OFFICE OF CYBERSECURITY (OCS)
FY2027

Raja Sambandam, State Chief Information Security Officer
October 23, 2025

New Mexico Legislature
Science, Technology & Telecommunications Committee

AGENDA

August

- FY25 Activities & Achievements

September

- FY26 Plans & Beyond

October

- Funding & Proposals

Threat Landscape

OCS Recurring & Special Funding

Governance Silos

Building Synergies and Sharing Risk

Cybersecurity and AI Convergence

THREAT LANDSCAPE

- Attacks are persistent, coordinated, and increasingly supercharged by artificial intelligence
- Threats, include ransomware, phishing, supply chain attacks, and exploitation of known vulnerabilities
- AI-driven attacks are amplifying the speed, scale, and sophistication of cyber threats, making detection and response more challenging
- Security improvements are ongoing, but gaps persist due to resource and coordination challenges
- Unified, funded and adaptive strategies are critical to ongoing risk reduction and response to emerging threats
- OCS prevents thousands of incidents yearly through its network monitoring, security endpoint monitoring services and cybersecurity awareness training

Slide Pages 4-18 are Confidential and for Closed Session

FUNDING AND SUPPORTING A CYBER-SECURE FUTURE

For FY27 OSC is Requesting Increased Recurring and Special Appropriations to Sustain and Expand Services

OCS OPERATING BUDGET

(in thousands)

Category	FY26	Increase	FY27 Request
PS&EB (200s)	$1,635.0	$765.0 (46%)	$2,400.0
Contractual Services (300s)	$3,572.6	$745.4 (15%)	$4,118.0
Other (400s)	$832.8	$5,367.2 (620%)	$6,000.0
Other Financing Uses (500s)	$482.0	$0	$482.0
Total	**$6,522.4**	**$6,477.6** (100%)	**$13,000.0**

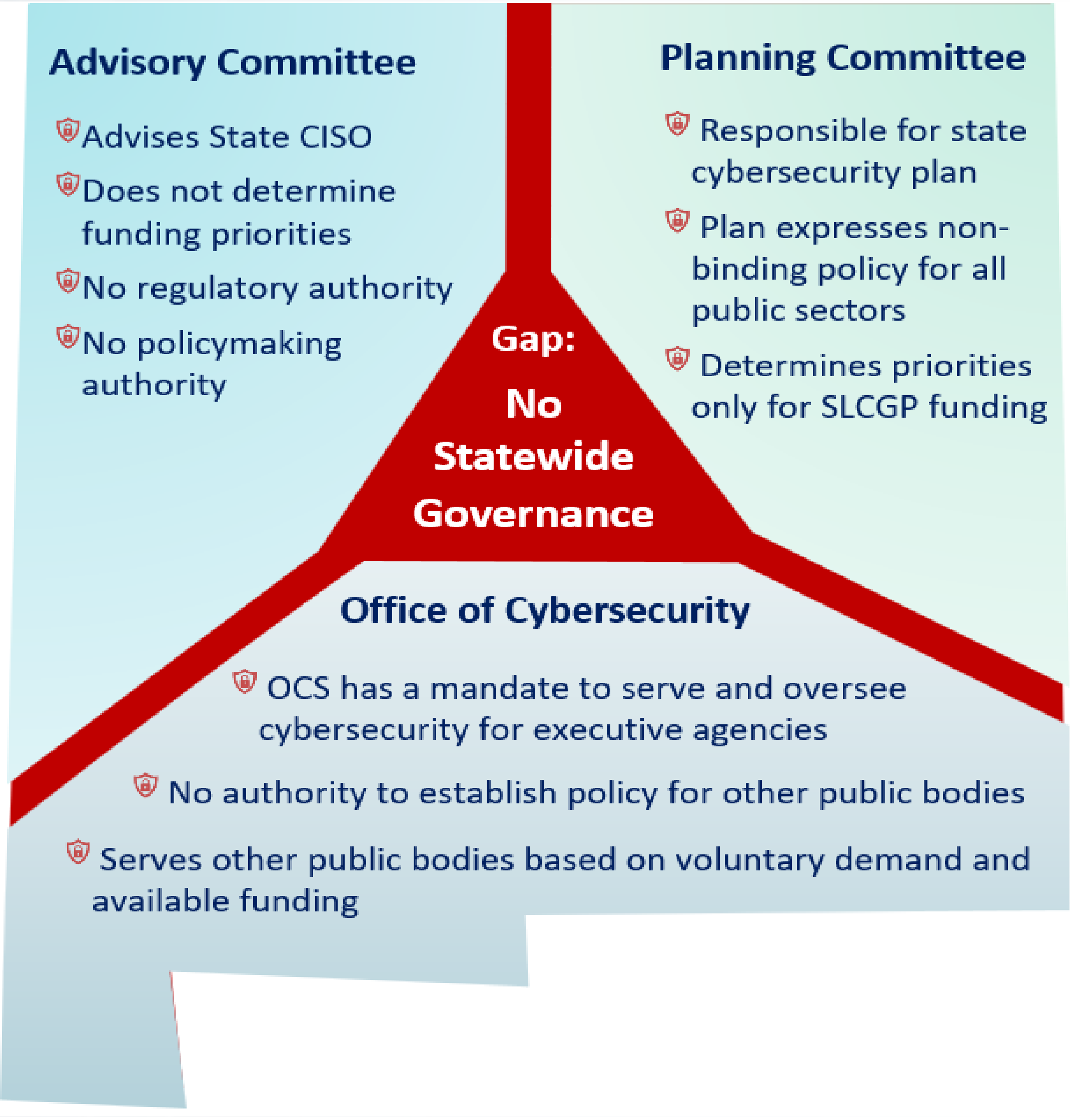
OCS SPECIALS REQUEST

(in thousands)

Total Request $21,000

FY26 Subscribers*	FY26 Services	FY27 Change	Request
State Agencies (76)	VMaaS & Pen Test	No Change	$6,000
K-12 (21)	VMaaS & Pen Test	30% increase subscribers	$7,000
HEI (19)	VMaaS & Pen Test	10% increase asset coverage	$6,000
Counties, Municipalities & Tribal (24)	VMaaS	No Change	$500
Water and Wastewater	Assessment/ASM	Increase # subscribers	$250
Political Subdivisions	Assessment/ASM	Increase # subscribers	$250
Expand and Study Third Party Risk Management (TPRM)	Pilot Program	Increase	$1,000

SILOED GOVERNANCE =
PROTECTION GAPS & COLLATERAL RISK



Advisory Committee

- Advises State CISO
- Does not determine funding priorities
- No regulatory authority
- No policymaking authority

Planning Committee

- Responsible for state cybersecurity plan
- Plan expresses non-binding policy for all public sectors
- Determines priorities only for SLCGP funding

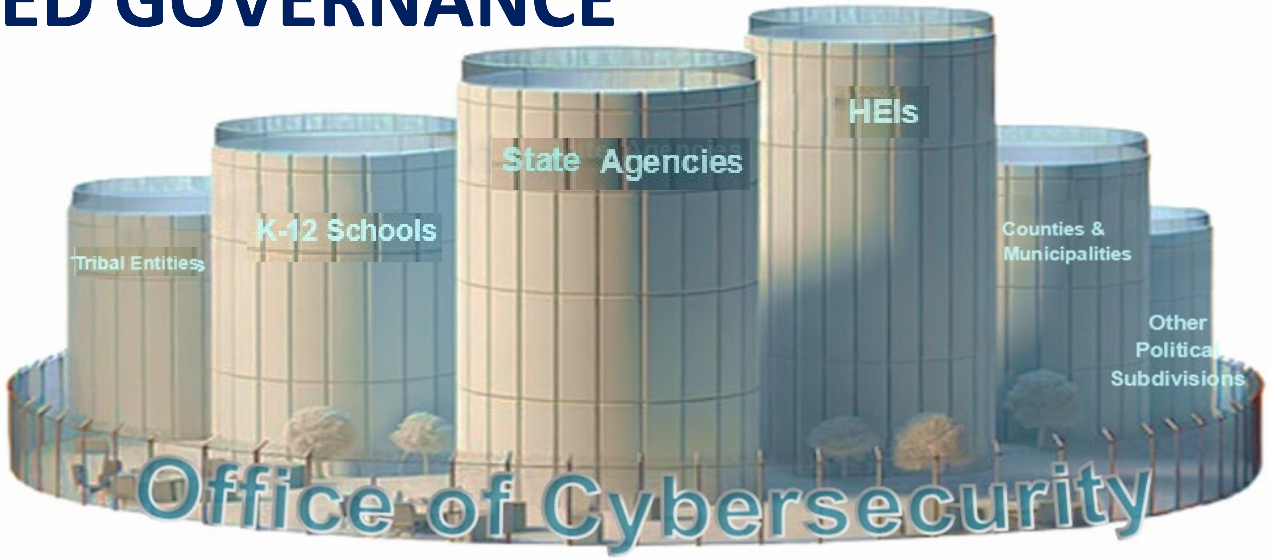
Gap:

No Statewide Governance

Office of Cybersecurity

- OCS has a mandate to serve and oversee cybersecurity for executive agencies
- No authority to establish policy for other public bodies
- Serves other public bodies based on voluntary demand and available funding

CONTAINING COLLATERAL RISK THROUGH UNIFIED GOVERNANCE



…Unified Policies/Standards

- Decrease policy development workload
- Ensure all entities meet NIST policy documentation standards
- Policies drive adoption of entity specific NIST compliant controls

… Unified Cybersecurity Services

- Decrease overall state cyber spend
- Enhance compliance with minimum standards
- Leverage for all entities expertise and resources typically reserved to larger entities
- Provide opportunities for traveling CIO
- Does not intrude on local control – All entities must adopt additional entity-specific controls

… Unified Incident Response and Recovery

- Drives strategic planning
- Promotes public sector control over management, response and information sharing
- Equalizes resources
- Improves response time and decreases insurance red tape

CONTAINING RISK THROUGH A UNIFIED CYBER COMMITTEE

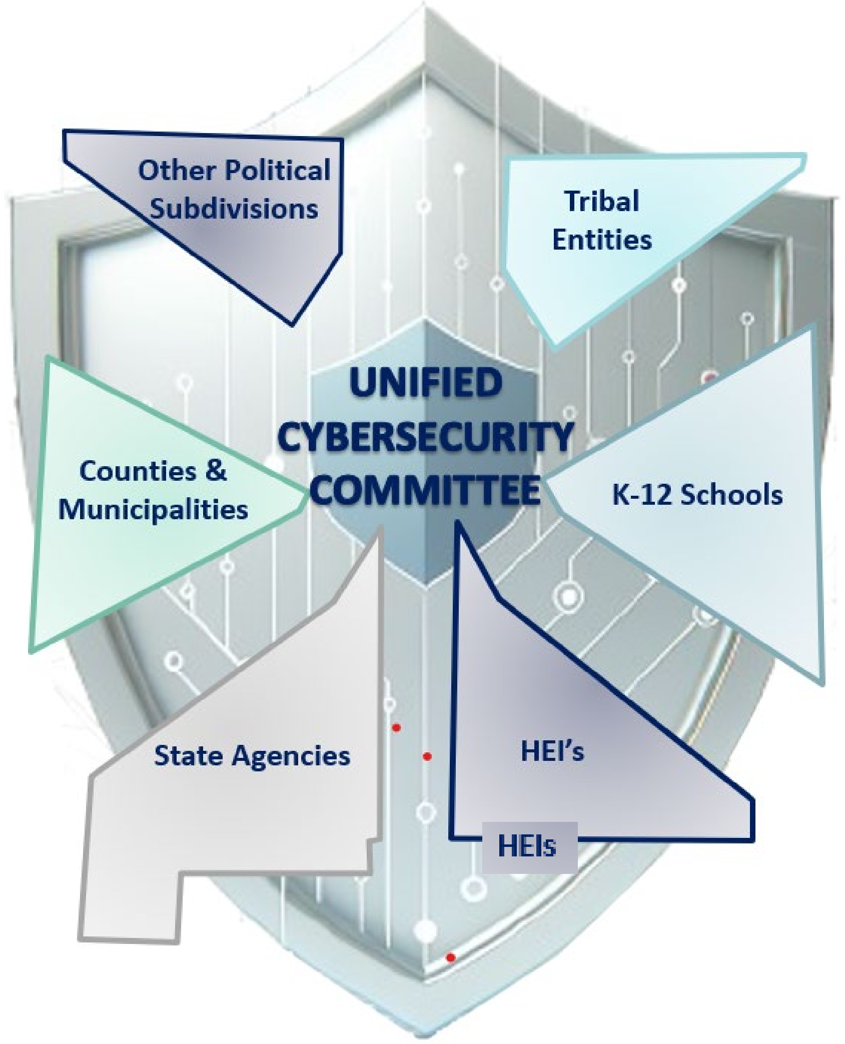
- A unified committee approving statewide projects will build trust and engagement

- There is precedent for a committee to have statewide oversight authority

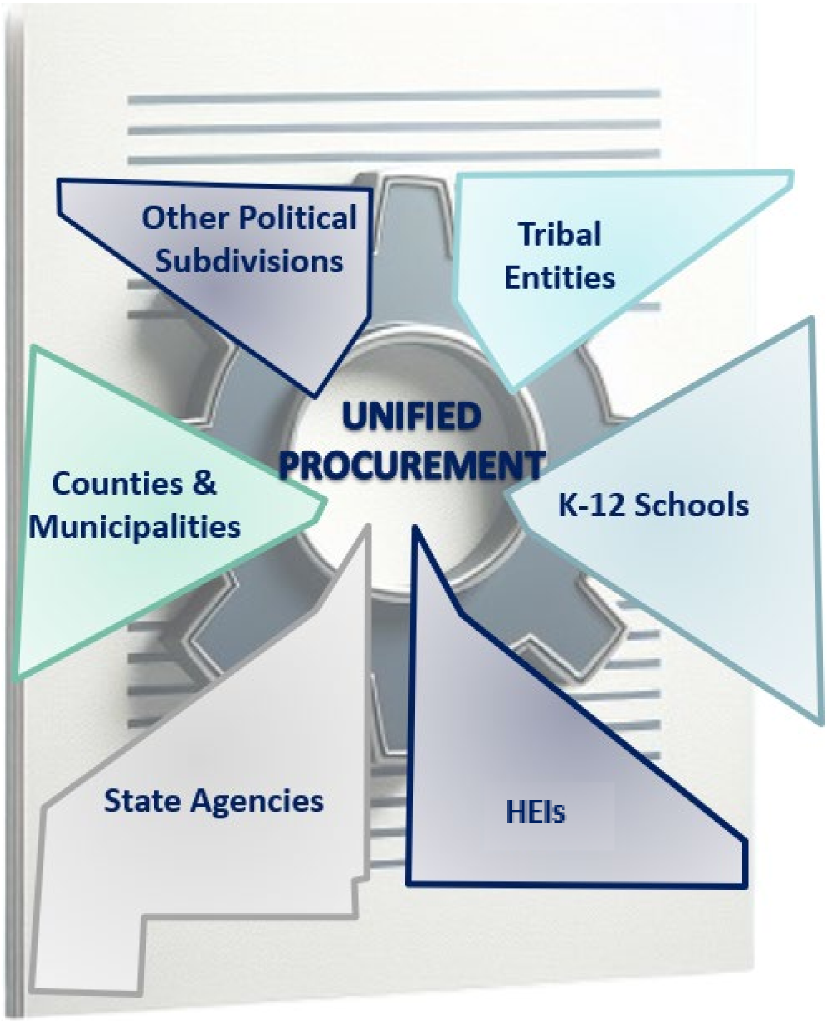
  E.G., the State Ethics Commission

- Proposed 10-year extension of SLCGP justifies unification

- Any "weak link" in a state or local government agency can spread and affect the entire state


Other Political Subdivisions
Tribal Entities
UNIFIED CYBERSECURITY COMMITTEE
Counties & Municipalities
K-12 Schools
State Agencies
HEI's
HEIs

CONTAINING RISK THROUGH UNIFIED CYBER PROCUREMENT



- Public sector does not have access to price agreements to obtain competitively priced, commodity cyber security services, such as VMaas, ASM or Pen Testing

- Procuring cybersecurity services through resellers drives ad hoc solutions

  Ad hoc solutions build silos

  - Prevent central support
  - Increased workforce challenges
  - Drive increased overall cyber spend

- State cybersecurity price agreements would promote:
  - Cost savings
  - Shared support
  - Increased efficiencies
  - More effective solutions

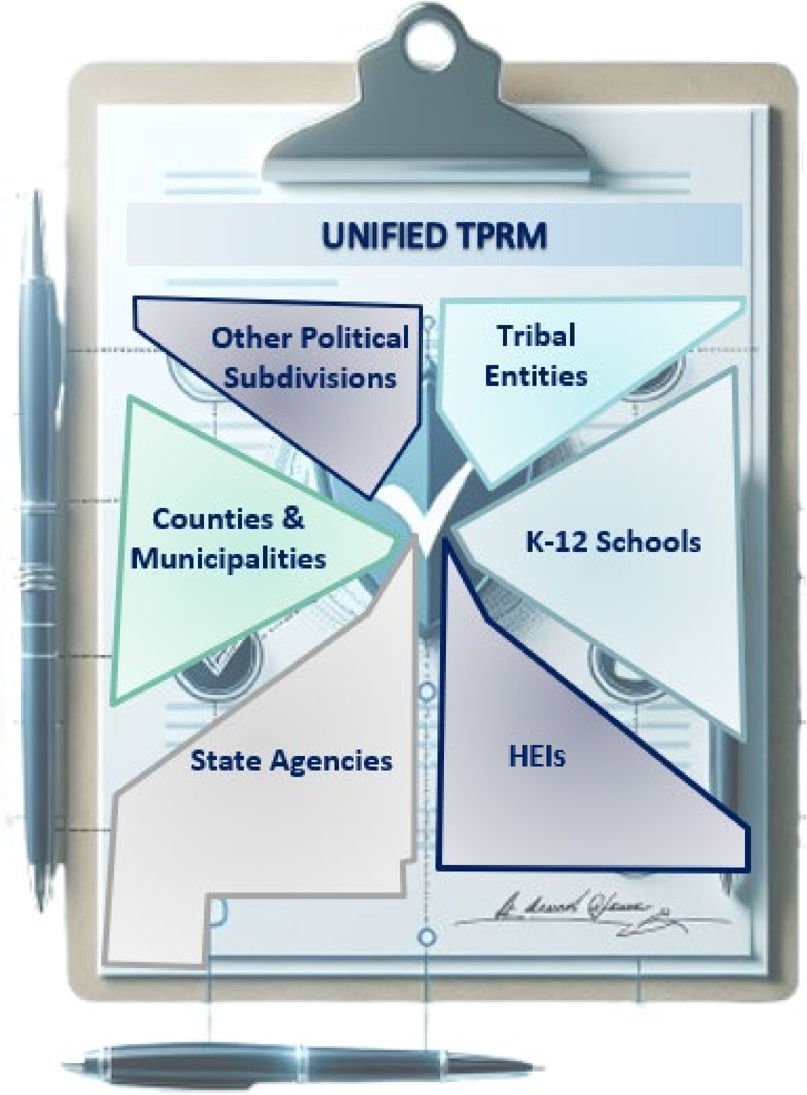
CONTAINING VENDOR RISK THROUGH UNIFIED THIRD-PARTY RISK MANAGEMENT (TPRM)

- State Government operations heavily dependent on vendor/partners

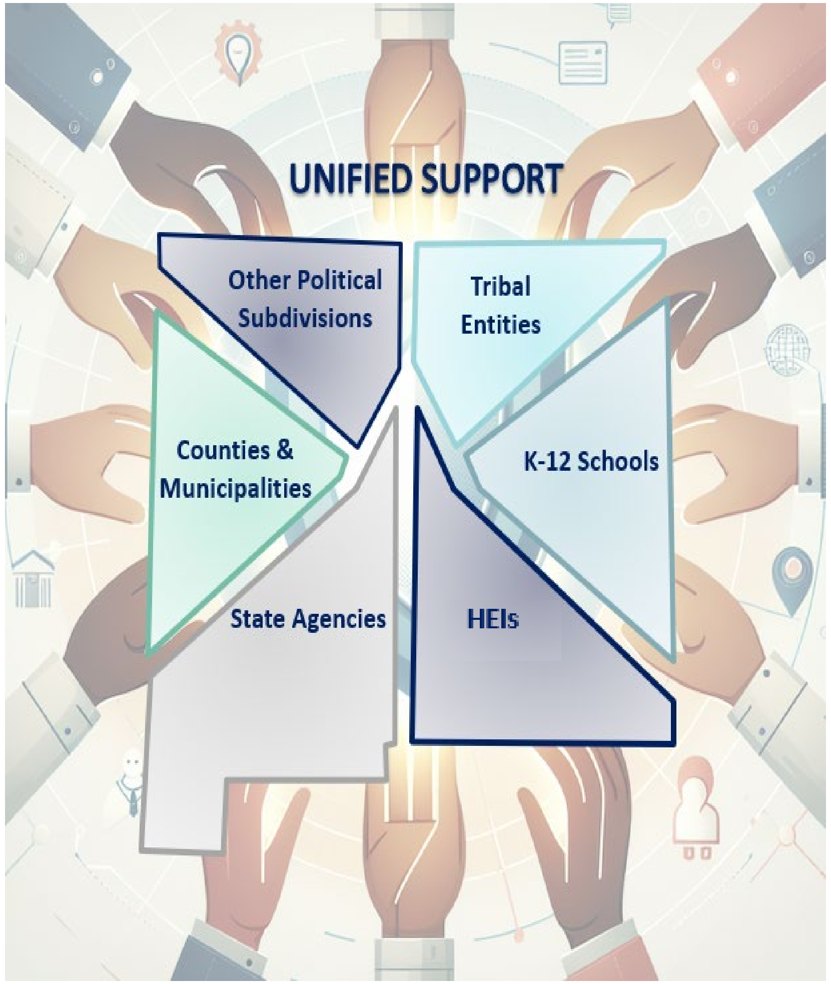
- Extent of vendor cyber risk is unknown and embedded in most services and products procured by NM

- TPRM approach involves assessing security posture of vendors weighed against criticality of project to ensure risk/return/sustainability alignment – A Security Matrix

- Implementing an effective TPRM program will require legislative reform to mandate adherence to process and to empower partner oversight agencies (OCS and GSD)



CONTAINING RISK THROUGH UNIFIED SUPPORT



Many agencies and political subdivisions lack incident response and recovery capabilities

Solution

- Establish state cyber risk pool
- Require participation
- Set assessments based on entity risk scores, compliance with standards and cybersecurity maturity

Benefits

- Incentivizes good cybersecurity hygiene
- Protection for high risk/uninsurable entities
- Public sector autonomy over incident management and response
- Catastrophic risk managed through re-insurance at lower over-all cost to state

CONTAINING AI AND EMERGING TECHNOLOGY RISK THROUGH UNIFIED POLICY AND OVERSIGHT

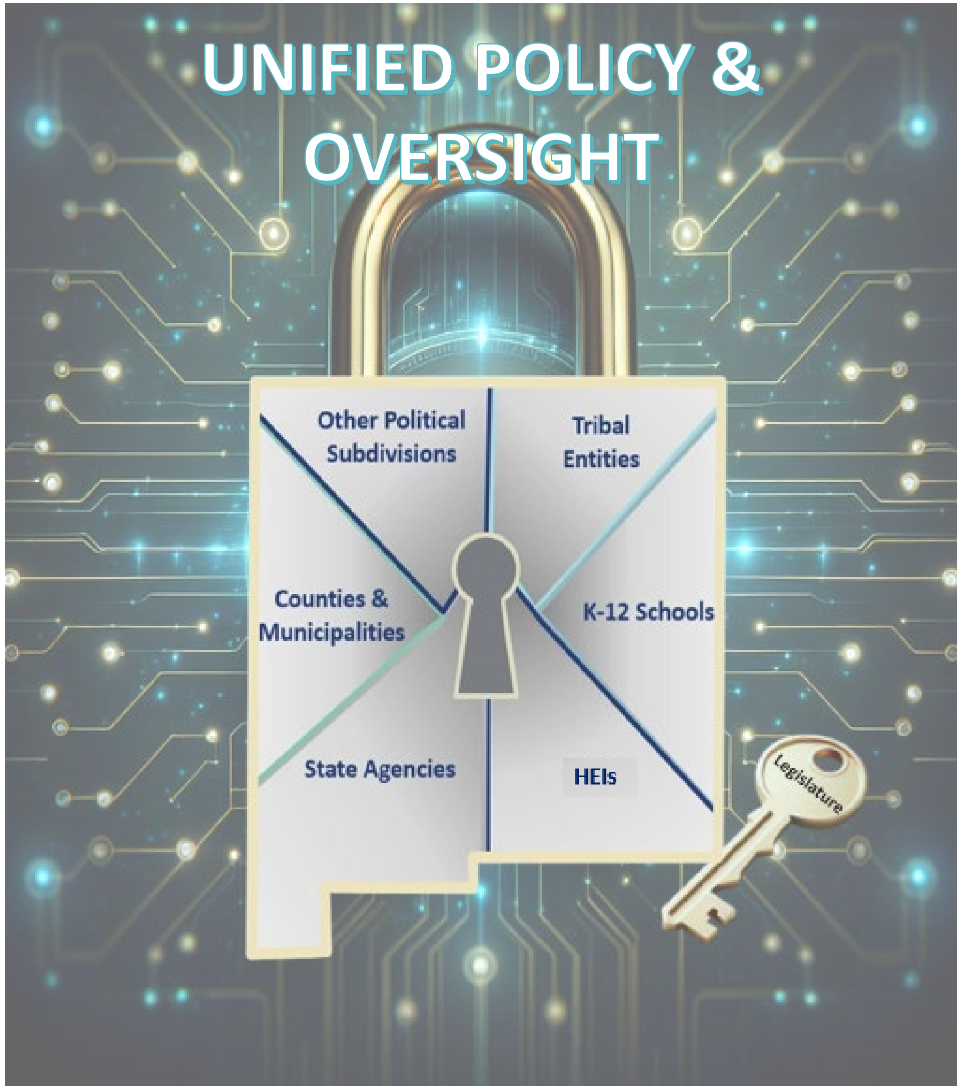
- AI and emerging technology risks do not respect public sector boundaries

  Privacy Risks
  - Data breaches
  - Identity theft
  - Commercial espionage/intellectual property theft

  IT Security Risks
  - Supercharged network attacks and
  - Sophisticated phishing campaigns

  Financial Risks
  - Fraud
  - Market manipulation
  - Brute force hacking

- Risks that do not respect public sector boundaries must be addressed by unified cross-sector policies and oversight


UNIFIED POLICY & OVERSIGHT
Other Political Subdivisions
Tribal Entities
Counties & Municipalities
K-12 Schools
State Agencies
HEIs
Legislature

THANK YOU

Protect Our State: Report Cybersecurity Incidents Immediately!

The Office of Cybersecurity's services are limited to Public Entities

Your vigilance and quick action is crucial in safeguarding
New Mexico and can prevent disruptions and
protect sensitive information

Call the New Mexico Office of Cybersecurity at:

(833) 42-CYBER