



Presentation to the Legislative Science, Technology, and Telecommunications Committee  
by the Consortium of Higher Education Computing and Communications Services (CHECS)

September 23, 2025

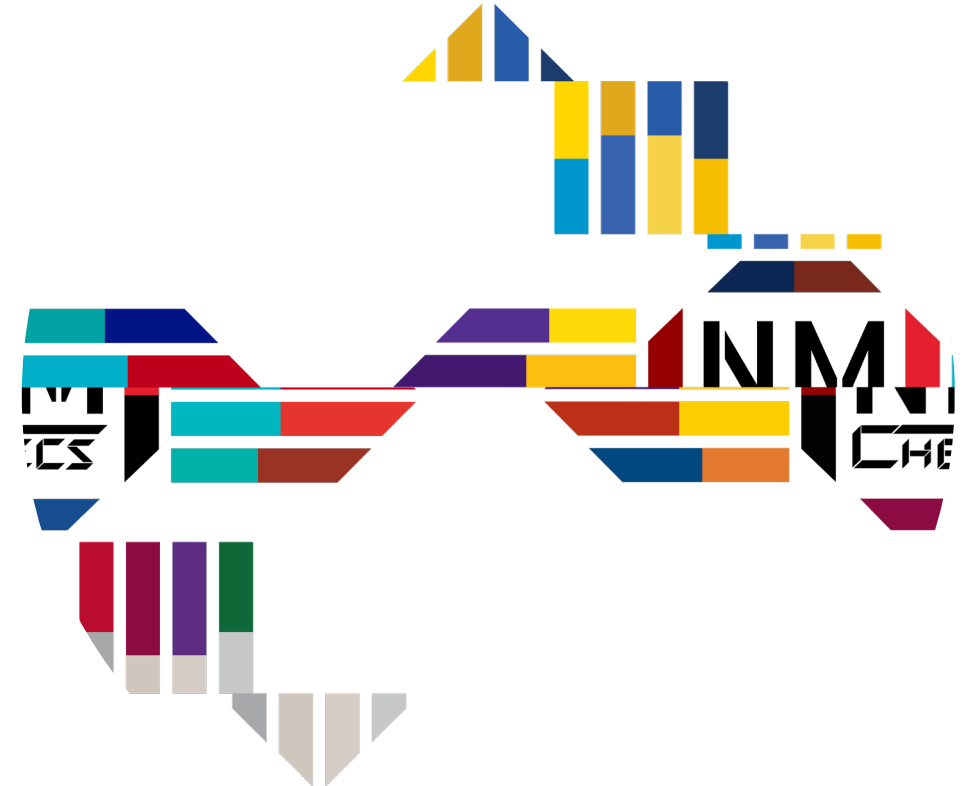


# Speakers

- Duane Arruti, UNM CIO
- Victor Leon, CNM CIO
- Michael Acosta, WNMU CIO
- Raja Sambandam, NM DoIT, CISO
- Isaac Bush, NM Higher Education Department CIO

# Key Collaborators

- Cori Bergen, SFCC CIO, Current CHECS President
- Jeff Gassaway, UNM Information Security and Privacy Officer
- Vanessa Hawker, NMICC Executive Director
- Kevin Kouri, CNM Senior Director of Enterprise Infrastructure
- Barbara Medina, NMACC Executive Director
- Kirsten Moeller, UNM Director of IT Business Operations
- Alan Roes, CNM CISO
- Marc Saavedra, CUP Executive Director





# Goals for today

- Explain the role of CHECS within NM Higher Education and the State of NM.
- Describe our common and unique challenges with managing cyber security risks.
- Provide an update on current year collaborative cyber security initiatives.
- Discuss critical and ongoing needs to address continuing and emerging cyber security threats.



# CHECS Member Organizations

\*  Clovis Community College

\*  **CNM**  
Central New Mexico  
Community College

\*  Luna  
Community  
College

 MESALANDS  
Community  
COLLEGE

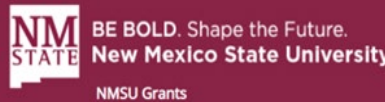
 **SEMC**  
Southeast New Mexico College

\*  **SAN JUAN COLLEGE**

\*  **SFCC**  
SANTA FE COMMUNITY COLLEGE

 **ENMUR**  
EASTERN NEW MEXICO UNIVERSITY  
ROSWELL

 **NM STATE** BE BOLD. SHAPE THE FUTURE.  
Alamogordo

 **NM STATE** BE BOLD. Shape the Future.  
New Mexico State University  
NMSU Grants

 **NM STATE DACC**

 **NM GALLUP**

 **NM LOS ALAMOS**

 **NM TAOS**

 **NM VALENCIA**


 **EASTERN  
NEW MEXICO  
UNIVERSITY**

 **H NEW MEXICO  
HIGHLANDS  
UNIVERSITY**

\*  **NORTHERN  
New Mexico College**

 **WESTERN  
NEW MEXICO UNIVERSITY**

 **NM STATE** BE BOLD. Shape the Future.  
New Mexico State University

 **NEW MEXICO TECH**  
SCIENCE • ENGINEERING • RESEARCH UNIVERSITY

 **NM THE UNIVERSITY OF  
NEW MEXICO.**

 **NM HEALTH  
SCIENCES**

 **NM NEW MEXICO MILITARY INSTITUTE**

 **IAIA**  
INSTITUTE of  
AMERICAN INDIAN ARTS

 **NAVAJO  
TECHNICAL UNIVERSITY**

 **Dine College**

 **SIPI SOUTHWESTERN INDIAN  
POLYTECHNIC INSTITUTE**

 **NEW MEXICO JUNIOR COLLEGE**  
EST. 1965

Note - the six institutions marked by "\*" are individually members of CHECS and are also part of the separate 501C3 known as CHES. CHES is not affiliated with CHECS, but CHES institutions are members of CHECS.



# A History of Successful Collaboration

- NMSU, NMT and DOIT – Rio Grande Optical Network (RGON) Fiber Project
- Banner Training and Consulting Services
- NM Research Partners
- UNM’s Albuquerque Giga-Pop (ABQG)
- Banner Consortium – JASI
- LIBROS – Consortium of Libraries
- NMSU CHECSnet – MagNet, EPSCoR Grant, Eastern Loop
- Western Regional Network (WRN) (NM, CA, UT, and CO)
- Microsoft and Adobe Master Agreement (35% to 82% savings on Microsoft; 85% savings on Adobe)
- Rocky Mountain Online Library
- Numerous fiber projects with local governments, school districts, DoIT and Telco’s
- Colocation/Aggregation Services in support of Statewide Education Network
- **FY2021 GEER Funding with Cybersecurity Components**
- **FY2022 Cyber Security \$1.7M request through HED, funded FY24**
- **FY2023 Cyber Security \$3M request through HED/DoIT**
- **FY2026 Cyber Security \$7.5M Funding through HED/DoIT**



# How NM HEIs Manage Cyber Security Risk

- We have varying approaches and resources to address our risks.
  - Cyber security operations may be managed by IT staff.
- We implement and improve internal controls.
  - People, processes, and technologies.
- We have varying specific risks.
  - Specific end-of-life hardware, software, or other dependencies.
- We are at different points on our cybersecurity maturity journeys
  - Cybersecurity processes, staffing, tools, training.



# What can be unique to HEIs

- Small cities with instruction, libraries, public/community service, residency, health care, credit card processing, research, large employers, and many other functions with associated risks.
  - AI-related risks as they apply to the substantial personal data and
- Highly-regulated research with strict security requirements and penalties for non-compliance.
- Employee and students can often access institutional data and IT services with their own devices.



# HEI Compliance Requirements and Standards

- FERPA (Education records and systems)
- GLBA (Financial Aid and related records and systems)
- FTI (Federal Tax Information, now part of financial aid applications)
- HIPAA (Healthcare records and systems)
- PCI (Credit card records and systems)
- IRBs (for protecting human research subjects)
- NSPM-33 (National directive for securing federal research)
- NIST 800-171 (Standard for protecting federal research data and systems)
- CMMC (Audit for Defense contract systems)





# HEI Standard Practices to Manage Cyber Security Risk

- IT systems and infrastructure must be
  - Configured, patched, and maintained
  - Subject to routine penetration testing and compliance audits
- Information and business risks must address
  - Public data and internet-facing devices
  - Regulated data and internal-facing devices
- Like the State, many HEIs are aligned on Microsoft identity and cyber security tools, creating opportunities for shared knowledge and economies of scale



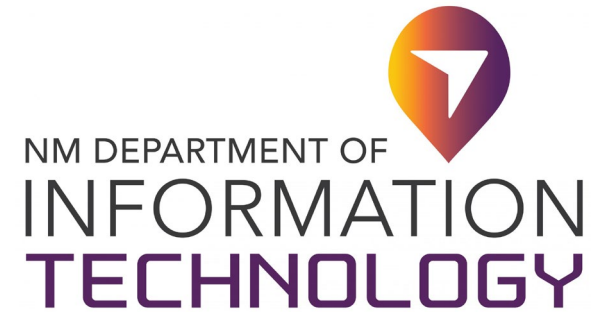
# Critical Ongoing Needs

- Cyber security functions need additional funding to keep pace with current and emerging risks and threats.
  - Personnel
  - Policies and processes
  - Tools
  - Training
- IT and cybersecurity vendor software costs and escalators substantially outpace funding, which is often not recurring.
- Access to cyber insurance can offset not just losses but also, can provide immediate access to pre-negotiated critical services.



# DoIT Cyber Security Telemetry Services

- Attack Surface Management
- Vulnerability Management
- Other Key Security Services





# FY2026 Cyber Security \$7.5M initiative w/ HED/DoIT

- MOU
- Licensing Procurement
- Implementation
- Workshops
  - Kickoff & Strategic Framing
  - Security & Identity Foundations
  - Compliance & Information Governance
- Future Planning
  - Voice & Collaboration Modernization
  - Analytics & Insights
  - AI & Copilot Readiness





# Key Security Features of Microsoft A5

- Single Sign On (SSO)
- Multi Factor Authentication (MFA)
- Self-Service Password Reset (SSPR)
- Conditional Access
- Azure Information Protection
- Advanced Threat Analytics
- InTune
- Privileged Identity Management (PIM)
- Azure Advanced Threat Protection
- And many, many more

HED/DoIT/Consortium of Higher Education Communication and Computing Services (CHECS) FY 2026 Cybersecurity Proposal Revised Summary v2.0

Description	FY26 Request (Revised)
Microsoft Licensing (or other) - 3 years	\$5,600,000.00
Micosoft (or other) implementation services and/or information security risk mitigation staff/service augmentation	\$1,580,000.00
FERPA, GLBA, HIPAA, and CUI Regulatory Security and Compliance assessments (leveraging and augmenting State provided services)	\$2,820,000.00
<b>Total</b>	<b>\$10,000,000.00</b>

Breakdown by institution reflected in table below.



- Developed in partnership with HED and DoIT
- Funding for all Public Institutions and Tribal Colleges in NM
- Supported by CUP, NMICC, and NMACC
- Aligns with DoIT Cyber Security Strategy/Augments State provided security assessment services
- Takes advantage of shared processes and tools
- Economies of scale in Higher Ed licensing and services

- Need to finalize license counts/ costs with updated information.

Institution	Qty	Total A3 (Current)	Total A5 (Current)	A5 Licensing (new cost less current investment) FY26	A5 Licensing (new cost less current investment) FY27	A5 Licensing (new cost less current investment) FY28	Total A5 Licensing (FY26 - FY28)	Implementation/ Mitigation Services FY26	FERPA, GLBA, HIPAA, and CUI Regulatory Security and Compliance Assessments (Estimated) FY26
University of New Mexico - Main, Gallup, Taos, Valencia, Los Alamos	7,000		\$ 644,015	\$ 129,834.96	\$ 323,297	\$ 323,297	\$ 776,430	TBD	\$ 134,286
University of New Mexico - HSC/UH/SRMC/UNMMG	17,217	\$ 469,165		\$ 622,295	\$ 895,160	\$ 895,160	\$ 2,412,616	TBD	\$ 134,286
New Mexico Junior College	450	\$ 21,384		\$ 28,364	\$ 40,800	\$ 40,800	\$ 109,964	TBD	\$ 134,286
Santa Fe CC	525		\$ 46,431	\$ 11,608	\$ 26,117	\$ 26,117	\$ 63,843	TBD	\$ 134,286
Northern New Mexico College	255	\$ 12,118		\$ 16,073	\$ 23,120	\$ 23,120	\$ 62,313	TBD	\$ 134,286
New Mexico Military Institute	380		\$ 33,607	\$ 8,402	\$ 18,904	\$ 18,904	\$ 46,210	TBD	\$ 134,286
Clovis Community College	200	\$ 17,688		\$ 4,422	\$ 9,950	\$ 9,950	\$ 24,321	TBD	\$ 134,286
Mesalands Community College	100	\$ 4,752		\$ 6,303	\$ 9,067	\$ 9,067	\$ 24,437	TBD	\$ 134,286
San Juan College	1,000	\$ 47,520		\$ 63,030	\$ 90,668	\$ 90,668	\$ 244,365	TBD	\$ 134,286
Eastern New Mexico University (Portales, Ruidoso, Roswell)	1,445		\$ 127,796	\$ 31,949	\$ 71,885	\$ 71,885	\$ 175,719	TBD	\$ 134,286
New Mexico Highlands University	665	\$ 26,136	\$ 10,171	\$ 37,209	\$ 55,588	\$ 55,588	\$ 148,385	TBD	\$ 134,286
New Mexico Tech	875		\$ 77,385	\$ 19,346	\$ 43,529	\$ 43,529	\$ 106,404	TBD	\$ 134,286
Western New Mexico University	585	\$ 27,799		\$ 36,873	\$ 53,040	\$ 53,040	\$ 142,954	TBD	\$ 134,286
New Mexico State University (Las Cruces, Alamogordo, Grants, Dona Ana) <sup>1</sup>	4,206		\$ 390,109	\$ 74,864	\$ 191,108	\$ 191,108	\$ 457,080	TBD	\$ 134,286
Institute of American Indian Arts <sup>2</sup>	157	\$ 7,461		\$ 9,896	\$ 14,235	\$ 14,235	\$ 38,365	TBD	\$ 134,286
Dine College <sup>1</sup> (A1 license currently)	330			\$ 36,482	\$ 45,602	\$ 45,602	\$ 127,685	TBD	\$ 134,286
Navajo Technical University <sup>1</sup>	160	\$ 7,603		\$ 10,085	\$ 14,507	\$ 14,507	\$ 39,098	TBD	\$ 134,286
Southeast New Mexico College <sup>1</sup>	205			\$ 22,663	\$ 28,328	\$ 28,328	\$ 79,320	TBD	\$ 134,286
Luna Community College	100	\$ 4,752		\$ 6,303	\$ 9,067	\$ 9,067	\$ 24,437	TBD	\$ 134,286
Southwestern Indian Polytechnic Institute <sup>1</sup>	60	\$ 2,851		\$ 3,782	\$ 5,440	\$ 5,440	\$ 14,662	TBD	\$ 134,286
Central New Mexico Community College <sup>1</sup>	1,847	\$ 87,769		\$ 116,416	\$ 167,463	\$ 167,463	\$ 451,342	TBD	\$ 134,286
<b>Totals</b>	<b>37,762</b>	<b>\$ 719,310</b>	<b>\$ 1,347,201</b>	<b>\$ 1,296,198</b>	<b>\$ 2,136,876</b>	<b>\$ 2,136,876</b>	<b>\$ 5,569,949</b>	<b>\$ 1,580,000</b>	<b>\$ 2,820,000</b>

<sup>1</sup>Not currently part of NM Microsoft licensing consortium - quantities are estimates based on available faculty/staff data.

<sup>2</sup>Elected not to participate in cybersecurity proposal - included with same funding formula for planning/discussion purposes.



# Controlled Unclassified Information (CUI)

- CUI Information System Vulnerability Information (CUI-ISVI) contained in this document may not be disclosed to other individuals or entities without prior authorization. Individuals to whom access to CUI-ISVI is granted, must have a strict need-to-know such information in order to safeguard information and systems, and in order to comply with Executive Order 13556, “Controlled Unclassified Information,” and its implementing regulations (32 CFR Part 2000, 44 USC 3554, 44 USC 3555) pursuant to safeguarding information about information systems vulnerabilities that, if not protected, could result in adverse effects to information systems.



# True Stories in Higher Education

- Information Redacted from Presentation Material





# True Stories - Cybersecurity Incident

## **2025 Incident**

- Information Redacted from Presentation Materials



# HEI Cyber Security Service Needs

- One time and Recurring Funding (detail needed)
- Continue aligning effectiveness and efficiency efforts with CUP, NMICC, NMACC, HED, and DoIT, including aligned support for the CHECS cybersecurity proposal.
- Shared processes and tools
  - IT management tools to effect security improvements
    - Server and workstation security configurations and compliance checks
    - Security settings and tools for accounts and access
    - Security analysis/ auditing, and logging tools
  - To ideally prevent but to always detect malicious activity and attacks
- Shared resources and services
  - To prevent likely attacks by addressing legacy IT service risks
  - To enable timely response when attacks are first detected
  - To quickly contain and remediate attacks
- Find mechanisms to address funding gap between legacy IT environments (CAPEX) and contemporary Software/Infrastructure as a Service (OPEX), recurring and increasingly more expensive



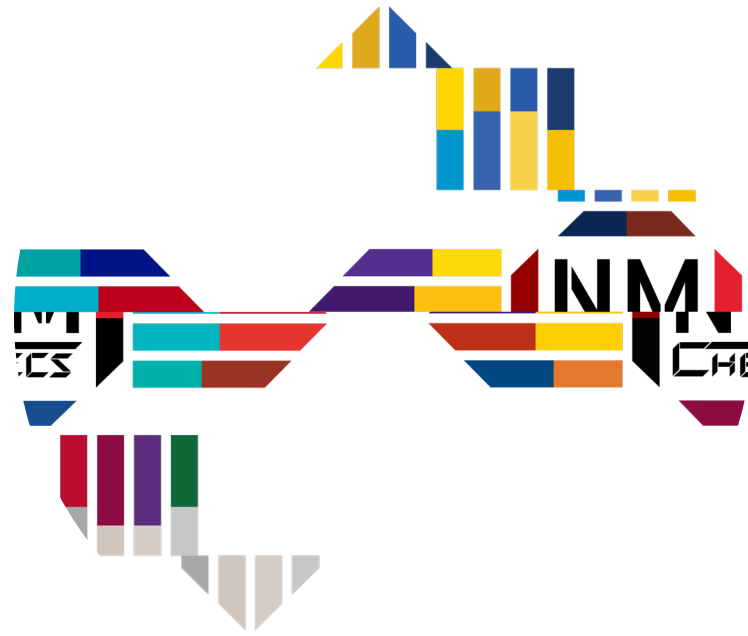
# Funding Proposal for Fiscal Year 2027 (Tentative) - ~\$6.5M/year for 2 years (\$13M)

- **Recurring Funding:** Ongoing funding to support funded recurring expenses, such as Microsoft licensing. **(6.5M)**
- **Microsoft Licensing:** Continued funding for Microsoft A5 Licensing **(\$2M)**
- **Security Awareness Training for Employees and Students:** Fund purchase of security training programs (e.g., SANS or similar) to educate employees and students on best practices and phishing prevention. **(\$300K)**
- **Enhanced Microsoft Support (Unified Support):** Request funding for additional support resources to ensure rapid incident response across Microsoft services. **\$2M)**
- **Security Staffing:** Funding for (a) staff augmentation and (b) permanent positions to strengthen cybersecurity capabilities. Utilize for proactive security functions and ongoing initiatives, not primary incident response (continue to leverage DoIT's security partners as needed). **(\$2.2M)**
- **Cyber Insurance:** Request funding to secure cyber insurance, providing access to critical services during incidents at preferred rates. **(TBD)**
- **REN-ISAC Membership (or similar service):** Fund access to threat intelligence, alerts, and collaborative security resources tailored to higher education. **(30K)**
- **Cybersecurity Budget Allocation:** Request base funding for each institution to address urgent needs, close security gaps, and ensure compliance. Recommendation: 10% of IT budget for general cybersecurity, plus 3% for compliance. **(TBD)**



# Operational Next Steps

- Implement Microsoft A5.
- Finalize special appropriations request for Legislative consideration in CY 2026.
- Continue collaborations/coordination across HEI's, HED, and DoIT.
- Coordinate on approaches for recurring Cyber Security requests.



- Closing comments from our partners
- Questions from the Council