Protecting Voter Information and Our Democracy

Executive Summary

It's a pivotal moment in US history. We're coming together on long-overdue reforms amid a deadly pandemic, while restarting our economy. It's also an election year, and soon we'll decide our nation's leaders.

Democracy depends on fair and legitimate elections, so it's essential to secure the systems that make it work. In most states, the voter registration database (VRDB) is key. It holds vital information on millions of Americans, and it integrates with several other systems both in and out of the state's network.

It's also an attractive target. In 2016, foreign adversaries launched cyberattacks that compromised VRDBs in some states and accessed voter records. These attacks are almost certain to continue and worsen this year. We simply can't afford to let them succeed and undermine our democracy.

Recently the MITRE Corporation developed a set of recommendations to defend voter registration systems.

These five recommendations are extremely important and reinforced by cybersecurity best practices. However, they cover more than just five things, and the report is almost thirty pages. It's a lot to take in.

This paper simplifies MITRE's report. We summarize their recommendations without the extensive detail, and we offer starting points for each recommendation. Furthermore, we prescribe specific solutions that let you take action now.

Contents

Defend voter registration systems with these recommendations from MITRE.

1. Secure external communications
2. Strengthen external and internal network defenses
3. Enhance access management
4. Improve system management and monitoring
5. Facilitate recovery and ensure continuity of operations

Election Security Recommendations

Consistency in the Inconsistent

"If you've seen one election system, you've seen one election system."

For the past several years, Cisco Talos has been investigating election security by talking to the very people who run the systems. We're not sure who deserves credit for the above quote, but Talos heard the same theme over and over: States runs their own election infrastructure individually, and there are no national standards. That's why election systems' design and security differ greatly from state to state. And unfortunately, inconsistency breeds security risk.

A constant in all of this? Complexity.
Election infrastructure has many components, and typically includes the Voter Registration Database (VRDB), Election Night Reporting (ENR) systems, electronic pollbooks, voting machines, ballot counting machines, and integrations with other systems both inside and outside the state's network. Mail-in voting will probably expand, due to the pandemic, requiring even more systems to support it. Layer complexity atop inconsistency, and it can seem almost impossible to make simple yet impactful security recommendations that make a difference.

Talos believes that election security cannot be solved just by looking at individual components, and that's certainly true. An architectural approach is ideal. At the same time, you must break big problems down into manageable parts and prioritize action to make progress.

MITRE's Recommended Security Controls for Voter Registration report takes that approach, and focuses on the VRDB first. It's sound advice and we agree with it.

Voter Registration Systems in the Spotlight

The VRDB is at the center of nearly every state's election system. It holds important information on voters, and shares this data with state motor vehicle departments, federal agencies, and other third-party organizations. Defending VRDBs means more than database security: you must also secure its internal and external connections too.

> "Voter registration databases are of particular interest to sophisticated adversaries"
>
> -MITRE

MITRE's report explains why they're important to secure first: "Voter registration databases are of particular interest to sophisticated adversaries," they write, "and even attacks that do not change any information can be used to undermine confidence in U.S. institutions and the perceived legitimacy of election outcomes."

Recommended Security Controls

MITRE didn't try to boil the ocean. Instead, they focused on what's common among voter registration systems and the protections that matter most.

Here's a summary of their recommended controls:

1. **Secure external communications** with authentication, encryption and monitoring of all network traffic
2. **Strengthen external and internal network defenses** using segmentation, intrusion detection and content filtering
3. **Enhance access management** with multifactor authentication and role-based access control
4. **Improve system management and monitoring** with asset visibility, logging, and endpoint security
5. **Facilitate recovery and ensure continuity of operations** with recovery plans, system backups, and failover methodology

In the next section, we'll provide more insight into MITRE's recommendations. We'll offer a prioritized action plan: the most important actions you can take right now. After that, we'll show you how our integrated security platform and comprehensive portfolio enables a more holistic approach to election security over time.

Getting Started with MITRE's Recommended Controls

Let's take a closer look at MITRE's five recommendations, each of which have several subcomponents. We'll cut to the most important things to know, and we'll align their recommendations with the NIST Cybersecurity Framework (CSF) and CIS Controls cybersecurity best practices.

Unlike MITRE, though, we'll offer a prioritized action plan and specific solutions to get started right now.

1 Secure External Communications

To do this, MITRE recommends the following: "Evaluate, protect, and authenticate communications with the external systems that share and validate voter information to ensure that connections are secure and do not offer a point of entry for external attack."

A Closer Look

Voter registration databases integrate with many systems outside the core election infrastructure, like the motor vehicle authority mentioned above, bureau of vital statistics, and others on the same state's network. Furthermore, they integrate with federal agencies like the Social Security Administration, and other non-governmental organizations like the Electronic Registration Information Center (ERIC).

Attackers often start by breaching external network connections first, then pivoting into the state's network. That's the reason why MITRE opened their recommendations with this topic, breaking it down into four parts:

- **Patterns of Communication.** Network visibility is key, but it's often difficult to attain. MITRE explains that you must understand how systems communicate with the VRDB and exchange data with it before putting any other security controls in place. Otherwise you could miss something important or, worse, you could break something.
- **Protecting Connections.** Encrypting network communication helps protect the privacy and integrity of data in transit. MITRE recommends strong, end-to-end encryption between applications, bolstered by network-layer encryption that VPNs provide. They also recommend enforcing your encryption policy so that it's not just enabled and bypassed.
- **Authenticating Endpoints.** Both sides of an integration should prove they are who they claim to be. "Encryption is only useful between trusted endpoints; without that trust, a malicious host can impersonate a legitimate host," MITRE says. Therefore, they recommend digital certificates to prove identity with a focus on mutual authentication for machine-to-machine (M2M) communication.
- **Verifying Data.** Trusted digital signatures are required to verify data after it's been sent and stored, so you can trace where the voter information went. Digital signatures are available through most communication channels, including email, and in standard databases.

First Step: Start with Patterns of Communication

Here's the reason why MITRE lists this first and foremost: You need to know how systems are intended to communicate on the network -- before you can control it. Without that knowledge, you might overlook suspicious activity that leads to a breach, and you risk blocking valid traffic that halts the election system. It's why MITRE began the definition of Secure External Connections with the word "evaluate."

It sounds simple, but the devil is in the details. To get this level of visibility, you must first collect and analyze large volumes of network traffic flow records, but that can easily overwhelm log management products and the people who use them.

More important: many products lack the advanced, built-in analysis that baselines normal network activity and spots anomalies at scale. **You need a better way.**

You need to know how systems are intended to communicate on the network before you can control it.

We recommend Cisco Stealthwatch Cloud.

It's our purpose-built solution that monitors and analyzes network flow records. Stealthwatch Cloud provides essential visibility, advanced detection, and critical alerting. It integrates with other security controls like Cisco ISE that can take immediate, automated corrective action based on your security policy to stop suspicious or unauthorized traffic. And because it's cloud based, you can get started right away with minimal effort.

This recommendation aligns with industry best practices:

CIS Controls	NIST Cybersecurity Framework
Control 12: Boundary Defense	**ID.AM-3:** Organizational communication and data flows are mapped

Once you fully understand network communication patterns, both normal and abnormal, you'll have the information and confidence necessary to add more security controls.

Next Steps

Now that you understand communications patterns using Stealthwatch Cloud, here's how we help you do more:

Protecting Connections. Cisco NGFW and AnyConnect provide highly secure, remote access for authorized external users. And our SD-WAN solution connects authorized users to applications through integrated security, unified communications, and application optimization.

Authenticating Endpoints. Cisco ISE is a key part of our Software-Defined Access and Zero Trust Security solutions. It authenticates and authorizes endpoints, enabling a dynamic and automated approach to access policy enforcement.

Verifying Data. Cisco Registered Envelope Service is our email encryption solution. It secures traditional email tools and is fully integrated into the most common email technologies. It provides two-step verification to ensure that the intended recipient is registered and authenticated before reading the email.

Securing external connections naturally leads to MITRE's next recommendation on strengthening network defenses, so let's proceed.

2 Strengthen External and Internal Network Defenses

MITRE recommends strengthening network defenses like this: "Deploy network segmentation, additional firewall and intrusion detection layers, and email and web content filtering to detect and halt attacks made through network connections."

A Closer Look

As discussed earlier, voter registration systems integrate with many systems both on and off the state's network. And MITRE's first recommendation placed external communications in the spotlight, highlighting the need to understand traffic patterns, authenticate endpoints, encrypt traffic, and digitally sign data transfers for traceability. Now the focus is on additional security layers that focus on threat detection and response.

MITRE breaks this recommendation down into five parts:

Network Segmentation and Isolation. If a breach occurs, a network divided into smaller subsections can contain the damage. MITRE recommends using a demilitarized zone (DMZ) to isolate the core election infrastructure and segmenting the internal network as well. That way, no one can reach the VRDB directly over the internet, and all internet-facing systems authorized to communicate with it, like a web front end, will not have direct access to it either. Network segmentation dramatically reduces the VRDB's attack surface.

Firewalls. These have been protecting perimeters for a long time, but what's new here is MITRE's focus on application-specific firewalls. For instance, they recommend web application firewalls for online voter registration portals, gateways, and reverse proxies to allow functionality without direct access to the VRDB.

Intrusion Detection Systems. Like firewalls, Intrusion Detection Systems have been around for a long time. They evolved into Intrusion Prevention Systems (IPS) to be more proactive, automatically stopping the threats they detect. No IPS is perfect, though, and a single false positive can block legitimate network traffic. Critical infrastructure operators demand system uptime over everything else, and the same goes for election systems. In fact, DHS reclassified election networks as critical infrastructure shortly after the 2016 election. That's why MITRE emphasizes the importance of "detection" in this context rather than "prevention" to balance better security with all-important system availability. These technologies work together with people, process, and other technologies in the security operations center for careful analysis and human-guided response.

Device Access Control. Unauthorized devices should never appear on an election network, and neither should authorized devices that don't comply with your security policy. Therefore, MITRE recommends an updated inventory of authorized devices, and to verify authorizations against it through digital certificates. MITRE also recommends monitoring devices for behavior changes that could indicate a deviation from security policy, or even a potential intrusion.

Email, Web, and Content Filtering. Officials use their systems for multiple purposes beyond election-related activities, including email and web browsing. Ideally, they'd have dedicated systems on the election network, but that's often impractical. Therefore, MITRE recommends content filtering technologies to prevent attacks from arriving by email or the web.

There is a lot to consider here, each with varying degrees of difficulty. For example, network segmentation is incredibly important, but it's not as simple to do as some of the others. **Where do you start?**

MITRE recommends content filtering technologies to prevent attacks from arriving by email or the web.

First Step: Start with Email, Web, and Content Filtering

Users often get the blame for data breaches, but that's unfair. The fact is: no human being can be completely vigilant against all threats, all the time. It's just not possible. That's why attackers continue to target them first, and the way to reach them is through web and email access.

We need effective security controls that significantly reduce or eliminate the threats from reaching people in the first place. Fortunately, content filtering technologies today are more effective, simple to manage, and easy to deploy. Many are cloud based and don't require you to buy, install, and manage physical appliances. For these reasons and more, we recommend starting with email, web, and content filtering.

We recommend Cisco Umbrella **and** Email Security.

Both are cloud based and, together, they filter web and email content to stop threats from reaching your users.

Cisco Umbrella uses the DNS layer to block malicious and unwanted domains, IP addresses, and cloud applications before a connection is ever established. It also unifies multiple security services in the cloud for sharper visibility and consistent enforcement, and integrates with Cisco SD-WAN.

Email Security helps to stop phishing, malware, ransomware, and spam. It works with Cisco AMP to spot stealthy malware in attachments, and industry-leading URL intelligence combats malicious links. Cisco Email Security also enhances the security of Office 365.

Our approach aligns with industry best practices:

CIS Controls	NIST Cybersecurity Framework
Control 7: Email and Web Browser Protections	**DE.CM-3:** Personnel activity is monitored **DE.CM-4:** Malicious code is detected

Device Access Controls ensure only authorized and trusted devices are on your election network.

Next Steps

Once you've addressed content filtering, here's what to do next:

Network Segmentation and Isolation. Cisco ISE builds scalable, manageable network segmentation directly into the network without the typical configuration complexity. It enables the network to enforce role-based, least privilege access throughout your election infrastructure. Group Based Policy, formerly known as TrustSec, is the software-defined segmentation technology ISE uses to enforce segmentation through security group tags. Furthermore, Cisco Tetration reduces the attack surface through application and workload micro-segmentation.

Firewalls. Cisco NGFW sets the foundation for integrating powerful threat prevention capabilities into your existing network infrastructure, making the network a logical extension of your firewall solution. It enables your DMZ to contain internet-facing services that should not be exposed from the internal network, and it allows only authorized internal devices to reach the internet. NGFW supports Group Based Policy for consistent segmentation policy enforcement with ISE.

Intrusion Detection Systems. Cisco NGIPS provides unparalleled visibility into applications, signs of compromise, host profiles, file trajectory, sandboxing, vulnerability information, and device-level OS visibility. Its threat intelligence is continually updated through new policy rules and signatures received every two hours. And although NGIPS is designed to block detected threats, it also acts as an IDS-focused early-warning system to complement the people and technology in your security operations center.

Device Access Control. Cisco Duo and ISE are critical components of our Zero Trust solution, offering complete visibility and control over all devices on your election network. Together they provide secure network access through multifactor authentication, authorization, and device posture to ensure that only authorized and trusted devices are on your election network.

Device access control is also part of MITRE's access management recommendation, which we'll discuss next.

3 Enhance Access Management

MITRE summarizes access management recommendations like this: “Implement role-based access, multifactor authentication, device access control, and centralized and federated identity management, and perform supply chain risk assessment.”

A Closer Look

Access control is a security fundamental. People and systems need access to function, but too much often leads to security and operational problems. To manage access effectively, though, you need to understand who and what is on your network, what rights they should have, and whether and when to change or revoke access. In large and complicated environments like election systems, access management is certainly no trivial matter.

That’s why MITRE splits access management into four subcomponents:

Role-Based Access. Least privilege is a key cybersecurity concept, meaning that people and devices should receive only the minimum level of access based on the role they perform. Any access beyond that is unnecessary and should be taken away. The Voter Registration Database, for example, requires network connections to other federal and state systems, but it doesn’t need direct internet access to function properly.

Multi-factor Authentication. Password-based authentication was never enough, no matter how strong passwords are or how effectively they’re managed. Beyond “something you know” (like a password or PIN), authentication should depend on “something you have” (like a digital certificate, mobile phone, token) or “something you are” (like your fingerprint or face). That way hackers can’t get in just because they’ve stolen a password.

Centralized and Federated Identity Management. At a basic level, identity management means that you can track authorized individuals, their roles, locations, credentials, access rights, and more. It means revoking access when people leave, or adjusting privileges based on role changes. That’s hard enough. But doing this securely across organizational domains -- say, between the state election network and an external third-party -- gets even more complicated. MITRE recommends both centralized and federated identity management so that you can share identities and manage their access domains.

Supply Chain Risk. Election infrastructure, like all IT-based systems, relies on a vendor ecosystem to make it all work: hardware, software, cloud-based technologies, and professional services. NIST says you must “identify, prioritize and assess suppliers and partners of critical information systems, components and services using a cyber supply chain risk assessment process.” Mitigating supply chain risk is a key reason why the Cisco Trust Center exists: to be confident that we’re a trustworthy, transparent, and accountable technology partner.

First Step: Start with Multi-factor Authentication

Recall that election officials often access voter registration systems from their everyday workstations, the ones they also use for email and web browsing. They already have too many passwords to manage. And attackers have
many ways to steal passwords through email and web vectors. Start with multi-factor authentication because it can render any stolen passwords essentially worthless.

And the good news continues. The right multi-factor authentication technology makes things simpler, just like fingerprint identification and facial recognition technology has made mobile phones faster and easier to use.
It streamlines the login experience without the aggravation or disruption.

Attackers have many ways to steal passwords through email and web vectors.

There's no easier way to adopt multi-factor authentication than Cisco Duo.

Backed by a zero-trust philosophy, Duo protects voter registration systems by using a second source of validation, like a phone or token, to verify user identity before granting access. It verifies identities in seconds, protects any application or device, and is easily deployed in any environment. It ensures device trustworthiness by inspecting security posture; those that fail your security and trust requirements are denied access to protected applications like the VRDB.

This recommendation aligns with industry best practices:

CIS Controls	NIST Cybersecurity Framework
Control 16: Account Monitoring and Control	**PR.AC:** Identity Management and Access Control

Next Steps

Once you've succeeded with Duo, here's how to handle the rest of MITRE's advice:

Role-Based Access. Cisco ISE provides consistent, secure network access through wired, wireless, and VPN connections. It's the centerpiece in zero-trust security for the workplace, providing least-privilege access to users and devices based on their roles. With ISE, you can know who, what, where, and how endpoints and devices are connecting, while looking deep into devices to ensure compliance with your security policy.

Centralized and Federated Identity Management. The Cisco Security Technology Alliance is a security ecosystem that facilitates open, multi vendor product integrations to improve security effectiveness through automation and operational simplicity. We have identity management partners that integrate with Cisco ISE secure network access and Cisco Cloudlock cloud access security broker.

Supply Chain Risk. Make Cisco your trusted partner to minimize supply chain risk. Our Cisco Secure portfolio simplifies security with the broadest, most integrated platform. And the Cisco Trust Center ensures that we're always trustworthy, transparent, and accountable.

Now that you've improved identity and access management, MITRE's next recommendation addresses system management and ongoing monitoring. It aims to prevent risky system misconfigurations, detect suspicious system activity, remediate vulnerabilities, and maintain continuous compliance.

According to MITRE, the small teams that manage voter registration systems can still identify malicious activity through "well-structured monitoring."

4 Improve System Management and Monitoring

MITRE's summary of this recommendation: "Implement logging and vulnerability management to improve visibility. Perform regular audits to ensure validity of the database and compliance to policies and procedures, and to verify and validate file authenticity."

A Closer Look

MITRE reminds us that small teams manage and secure voter registration systems, and they shoulder a heavy burden. Therefore, they need efficient tools for visibility and control, as well as fast detection and response. "Well-structured monitoring can identify malicious activity," they say, and recommend the following:

Logging, Aggregation, and Analysis. As voter registration systems operate, they generate system activity logs over time. These logs are point-in-time records of user logins, configuration changes, system restarts, and other events. However, even just a few system logs per second will easily overwhelm any human being. Security Information and Event Management (SIEM) solutions collect and analyze high volumes of IT activity logs, ideally limiting alerts to real security problems. They must also ensure log integrity; that is, ensuring that all logs that require collection are collected, and haven't been tampered with or modified in transit.

Vulnerability Scanning. No software is perfect. Vulnerabilities found in applications, operating system software, and device firmware will undoubtedly continue. Since voter registration systems typically comprise multiple technologies from multiple vendors, managing their vulnerabilities consistently across a heterogeneous environment is very challenging. That's why MITRE recommends tools to find and fix vulnerabilities before attackers exploit them.

Asset Management. You can't remove unauthorized systems from an election network if you don't know what's authorized. And you can't protect authorized systems unless you know they're there. That's why asset management is so vital: you can't allow rogue devices to affect election infrastructure, and you can't allow critical systems to be susceptible.

Patch Management. Outdated software is often riddled with security problems. After all, most system updates include security patches alongside new features and performance enhancements. Patch management, like vulnerability scanning, requires tools to identify out-of-date systems, validate and evaluate updates, and quickly apply approved patches.

Audits. Voter registration systems should follow compliance standards, but they can drift out of compliance. MITRE recommends auditing database transactions through log analysis and random transaction analysis. They also suggest verifying system security policy and automated file integrity checks to ensure applications and data are authentic.

MITRE emphasizes the importance of protecting privileged endpoints.

Privileged Endpoint Security Services. Some people and systems have elevated privileges, like database administrators and the workstations they use to access the database. Naturally they're the target of attackers. Therefore, MITRE emphasizes the importance of protecting privileged endpoints through anti-malware and host intrusion detection services that run directly on them.

First Step: Start with Privileged Endpoint Security Services

Attackers often target privileged users and systems first, and endpoint protection is a critical last line of defense. If you've started at the top of MITRE's recommendations and followed our prioritized plan, you've already accomplished the following:

1. You've secured external connections with Cisco Stealthwatch Cloud, and now you can spot and stop any threats or suspicious activity originating from third party networks.
2. You've strengthened network defenses with Cisco Umbrella and Email Security, a critical and effective first line of defense against malicious websites, phishing attempts, and other harmful content that arrives through normal web and email usage.
3. You've enhanced access management with Cisco Duo multifactor authentication, so even if attackers manage to get legitimate credentials, they still can't get in.

Now you can improve system management and continuous monitoring by ensuring that your privileged endpoints themselves are protected too. That way, even if threats manage to reach endpoints, host-based security will stop them. To do this, we recommend starting with AMP for Endpoints.

It protects privileged endpoints by blocking malware at the point of entry, provides visibility into file and executable-level activity, and removes malware from PCs, Macs, Linux, and mobile devices. It determines which endpoints have software with a specific Common Vulnerabilities and Exposures (CVE) entries, regardless of when the application last ran. You can then isolate endpoints that have critical vulnerabilities from the network before attackers can exploit them.

AMP's Exploit Prevention capability provides an integral preventative security layer for protecting endpoints, servers, and virtual environments from file-less and memory injection attacks, as well as obfuscated malware. AMP changes the static nature of the defense landscape to a dynamic one, making it more difficult for attackers to plan and execute successful attacks.

Following MITRE's recommendations help reduce the risk of a successful attack.

This recommendation aligns with industry best practices:

CIS Controls	NIST Cybersecurity Framework
Control 8: Malware Defenses	**DE.CM-4:** Malicious code is detected

Next Steps

Once you've secured privileged workstations with AMP for Endpoints, here's what we recommend next:

Logging, Aggregation, and Analysis. Cisco Security Analytics and Logging improves system management and monitoring to improve the accuracy of your policy decisions. It analyzes NGFW events and network telemetry in real time to quickly detect threats and remediate incidents with confidence and at scale. Powered by Stealthwatch Cloud, which we recommended earlier to strengthen external communications, Security Analytics and Logging uses machine learning to analyze massive amounts of network data so you can take action on severe threats immediately.

Vulnerability Scanning. Cisco AMP for Endpoints, Duo, and AnyConnect help control potentially vulnerable, untrusted devices from affecting voter registration systems and networks. Cisco Tetration provides essential visibility into application and workload vulnerabilities. The Cisco Security Technical Alliance program includes vulnerability management vendors that integrate with ISE, Threat Grid, Firepower Management Center, and other Cisco security solutions. Plus our Vulnerability Management services can help you assess and conduct penetration tests to find and correct weaknesses.

Asset Management. Cisco ISE discovers, identifies, and classifies all devices connecting to your network, and shares information with asset management solutions through its Platform Exchange Grid standards-based integrations.

Patch Management. Vulnerability and patch management go hand in hand. We also recommend Cisco Duo and AnyConnect to ensure device trust. They identify devices with out-of-date operating systems or risky applications to prevent them from affecting election networks. After all, healthy devices reduce security risk.

Audits. Cisco Duo, AMP, and AnyConnect help ensure that devices comply with your security policy. Beyond technology, our Strategy, Risk, and Compliance services can assess your security program, manage your risk, simplify your audit profile, and protect data.

By following MITRE's first four recommendations, you'll certainly reduce the risk of a successful attack. Yet the possibility is always there, and the threat landscape changes constantly. That's why MITRE also promotes readiness, so let's discuss that now.

MITRE encourages election officials to apply incident response plans to enhance operational readiness.

5 Facilitate Recovery and Ensure Continuity of Operations

Here's how MITRE summarizes this recommendation: "Perform regular backups, frequent system audits, and institute clear recovery plans to mitigate damage to election systems. Identify and test failover methodology to ensure that operations can continue if a system fails."

Some cybersecurity best practices separate response and recovery concepts. The NIST Cybersecurity Framework, for example, defines Respond as "contain the impact of a potential cybersecurity event" and Recover as "restore any capabilities or services that were impaired due to a cybersecurity event." Logically, you need to "respond" by stopping the attack before you can "recover" by restoring operations. But in this recommendation, MITRE is bundling the two together under Recover. They haven't skipped past incident response. In fact, they praise election officials for understanding the importance of incident response planning.

A Closer Look

MITRE encourages election officials to apply what they know about incident response planning to enhance operational readiness through system backups and failover strategies. Therefore, this recommendation includes:

Recovery Strategy. "It is crucial to have an incident response plan that includes a risk assessment of the architecture," MITRE writes. Therefore, they're recommending a close examination of all critical components as well as training the incident response team well ahead of any cyberattack.

Backups. Ransomware attacks that hold systems hostage remind us that some security problems appear as operational problems, and vice versa. If a system fails and loses important data locally, it's vital to have that data backed up elsewhere. MITRE suggests that backup strategies include policies for data retention, VRDB backup, and transaction logs.

Continuity of Operations. Election systems are critical infrastructure that must maintain availability despite system failures. It almost doesn't matter if the problem was caused by a cyberattack or an operational issue. MITRE recommends planning for failures in advance by minimizing complexity and maintaining hot failover capabilities. They also suggest more frequent VRDB backups as election day draws closer.

First Step: Start with Recovery Strategy

All incident response and recovery plans should include specific actions to ensure system backup and continuity of operations. "When an incident occurs," CIS says in Control 19, "it is too late to develop the right procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover." Therefore, this is the first and most important step.

Cisco can help you develop your incident response plan, recovery strategy, and much more.

Do you already have incident response and recovery plans in place? If not, we recommend Talos Incident Response.

It's a full suite of proactive and reactive services to help you prepare, respond and recover from a breach. With Talos IR, you have direct access to the same threat intelligence available to Cisco and world-class emergency response capabilities – in addition to more than 350 threat researchers for questions and analysis. Let our experts work with you to evaluate existing plans, develop a new plan, and provide rapid assistance when you need it most.

This recommendation aligns with industry best practices:

CIS Controls	NIST Cybersecurity Framework
Control 19: Incident Response and Management	**RS.RP:** Response Planning **RC.RP:** Recovery Planning

Next Steps

Once Cisco Talos has helped you develop your incident response plan and recovery strategy, we can help you do much more:

Emergency Incident Response. When you're actively under attack, you need help right now. With Talos, you gain an "IR on Demand" capability via Cisco WebEx Teams, our live secure collaboration platform.

Tabletop Exercises. Enhance preparedness by practicing for a cyber incident. That way, you can ensure that your IR plan and common threat playbooks are effective and well understood.

Compromise Assessments. Gain a more holistic view of your election infrastructure that doesn't rely on hypothesis or limited scope.

Threat Hunting. Find out if you're already compromised. Our threat hunters dive deep into findings to help you validate and eliminate any threats.

Cyber Range Training. A three-day, immersive workshop targeted at training your defenders in a controlled environment to prepare and respond to the latest attacks using open source and Cisco Security solutions.

Summary

On the surface, MITRE's recommendations seem rather short and simple. However, a closer look reveals the full extent of their advice. **What looks like five things is really twenty-one.** And it's not clear where to start.

This paper is exactly what you need: A short overview of each recommendation, focusing on what to do first, and how to do it quickly and effectively with specific Cisco Security solutions. Our advice is based on cybersecurity best practices and effective defenses that you can deploy right now.

The table below summarizes everything we discussed:

Control	Priority	Detail	Cisco Security
Strengthen external communications	1	**Patterns of communication** Protecting connections Authenticating endpoints Verifying data	**Stealthwatch Cloud/Enterprise** NGFW/AnyConnect Identity Services Engine (ISE) Registered Envelope Service
Strengthen network defenses	1	**Email, web, content filtering** Network segmentation Firewalls Intrusion detection systems Device Access Control	**Email Security/Umbrella/Web** ISE/Group Based Policy/Tetration NGFW NGFW/NGIPS Duo/ISE
Enhance access management	1	**Multifactor Authentication** Role-Based Access Identity Management Supply Chain Risk	**Duo/ISE** ISE/Group Based Policy
Improve system management	1	**Endpoint Security Services** Logging, Aggregation, Analysis Vulnerability Scanning Asset Management Patch Management Audits	**AMP for Endpoints** Security Analytics and Logging Duo/AMP/AnyConnect/Tetration ISE Duo/AMP/AnyConnect Duo/AMP/AnyConnect
Facilitate recovery	1	**Recovery Strategy** Backups Continuity of Operations	**Talos Incident Response**

You can confidently #Protect2020 and beyond with an architectural approach and SecureX.

Learn more today.

- Cisco Security
- Cybersecurity Solutions for Government

2020 and Beyond: An Architectural Approach

Since 2016, Cisco Talos researchers saw improvement in election security, yet they encourage ongoing vigilance and investment. For this year, let's focus first on voter registration systems by heeding MITRE's advice and using the Cisco Security solutions we discussed. You'll make a lot of progress right away.

And let's not stop there. Talos reminds us that election security cannot be solved just by looking at individual components of the system, which is essentially what we've done so far. "While reviewing the security of each of these point systems independently is almost certainly the most effective way to move forward to start," they write, "stepping back and reviewing the system as a functioning whole is also necessary."

They recommend an architectural approach that covers the entire infrastructure. A systemic review examines all technology, processes, and even the people who run the election. The cybersecurity controls must be integrated into the election infrastructure itself, not bolted on later.

At Cisco, we're making it happen. SecureX is our broad, integrated platform that simplifies security, unifies visibility, and enables automation. It's a built-in experience in all Cisco Security products that strengthens your election security program.

SecureX

- Fully integrates all of your solutions, not just ours
- Shares context between tools and teams
- Automates and completes workflows
- Harmonizes policies across the election infrastructure

[i]MITRE's Appendix A also aligns their recommendations with the NIST CSF, and Appendix B with the Belfer Center State and Local Playbook.