A new Part 6220 is added to read as follows:

PART 6220- Cyber Security Requirements for Boards of Elections

6220.1 Definitions

(a) “**Authentication**” Means the process or action of verifying the identity of a user, process or device.

(b) “**Board of Elections**” or “**County Board**” Means each County Board of Elections.

(c) “**Cloud Service**” Means a wide range of services delivered on-demand over the Internet. These services are designed to provide affordable and easy access to applications and resources.

(d) “**Complex Password Management Policy**” Means a password policy on any information system that supports Election Data and is capable of complying with guidelines set forth in National Institute of Standards and Technology (NIST) Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management.

(e) “**Cyber Incident Reporting Procedure**” Means the process created by the State Board of Elections to be followed by both the County Board and/or the State Board of Elections when reporting a cyber security incident.

(f) “**Cyber Security Incident**” Means any imminent or successful act to gain unauthorized access to, or create disruption resulting in the misuse of, any information system that processes election data or any non-public information by the Boards of Elections.

(g) “**Data Assets**” Means the data that an organization collects, manages, produces, modifies or stores either electronically or physically. This can refer to any application output file, document, database information, web page code, etc.

(h) “**Domain-based Messaging, Authentication, Reporting & Conformance (DMARC)**” Means an email authentication, policy, and reporting protocol that can improve email protection by monitoring email messages to help mitigate risk to the organization.

(i) “**Domain Naming System (DNS)**” Means a hierarchical and decentralized system for computers, services, or other resources connected to the Internet or a private network that translates a name to an Internet Protocol address.

(j) “**Election Data**” Means all data contained on servers, workstations and devices, other than voting systems, used for the administration of elections, including but not limited to:

(1) voter registration data;
(2) election management data;
(3) poll site data;
(4) ballot access data;
(5) electronic transmission of absentee ballot data; and
(5) public-facing website data.

(k) **“Baseline Image”** Means an organization’s standard set of necessary, trusted applications, including operating system with up-to-date patch levels, installed for the set of systems for which it is designed.

(l) “**Information System**” Means integrated components that collect, store and process data which are used to provide information, or perform tasks.

(m) “**Intrusion Detection System (IDS) or Intrusion Prevention System (IPS)**” Means a device that monitors a network for malicious activity or security policy violations and, in the case of an Intrusion Prevention System, blocks such activity.

(n) “**Managed Services Provider**” Means a vendor providing outsourced administration, maintenance, security, operations, and/or support of information technology operations and assets. The relationship is often managed with performance and service metrics outlined in a service level agreement.

(o) “**Penetration Test**” Means an authorized simulated cyber attack on a computer system or network, performed to evaluate the security of the system or network. A penetration test can help determine whether a system is vulnerable to attack, if the controls in place are sufficient, and which controls (if any) the test bypassed. Penetration test reports may also assess potential impacts to the organization and suggest countermeasures to reduce risk.

(p) “**Phishing**” Means a fraudulent attempt to obtain sensitive information or data such as usernames, passwords and credit card details, or install malicious software, by disguising oneself as a trustworthy entity in an electronic communication.

(q) “**Risk Remediation Plan**” Means the process of developing an approach and actions to reduce the likelihood of an adverse event from occurring due to an exploit of a vulnerability by a threat actor.

(r) “**State Board of Elections**” or “**State Board**” Means the New York State Board of Elections.

(s) “**Secure Elections Center**” Means the State Board of Elections organizational unit that offers services to Boards of Elections that help assess, manage, and reduce risk to the administration of elections.

(t) “**Secure System Development Life Cycle (SSDLC)**”Means a process for defining security requirements and tasks that must be considered and addressed within every system, project or application throughout every phase (from design through disposal).

(u) “**Server Message Block (SMB) Protocol**” Means a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network.

(v) “**Transport Layer Security (TLS)**” Means a cryptographic protocol designed to provide secure communication over a computer network.

(w) “**The Principle of Least Privilege**” Means any user, program, or process shall have only the bare minimum privileges necessary to perform its function.

(x) “**Validated**” Means a particular hardware, software, network appliance, or service is still supported by the manufacturer or vendor.

(y) “**Virtual Local Area Network (VLAN)”** Means a broadcast domain that is partitioned and isolated in a computer.

(z) “**Vulnerability Scan**” Means the process of discovering, and the inspection of, a network and networked systems to identify potential weaknesses which could be exploited.

(aa) **"Authenticated vulnerability scanning"** Means the process of performing a Vulnerability Scan using credentials. Authenticated vulnerability scans obtain vulnerability information on protected devices to obtain detailed and accurate information about the operating system, installed software, including configuration issues and missing security patches.

6220.2 Cyber Security Program

(a) Each Board of Elections shall establish a cyber security program that includes all of the elements required under section 6220.3 of this part to ensure the protection and safety of all systems and machines that access, store, process, and transmit election data, other than voting systems which already have security protocols pursuant to section 6210.11 of this part.

(b) Each Board of Elections shall certify compliance of its cyber security program to the State Board of Elections annually but no later than August 1st in any given year.

(c) Such certification shall include a statement stating that it has successfully established each element outlined in section 6220.3 of this part, or, in the alternative, submit a plan for compliance to the State Board of Elections that includes a target completion date for any outstanding elements.

(d) Each Board of Elections must designate two, bi-partisan Elections System Security Officers (ESSOs) to the Secure Elections Center in a letter to the Co-Executive Directors of the State Board of Elections signed by both County Commissioners, who are:

(1) responsible for the establishment of the cyber security program.

(2) designated as the points of contact with regard to the board of elections cyber security program, and in addition but not limited to, emergency response, incident communications, and recovery of election operations.

(e) Each Board of Elections must have an agreement in place with its Information Technology Director, the head of the county Information Technology Department or a contracted Managed Services Provider to facilitate implementation of this cyber regulation.

6220.3 Cyber Security Program Requirements

(a) A cyber security program shall have the following elements:

(1) Data Classification

(i) Each Board of Elections shall conduct a data classification exercise to: identify Board of Elections data assets and information systems; determine the criticality of data assets and information systems; determine the order and scope of data assets required to be backed up based on the criticality derived from the data classification exercise; and determine the priority to restore data based on the criticality derived from the data classification exercise.

(ii) Each Board of Elections shall conduct such data classification exercise for each new information system that creates, modifies, stores, or transmits election data.

(iii) The data classification exercise must be initiated in the first year of this regulation and must be completed no later than August 1st prior to the general election each year; however, if a new information system is created subsequent to August 1st, but prior to election day, a new data classification exercise must be conducted as soon as practicable.

(2) Asset Inventory

(i) Each Board of Elections shall maintain an asset inventory of all devices and software that access, store, process, and transmit election data. At a minimum, the Board shall review said inventory for accuracy on a monthly basis.

(ii) At a minimum, the inventory shall include: network address(es), machine name(s), purpose of each device, whether the device is portable, and an asset owner responsible for each device. Mobile devices that handle election data must be included whether or not they connect to the Board of Elections network.

(iii) Each Board of Elections shall deploy a network-based asset discovery tool to build an initial asset inventory of Board of Elections systems, both hardware and software. The network-based asset discovery tool must be run on a monthly basis to discover new assets on the Board of Elections network segment and update the asset inventory. Any non-approved or unknown devices or software should be documented, investigated, and removed.

(3) Patch Management

(i) Each Board of Elections shall ensure all information systems and electronic equipment, other than voting systems, that access, store, process, and transmit election data are up-to-date through the use of a monthly patching program. This includes every network-connected device, including but not limited to desktops, laptops, tablets, servers, virtual machines, network equipment (routers, switches, firewalls, wireless access points, etc.), mobile devices, printers, storage area networks, and Voice Over-IP telephones.

(ii) Each Board of Elections shall implement automated patch management and software update tools for operating systems and applications identified in the asset inventory.

(iii) Any software products that cannot be automatically patched should be reviewed on a monthly basis and updated manually.

(iv) Each Board of Elections shall implement an evaluation process for available patches and accelerate its deployment where they are critical in nature.

(v) When checking for updates, the version should be validated to ensure it is still supported by the vendor. If not, the technology must be updated following vendor best practices. Any technology that cannot be updated or patched must be documented and communicated to the State Board of Elections when certifying the cyber security program.

(vi) No system that requires State Board certification or approval for use, such as voting systems, shall be updated without express written approval of the State Board.

(4) Vulnerability scanning

(i) Each Board of Elections shall run vulnerability scans and, where practicable, authenticated vulnerability scanning tools, against all information systems and electronic equipment that accesses, stores, processes, and transmits election data on the network. At a minimum, such vulnerability scanning tools shall comply with the following:

(1) the scanning interval must occur on a continuous basis, but not less than a bi-weekly basis.

(2) reports must deliver a prioritized list based on criticality.

(3) the scans must assess code-based vulnerabilities, configuration-based vulnerabilities, and web application vulnerabilities.

(4) The network border must undergo a vulnerability scan on at least a bi-weekly basis.

(ii) Each Board of Elections shall undergo an annual penetration test of its network(s) to identify vulnerabilities in the environment. Verified vulnerabilities must be added to existing Remediation Plans.

(5) Backups of Election Data

(i) At a minimum, to ensure recovery of information systems and data, Boards of Elections shall, at weekly intervals, perform a full backup Election Data.

(ii) Each Board of Elections shall store at least one full backup, rotated weekly, at an off-site location. This backup shall be stored securely and offline (not connected to a network).

(iii) Each Board of Elections utilize a separate service account for backups that is prevented from interactive logon of workstations and servers.

(iv) Each Board of Elections shall attest to the proper configuration of backup accounts and services in its annual compliance certification to the State Board pursuant to section 6220.2(b) of this regulation.

(6) Restoration of Data

(i) Each Board of Elections shall test, at least once ninety days prior to each primary and general election, the restoration of critical data and information systems from its backup and verify that the restored data and information systems are useful, accessible, and fully functional to meet operational requirements.

(ii) Each Board of Elections shall attest to completion of the restoration tests in its annual compliance certification to the State Board pursuant to section 6220.2(b) of this regulation.

(iii) If such tests are unsuccessful, results shall be reported to the Secure Elections Center no later than two weeks from the date of the test.

(7) Network Segmentation

(i) Each Board of Elections shall establish its own network segment(s), segregating data communications from other interconnected networks, by establishing separate Virtual Local Area Networks (VLANs) and, if feasible, physical network segmentation.

(ii) Each Board of Elections network traffic must be restricted following the principle of least privilege (e.g. network traffic shall be restricted solely for legitimate election administration purposes) implemented through access control lists and updated documentation must be maintained.

(iii) Each Board of Elections shall only allow elections-related VLANs to communicate with information systems unrelated to elections on an as-needed basis.

(iv) Any communications to information systems unrelated to elections must be documented and submitted annually when certifying the cyber security program pursuant to section 6220.2(b) of this regulation.

(v) Other network traffic, such as wireless communications or public terminals, shall be segmented or explicitly denied.

(vi) Security features on any network appliance, cloud service, or security software that blocks or prevents malware and malicious network traffic shall be enabled.

(vii) Each Board of Elections shall use dedicated servers or electronic devices for elections-related tasks, such as but not limited to voter registration, election management systems, and election night reporting.

(viii) For dedicated servers or electronic devices for elections-related tasks, only software necessary and relevant to carry out said tasks shall be installed.

(ix) Dedicated servers or specialized electronic devices for elections-related tasks, such as poll pads, shall not be used for general purpose computing, such as word processing or browsing the internet.

(x) Technical controls shall be implemented to prevent internet browsing from dedicated servers or specialized electronic devices intended for elections-related tasks.

(xi) Each Board of Elections shall use secure protocols for all remote connections on the Board of Elections network segment(s).

(xii) Each Board of Elections shall use encryption to protect elections data both in transit and at rest where practicable.

(xiii) Each Board of Elections shall disable Server Message Block (SMB) Protocol version 1 communications on the Board of Elections network segment.

(xiv) Each Board of Elections shall disable all Server Message Block (SMB) Protocol communications at the private/public network boundary.

(xv) Each Board of Elections shall disable macros, programs common in office documents, on Board of Elections workstations unless there is an explicit need.

(xvi) Any macros enabled on a Board of Elections workstation must be documented and submitted annually when certifying the cyber security program pursuant to section 6220.2(b) of this regulation.

(xvii) Any Windows system that supports PowerShell must be updated to a current supported version and must enable module, script block, and transcript logging or have PowerShell disabled from running.

(xviii) Each Board of Elections must compare their expected network traffic with the rules from their network boundary firewalls to ensure that the rules are acting as intended and align with industry best practices on an annual basis.

(xix) Each Board of Elections must establish and document the configuration of a “Baseline Image” for user workstations and dedicated servers on their network(s), including but not limited to: voter registration systems, desktops, and laptops. The documentation should be updated, along with the image, on regular intervals but no less than quarterly. Any exceptions to the Baseline Image must be documented and submitted annually when certifying the cyber security program.

(8) Remote Access

(i) Each Board of Elections shall follow best practices for remote access to its network segment(s), which shall include, but is not limited to:

(1) the use of bi-directional authentication to establish trust between the sender and receiver.

(2) the use of secure protocols for all remote connections to the systems and applications of the board of elections network segment, such as transport layer security (TLS) or Internet protocol security (IPSEC).

(9) Logging

(i) Each Board of Elections shall enable, retain, and secure logs from network devices and network-connected servers, desktops, and laptops that access, store, modify, and transmit election data.

(ii) Such log data must be forwarded to a centralized log management server that is separated from the current network for retention of a minimum of ninety-two days.

(10) Incident Response

(i) Each Board of Elections shall ensure that a written incident response plan is maintained and designed to promptly respond to any cyber security incident materially affecting the confidentiality, integrity or availability of the Board's information systems or the continuing functionality of any aspect of the Board's operations.

(ii) At a minimum, the incident response plan must address: the internal processes for responding to a cyber security incident; the goals of the incident response plan; the definition of clear roles, responsibilities and levels of decision-making authority; and external and internal communications and information sharing.

(iii) Each Board of Elections shall update its incident response contacts list and shall notify the State Board upon any changes and, at a minimum, shall submit a copy of the incident response contact list to the State Board bi-annually, but no later than ninety days prior to the primary and general election.

(iv) Each Board of Elections shall must report to the State Board of Elections, through the cyber incident reporting procedure, all cyber security incidents or any disruptions which impact or have the potential to impact election operations. Cyber security incidents includes, but is not limited to: (I) any unauthorized entry or attempt to gain unauthorized access to storage facilities, polling sites, early vote centers, and/or offices of the county Board of Elections (regardless of whether on private or public property that is used by the county Board of Elections); (II) incidences of phishing, including spear-phishing, which seemingly target the county Board of Elections; (III) attempts to access, alter, or destroy the county Board of Elections critical information systems or public-facing websites; (IV) attempts to hack, phish, or compromise professional e-mail accounts and the county Board of Elections social media accounts; (V) attempts to interfere with votes sent through the U.S. Postal Service; or (VI) instances of any unexplained disruption at a polling place or training locations for Election Inspectors and other poll workers, including early voting locations, which block or inhibit voter participation. Disruptions may include social media posts or robocalls or texts reporting closed or changed polling places, or physical incidents at polling places, including distribution of false information; disinformation efforts to alter voter participation (including via US postal mail, social media, or other electronic or physical Means); impacts to critical infrastructure that limit access to polling places or information from elections officials, such as power, natural gas, water, internet, telephone (including cellular), and transportation (including traffic controls and roads) outages.

(v) Each Board of Elections shall allow on-site visits for incident handling and response by the State Board of Elections and its employees and/or designees.

(11) Continuity of Operations

(i) Each Board of Elections shall create or update and maintain a continuity of operations plan to recover from incidents and ensures that the Board of Elections is able to perform essential functions under a broad range of circumstances

(ii) The continuity of operations plan must address recovery, contingency processes, communication plans, and processes for operational data availability.

(iii) Each Board of Elections shall submit a copy of the continuity of operations plan to the State Board annually pursuant to section 6220.2(b) of this regulation.

(12) Credential Management and Access

(i) Each Board of Elections shall ensure that a Complex Password Management Policy is implemented on all information technology systems and assets in use by the Board and, at minimum, all passwords shall be changed on a regular basis but no less than annually.

(ii) Passwords or Pass Phrases must be at least fourteen characters in length, must support special characters, and must be changed at least once every year. When passwords are used as part of multi-factor authentication, a minimum of eight characters in length shall be used. Information systems that do not support these password settings must be documented and submitted annually when certifying the cyber security program pursuant to section 6220.2(b) of this regulation.

(iii) Default passwords must be changed and may not be used on any device or software for elections-related tasks.

(iv) Access to Board of Elections systems and devices must utilize unique and individually accountable credentials. Use of logins such as anonymous, guest, etc. or sharing of credentials among multiple users is not allowed. Information systems that do not support the use of unique credentials must be documented and submitted annually when certifying the cyber security program pursuant to section 6220.2(b) of this regulation.

(v) Each Board of Elections shall review all users who have data entry access or change privileges, based on the principle of least privilege, and shall review such access whenever an employee's status changes and users who are no longer employed by the Board of Elections shall have their accounts disabled.

(vi) Each Board of Elections shall conduct periodic reviews of all user accounts who have access to Board of Elections information systems at least annually.

(13) Multi-factor Authentication

(i) Each Board of Elections shall implement multi-factor authentication for administrative access to information systems that store, process, and grant access to election data, including domain administrative access. Multi-factor authentication may be employed through a variety of methods, including smart cards, certificates, one-time password (OTP) tokens, biometrics, or similar authentication methods.

(ii) Each Board of Elections shall implement multi-factor authentication on remote access to county Board of Elections assets.

(iii) Each Board of Elections shall implement multi-factor authentication for all user accounts that have access to election data or systems that create, modify, transmit, or store election data.

(iv) Any information system that manages election data in the aforementioned manner and does not support multi-factor authentication shall be documented and reported when certifying the cyber security program.

(14) Email and Web Protections

(i) Each Board of Elections shall ensure all incoming emails are scanned for malicious attachments and links prior to delivery and shall quarantine emails as necessary.

(ii) Each Board of Elections shall implement transport layer security (TLS) to secure web and email communications and ensure any certificates used do not expire.

(iii) Each Board of Elections shall implement a mechanism, through an automated service, to protect Domain Naming System (DNS) queries from connecting to malicious domains.

(iv) Each Board of Elections shall implement a web application firewall to protect its web applications and web sites from malicious traffic.

(v) Each Board of Elections shall utilize .GOV domains for email communications and web traffic to the extent practicable.

(vi) Starting no later than August 1, 2024, the Board of Elections shall implement domain-based message authentication, reporting, and conformance (DMARC) for email.

(15) Third Party Risk Management

(i) Each Board of Elections shall address technology procurement risk through an appropriate risk assessment prior to the adoption of new technologies or managed services.

(ii) Each Board of Elections shall follow a Secure System Development Life Cycle in the development of all Board of Elections applications and systems, including applications and systems developed for the Board by outside entities.

(16) Continuous Monitoring and Reporting

(i) In order to maintain awareness of elections assets and any malicious activity, the Board of Elections shall maintain an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) on network-connected election systems.

(ii) Each Board of Elections shall maintain up-to-date contacts for alerts generated by such system.

(17) Removable Media

(i) Any information system which utilizes removable media and handles Election Data, shall sanitize, scan for viruses and malware, encrypt, and physically secure the device pursuant to guidance provided by the State Board.

(ii) Any information system that does not have a documented business requirement for using removable media shall have its ability to access removable media disabled.

(18) Security Awareness Training

(i) All employees of a Board of Elections that access and use any Board of Elections systems, including but not limited to email and voter registration systems, shall successfully complete a cyber security awareness training program and must attest to successful completion annually.

(ii) Each Board of Elections shall conduct a phishing assessment of employees of the Board of Elections at least once annually and shall report the results to the State Board of Elections.

(iii) Each Board of Elections shall participate in tabletop exercises hosted by the State Board of Elections, including Commissioners, Deputy Commissioners, and significant staff as selected by Commissioners of Boards of Elections.

(19) Elections Infrastructure Information Sharing and Analysis Center

(i) Each Board of Elections shall be responsible for acquiring and maintaining membership in the Center for Internet Security's Elections Infrastructure Information Sharing and Analysis Center ("EI-ISAC").