



OFFICE OF CYBERSECURITY (OCS) FY2026 AND BEYOND

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

New Mexico Legislative Science,
Technology & Telecommunications Committee

AGENDA

August

- FY25 Activities & Achievements



Enhance existing services

September

- FY26 Plans & Beyond



Expand customer base

October

- Funding & Legislative Initiatives



Evolve service offerings



Launch new initiatives

ENHANCE AND EXPAND EXISTING SERVICES

Section 9-27A-3(B)(7) authorizes OCS to *“develop a service catalog of cybersecurity services to be offered to agencies and to political subdivisions of the state”*

OCS provides six core cybersecurity services:

- 🛡️ Attack Surface Management (ASM)
- 🛡️ Vulnerability Management as a Service (VMaaS)
- 🛡️ Penetration Testing (PT)
- 🛡️ Security Operations Center (SOC)
- 🛡️ Cybersecurity Awareness Training (CAT)
- 🛡️ Risk Assessment (RA)

There are significant coverage gaps outside of the executive branch

OCS will use FY26 funding to expand coverage across the identified sectors

Projected Increase in Service Coverage Based on Available Budget

After full implementation of FY26 funding, significant coverage gaps will remain due to funding deficiencies and lack of voluntary participation of entities outside of executive branch

All subscribers will be onboarded to new AI driven reporting and tracking dashboard that will identify threats, risk scores, mitigation priorities and mitigation progress

Services	FY25 #Served	FY26 #Served	%Change	%Not covered
ASM	442	420	-5%	-22%
VMaaS	118	156	32%	-29%
PT	90	149	60%	-28%
SOC	75	75	0%	-86%
CAT	61	61	0%	-88%
RA	95	97	2%	-82%

EVOLVING THREAT INTELLIGENCE AND PROACTIVE HUNTING

Section 9-27A-3(B)(6) authorizes OCS to “*serve as a cybersecurity resources for local governments*”

- Threat intelligence is critical to cyber preparedness
- Identifying and understanding cyber threats facilitates detection, defense and mitigation
- New Mexico has never had a central threat intelligence gathering and reporting function
- To better serve all political subdivisions and ensure cyber resilience, OCS is building an intelligence program

Threat Intelligence & Hunting Capabilities

- 🛡️ Threat Intelligence Sharing
- 🛡️ Real-time threat intelligence feeds from the Multi-State Information Sharing and Analysis Center (MS-ISAC), Securix, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the New Mexico Department of Homeland Security and Emergency Management (DHSEM)
- 🛡️ Public and private sector research integration
- 🛡️ SOC-driven contextual analysis
- 🛡️ Proactive Threat Hunting and continuous monitoring
- 🛡️ Behavior-based anomaly detection
- 🛡️ Root cause analysis and long-term remediation

Key Program Functions

- 🛡️ Integration of curated commercial & federal threat feeds
- 🛡️ Adversary emulation and hypothesis-based threat hunting
- 🛡️ Identification of state-specific and sector-specific threats
- 🛡️ Early warning systems & automated threat correlation

ENHANCED INCIDENT RESPONSE

Section 9-27A-3(B)(5) authorizes OCS to *“create a model incident-response plan for public bodies to adopt with the cybersecurity office as the incident-response coordinator for incidents”*

Planning



- critical to effective incident response
- ensures that an entity is prepared to detect, contain, and recover from a cyber incident

OCS Incident response support



- OCS is developing a NIST compliant incident response plan template for all public entities
- OCS will publish an updated incident response playbook with step-by-step guidance
- OCS will increase the frequency of tabletop exercises to instill good incident response practices and plan comprehension
- OCS established centralized reporting, triage and support to streamline response assessment and coordination
- Incident response tiger team

Lack of effective backup increases ransomware harm

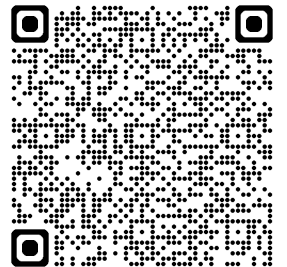


- Entities without tested, reliable and isolated backups are more vulnerable to leverage
- State must pay to recover access to unprotected systems/data

Solutions



- Centralized, up-to-date, tested backup solutions across government
- Expanded SOC participation
- Cyber Incident Insurance?
- Self-Insurance?
- Cyber Incident Recovery Fund?



Order from CISO
regarding reporting
an incident

ENHANCE CYBERSECURITY FOR HIGHER EDUCATION

Laws 2025, Chapter 160 Section 5(65) appropriated \$7.5MM to OCS to support cybersecurity posture of HEIs



Office of Cybersecurity

NMcyber@cyber.nm.gov

(833) 422-9237

NEW MEXICO
HIGHER EDUCATION
DEPARTMENT



Fostering Student Success from Cradle to Career



- 🛡️ Funding will be used to upgrade HEIs from A3 to A5 M365 licensing
- 🛡️ The A5 license supports centralized advanced threat monitoring and data loss prevention (“DLP”) tools
- 🛡️ OCS will collaborate with Higher Education Department and The New Mexico Consortium for Higher Education Computing/Communication Services (“CHECS”) to share threat telemetry and address security concerns
- 🛡️ HEIs will establish Security Operations Center and cybersecurity job training/internship programs
- 🛡️ OCS, in collaboration with the Cybersecurity Planning Committee, will leverage State and Local Cybersecurity Grant Program (SLCGP) funding to onboard all HEIs to cybersecurity awareness training
- 🛡️ These initiatives will equalize cybersecurity posture of HEIs with state agencies

POLICY TEMPLATE INITIATIVES -

Section 9-27A-3(B)(1) directs OCS to “*adopt and implement standards and policies to protect agency information technology systems and infrastructure . . .*”

To bridge gaps, OCS will offer agencies a library of policy templates that meet NIST 800-53 moderate standards

Where we are

State agencies must meet National Institute of Standards and Technology (NIST) 800-53 Moderate

NIST standards require entities to have documented cybersecurity policies

2025 risk assessment initiative revealed a lack of policies across all agency levels

Risk

No Written Policies
Lack of Standardization

Documented cybersecurity policies serve as a roadmap to a strong cybersecurity posture.

Where are we going

Template adoption and implementation will significantly improve agency compliance posture and score


OCS will work with Cybersecurity Advisory Committee to adapt and publish templates for use by local, educational and tribal entities

OCS will work with Cybersecurity Planning Committee to leverage SLCGP funding to assist with adoption

ARTIFICIAL INTELLIGENCE (AI) INITIATIVES -

Section 9-27A-3(B)(2) directs OCS to *“develop minimum cybersecurity controls for managing and protecting information technology assets...”*



-  OCS will establish AI application approval request dashboard for agencies
-  OCS will collaborate with Advisory Committee to establish AI guidance for local, educational and tribal entities
-  OCS lacks authority to govern local, educational and tribal AI deployments interconnected with state network
-  Patchwork AI oversight creates risk by preventing universal implementation of best practices and standardized oversight

THIRD PARTY RISK MANAGEMENT (TPRM)

Section 9-27A-3(B)(1) authorizes OCS to establish *“minimum security standards and policies to protect agency information technology systems and infrastructure and provide appropriate governance and application of the standards and policies across information technology resources used by agencies...”*

9

Concern

- 🛡️ Critical public sector operations and projects are heavily supported by private sector vendors and contractors
- 🛡️ Third-party risk is the state’s risk
- 🛡️ Risks can include offshoring, data breach, denial of service
- 🛡️ Past third party incidents

Recommendation

According to OCS sponsored study:

- 🛡️ Project criticality assessment
- 🛡️ Vendor risk assessment
- 🛡️ Risk matrix
- 🛡️ Vendor selection process changes
- 🛡️ IT Contractual risk management tools

Implementation

OCS will engage with stakeholders to:

- 🛡️ Contract template improvements
- 🛡️ Implement TPRM for Executive branch IT projects
- 🛡️ Create risk assessment, risk matrix, and processes tools
- 🛡️ Procurement Code and Cybersecurity Act Updates

Enterprise Network Assessment

HB2 2025 - Section 5 (68) OCS appropriated \$1MM *“to assess and secure enterprise networks statewide to comply with state cybersecurity standards.”*

10



End of Life (EOL) network equipment presents a significant cybersecurity risk

- 🛡️ EOL devices not supported with patches against emerging threats
- 🛡️ EOL devices can fail and cause network disruption, vulnerabilities, and agency shutdown



State network configuration includes high percentage of EOL network equipment

- 🛡️ Full extent of current EOL conditions unknown due to siloed environment



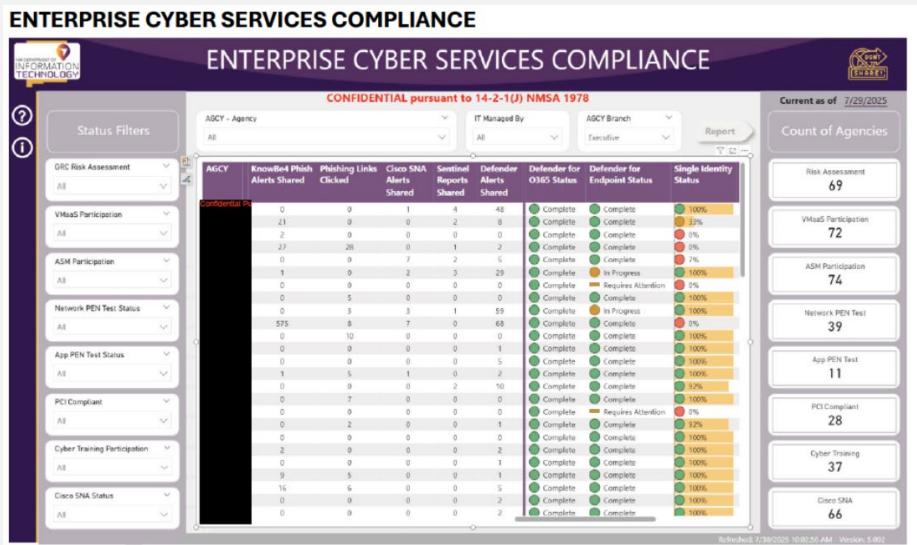
OCS will use funding to inventory, map, and plan

- 🛡️ Identify EOL network equipment, redundancies and waste
- 🛡️ Develop phased modernization plan
- 🛡️ Consolidation and simplification of circuits
- 🛡️ Support cybersecurity standards including Zero Trust, SD-WAN and Wi-Fi security

DATA ANALYTICS & REPORTING

Section 9-27A-5(G) directs the cybersecurity advisory committee to prepare and present an annual report *“regarding the status of cybersecurity preparedness within agencies and elsewhere in the state.”*

- 🛡️ Cybersecurity oversight and reporting is data driven
- 🛡️ Data reveals status, trends and vulnerabilities
- 🛡️ Data ensures transparency and accountability
- 🛡️ OCS is using Microsoft tools to establish robust data analytics and reporting capabilities



Shows onboarding to Enterprise Controls



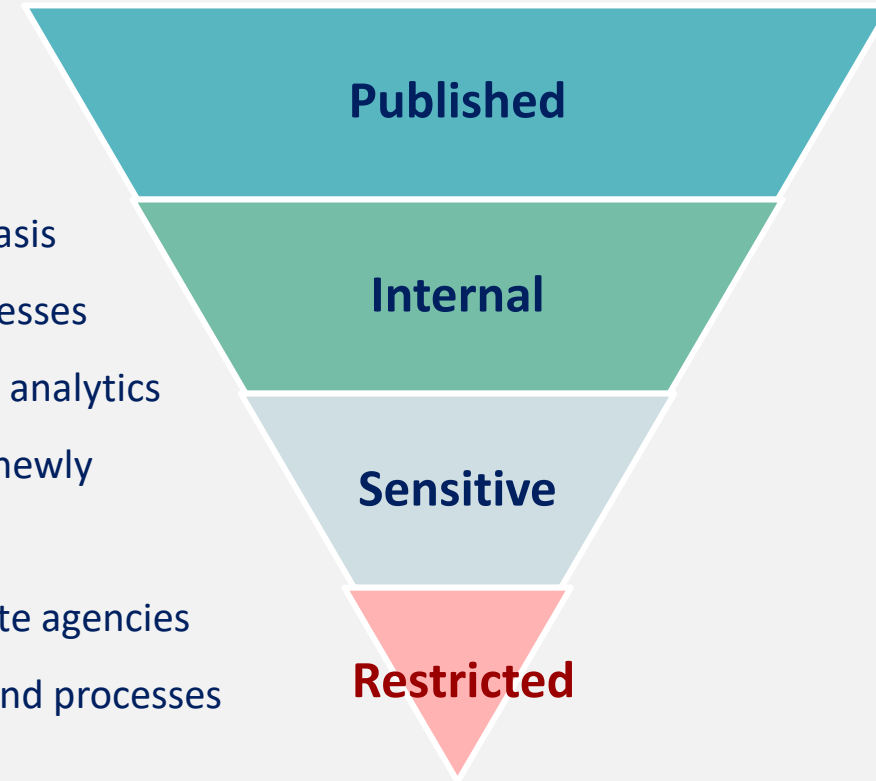
Shows agency compliance posture

These tools empower OCS to direct resources to address critical risks in the state agency enterprise, and will enable agencies and external stakeholders to better understand and address risk

DATA AND PRIVACY

Section 9-27A-3(B)(10) directs OCS to “**establish minimum data classification policies and standards and design controls to support compliance with classifications and report on exceptions . . .**”




- Protecting data and privacy are core objectives of an effective cybersecurity program
- Data loss prevention (DLP) and privacy protection depend on data classification
- No central data classification/DLP oversight authority for non-executive agencies
- Public entities are implementing data classification/DLP on an ad hoc, entity-by-entity basis
- Entities subject to the same compliance standards often have different compliance processes
- Ad hoc processes complicate risk assessment, compliance verification, data sharing, and analytics
- Executive agencies and HEIs have access to powerful data classification tools under the newly procured G5 and A5 licenses, allowing standardization
- OCS will engage with Advisory Committee to develop classification/DLP guidance for state agencies
- Legislative changes required to implement statewide data classification/DLP standards and processes



WORKFORCE DEVELOPMENT

6 U.S. Code § 665g - State and Local Cybersecurity Grant Program (SLCGP) *“...use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by the National Institute of Standards and Technology to identify and mitigate any gaps in the cybersecurity workforces...”*

SLCGP & State Workforce Development Request for Quotes (RFQ)

-  Conduct needs assessment, capabilities assessment, and gap analysis
-  Provide remediation recommendations tailored to local entities
-  Align with the NICE Framework

The State RFQ was developed in parallel with the SLCGP RFQ but is distinct in its audience and scope targeting New Mexico’s Executive Branch agencies.

ADVANCING CENTRALIZED CYBERSECURITY IN NEW MEXICO

14



Strengthen New Mexico's cybersecurity posture by expanding centralized operations across the state



Align with national best practices



Protect the infrastructure of our state agencies, counties, municipalities, tribal entities, K-12 schools, higher education institutions, and other public bodies



CENTRALIZED CYBERSECURITY

Challenges and Solutions

Challenge	Description	Solution	Description
Inconsistent Standards	Entities use varied protocols, creating exploitable gaps	Standardized Policies	Reduces vulnerabilities and ensures compliance
Limited Visibility	No unified monitoring means slower detection and response	Real-Time Monitoring	Centralized SOCs detect and respond 24/7
Redundant Spending	Multiple entities buying similar tools = wasted taxpayer dollars	Cost Efficiency	Shared tools and services lower expenses
Disjointed Response	Lack of coordination delays containment and recovery	Collaboration	Faster communication and intelligence sharing
Talent Shortages	Smaller entities struggle to recruit cybersecurity experts	Workforce Capacity	Central teams attract top talent and support smaller entities

STATES LEADING THE WAY IN CENTRALIZED CYBERSECURITY

State	Model	Highlights
New York	Joint Security Operations Center (JSOC)	24/7 coordination across state, local, and federal entities
California	SOC-as-a-Service	Centralized monitoring, detection and notification services for state, local, education and other public sector entities
Ohio	CyberOhio	Statewide training and incident response
Maryland	Cybersecurity Coordinating Council	Unified cyber strategy and policies for state agencies, local governments, schools and other political subdivisions
Texas	Regional SOCs	Regional command centers to monitor data to stop or mitigate cyber-incidents in defined regions of the state
Arizona	Cyber Command	Statewide SOC, enterprise infrastructure and services, and central policy enforcement

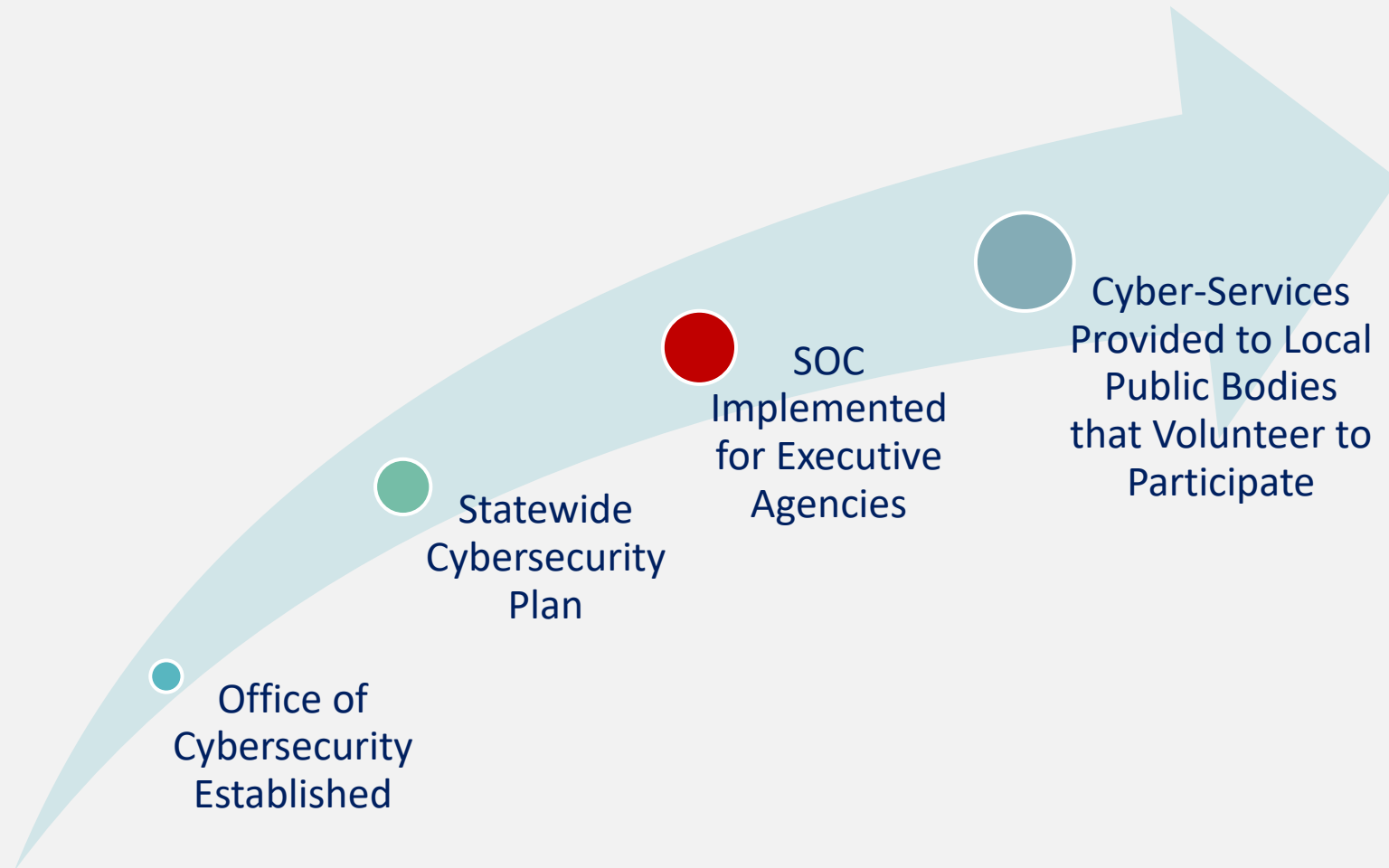
ACCELERATING CENTRALIZED CYBERSECURITY IN NEW MEXICO

17



GOAL

Fully Unify Cybersecurity Across State Agencies, Counties, Municipalities, Tribal Entities, K-12 Schools, Higher Education Institutions, and Other Public Bodies



Office of
Cybersecurity
Established

Statewide
Cybersecurity
Plan

SOC
Implemented
for Executive
Agencies

Cyber-Services
Provided to Local
Public Bodies
that Volunteer to
Participate

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