

STATE BOARD OF COMMUNITY COLLEGES
Cyber Security Update – October 2026

State and Local Cybersecurity Grant Program (SLCGP)

The State and Local Cybersecurity Grant Program (SLCGP) provided funding opportunities to eligible state, local, and tribal government entities to strengthen cybersecurity capabilities and address risks to information systems. The North Carolina SLCGP program concluded in FY2025, and as of the date of this report, no additional federal funding has been announced for future SLCGP award cycles.

During the FY2025 grant cycle, eight community colleges were identified as potential award recipients, representing 44.4% of the eighteen organizations selected for funding consideration statewide.

Identified recipient colleges are eligible to receive various portions totaling approximately \$806,000 in funding from the estimated \$2.1 million total award pool. Award offer letters were distributed to participating colleges in mid-August to facilitate project planning and implementation.

These grant awards have helped advance cybersecurity maturity across participating colleges by supporting initiatives designed to strengthen security controls, reduce cyber risk, and enhance the protection of institutional information systems and data assets.

Fraudulent Student Applications

Since March, the System Office has strengthened its efforts to identify and prevent fraudulent student applications through enhanced collaboration between the System Effectiveness, Student Programs, and Information Security teams. New registration processes within Colleague now allow colleges to flag suspicious and confirmed fraudulent applications. These indicators are replicated to the Data Warehouse, enabling the Information Security Office (ISO) to identify matching identities across institutions and proactively notify colleges of potentially fraudulent applications that have not yet been flagged. This capability has improved system-wide fraud detection and continues to be refined.

In April, Federal Student Aid (FSA) introduced a Real-Time Fraud Detection process that categorizes applications by risk level. Applicants identified as high risk are required to complete an interactive identity verification process, providing an additional layer of protection against fraudulent enrollment activity.

The System Office remains actively engaged with key partners, including College Foundation of North Carolina (CFNC), College Foundation, Inc. (CFI), the University of North Carolina (UNC) System, and constituent colleges, to develop and implement coordinated strategies that reduce fraudulent application activity and strengthen the integrity of student registration processes across North Carolina's community colleges.

Contact(s)

Stephen S. Reeves
AVP, Chief Information Security Officer