THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and Compliance

October 21, 2020 at 11:00 a.m.
Via Videoconference and UNC-TV Live Stream
University of North Carolina System Office
Center for School Leadership Development, Board Room
Chapel Hill, North Carolina

AGENDA

A-1. Approval of the Minutes of September 16, 2020 ..... Mark Holton

A-2. UNC System Office Chief Information Security Officer Update ..... Kevin Lanning

A-3. MCNC Security Services Update ..... Tracy Doaks and Chris Beal, MCNC

A-4. Update on UNC System Public Safety Training Center ..... Brent Herron

A-5. Adjourn

DRAFT MINUTES

September 16, 2020
Via Videoconference and UNC-TV Live Stream
University of North Carolina System Office
Center for School Leadership Development, Room 128
Chapel Hill, North Carolina

This meeting of the Committee on Audit, Risk Management, and Compliance was presided over by Chair Mark Holton. The following committee members, constituting a quorum, were also present: Pearl Burris-Floyd, James L. Holmes, Jr., Terry Hutchens, Wendy Floyd Murphy, and Art Pope.

Pearl Burris-Floyd joined the meeting by phone at 12:24 p.m.

Chancellors participating were Nancy Cable and Sharon Gaber.

Staff members present included Lynne Sanders, Thomas Shanahan, and others from the UNC System Office.

---

1. Call to Order and Reading of Conflict of Interest Statement (Item A-1)

The chair called the meeting to order at 12:18 p.m., on Wednesday, September 16, 2020, and read the Conflict of Interest Statement. The chair then called upon Lynne Sanders to read the roll.

2. Approval of the Minutes of July 22, 2020 (Item A-2)

The chair called for a motion to approve the open session minutes of July 22, 2020.

MOTION: Resolved, that the Committee on Audit, Risk Management, and Compliance approve the open session minutes of July 22, 2020, as distributed.

Motion: Art Pope
Motion carried

Roll Call Vote	
Holton	Yes
Burris-Floyd	Absent for vote
Holmes	Yes
Hutchens	Yes
Murphy	Yes
Pope	Yes

3. Presentation of OSA Audit Report (Item A-3)

Chair Holton welcomed State Auditor Beth Wood, who then shared the results of the Office of State Auditor's (OSA) information systems audit report dated September 2020. The OSA audit identified a deficiency related to the development and issuance of guidance for IT governance and a recommendation for improvement. The committee has requested the UNC System Office to implement corrective action by December 31, 2020.

This item was for information only.

4. Annual CARMC Report (Item A-4)

The chair called on Ms. Sanders to present to the committee for approval the annual report on the activities of the Committee on Audit, Risk Management, and Compliance for fiscal year 2019-20. The report for July 1, 2019, through June 30, 2020, required a vote by the committee to accept the report for submission to the Board of Governors.

MOTION: Resolved, that the Committee on Audit, Risk Management, and Compliance approve the Annual Report of CARMC for 2019-20 and accept the report for submission to the Board of Governors.

Motion: James L. Holmes, Jr.
Motion carried

Roll Call Vote	
Holton	Yes
Burris-Floyd	No response/technical difficulties
Holmes	Yes
Hutchens	Yes
Murphy	Yes
Pope	Yes

5. Summary Report of Associated Entities (Item A-5)

Ms. Sanders presented the annual summary report of the University's major Associated Entities. Across 89 Associated Entities that required annual audits for fiscal year ending June 30, 2019, five had audit findings reported by the external auditors.

This item was for information only.

6. Implementation of Insurance Policy Status Update (Item A-6)

Ms. Sanders presented to the committee an update on the implementation of the Policy on Insurance Coverage. The System Office is directing efforts towards policy implementation to include updating property records and valuations, defining limited exceptions, and establishing the process for conducting reviews of requests for limited exceptions. Great progress has been made towards implementation of the policy with the assistance of the risk managers at the constituent institutions and the Department of Insurance.

This item was for information only.

7. Update on OSA Federal Compliance Audits (Item A-7)

Ms. Sanders provided the committee with a status update on the federal compliance audit findings across three of the constituent institutions, which was reported by the Office of the State Auditor in May. Based on follow up work in response to the internal audit, each of these institutions has made satisfactory progress towards implementing corrective actions.

This item was for information only.

8. Update on UNC System Public Safety Training Center (Item A-8)

The chair called on Brent Herron to present an update to the committee on the UNC System Public Safety Training Center. The onsite training courses for the 17 UNC System Campus police departments began on July 13, and future training courses have been scheduled.

The committee also welcomed the new Senior Associate Vice President for Safety and Emergency Operations, Fred Sellers.

This item was for information only.

9. Adjourn

There being no further business, the meeting adjourned at 12:55 p.m.

_____

Terry Hutchens, Secretary

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and Compliance
October 21, 2020

AGENDA ITEM

A-2. UNC System Office Chief Information Security Officer Update ..... Kevin Lanning

Situation: Every day we hear about new cybersecurity incidents, including at universities. Periodic updates to the Board of Governors on this topic are prudent and are also required by policy.

Background: The UNC System has taken a variety of actions over the years to respond.

Assessment: Attacks originate from a wide variety of sources and are persistent, occurring 24x7x365.

Action: This item is for information only.

Cybersecurity Landscape, Challenges & Higher Education Strategy

Kevin Lanning

UNC System Office
Chief Information Security Officer

2020

Information Security

Threats, Challenges & Strategy

BACKGROUND

We hear about cybersecurity incidents every day. The UNC constituent institutions experience a steady stream of attacks. Our mission requires openness and collaboration. We cannot build a digital fortress. Intruders can leverage our openness. We have a strong community of CIOs, CISOs and other partners. MCNC has been a longstanding, trusted partner and is at an ideal physical location to support us.

Threats, Challenges & Opportunities

Information Security Landscape

Threats

- Social Engineering
- Password theft
- Malware
- Hacking
- Business disruption
- 3rd party supplier compromise

Challenges

- An emphasis on functionality
- Openness
- Collaboration
- Network borders
- Relentlessness
- Cloud/s
- Device ownership

Our Strategy

- Understand and support the business
- Prioritize risks
- Focus protections on prioritized assets
- Defense-in-Depth
- Assessments
- Continuous improvement
- Manage the risk

Threat Vectors

- Social engineering, phishing & credential theft
  - Emails with malicious attachments and links to malware
  - Password reuse
  - Weak encryption
- Malware scenarios (e.g., ransomware)
  - Business disruption
  - Monetize via leak extortion
- Hacking (e.g., nation-state actors, criminal networks)
  - Theft of Intellectual Property
  - Highly skilled, relentless, resourced
- Suppliers

Higher Education Challenges

- The culture tends to focus on availability & functionality
- Our mission requires collaboration & openness
- Rules of engagement
- We don’t own student computers
- We tend to have huge network pipes
- Less standardization
- Supplier assessments
- Complex compliance space with multiple laws, standards & regulations
- Need sustainable funding model for cyber security

Strategy, Tactics & Operations

- Social engineering & phishing
- Training, policies, standards & procedures in place to clarify & direct (e.g., 1400.3, ISO 27002 best practices, NIST)
- Weave security into the business
- Sensitive information inventory & lifecycle
- Suppliers-assessments, audits & contracts
- Team with cyber defender partners

Strategy, Tactics and Operations (cont'd)

- Automate leveraging tools like behavioral analytics & AI to predict & manage
  - Detect
  - Respond
  - Learn
- Defense-in-Depth design
- Tabletop exercises
- Metrics to support continuous improvement
- Assessments & penetration tests to validate

Information Security Risk Management

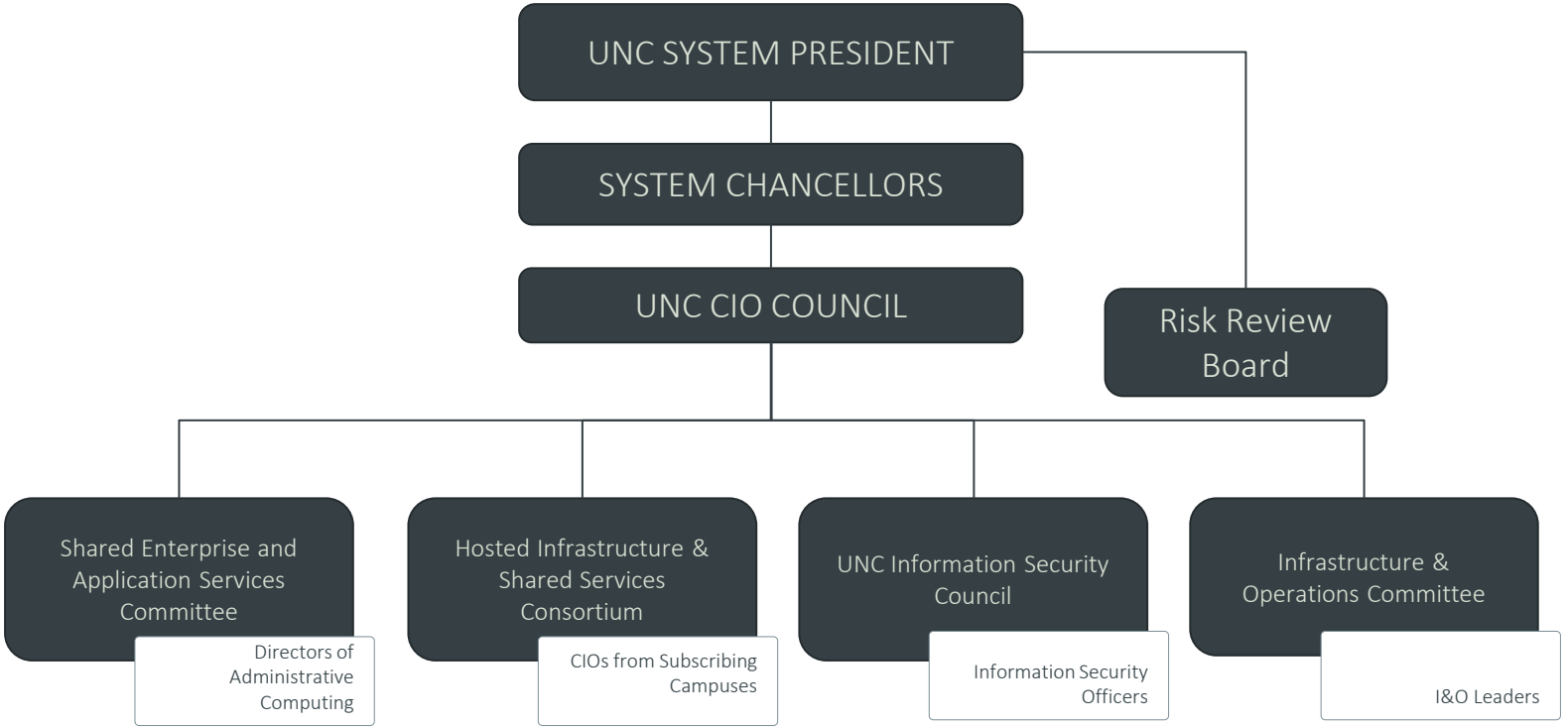
Prioritization, Mitigation, Management

ISO 27002 Best Practices
ISO 27005 Risk Management

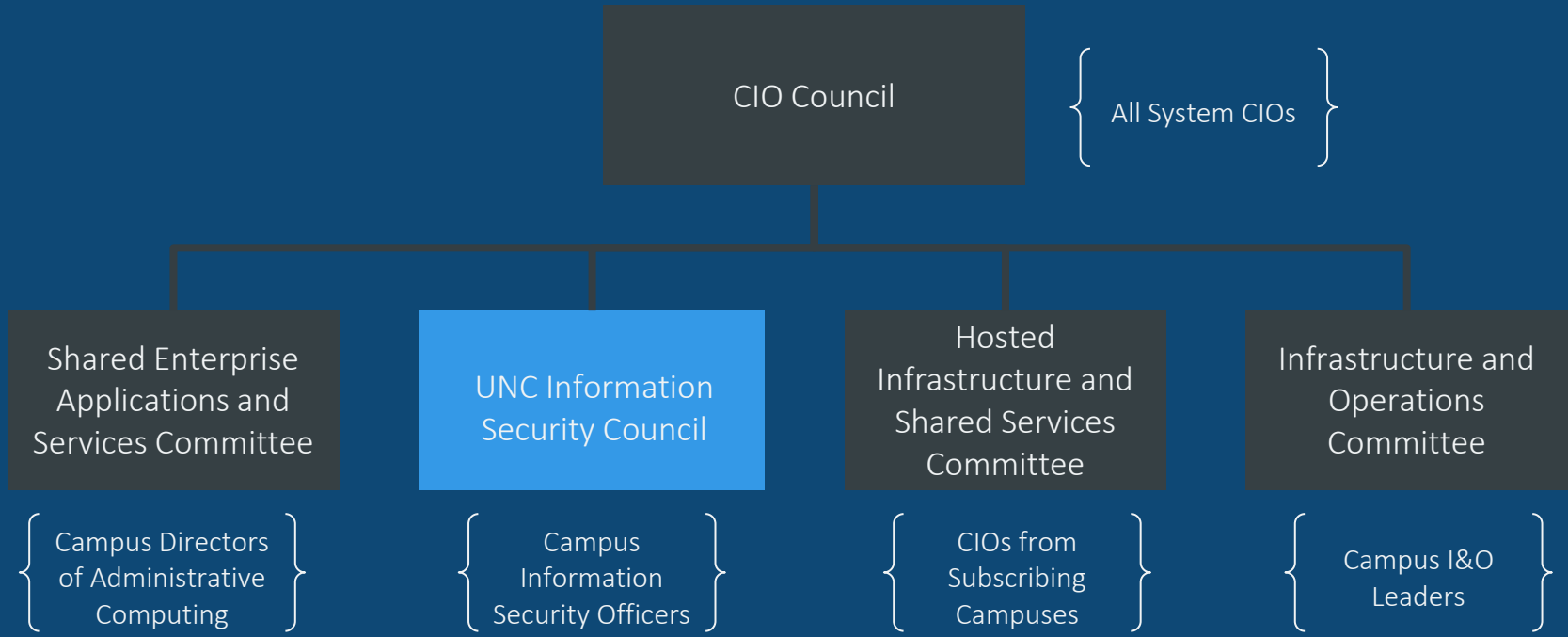
- Focus on business needs & risks
- Prioritize-what are the highest impact AND likelihood threat vectors?
- Manage in ranked priority order
- Options for dealing with highest ranked risks?
- Commit to strategies, tactics & operational approaches
- Align approach with resources. Leverage opportunities for efficiencies
- Lather, rinse & repeat for continuous improvement…

IT Governance Overview

(UNC System Governance Reporting to Board of Governors)



CIO Governance



Higher Education Cybersecurity Landscape

Closing and Q&A

Our request to visit with you again soon!

2020

Keith Werner
UNC System Office CIO

Kevin Lanning
UNC System Office CISO

Background & Summary

Threats

Challenges

Strategy

Closing and Q&A

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and Compliance
October 21, 2020

AGENDA ITEM

A-3. MCNC Security Services Update..... Tracy Doaks and Chris Beal, MCNC

Situation: NC's higher-education institutions increasingly rely on access to technology as a key driver for growth, innovation, and success. Increased reliance on these digital resources means that organizational success depends on an ability to adequately protect these resources. Organizations that cannot implement and operate effective cybersecurity protections will find it difficult to succeed in their mission to educate and serve the citizens of NC.

Background: K-20 education institutions in NC are increasingly under cyber-attack. These attacks range from cyber criminals conducting ransomware attacks to extorting money, to nation-state actors looking to steal cutting edge intellectual property from our state's research universities.

Assessment: Most organizations in our community do not have adequate access to the resources and expertise required to maintain effective cyber defenses. MCNC has a long history of partnering with NC's education community to deliver cost-effective solutions to solve tough technology challenges. MCNC offers cybersecurity solutions and partnership opportunities uniquely tailored to NC's education community.

Action: This item is for information only.

MCNC®

Connecting North Carolina to What's Next

MCNC develops and delivers high-quality Internet connectivity solutions and value-added technology services to propel our state forward.

Who Are We?

Founded in **1980** as a research institute to serve NC

Private, Non-Profit Organization

501(c)(3)

A Public-Private partnership serving education in NC

Who Do We Serve?

Our Community

MCNC provides network services to more than 850 anchor institutions in all 100 counties, helping to power every sector of North Carolina's economy.

- Colleges & Universities
- Community Colleges
- K-12 Schools
- Healthcare Institution
- Libraries
- Governments
- Cultural Institutions
- Electric Cooperatives
- Nonprofits
- Public Safety
- Research Institutions
- Agriculture Research & Co-ops

What Do We Do?

MCNC®

CONNECTIVITY

SECURITY

CONSULTING

DATA CENTER

COLLABORATION

MCNC Fiber Footprint

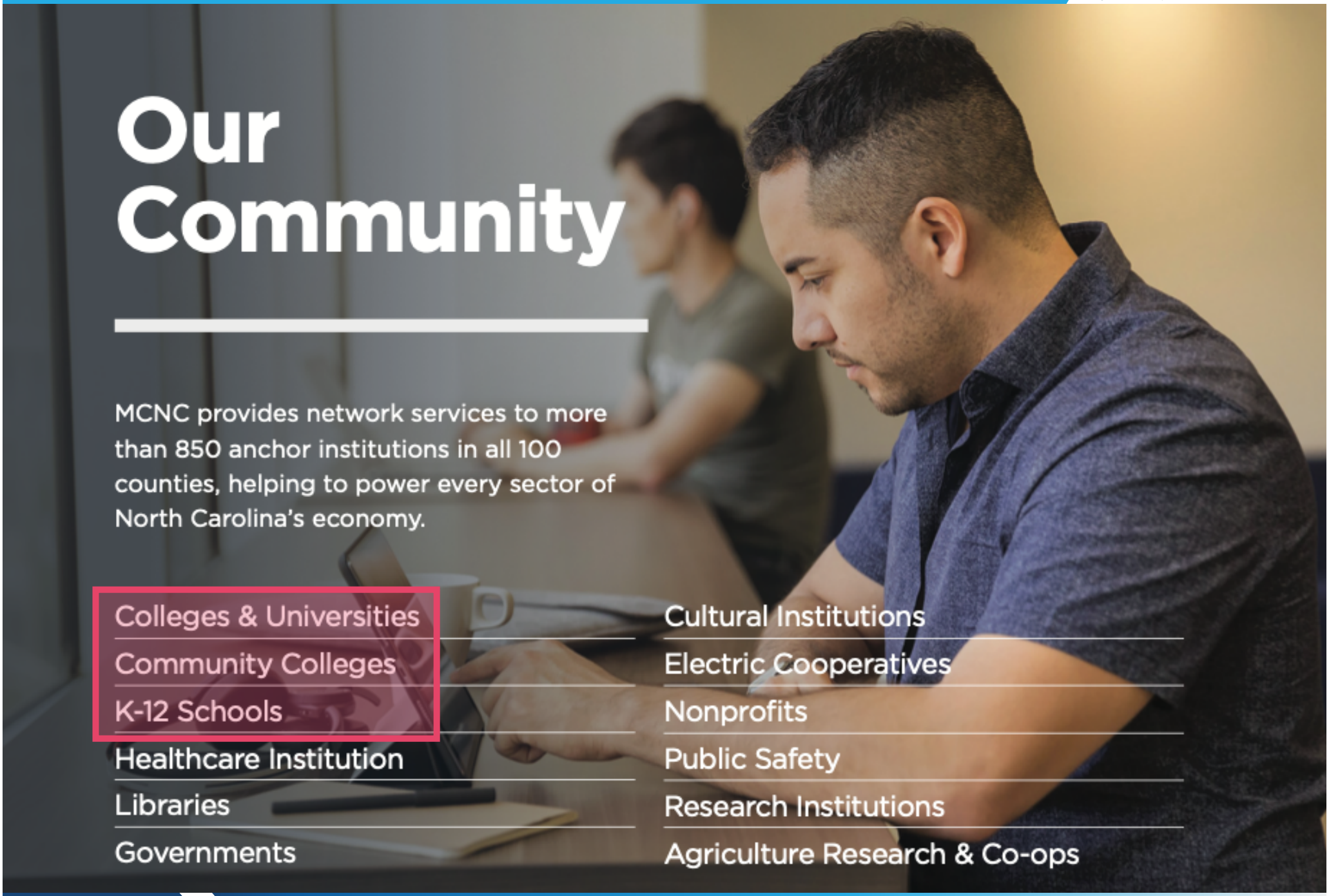
NCREN – The North Carolina Research and Education Network

LEGEND

- MCNC Fiber
- MCNC Co-location Facility
- MCNC Fiber (Triangle Ring)
- City

As of July 2020

Who Do We Serve?

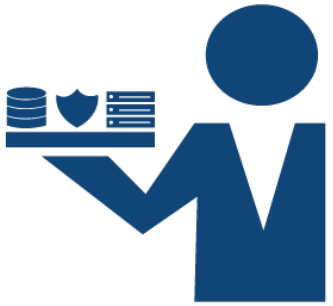


Our Community

MCNC provides network services to more than 850 anchor institutions in all 100 counties, helping to power every sector of North Carolina's economy.

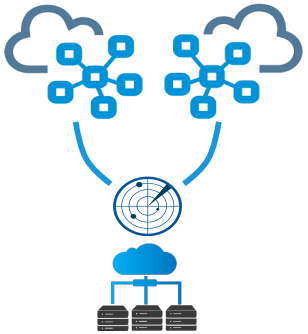
- Colleges & Universities
- Community Colleges
- K-12 Schools
- Healthcare Institution
- Libraries
- Governments
- Cultural Institutions
- Electric Cooperatives
- Nonprofits
- Public Safety
- Research Institutions
- Agriculture Research & Co-ops

MCNC Security Services

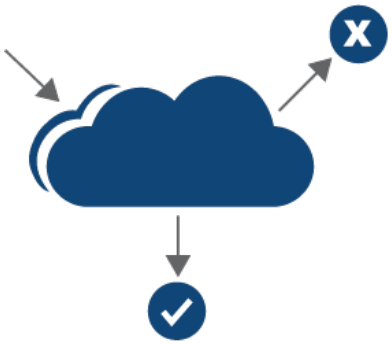


Security Consulting

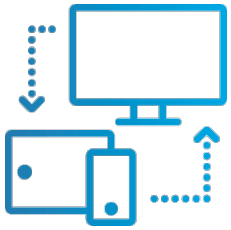
DDoS Protection



Active Vulnerability Analysis



Web Security



Secure Application Access

DNS Security Filtering

Security Advisory Consulting Services

Cybersecurity Program Assessments

Risk Assessments

Audit Finding Remediation

Application / System Security Testing

Security Policy Creation

Security Technology Evaluation

Staff Augmentation (Virtual CISO)

The Challenge

Reliance on Technology

Our community of K-12, higher-ed, and healthcare institutions increasingly rely on access to technology as the key driver for growth, innovation, and success.

Increased reliance on these digital resources means that organizational success depends on an ability to adequately protect these resources.

Security Is Essential to Success

Organizations that cannot implement and operate effective cybersecurity protections will find it difficult to succeed in their mission to educate and serve the citizens of NC.

The Struggle is Real

Most organizations in our community do not have adequate access to the resources and expertise required to maintain effective cyber defenses.

Cybersecurity skills are in high demand and institutions struggle to attract and retain strong talent.

Existing cyber defense technology is too expensive.

Organizations do not have enough people to respond to alerts generated by existing tools.

Legacy systems and approaches hamper defense efforts.

The Opportunity

MCNC can leverage its advanced technology, considerable cybersecurity expertise, the NCREN network, and economies of scale to develop and implement Managed Security Services that help our community address modern cyber threats.

We are not motivated to profit from the challenges of the community. We are motivated to leverage our strengths to help our community address hard cybersecurity challenges.

We can help our community address these challenges in ways that they cannot easily accomplish on their own.

Our Vision

Achieving the Vision

1. Design and implement a full suite of Managed Security Services to Protect, Detect, and Respond to cybersecurity threats on behalf of our community.

2. Centrally housed at MCNC to leverage the vantage point of NCREN – the statewide education backbone network.

3. Achieve economies of scale to provide world-class cybersecurity protection to all of NC's education community.

Thank You!

MCNC®

Connecting North Carolina to What's Next

MCNC develops and delivers high-quality Internet connectivity solutions and value-added technology services to propel our state forward.

THE UNIVERSITY OF NORTH CAROLINA SYSTEM

MEETING OF THE BOARD OF GOVERNORS
Committee on Audit, Risk Management, and Compliance
October 21, 2020

AGENDA ITEM

A-4. Update on UNC System Public Safety Training Center..... Brent Herron

Situation: The UNC System, in partnership with the Department of Public Safety (DPS) Samarcand Training Academy, will offer a series of training courses and activities for public safety personnel from UNC System institutions.

Background: Each institution in the UNC System maintains a public safety department staffed by sworn officers and headed by a police chief. In addition to performing traditional law enforcement functions, University law enforcement officers require specialized training and skills to work in and meet the unique public safety needs of the academic communities in which our students, faculty, and staff collaborate and interact. A UNC System study conducted during 2019 identified joint training programs as one area of potential collaboration between and among UNC System public safety departments. The DPS Samarcand Training Academy provides excellent facilities in a central location conducive to facilitating joint training programs.

Assessment: The UNC System Public Safety Training Center is fully engaged with staff from the Samarcand Training Academy to conduct in-service training for the 17 UNC System campus police departments. An on-site UNC System training coordinator, under the supervision of the associate vice president for Campus Safety & Emergency Operations at the UNC System Office, has been hired to fill the role on a temporary basis for one year. In-service training courses began effective July 13, 2020. At this time, the following courses have been scheduled or are in the planning stage: Response to Sexual Assault for Law Enforcement, Orientation for UNC System Campus Training Coordinators, Civil Disturbance Train the Trainer Course, and Impartial and Non-Biased Policing.

Action: This item is for information only.