STATE BOARD OF COMMUNITY COLLEGES
Cyber Security Update – November 2024

The quarterly Cyber Security report to the Audit and Compliance (AUD) Committee, unless noted, covers agency activities to-date since the last AUD report. The summaries below are separated into two categories: System Office and Enterprise/System-wide efforts.

System Office

Cybersecurity and Awareness Training (Calendar Year/Year-to-Date)

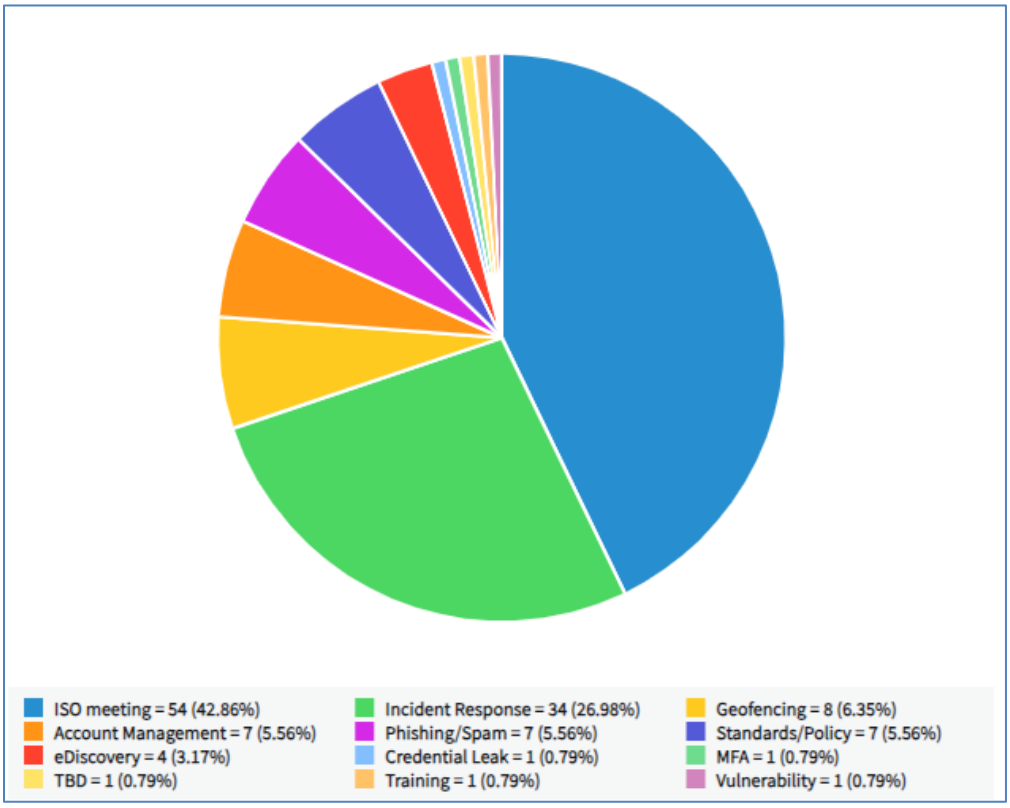
NC Department of Information Technology (NCDIT) Enterprise Security & Risk Management Office (ESRMO) assigns mandatory training for all State employees.
The State's required standard for completion is 95%. As of Oct. 28th, the System Office has an overall 91.46% rate of completion for assigned training YTD. The drop in percentage from the previous reporting is due to new training (highlighted in yellow) being assigned on Oct. 1st that is still within the allowed timeframe.
The modules assigned thus far are:

Training Module Title	Completed
Cyber Security: 2024 Security Awareness Training	62.05%
Cyber Security: 2024 Social Engineering Red Flags	99.52%
Cyber Security: AI Chatbots: Understanding Their Use, Risks, and Limitations in the Workplace	97.69%
Cyber Security: How To Behave: Protecting Sensitive Information	100.00%
Cyber Security: Security and Disaster Preparedness	94.12%
Privacy: Controlled Unclassified Information (CUI)	62.78%
Privacy: Family Educational Rights and Privacy Act (FERPA) Overview	94.57%
Privacy: Privacy vs Security - What's the Difference?	100.00%
Privacy: Remote Work: Keeping It Private	100.00%
Privacy: Restricted Intelligence Privacy Edition S1 Ep2 – Nobody Reads That Stuff (Privacy by Design	94.12%
Privacy: Restricted Intelligence Privacy Edition S1 Ep6 - Partners (Third Party Partners) (2024)	99.52%
Privacy: Security Bytes: PII	100.00%
Privacy: Staying Safe in the Cloud	64.57%
Privacy: The Fair Information Practice Principles v2	98.08%
Privacy: The Value of Data	100.00%
Privacy: The What, Why, and How of Data Privacy (2024)	100.00%
Privacy: The What, Why, and How of HIPAA	99.52%
Grand Total	**91.46%**

ISO Team Engagement Overview Since August AUD Report:

- Following the impact of Hurricane Helene, the ISO team assisted in tracking the impact of the 14 impacted colleges. Additional assistance was provided to Patrick Fleming in identifying a strategy to deploy Starlink 'kits' to impacted colleges to support and augment critical communication needs.

- For the last three months, the ISO team has completed 126 engagements with colleges. The chart below is the breakdown of those 126 engagements. Of note, each engagement may include support from multiple ISO team members.



- October was Cybersecurity Awareness Month 2024, and the ISO team conducted two townhall style sessions focusing on cybersecurity in their personal lives. Those sessions focused on the four main themes of CAM2025, which are:
    - Strong Passwords and Password Management,
    - Using Multi-Factor Authentication,
    - Recognizing and Reporting Phishing and Social Engineered Attacks and
    - Maintaining software on all devices.
- ISO Team attended the Fall IIPS Conference and provided sessions on the following topics:
    - General Session: Tabletop Exercise (TTX) Incident Response game called Backdoors and Breaches.
    - 3rd Party Vendor Risk Management
    - Birds of a Feather - Open Security Office Hours
    - CIS Controls 3: Data Protection
    - Cybersecurity Maturity Model Certification (CMMC)
    - CIS Controls Self-Assessment Tool (CIS CSAT)
- Since the previous Cybersecurity AUD report the ISO has shared 22 email notices on threat alerts, exploited vulnerabilities, training opportunities and other cybersecurity information.
- In mid-August, the ISO started getting reports of bogus student applications and appeared to be applying for Pell Grants. In total 18 colleges reported bogus applications. Examples of

Indicators of Compromise (IoCs) were shared with multiple constituent groups systemwide. Additionally, information regarding the bogus applications was provided the FBI Internet Crime Compliant Center (IC3) for tracking. Currently the best defense against these bogus applications is for the registrars and admissions officers to include manual review processes of new applications and to be vigilant of any inconsistencies in the application that may indicate that it is fraudulent.

Rural College Broadband Access – Third party security assessments conducted in partnership with Accenture for the 28 participating colleges and the System Office. This effort will run through December 2024.

- Functional Controls Assessment Status – 19 schools and NCCCS completed, 5 scheduled, remaining 3 to be scheduled after August.
- Functional Phishing Test – 22 Colleges Phished, Completed in April. Results have been provided back to the College IT Staff.
- Technical Assessments will include External Vulnerability Scans and Penetration Testing planned for June/July and Internal Vulnerability Scans planned for August.
    - All 27 schools and NCCCS had scans in preparation for external Pen-Testing
    - External Pen-Test scheduled to begin July 15th.
- Resiliency Testing – 2 Schools with different but common infrastructure/systems
    - In process, began July 1st.
- Internal Pen Testing –
    - Begin collecting information from colleges in mid-August.
    - Both credential and non-credential testing
- Wi-Fi testing
    - 4 Schools to be tested in October (work in progress)
    - NCCCS Office to be tested at the end of September.
- Web Scans
    - Work in progress.

State and Local Cybersecurity Grant Program (SLCGP) - State and Local Cybersecurity Grant Program | NC DPS

- The FY23 SLCGP Federal Award for North Carolina is projected to be approx. $10.8 million. State match/cost share is projected to be another $2.7 million for a total of approx. $13.5 million (less management & administration costs) to be awarded to state, tribal and local govt. entities, including Community Colleges.
  42 College submitted applications for the FY23 SLCGP. There were 121 total applications submitted statewide.
- On Oct 10th, the SLCGP Committee started communicating awards to applicants.
    - 34 Colleges were identified to receive awards of up to $200,000.00. Some award offers were less based on college funding requests or exclusion of some elements of the application.

- Total award potential for the colleges is approximately $5,175,716
- The list of colleges and the exact grant funding levels are confidential until all awards have been accepted.

Contact(s)

Stephen S. Reeves
AVP, Chief Information Security Officer

Deante Tyler
AVP, Chief Technology Officer