governor's office announced the establishment of an Elections Security Rapid Response Team. This "Cyber SWAT Team" includes staff with expertise from State Police, NYS Department of Homeland Security and Emergency Services (DHSES), Department of Financial Services (DFS), and other agencies, to work closely with local boards of election to supplement and provide additional support to the work of the NYSBOE Secure Election Center ahead of the 2020 election cycle. This unit will work hand-in-hand as part of the SEC in responding quickly and decisively to cybersecurity incidents, natural disasters, or other threats with potential impact on elections. As part of the Elections Security Rapid Response Team activity over the past three years, NYSBOE has led daily pre-election operation center statewide calls with relevant federal and State agencies leading up to each election. These calls have facilitated coordinated response to cybersecurity threats, health threats, flooding, active shooter, and other incidents that may have otherwise threatened to impact the security of elections.

Further, recognizing that even if all necessary safeguards are in place that a cyber attack can still occur, the proposed additional measures to protect the public's trust in election outcomes. Relevant state agencies will work with NYSBOE and CBOEs to establish, in advance of the 2020 elections, a comprehensive plan that is ready to be executed immediately if a cyber attack should jeopardize the timely and accurate counting and reporting of all eligible ballots. This will ensure that a comprehensive plan is in place in advance of the election for a fast and responsive approach to ensure the public has full trust in the election outcome, even if a cyber attack should occur. Key to this is a plan to conduct a quick and efficient recount, if necessary, that provides the public with confidence that even in the face of a cyber attack, that the proper procedures are in place to accurately certify the election outcome.

Table-Top Exercises

With the help of previous cybersecurity designated funding, NYSBOE conducted a series of regional tabletop exercises in conjunction with our Federal and State partners, including the US Department of Homeland Security, the NYS Department of Homeland Security & Emergency Services, and County Boards of Elections, to discuss hypothetical cyber events that may impact a Board's ability to administer an election. These exercises are used to identify additional mitigation strategies, preparedness needs and enhance collaboration between stakeholders. NYSBOE also participated in three national tabletops (2018, 2019 Tabletop the Vote), and in the 2020 DHS tabletop for State Election Officials. With this additional funding, NYSBOE has outlined a plan for an additional two-year series of these exercises. The first round will be comprised of six (6) geographically disparate exercises conducted throughout New York State in July 2020, in order to provide rigorous elections incident response training and exercise for all counties in advance of the 2020 General Election.