ELECTION SECURITY PLANNER

IT Pre-Questionnaire

To make the most of the Election Security Planner, users should gather key details about their current IT environment in advance. This questionnaire mirrors the questions you'll encounter while using the tool, helping you prepare effectively. We recommend discussing these topics with your technology support team beforehand to ensure a smooth and informed planning experience.

☐ Yes ☐ No **Does your office or county have a way to prevent a user from accessing a suspicious/ harmful website?**

Protective DNS. This service filters internet requests to prevent connections to harmful web domains, limiting infections (e.g., malware, ransomware, phishing, other cyber threats) by acting as a security checkpoint for the internet's address book.

☐ Yes ☐ No **Do you and your staff take regularly scheduled (monthly, quarterly, or annually (minimum) cybersecurity training?**

Staff Training & Awareness. Teach staff best practices essential to security, including spotting phishing, using secure passwords, and avoiding risky behavior.

☐ Yes ☐ No **Does your office and/or county participate in unannounced phishing assessments?**

Phishing Campaign Assessments. This security test sends simulated phishing emails to employees to evaluate how likely they are to fall for real phishing attacks. The goal is to identify vulnerabilities in user behavior, raise awareness, and improve an organization’s ability to detect and respond to phishing threats.

☐ Yes ☐ No **When accessing a local resource (computer, laptop, iPad, etc.), do you login with a password and a second type of verification like a code received via text, a code generated by an app or the use of a special physical security key?**

Multifactor Authentication (MFA). This security product/practice requires users to verify their identity through multiple methods during log-in, such as a password and a temporary code from your phone or an app.

☐ Yes ☐ No **Do you have a security system in place beyond typical antivirus software that constantly monitors computers and other devices for suspicious activity and that can react quickly in the event of a cyberattack or similar event?**

Endpoint Detection and Response (EDR). This cybersecurity product continuously monitors devices, such as computers, phones, and servers, to detect, investigate, and respond to suspicious activity or threats.

☐ Yes ☐ No **Does your office proactively check for weaknesses or potential security problems in computer systems and software?**

Vulnerability Scanning & Management. This cybersecurity product continuously evaluates an organization's public-facing systems, including computer systems, networks, websites, and/or software, to identify weak spots that hackers could potentially exploit.

☐ Yes ☐ No **When important files are backed up, does your office have a copy stored somewhere completely separate from your computers and the internet – like on an external hard drive that's not plugged in?**

Also, is that backup protected with a password so no one else can read it if they found it?

Encrypted & Offline Data Backups. This practice keeps secure copies of important files/data protected and disconnected from the internet so malicious actors/software cannot access them.

☐ Yes ☐ No **Does your office ensure that the latest security updates and fixes are regularly applied to all of your computers, network devices, and other systems such as SmartTV's, security systems, and telephones?**

Regular Software & Patch Management. This practice keeps programs and systems up to date by installing the latest updates and security fixes on network devices and computers as well as phones, smart TVs, smart security systems (e.g., security cameras, doorbells, thermostats), etc.

☐ Yes ☐ No **Does your office have a way to monitor activity and system changes across all devices (computers, servers) to detect suspicious behavior?**

Centralized Log Management. This product is used to collect and store logs (records of system activity) from computers, servers, and devices in one place for more efficient searches and problem or attack detection.

☐ Yes ☐ No **Does your office have a system in place, like a Security Information & Event Management System (SIEM), that collects and analyzes data from your computers and networks, and alerts you when you have a possible security threat?**

Security Information & Event Management System (SIEM). This product collects and analyzes security data to search for, detect, and alert on threats or suspicious activity.

☐ Yes ☐ No **Does your office ensure the network and systems are constantly monitored for issues, even outside of normal business hours, so everything is always running smoothly?**

24/7 Network Monitoring. This product continuously monitors computer networks to quickly spot and fix problems or security threats.

☐ Yes ☐ No **Is your network divided into different sections, so that if one part gets infected with a virus or hacked, it doesn't spread to the entire network?**

Network Segmentation. This practice divides a computer network into smaller segments to improve security and performance. It creates "walls" to contain any attacks to isolated sections and protect the overall integrity of the network.

☐ Yes ☐ No **Does your office have a system in place that monitors network traffic and alerts you to potential security threats such as unauthorized access or malware?**

Intrusion Detection & Protection Systems/Albert Sensors. This security tool monitors network or computer activity to detect suspicious behavior or potential cyberattacks and provide alerts when something unusual or unauthorized happens.

☐ Yes ☐ No **Does your office periodically engage a third party to conduct an external security assessment, where they attempt to identify vulnerabilities in your systems from the outside like a hacker would?**

Remote Penetration Testing (RPT). Ethical hackers conduct an assessment by attempting to break into a network or systems from a remote location just as real hackers would.

☐ Yes ☐ No **Does your office conduct evaluations to determine how well prepared your office is to prevent, detect and recover from a ransomware attack?**

Ransomware Readiness Assessment. This review of an organization's ability to prevent, detect, respond to, and recover from a ransomware attack helps identify weaknesses and recommends improvements to reduce the risk and impact of such attacks.

☐ Yes ☐ No **Does your office use a service that provides information or warnings about emerging cybersecurity threats so that the office can proactively defend against potential attacks?**

Threat Intelligence Services. This product can help an organization understand the threat landscape by providing actionable information about evolving or emerging cyber threats. It is information that has been collected, processed, and analyzed to understand a threat actor's motives, tactics, and behaviors.

☐ Yes ☐ No **Does your organization have a security strategy where trust is never assumed, and access is always verified, even for someone inside the network?**

Zero Trust Architecture. This is a security model that assumes no one—inside or outside the network—should be trusted automatically. It means "never trust, always verify." Every user and device must prove they are safe before getting access.