Securing Voter Registration Systems

Democracy thrives when there's trust in election results

Election systems are vital. They hold critical voter information and enable the entire process that decides our nation's leaders. Today, ensuring election integrity is more important than ever.

Yet election systems are complex and difficult to secure. Attackers exploit complexity, targeting voter registration databases to disrupt our elections and possibly affect outcomes.

MITRE provides specific guidance to secure voter registration databases, and we can help you take action on their advice today.

> "The voter registration database is the foundation of almost every state election system in the United States.
>
> It's a center-piece of our discussions with election officials and a key target for our adversaries.
>
> MITRE's controls are well-aligned with Talos' own analysis and recommendations for defending these vital systems."
>
> Matt Olney, Director of Talos Threat Intelligence

Why Cisco Security is the right choice

Get the right solutions to act on MITRE's recommendations

Benefit from security that's surprisingly simple and highly effective

Act now and defer payments until 2021

Start here

MITRE recommends:	Where to start:
Secure external communications with authentication, encryption and monitoring of all network traffic	**Cisco Stealthwatch Cloud** monitors and analyzes network traffic to spot suspicious patterns
Strengthen network defenses using segmentation, intrusion detection and content filtering	**Cisco Umbrella and Email Security** filters web and email traffic to stop threats from reaching your users
Enhance access management with multifactor authentication and role-based access control	**Cisco Duo** simplifies multifactor authentication while ensuring device trust
Improve system management and monitoring with asset visibility, logging, and endpoint security	**Cisco AMP for Endpoints** monitors high-risk endpoints for malware threats and vulnerabilities
Facilitate recovery and uptime with recovery plans, system backups, and failover methodology	**Cisco Talos Incident Response** proactive and reactive services help you prepare, respond, and recover

Recommended Control 1:

Secure external connections

MITRE recommends understanding normal communication patterns between registration databases and external systems like the state's motor vehicle authority. It establishes baselines that help you spot abnormal activity often associated with cyber threats.

Enter Stealthwatch Cloud. It combines network telemetry with industry-leading machine learning and behavioral modeling to detect advanced threats and respond to them quickly. It spots threats in encrypted traffic too, without any decryption. Stealthwatch Cloud is a Software-as-a-Service solution delivered from the cloud that can monitor your internal election network.

It is easy to try, easy to buy, and simple to operate and maintain.

Recommended Control 2:

Strengthen network defenses

MITRE discusses how officials use their workstations for a variety of activities beyond election-specific purposes like email and web browsing, adding to the cyber risks. It's not always practical to have separate systems. That's why they recommend email and web content filtering for those workstations.

Cisco Umbrella and Email Security do precisely that. Umbrella uses the DNS layer to block malicious and unwanted domains, IP addresses, and cloud applications before a connection is ever established. Email Security stops phishing, business email compromise, ransomware, and spam while enhancing Office 365 email security. And because they're cloud-delivered, implementation is practically effortless.

Recommended Control 3:

Enhance access management

MITRE reminds us what we all know about passwords: Strong ones are necessary, but complex password requirements have been detrimental to security overall. That's why they recommend multifactor authentication: Something you have, like a phone, in addition to something you know.

There's no easier way to use multi-factor authentication than Cisco Duo. It's the cloud-based, user-friendly, scalable way to enhance access management through multifactor authentication.

With Duo, you can:

- Verify identity in seconds
- Protect any application on any device
- Easily deploy in any environment

You can also defer 95% of payments until after the election

Alleviate the financial burden

- Tax revenue and collections have been dramatically impacted by the pandemic, causing state budget crises across the nation.

Cisco Capital® is ready to help

- Our 2020 Business Resiliency Program enables you to secure voter registration databases now with Cisco Security solutions, while managing short-term cash flow and liquidity concerns.

This too shall pass

- But through it all, you can still bolster election security without the financial strain.

Recommended Control 4:

Improve system management

What's the highest value target for attackers? MITRE says they're systems with privileged access, like administrator workstations and servers that manage other components. These systems "represent a high risk to the entire system if not monitored properly for threats," so MITRE recommends endpoint security services to protect them from compromise.

Cisco AMP for Endpoints is the perfect solution. It protects important systems through continuous monitoring of malicious behavior, rapid malware detection, and removal across your election networks.

With AMP for Endpoints, you can:

- Block malware at the point of entry
- Gain visibility into file and executable-level activity
- Remove malware from PCs, Macs, Linux, and mobile devices.

Recommended Control 5:

Facilitate recovery and availability

MITRE highlights clear recovery plans to mitigate any threats that have impacted election systems.

Cisco Talos Incident Response Services will help you strengthen your readiness and response to attacks. Our full suite of proactive and reactive incident response services help you prepare, respond, and recover from a breach. With Talos IR, you have direct access to the same threat intelligence available to Cisco.

Let our experts work with you to evaluate existing plans, develop a new plan, and provide rapid assistance when you need it most.

> "As election officials work to improve their defenses against attacks, they should also prepare to deal with any failures that do arise."
>
> **MITRE**

And once we get through this together, we can do much more

Get security that works together

- SecureX is our broad, integrated security platform that unifies visibility, enables automation, and strengthens your security across network, endpoint, cloud, and applications.
- It's a built-in experience for all Cisco Security products that connects with your entire security infrastructure.
- And because it's already built in, there's nothing more to buy: SecureX is available to all Cisco Security customers.

Act on every MITRE recommendation with Cisco Security

Recommended Control	Detailed Control	Cisco Security
Strengthen External Communications	Patterns of communication Protecting connections Authenticating endpoints Verifying data	Stealthwatch Cloud/Enterprise NGFW/AnyConnect Identity Services Engine (ISE) Registered Envelope Service
Strengthen Network Defenses	Network segmentation Firewalls Intrusion Detection Systems Device Access Control Email, Web, Content Filtering	ISE/Group Based Policy NGFW IDS Duo/ISE Umbrella/Web/Email Security
Enhance Access Management	Role-Based Access Multifactor Authentication Identity Management Supply Chain Risk	Duo/ISE Duo/ISE
Improve System Management	Logging, Aggregation, Analysis Vulnerability Scanning Asset Management Patch Management Audits Endpoint Security Services	Security Analytics and Logging Duo/AMP/AnyConnect ISE Duo/AMP/AnyConnect Duo/AMP/AnyConnect Advanced Malware Protection (AMP)
Facilitate Recovery	Recovery Strategy Backups Continuity of Operations	Talos Incident Response Service

#Protect2020 with Cisco Security