

STATE BOARD OF COMMUNITY COLLEGES
Cyber Security Update – October 2025

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

State and Local Cybersecurity Grant Program (SLCGP) – Information Only

Direct link to North Carolina SLCGP website: <https://www.ncdps.gov/SLCGP>

Historical Notes:

- The SLCGP program is administered by the Department of Public Safety. The System Office Chief Information Security Officer is a voting member of the committee supporting the identification of grant recipients.
- 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.
 - o 42 College submitted applications for the FY23 SLCGP. There were 121 total applications submitted statewide.
 - o 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.
 - o Total award potential for the colleges is approximately \$5,175,716
 - o The list of colleges and the exact grant funding levels are confidential until all awards have been accepted.

FY 24SLCGP Status:

- FY24 SLCGP Funds allocated to the State are approximately \$8,037,374
- The maximum amount eligible applicants may apply for has increased to \$250,000 for FY24 SLCGP.
- For FY24, there is a required 30% match that must be funded by the applicant organization. This is explained in greater detail in the Match/Cost Sharing section on the NC SLCGP webpage.
- The last week of September FEMA approved the State's FY24 SLCGP Project Worksheet. The NC Emergency Management team is in the process of sending out award and declination notifications for the week of Oct. 6th. The specific details of number of colleges and amounts of aware are pending.

Fraudulent Student Applications – Information Only

This topic was previously reported on. The discovery of suspicious and known fraudulent student applications is an on-going process.

The types of fraud include, but are not limited to, launching general phishing attacks, Fake Jobs phishing, Pell Grant fraud, Credit Card Fraud and other types of financial fraud.

Historical Actions:

- ISO Team partnered with Department of Education, Office of Inspector General, for two (2) webinars on Fraud Awareness.

- Webinars were held on May 22nd and June 18th.
- The webinars had 316 total attendees, representing 54 of our 58 community colleges
- Dr. Monty Hickman and ISO team are collaborating with College for North Carolina (CFNC) and the College Foundation Incorporated (CFI) on strategies that may augment the Residency Determination Service (RDS) with the ability to identify, reduce or eliminate fraudulent applications prior to being sent to colleges. This work is in the early stages. Planning is underway for collaboration on drafting a Request for Information (RFI) to determine what 3rd party may solutions exist that can address this challenge.
- In response to this national issued, on June 6, the Department of Education, Federal Student Aid, published Electronic Announcement (APP-25-16) [Significant Actions to Prevent Fraud through Identity Verification](#).
 - Changes to the types of documentation schools are required to maintain and steps to take if fraud is detected.
 - Requires additional verification steps of student identify prior to grant funding award.
- The Data Warehouse Team have developed a process to determine if college identified suspicious students accounts are present at other colleges. This process is intended to assist colleges in validating local determinations and identify other colleges who may have applications that need additional scrutiny and actions.
- From July 1 to Oct 2, 2025, the colleges reported, and ISO and Data Warehouse Teams have reviewed:
 - 1213 unique identified suspicious or known fraudulent student accounts
 - All 58 colleges had some element of identified suspicious or fraudulent student account.
 - In discussion with the Department of Education, Office of Inspector General, the recommendation is to focus on Academic Year 2025 and forward.
- This is a system-wide problem that requires each individual college to address the issue locally as a team, Registrars, Student Services, Instructors and IT.

Contact(s)

Stephen S. Reeves

AVP, Chief Information Security Officer

**STATE BOARD OF COMMUNITY COLLEGES
Cyber Security Update – October 2025**

REPORT SUMMARY

State and Local Cybersecurity Grant Program (SLCGP)

The applications for the FY24 SLCGP have been submitted to FEMA and were approved the last week of September. NC Emergency Management team is in the process of sending out award and declination notifications.

Fraudulent Student Applications

Fraudulent student applications involving various types of financial fraud, including Pell Grant and credit card fraud are being identified in greater numbers. In response, the team is collaborating with the Department of Education's Office of Inspector General, CFNC/CFI and additional System Office leadership to explore remediation strategies. Meanwhile, the Data Warehouse Team has developed a process to identify whether suspected fraudulent student accounts are active across multiple colleges. The Department of Education issued new guidance requiring stricter identity verification and documentation protocols to combat fraud. Addressing this issue requires coordinated local efforts involving Registrars, Student Services, Instructors, and IT teams at each college.