OFFICE OF CYBERSECURITY (OCS)
FY2025 ACTIVITIES AND ACHIEVEMENTS

Raja Sambandam, State Chief Information Security Officer
August 25, 2025

New Mexico Legislative Science, Technology & Telecommunications Committee

AGENDA

August
- FY25 Activities & Achievements

September
- FY26 Plans & Beyond

October
- Funding & Legislative Initiatives

What is Cybersecurity?

OCS Mission & Programs

Water & Wastewater Cybersecurity

State & Local Cybersecurity Grant Program

Other Significant FY25 Events

What is Cybersecurity?

The art of protecting information technology networks, electronic devices and digital data from unauthorized access or criminal use.

The practice of ensuring confidentiality, integrity and availability of information.

Common Vulnerabilities

- Human factors
- Credential Misuse
- Ransomware
- Malware
- Virus
- Unprotected Data
- Lack of backup
- Absence of Policies & Plans
- Personnel loss

Consequences

- Financial Loss
- Business & Service Interruptions
- Reputational Damage
- Legal & Compliance
- Compromised Sensitive Information
- Public Safety/Critical Infrastructure

Defenses & Controls

- Cybersecurity User Awareness Training
- Multi-Factor Authentication
- Endpoint Protection and Response
- Distributed Denial-of-Service Protection
- Domain Name Server Layer Security
- Threat Intelligence
- Phishing Response
- Network Anomaly Detection
- Log Correlation and Incident Orchestration

OCS Mission

The statutory mission of the **OCS** is to promote cybersecurity in the public sector.

- OCS provides services to all Executive agencies
- OCS provides services to interested public entities such as K-12 Schools, Higher Educational Institutions, Counties, Municipalities, Tribal Entities, Water and Wastewater Systems
- Legislative and Judiciary entities have declined OCS services
- OCS is not currently funded to support all public entities

Subscribers that receive OCS services have a demonstrably stronger cybersecurity posture

Program Objectives

OCS fulfills its mission through strategic initiatives and its Enterprise Cybersecurity Program **(ECP)**

Through these initiatives and programs, OCS serves to:

- **Protect the privacy and security** of state owned or operated IT, including networks, applications and devices
- **Establish and Standardize cybersecurity practices** through policies, procedures, and training
- **Coordinate cyber incident response** and risk mitigation across state agencies and political subdivisions
- **Serve as Central Cybersecurity Point-of-Contact** for all public entities
- **Provide support and guidance** to the Cybersecurity Advisory and Cybersecurity Planning committees
- **Enable informed decision-making** through risk analysis, gap discovery, and mitigation planning tailored to each subscriber

ECP Services

Attack Surface Management (ASM) – Continuous scanning of state networks and devices to discover, monitor, and analyze external facing vulnerabilities

Vulnerability Management (VMaaS) – Monthly scanning of internal networks to identify vulnerabilities and prioritize mitigation

Risk Assessments (RA) – A process to identify cybersecurity risks and defenses within an organization's unique information technology environment

Cybersecurity User Awareness Training (CAT) – Annual training, Phishing Campaigns, and Phishing reporting/monitoring

Penetration Testing (PT) – Authorized attacks to Subscriber assets and applications to identify weakness in security

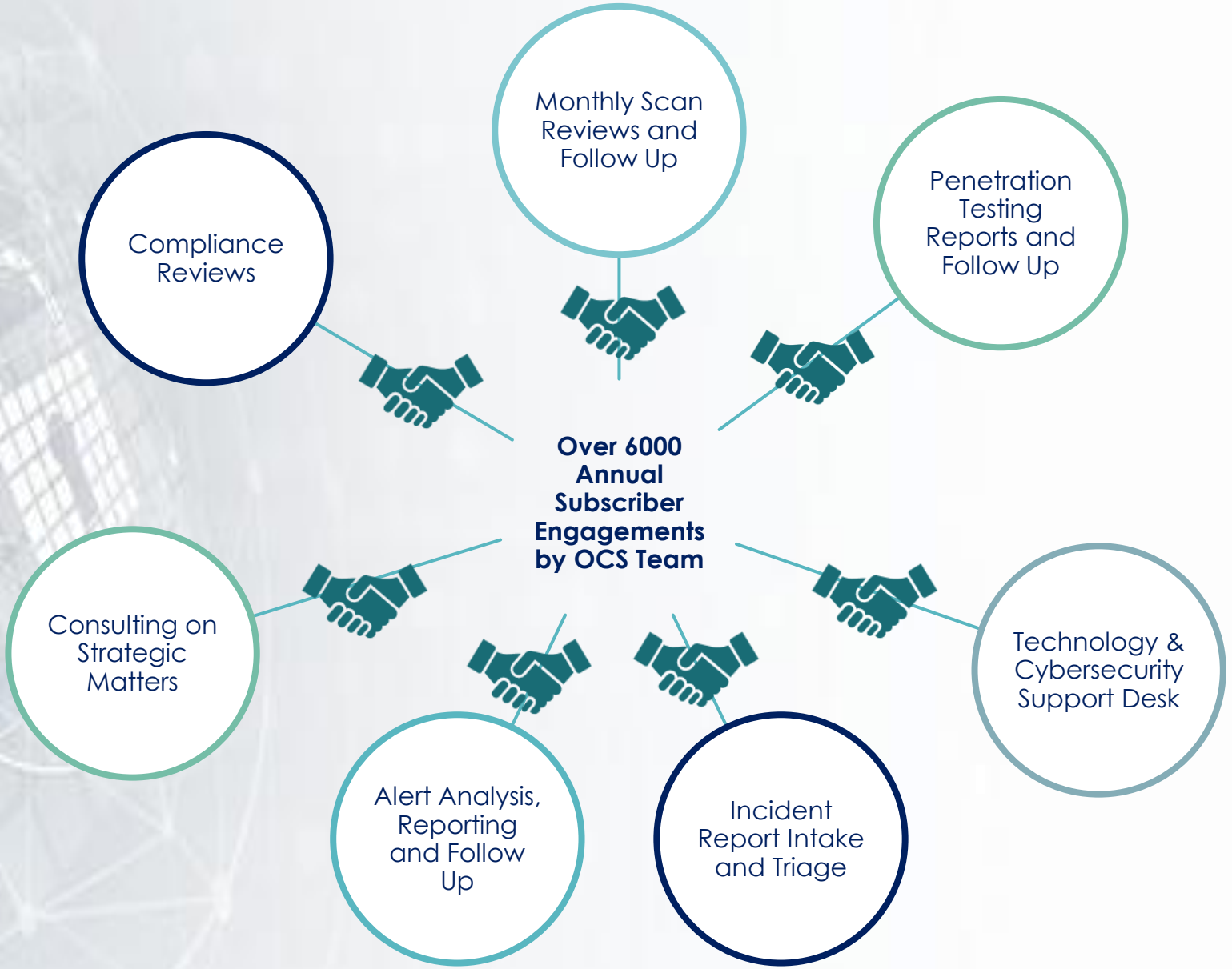
Security Operations Center (SOC) – Centralized and continuous monitoring of networks, alerts and devices to prevent, detect and respond to security threats in real time

Participation by Subscriber

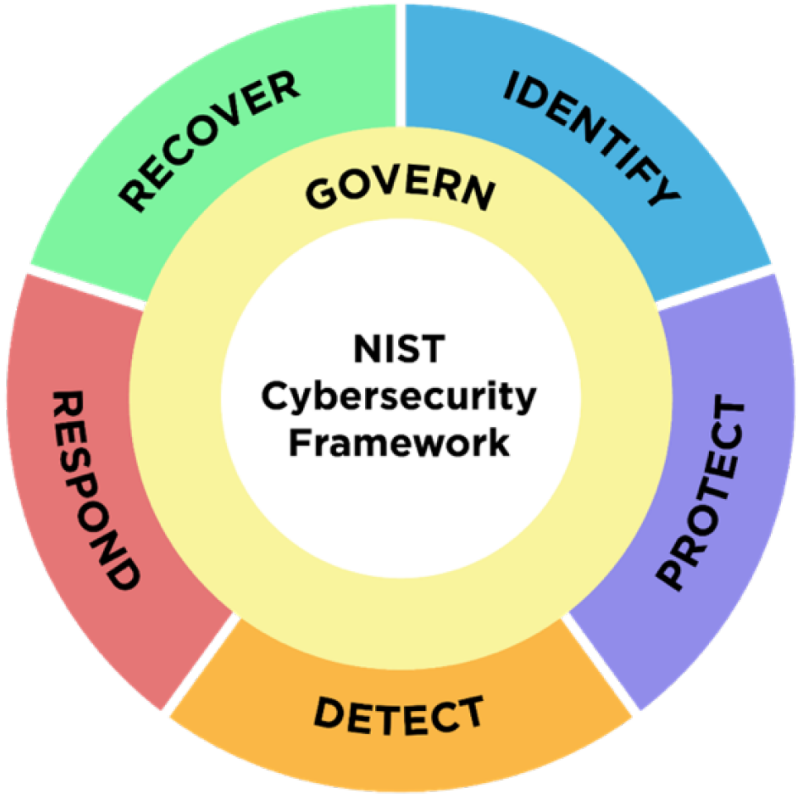
Political Subdivision Type	Potential Subscribers by Type	ASM	VMaaS	PT	CAT	RA
State Agency	73	73	70	52	41	73
County	33	33	9	0	7	9
Municipality	105	105	5	0	3	5
K12 - District and Charter	188	188	17	21	6	2
HEI	19	17	14	17	2	3
Tribal	23	23	0	0	2	2
Judicial	18	1	1	0	0	0
Legislative	1	0	0	0	0	0
Water/Wastewater	73	1	1	0	0	0
Other	1	1	1	0	0	1
Total	**534**	**442** (-92/17%)	**118** (-416/78%)	**90** (-444/79%)	**61** (-473/89%)	**95** (-439/82%)

- Special appropriations and grant funding used to provision services
- Services identified in **green** were grant funded

Subscriber Engagements



Cybersecurity Standards



The National Institute of Standards and Technology **(NIST)** promulgates benchmark cybersecurity standards

NIST publication 800-53 compiles a set of over 800 cybersecurity defense practices, and groups those by category and impact/efficacy

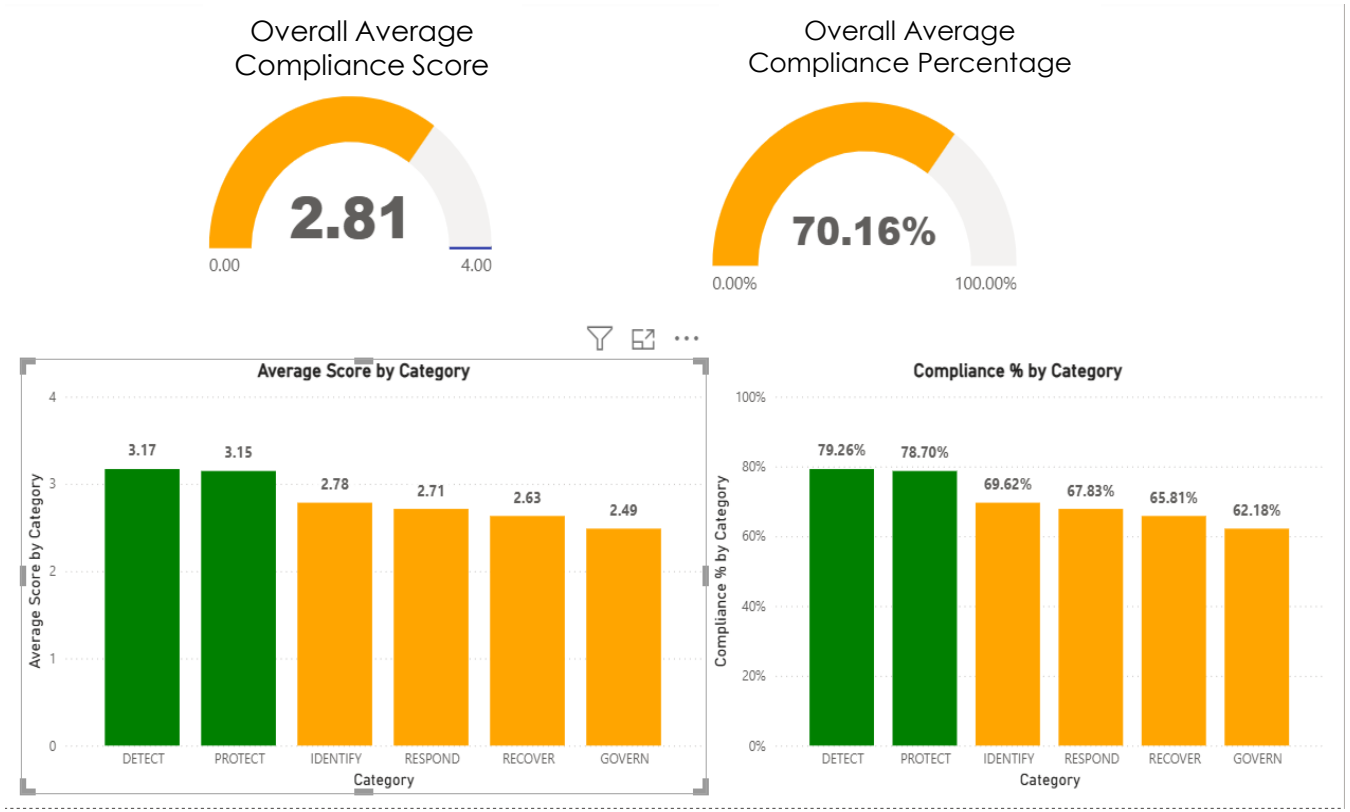
Compliance with NIST 800-53 standards makes IT systems more resilient, and promotes integrity, confidentiality, and security

OCS holds New Mexico executive agencies to the NIST 800-53 moderate impact security posture

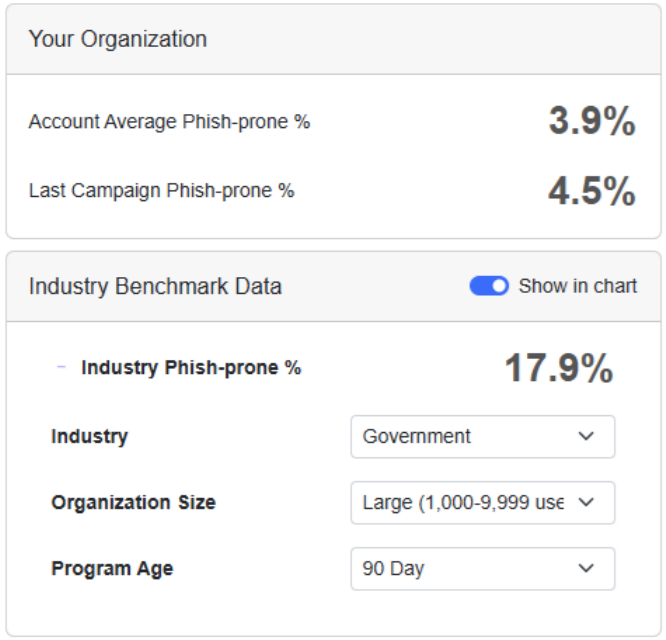
IT-Cybersecurity Risk Assessment

OCS launched a Governance, Risk and Compliance (GRC) platform for risk assessments

- All executive agencies have completed a risk assessment
- OCS is using third party data to validate and assess actual compliance
- Sample validation indicates significant gaps between reported and actual compliance
- Additional validation required



Cybersecurity User Awareness Training



DATA: Training Reduces Susceptibility to Phishing Attacks

- Government Sector Susceptibility Average: **17.9%**
- Executive Agencies Participating in OCS-Managed Training: **3.9%**

Nearly three-quarters of security incidents involve human error

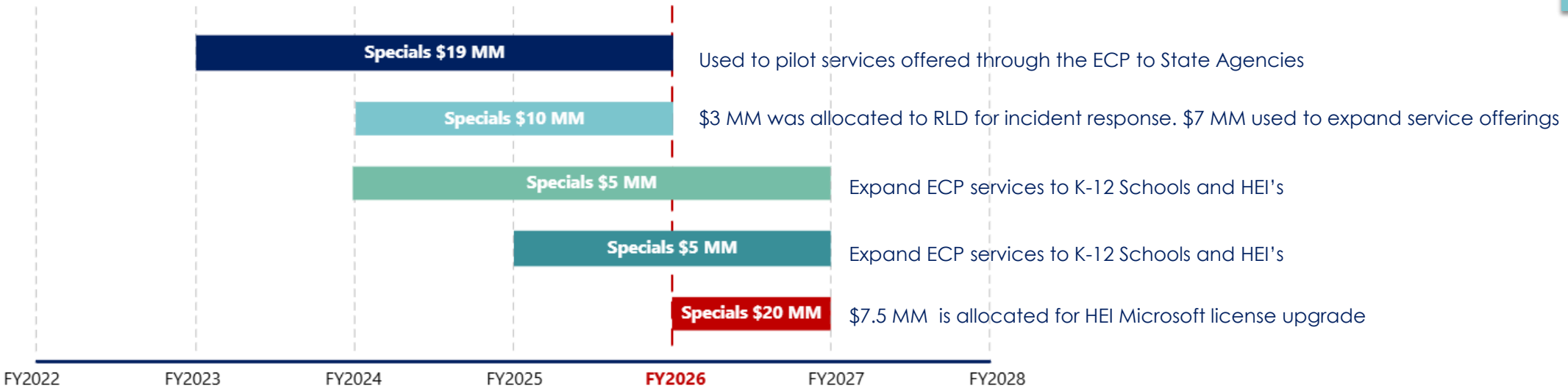
Common errors include clicking on malicious links or falling victim to credential phishing

Why provide training?

Training equips employees with skills to identify and avoid these pitfalls.

Compliance with NIST Standards

Funding for ECP Services



OCS Operating Budget (in thousands)			
Category	**FY25**	**FY26**	**Difference**
PS&EB (200s)	$1,605.5	$1,635.1	$29.50
Contractual Services (300s)	$3,739.5	$3,572.6	($166.90)
Other (400s)	$832.8	$832.8	$0.00
Other Financing Uses (500s)	$315.1	$482.0	$166.90
Total	**$6,492.90**	**$6,522.5**	**$29.60**

Through strategic deployment of recurring, special and grant funding OCS continually expands service offerings and its subscriber base, improving public sector cyber resilience.

Relying largely on voluntary participation by public entities, OCS is closing gaps and increasing security statewide! But gaps remain.

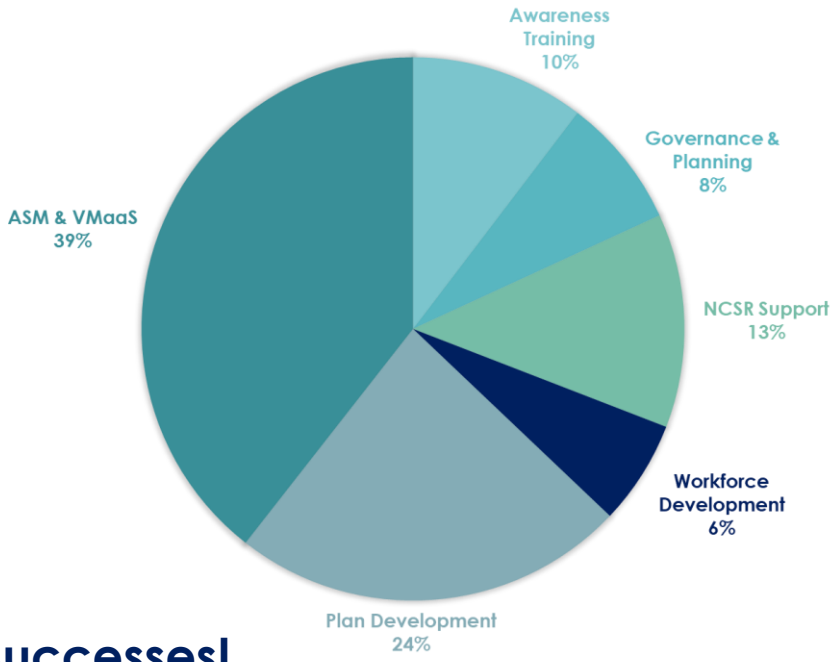
WATER AND WASTEWATER CYBERSECURITY

Progress, Concerns and Solutions

- Water and wastewater systems are critical infrastructure largely in the public domain
- Most systems lack strong cyber defenses and are frequent targets of malicious actors
- Cyber attacks on these systems can cripple industry, and threaten human life and habitation
- OCS, in coordination with DHSEM and ENV, developed a water and wastewater cybersecurity plan approved by the Biden administration
- OCS has partnered with the federal Cybersecurity Infrastructure and Security Agency (CISA)
- 73 systems approved to receive services
- OCS is engaged in outreach and onboarding to support plan implementation
  - GRC based risk assessments
  - CISA administered network scanning
  - Incident response plans
  - Desktop exercises
- **No current funding for additional ECP services or mitigation**

Critical Infrastructure Cybersecurity Benefits

State and Local Cybersecurity Grant Program (SLCGP) Year 1 of 4*



Total award amount after 5% NMDHSEM M&A share:
$2,413,383.00

	Project	Status	Budget
	Develop Statewide Cybersecurity Plan	**100% Complete**	$566,658.99
1	**Governance & Planning**	Dependent upon completion of the State Sponsored Policy Template Library Development project. OCS anticipates the library being available December of 2025.	$187,648.00
2	**National Cybersecurity Risk (NCSR) Assessment Support**	**100% Complete**	$307,298.00
3	**ASM & VMaaS**	**100% of participating entities being scanned for FY2026**	$951,395.00
4	**Cybersecurity Awareness Training**	• License were made available 1/1/2025 • Opened new application period in March. • More applicants than available licenses • Procured additional licenses and in the process of onboarding new participating entities. • Licenses are offered for FY2026	$250,000.00
5	**Workforce Development Planning**	• Request for quote (RFQ) issued in March • Quoted amounts exceeded the available budget • New RFQ with revised project scope	$150,000

Successes!

- Funding covered all **26** local entities that applied
- NCSR project completion on time and under budget
- Program desk review performed by CISA found **NO** issues
- Financial desk review performed by FEMA found **NO** issues

* SLCGP only provides four years of funding, with different award amounts each year.

Additional FY25 Achievements

- Adopting Multi-Factor Authentication for SHARE system
- Co-Issued Generative AI Policy
- Established E-Discovery access policy and user training program
- Issued statewide cyber incident notification order
- Leveraged Enterprise Level Security Features
- Adopted Unified Security Platform and Solutions

Significant Challenges

Federal Changes

- Elimination of funding for MS-ISAC
- Reduction of Cybersecurity workforce
- Elimination of threat intelligence concerning nation state actors
- Reductions of cybersecurity agencies and services
- Termination of NCSR

Emerging Technology Threats Including Increased use of AI by Malicious Actors

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