NORTHWEST FLORIDA STATE COLLEGE

Memo

To: Board of Trustees

From: Dr. Devin Stephenson, President

Date: November 15, 2022

Re: Gramm-Leach-Bliley Act Cyber Security Briefing

On December 9, 2021, the Federal Trade Commission (FTC) published a rule amending the requirements for safeguarding customer information under the Gramm-Leach-Bliley Act (GLBA) (the Safeguards Rule). The Safeguards Rule has long established cybersecurity standards under which financial institutions, including all higher education institutions that participate in federal student financial aid programs authorized by Title IV of the Higher Education Act of 1965, as amended (Title IV), must maintain customer information.

As required by these changes, we will begin to deliver an annual report of our Information Security (IS) program status and compliance with the updated Safeguards rule.

The new components of the revised GBLA Safeguards rule can be categorized into the following eight areas, along with the associated compliance status of the NWFSC IS program:

1. Designation of a single qualified individual for program oversight.
   1.1. Status: Compliant
2. The foundational role of written risk assessment in the IS program.
   2.1. Status: In Progress - Existing risk assessment procedures had to be modified for the revised Safeguards rule, and an updated assessment is in progress.
3. Design of IS safeguards to control the specific array of assessed risks.
   3.1. Status: Compliant
4. Testing, monitoring, and iterative evaluation.
   4.1. Status: Compliant
5. Ensure IS personnel training and continuing education.
   5.1. Status: Compliant
6. Oversight and assessment of service providers.
   6.1. Status: Compliant
7. Written incident response plan.
   7.1. Status: Compliant
8. Mandatory reporting to the board of directors.
   8.1. Status: In Progress - Compliant as of 11/15/22

The NWFSC IS program is a robust and complex combination of procedures, training, active monitoring, and security controls that are frequently reviewed and updated. Additionally, while numerous security threats have been identified and thwarted, there were no successful data breaches in the previous calendar year.

Because of the sensitive nature, the details of this program must remain confidential. However, detailed, one-on-one IS briefings are available to all board members when requested through the President's office.