ASSEMBLY HIGHER EDUCATION COMMITTEE

STATEMENT TO

ASSEMBLY, No. 817

with committee amendments

STATE OF NEW JERSEY

DATED: FEBRUARY 22, 2024

The Assembly Higher Education Committee reports favorably Assembly Bill No. 817, with committee amendments.

This amended bill requires public institutions of higher education to establish plans and procedures to enhance cyber security and prevent cyber attacks against the institution's information technology systems. Pursuant to the amended bill, the plans and procedures are required to address, at a minimum: system monitoring to identify potential cyber security risks and vulnerabilities; cyber threat assessment; techniques for mitigating risk and preventing cyber breaches; and response and recovery for cyber security incidents. The amended bill requires public institutions of higher education to regularly update their cyber security plans and procedures in order to reflect current technologies and information security techniques.

In connection with developing their cyber security plans, a public institution of higher education may consult with the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) regarding information and best practices on cyber security and data protection. The NJCCIC was established in 2015 by executive order as the State's central organization for cyber security information sharing and threat analysis.

Lastly, the amended bill requires a public institution of higher education to notify the New Jersey Office of Homeland Security and Preparedness of any cyber attack against the institution's information technology systems in a manner consistent with current law governing reporting of cybersecurity incidents. Pursuant to the amended bill, a phishing attempt, as defined in the amended bill, is not considered a cyber attack for the purposes of this notification. The amended bill generally defines a cyber attack as unauthorized access to electronic files, media, or data containing personal information. The amended bill stipulates that good faith acquisition of personal information by an employee or agent of the public institution of higher education for a legitimate purpose, or for a purpose authorized under State or federal law, is not considered a cyber attack, provided that this information is not used for a purpose unrelated to the institution or subject to further unauthorized disclosure.

This bill was pre-filed for introduction in the 2024-2025 session pending technical review. As reported, the bill includes the changes required by technical review, which has been performed.

COMMITTEE AMENDMENTS:

The committee amendments:

- define cyber attack, personal information, and phishing;
- remove the requirement that a public institution of higher education notifies the New Jersey Office of Homeland Security and Preparedness of a cyber attack within 24 hours and stipulates that this notification is to be conducted in a manner consistent with current law; and
- stipulate that a phishing attempt is not considered a cyber attack for the purposes of notification to the Office of Homeland Security and Preparedness as required under the bill.