STATE BOARD OF COMMUNITY COLLEGES
Cyber Security Update – March 2026

The quarterly Cyber Security report to the Audit and Compliance (AUD) Committee, unless noted, covers agency activities to date from the last October 2025 AUD report.

State and Local Cybersecurity Grant Program (SLCGP) – Information Only
The State and Local Cybersecurity Grant Program provides funding to eligible entities to address cybersecurity risks and threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments. The NC SLCGP grant opportunity is now in the final year of a four-year process.

For Fiscal Year 2025 SLCGP, North Carolina was awarded approximately $2,150,994 in federal funds for local government & community college subrecipients. FO FY25 applications, there is a 40% required match/cost share for each subrecipient. The NC FY25 SLCGP application process completed on November 30, 2025, and there were a total of 37 local government and community college applications.

FY25 SLCGP Status:
As of Jan. 16th, recommendations for award have been routed to Emergency Management Executive Management for approval. Once approved, the final project worksheet will be sent to Federal Emergency Management Agency (FEMA) for final approval.

Community Colleges represented 8, or 44.4%, of the total 18 identified awardees. Final totals for awards and the specific colleges identified to receive awards are pending FEMA approval. Additional details can be found at https://www.ncdps.gov/SLCGP

Fraudulent Student Applications – Information Only
The information below is a continuation of reporting based on previously reported information regarding Fraudulent Student Applications activities.

One challenge of tracking potentially fraudulent applications was having a consistent methodology that each college can use that will flag accounts and provided reporting to the System Office Data Warehouse.

On Feb. 6, the System Office Programs and Student Services team provided information regarding a new process that provides a new system-wide workflow to assist colleges and the System Office staff in identifying potential bogus records locally and across our system.

The System Office Information Security Office continues to receive Incidents identifying suspicious/known fraudulent applications. The information provided is cross matched with other colleges with similar applications, which is then reported back out with a recommendation to re-verify those applications for enrollment.

The System Office team continues to collaborate with partners from College Foundation North Carolina, College Foundation Inc, UNC and colleges on strategies to address bogus applications at the Residency Determination Service touch point.

On March 3, partners with the College For North Carolina and College Foundation Inc., demonstrated programmatic processes that are currently in development to identify potentially fraudulent applications prior to being sent to colleges. This development is ongoing but represents an opportunity to screen applications early in the process and reduce redundancy of work currently being conducted at all colleges.

College Hosted Cybersecurity Training Opportunity with NC Dept. of Public Safety/Emergency Management and Texas A&M Engineering – Information Only

On Jan. 15, the ISO team shared with college IT Leadership and Security Liaisons an opportunity for colleges to host one or two days, in-person, instructor lead, cybersecurity training from Texas A&M Engineering (TEEX). These training opportunities are FEMA funded, offered at no cost and available to college faculty, staff, students and the general public. Offering these courses represents an excellent opportunity for colleges to support the maturing of their local community's cybersecurity posture.

Colleges electing to host one of these events are only asked to provide facilities for the training.

The sharing of this announcement with Academic leaders was encouraged for broad awareness.

The following courses are part of the offering:
AWR-136 – Developing Cybersecurity Resiliency for Everyone (8 hrs.)
AWR-376 – Understanding Targeted Cyber Attacks (8 hrs.)
MGT-384 – Preparing for Cyber Attacks & Incidents (16 hrs.)
MGT-452 – Physical and Cybersecurity for Critical Infrastructure (8 hrs.)

College scheduling is on-going, but as of March 5, hosting colleges currently include Bladen CC, Blue Ridge CC, Durham Technical College.

Additional information can be found at Cybersecurity | TEEX.ORG

Contact(s)
Stephen S. Reeves
AVP, Chief Information Security Officer