State of New Mexico

Cybersecurity Plan

Continuous Security Posture

Federal Guidance & Directives

Binding Operational Directives (BOD)

cyber.dhs.gov

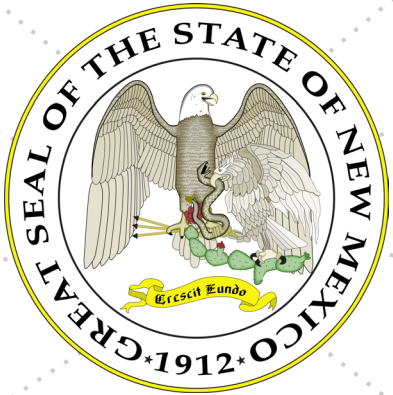
- **The White House Cybersecurity Executive Order Section 6:**
  Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents
- **The White House Cybersecurity Executive Order Section 7:**
  Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks
- **CISA Cross-Sector Cybersecurity Performance Goals (CPG)**
  Prioritized IT & OT Cybersecurity Practices With Known Risk-Reduction Value (38 Controls: Accounts, Devices, Data, Governance & Training, Vulnerability Management, Supply Chain / 3rd Party, Response & Recovery, Network, Threat and Email) + Focus on Metrics & Improving Maturity
- **BOD 23–01 | Improving Asset Visibility and Vulnerability Detection on Federal Networks**
  Asset Discovery Every 7 Days + Maintain Updated Inventory + Initiate Authenticated Vulnerability Scanning Every 14 Days + Update Scanners Every 24 Hours + Include Mobile Devices & Devices Outside Network + Ad Hoc Scanning Capabilities
- **BOD 22–01 | Reducing the Significant Risk of Known Exploited Vulnerabilities**
  Created Known Exploitable Vulnerabilities (KEV) + Establish Vulnerability Remediation Process + Roles & Responsibilities + Define Action & Tracking Plans + Continuous Reporting
  CISA KEV Catalog + CSW Enhanced KEV Tracker
- **BOD 19–02 | Vulnerability Remediation Requirements - Internet-Accessible Systems**
  Ensure Access & Verify Scope + Remediate Critical (15 Days) & High (30 Days) Vulnerabilities
- **BOD 18–02 | Securing High Value Assets**
  Identify Points of Contact for High Valued Assets (HVAs)
- **BOD 16–02 | Threat to Network Infrastructure Devices**
  Threats Targeting Data, Applications, Services & Multimedia + Create Action Plan

State announces major investments in Cybersecurity

- In September 2022, through an executive order the Governor established a Cybersecurity Planning Committee.
- The committee represents cyber and IT leaders from across the state of New Mexico.
  - The committee's primary objective is to develop a statewide cybersecurity plan.
- On January 10, received the first of a multi-year federal grant award for $2,540,403 from the U.S. Department of Homeland Security and a state match of $282,267 for a project total of $2,822,670.
  - Over the next four years the state will receive additional funding totaling nearly $13 million.
- The initial funding will be leveraged to stand up a holistic cybersecurity program to meet the mandatory requirements for the statewide cybersecurity plan.
  - Objectives of the program is to establish appropriate risk-based processes, services and make them available to various stakeholders to address cyber risk on how to identify, protect, detect, respond, and recover our information technology eco-systems.

Key Initiatives – State of New Mexico Executive Agencies

1. Deployed vulnerability management program to nearly all state agencies
2. Met PCI compliance across all agencies
3. Onboarded agencies into attack surface management platform
4. Expanded agency scanning coverage utilizing authenticated scanning
5. Implemented a security operations center
6. Completed a statewide risk assessment
7. Executed a statewide initiative for penetration testing
8. Increased windows patching for agencies assessed during penetration testing



CISA CPG

CISA Cybersecurity Performance Goals

Account Security (7)	Device Security (5)	Data Security (4)	Governance & Training (5)
Vulnerability Management (6)	Supply Chain / Third Party (3)	Response & Recovery (4)	Network Segmentation + Vulnerability Intel + Email Security (3)

8 Categories & 37 Goals

Account Security	Device Security	Data Security	Governance & Training	Vulnerability Management	Supply Chain / Third Party	Response & Recovery	Other
1.1 Detection of Unsuccessful (Automated) Login Attempts	2.1 Hardware and Software Approval Process	3.1 Log Collection	4.1 Organizational Cybersecurity Leadership	5.1 Mitigating Known Vulnerabilities	6.1 Vendor/Supplier Cybersecurity Requirements	7.1 Incident Reporting	8.1 Network Segmentation
1.2 Changing Default Passwords	2.2 Disable Macros by Default	3.2 Secure Log Storage	4.2 OT Cybersecurity Leadership	5.2 Vulnerability Disclosure / Reporting	6.2 Supply Chain Incident Reporting	7.2 Incident Response (IR) Plans	8.2 Detecting Relevant Threats and TTPs
1.3 Multi-Factor Authentication (MFA)	2.3 Asset Inventory	3.3 Strong and Agile Encryption	4.3 Basic Cybersecurity Training	5.3 Deploy Security.txt Files	6.3 Supply Chain Vulnerability Disclosure	7.3 System Back Ups	8.3 Email Security
1.4 Minimum Password Strength	2.4 Prohibit Connection of Unauthorized Devices	3.4 Secure Sensitive Data	4.4 OT Cybersecurity Training	5.4 No Exploitable Services on the Internet		7.4 Document Network Topology	
1.5 Separating User and Privileged Accounts	2.5 Document device configurations		4.5 Improving IT and OT Cybersecurity Relationships	5.5 Limit OT Connections to Public Internet			
1.6 Unique Credentials				5.6 Third-party Validation of Cybersecurity Control Effectiveness			
1.7 Revoking Credentials for Departing Employees							

Legend

- Existing State Initiative
- Planned Initiative
- Cybersecurity Plan Overlap*

*Orange outline indicates alignment with the SLCGP Cybersecurity Plan

8 Categories & 37 Goals

What are the benefits to participating agencies?

- Create Community of Excellence for Cybersecurity statewide.
  - Communication, Collaboration,
- Understanding of unique stakeholder needs.
- Statewide cybersecurity services and pricing agreements.
- Tools, systems, services
  - Incident Notification, SOC, etc
- Networking with peers industry.
- To accomplish this we need your input on the survey, through Meet Ups, and ongoing dialog.

Next Steps

- Complete the initial survey which has been sent out already, providing contact for who will respond to the upcoming Capability Assessment.
  - Look for email from
  - Value for initial survey
- Expect Capability Assessment Survey in coming weeks.
- Expect additional Meet Ups in coming months.

Q&A

New Mexico State Local Cybersecurity Grant Program Survey

https://www.doit.nm.gov/programs/cybersecurity/

cybersecurity.planningcommittee@doit.nm.gov