ELECTION CENTER

21946 Royal Montreal Drive, Suite 100, Katy, TX 77450 281-396-4309

Elections Security Checklist

Identify and Assess Critical Election Systems	
1.) Have you defined your inventory of critical election systems? *(for example, the Voter Registration Database; Websites like your Voter Data Lookup Tool; Election Tally System; Voting Machines, etc.)*	❑ YES ❑ NO
2.) For each system, do you regularly assess the value of the information contained within, the necessity of perfect functioning of the system, and potential risks to it?	❑ YES ❑ NO
3.) For each system, are you actively cataloging it and building/improving defenses to protect it?	❑ YES ❑ NO
4.) For each system, have you developed a plan to recover should disaster strike?	❑ YES ❑ NO
For each system identified, engage in the following critical analysis to assess the relative risks, defenses, and recovery plans you have in place.	
I. Risk Assessment **(Complete a Risk Assessment for every system)**	
A. Physical Security Risk	
1.) Have you developed a worst case scenario for potential damage if an unauthorized person enters your election headquarters?	❑ YES ❑ NO
2.) Have you developed a worst case scenario for potential damage if an unauthorized person enters your election warehouse?	❑ YES ❑ NO
3.) Have you developed a worst case scenario for potential damage if an unauthorized person enters your server room or data center?	❑ YES ❑ NO
4.) Have you examined your physical access authorization policy in the last three months?	❑ YES ❑ NO
5.) Do you perform scheduled audits of authorized personnel prior to each election?	❑ YES ❑ NO
6.) Do you reexamine your physical access policies on any regular schedule?	❑ YES ❑ NO

A. Physical Security Risk (con't)	
7.) Have you ever conducted a test to see if your facilities can be entered by unauthorized personnel?	❑ YES ❑ NO
8.) Do you have policies and procedures in place for intrusion incident response?	❑ YES ❑ NO
9.) Do you have surveillance cameras in place at key facilities?	❑ YES ❑ NO
10.) Do you have a system in place that automatically identifies suspicious behavior as seen on the surveillance system and creates a management alert?	❑ YES ❑ NO
11.) Do you regularly review your video if there is not a system to automatically identify suspicious behavior?	❑ YES ❑ NO
B. Network Security Risks	
1.) Do you have a complete map of your network and all its interconnections, both within your organization and with outside entities?	❑ YES ❑ NO
2.) Do your vendors and partners have a strong commitment to network security?	❑ YES ❑ NO
3.) Have you reviewed your vendors and partners' written plans and checkpoints that demonstrate implementation?"	❑ YES ❑ NO
4.) Do you have a map of the data elements that pass between each application system on your network and with outside entities?	❑ YES ❑ NO
5.) Are all of your network connections to outside entities secured by a Virtual Private Network (VPN) or something comparable?	❑ YES ❑ NO
6.) Is there any group or department within your organization whose mission is to monitor network security?	❑ YES ❑ NO
7.) Have you developed a worst case scenario for potential damage if an unauthorized person gains access to any part of your network?	❑ YES ❑ NO
8.) Do you have anti-virus software installed to detect "Advanced Persistent Threats"?	❑ YES ❑ NO
9.) Does any outside entity, such as a statewide voter registration system, have the ability to alter or delete data from any of your internal systems?	❑ YES ❑ NO
10.) Do you regularly conduct vulnerability and intrusion testing on your network?	❑ YES ❑ NO

C. Software Applications Security Risks *(Note: Systems may have numerous applications that touch them. For example, a voter registration system may be composed of a voter database application, and also connected e-poll book software application, and connected statewide voter database application. Running the application level analysis on each of the program level applications will give you your best sense of your security and preparedness.)*	
1.) Application (insert name) Security Risks (repeat a, b, c and d questions for every security risk application)	
a.) Information at Risk	
1.) Does your application house any information not subject to public disclosure? *(for example, any personally identifiable information (PII) such as SSN, Driver's license, date of birth, etc.)*	❑ YES ❑ NO
2.) Do you employ encryption standards for all data - specifically personal identifiable Information?	❑ YES ❑ NO
3.) Does this application share, transmit, or receive information with any other application or system?	❑ YES ❑ NO
4.) Does this application house any data that affects election results?	❑ YES ❑ NO
5.) Does this application have any type of network or internal system connection with any application that affects election results?	❑ YES ❑ NO
6.) Does this application house any data that is essential to the running of an election, and without which the election would either be impossible to administer or whose results might be questioned?	❑ YES ❑ NO
b.) Acceptable Use Policy	
1.) Do you have a written policy for this application describing who may use it and under what circumstances?	❑ YES ❑ NO
2.) Do you have an enforcement mechanism and management review process in place to ensure compliance with any such policy?	❑ YES ❑ NO
3.) Is your acceptable use policy implemented in software in such a manner that your systems enforce the policy?	❑ YES ❑ NO
c.) Worst Case Scenarios	
1.) If this application or its database were completely destroyed or disabled at a critical time, could you still conduct your election?	❑ YES ❑ NO

c.) Worst Case Scenarios (con't)	
2.) Even if you could conduct the election, would public confidence in the results be maintained? *(for example, a hacker had cancelled a large number of voter registrations for one competing party)*.	❑ YES ❑ NO
3.) Could you still ensure that no voters would be disenfranchised as a result of the application problem? *(for example, excessively long lines, or unavailable registration information, or for some other reasons)*.	❑ YES ❑ NO
II. Defense Layers	
A. Physical Defenses	
1.) Is physical access to your site restricted to authorized users?	❑ YES ❑ NO
2.) Is there site security staff at the location(s) where your system is located?	❑ YES ❑ NO
3.) Is there a log of the identities and access times of individuals physically accessing your site?	❑ YES ❑ NO
4.) Is your site security staff present at times when staff are not present?	❑ YES ❑ NO
5.) Are all entrances (including windows, etc.) secured by alarms and/or security cameras?	❑ YES ❑ NO
6.) Does your management regularly review physical security records such as logs, video footage, alarm notifications, etc.?	❑ YES ❑ NO
7.) Is the data center where your computer servers are located physically protected in the event of fire, terror attacks or flooding?	❑ YES ❑ NO
8.) Do you have a backup site available if any of your facilities become suddenly inoperable during a critical period?	❑ YES ❑ NO
9.) Have you determined how long it will take to get the backup site functioning? (including the determination of any loss of data).	❑ YES ❑ NO
10.) If any of your computer systems are housed in a vendor-supported data center, has that vendor supplied you with a detailed description of their physical security, fire protection, backup and recovery procedures?	❑ YES ❑ NO
11.) Are your temporary workers required to wear ID badges or other identification so that unauthorized persons in your facilities can be quickly spotted?	❑ YES ❑ NO

B. Network Defenses	
1.) Is there an "air gap" between the Internet and your election tally system *(i.e. is your tally system physically disconnected from the Internet)*?	❑ YES ❑ NO
2.) Do you employ encryption standards for all data - specifically personal identifiable Information?	❑ YES ❑ NO
3.) Are your public-facing voter systems, e.g. a "check my registration" application, built using copies of critical information rather than being directly connected to critical information databases?	❑ YES ❑ NO
4.) Do you review your network activity logs daily?	❑ YES ❑ NO
5.) Do you review your logs at least once a week?	❑ YES ❑ NO
6.) Do you have any User & Entity Behavior Analytics (UEBA) software running on any of your critical infrastructure that can alert you to suspicious network activity?	❑ YES ❑ NO
7.) Do you conduct any periodic vulnerability, intrusion and penetration testing on your networks?	❑ YES ❑ NO
8.) Do you create and store daily application system back-ups?	❑ YES ❑ NO
9.) Do you transfer data to or from the isolated network using a specified USB device that is used only for that purpose and verified to be clean?	❑ YES ❑ NO
10.) Do you have a network access control system that controls user access permission levels? *(e.g. Microsoft Active Directory)*	❑ YES ❑ NO
11.) Do you control access to any of your systems by outside organizations or individuals by using Virtual Private Networks (VPNs)?	❑ YES ❑ NO
12.) Is your network password-protected?	❑ YES ❑ NO
13.) Do you provide administrative passwords only to employees with a clearly defined "need to know/edit" status?	❑ YES ❑ NO
14.) Do you change critical system passwords regularly *(recommendation every 90 days)*?	❑ YES ❑ NO
15.) Do you ensure that servers, PCs and laptops are encrypted or updated with the most current security patches?	❑ YES ❑ NO
16.) Do you ensure the organization has the most current versions of virus protection software?	❑ YES ❑ NO

C. Software Applications Defenses	
1.) Application (insert name) Defenses **(repeat a., b., c., d questions for every software defense application)**	
a.) Data Protections	
1.) Are only authorized personnel granted access to the software?	❑ YES ❑ NO
2.) Is this application set up with different, unique passwords for each user?	❑ YES ❑ NO
3.) Is this application set up with different passwords for different elections?	❑ YES ❑ NO
4.) Is this application set up with robust passwords *(passwords include special characters and caps-best practices recommends changing passwords every 90 days)*?	❑ YES ❑ NO
5.) Is this application set up with tokens or other special access rights?	❑ YES ❑ NO
b.) Software level application level protections	
1.) Is the software platform protected by a firewall?	❑ YES ❑ NO
2.) Is the software platform isolated in the network environment?	❑ YES ❑ NO
c.) Software Logs	
1.) Does the software log the user name, time, date, and type of modification?	❑ YES ❑ NO
2.) Does the software log multiple log-in attempts, increased data traffic, and/or volume of data transmitted?	❑ YES ❑ NO
d.) User & Entity Behavior Analytics (EUBA)	
1.) Do you have baseline measurements for “normal” activity patterns within this application and an alert system that identifies abnormal activity patterns?	❑ YES ❑ NO
III. System Disaster Recovery	
A. Physical Disaster Recovery	
1.) Is there backup for the loss of hardware *(networks, servers, computers and laptops, wireless devices)*?	❑ YES ❑ NO
2.) Is hardware available at an alternate facility that can be configured to run similar hardware and software applications when needed?	❑ YES ❑ NO
3.) Is there backup for the loss of impounded voting equipment?	❑ YES ❑ NO

A. Physical Disaster Recovery (con't)	
4.) Is there a contingency for natural disasters or homeland security breach for data contained at data center?	❑ YES ❑ NO
5.) Are there plans for relocating Receiving Stations (where poll workers return election night supplies) in the event of a natural disaster or homeland security breach?	❑ YES ❑ NO
6.) Is there backup for the loss of data from election equipment damage?	❑ YES ❑ NO
7.) Is there access to network infrastructure hardware that could replace failed components?	❑ YES ❑ NO
8.) Is there ready access to your alternative physical locations?	❑ YES ❑ NO
9.) Is there a timeframe in place for the alternative facility to be functioning?	❑ YES ❑ NO
B. Network Disaster Recovery	
1.) Is there a plan for providing automatic redirects for interfaced systems should you need to move your system to a new network location?	❑ YES ❑ NO
2.) Is there access to network infrastructure hardware that could replace failed components?	❑ YES ❑ NO
3.) For the backup hardware and networking plan, is there necessary staff available during critical periods?	❑ YES ❑ NO
C. Software Applications Disaster Recovery	
1.) Application (insert name) Disaster Recovery **(repeat a., b., c., d questions for each software disaster application)**	
a.) Damage Assessment	
1.) Are vendors on standby for critical periods to assist with Assessment and Disaster Recovery?	❑ YES ❑ NO
2.) Are you able to run a hash comparison with the recovery (i.e. back-up) copy of your software application?	❑ YES ❑ NO
b.) Data Restore	
1.) Are your backup disks or file locations readily accessible?	❑ YES ❑ NO
2.) Are your backup files saved in an off-site location?	❑ YES ❑ NO
3.) If you have a parallel application running, is it up to date?	❑ YES ❑ NO

c.) Application Restore	
1.) Do you have necessary staff or vendor resources available to assist with the installation of the application in a mirrored physical and OS environment?	❑ YES ❑ NO
d.) Business Restore	
1.) Are you prepared to cut over to alternative applications that can manage limited business critical functions? *(For example, if your Voter Registration System crashes, can you quickly utilize your web based voter search application so that you can direct voters to their polling place on Election Day?)*	❑ YES ❑ NO
2.) Are there paper alternatives to allow you to continue with on-going critical processes while technical systems are diagnosed and brought back? *(For instance, do your voting machines create countable paper trails viewable by each voter?)*	❑ YES ❑ NO
3.) Can you quickly create paper voter lists in the event e-poll books go down?	❑ YES ❑ NO
The Election Center would like to acknowledge and thank the committee that worked on the initial draft of this checklist: Noah Praetz, Cook Co. IL; Dean Logan, Los Angeles Co. CA; Jennifer Morrell, Arapahoe Co. CO; Janice Case, King County, WA; Eric Fey, St. Louis Co. MO; Brian Corley, Pasco Co, FL and Ryan Macias, U.S. EAC	