TIDEWATER COMMUNITY COLLEGE

STUDENT FINANCIAL ASSISTANCE PROGRAMS CLUSTER

FOR THE YEAR ENDED JUNE 30, 2025

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

We audited the Student Financial Assistance Cluster of federal programs administered by Tidewater Community College (Tidewater) for the year ended June 30, 2025. We found:

- proper recording and reporting of all transactions, in all significant respects, in Tidewater's accounting and financial reporting system and U.S. Department of Education's federal student financial assistance systems and the federal attachment submitted to the Department of Accounts (Accounts);

- two matters involving internal control and its operation necessary to bring to management's attention that also represent instances of noncompliance with applicable laws and regulations or other matters that are required to be reported; and

- ongoing corrective action with respect to the prior audit finding identified in the Findings Summary in the Appendix.

In the section titled "Audit Findings and Recommendations," we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audit as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and develop and appropriately implement adequate corrective actions to resolve the findings as required by Accounts in Topic 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendations.

-TABLE OF CONTENTS-

AUDIT FINDINGS AND RECOMMENDATIONS

Improve Reporting to National Student Loan Data System
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2018

Tidewater Community College (Tidewater) Registrar's Office staff did not report accurate and timely enrollment data to the National Student Loan Data System (NSLDS) for students that graduated, withdrew, or changed enrollment levels. Management did not establish effective monitoring controls and clearly define communication procedures between the Financial Aid Office and Registrar's Office to ensure staff follow established enrollment reporting procedures. As a result, for a sample of 50 students, we identified the following instances of noncompliance:

- Tidewater reported an inaccurate enrollment status for three students (6%);
- Tidewater reported an inaccurate effective date for nine students (18%);
- Tidewater did not report enrollment status changes timely for nine students (18%); and
- Tidewater inaccurately reported at least one campus or program-level field deemed critical for ten students (20%).

In accordance with Title 34 Code of Federal Regulations (CFR) § 685.309, an institution shall submit, in accordance with deadline dates established by the Secretary of Education (Secretary), other reports and information the Secretary requires and shall comply with the procedures the Secretary finds necessary to ensure the reports are correct. As further outlined in Education's NSLDS Enrollment Guide, institutions are required to certify enrollment every 60 days. The accuracy of Title IV enrollment data depends heavily on information reported by institutions. Tidewater's inaccurate and untimely enrollment data submissions to NSLDS can affect Education's reliance on the system for monitoring purposes. Noncompliance may also impact an institution's participation in Title IV programs.

Tidewater's management should strengthen its policies and procedures and enhance monitoring to ensure staff consistently adhere to the federal reporting requirements by reporting accurate and timely student enrollment status changes to NSLDS.

Implement Information Security Program Requirements for the Gramm-Leach-Bliley Act
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2020
Prior Title: Perform Risk Assessments as Required by Gramm-Leach-Bliley Act

Tidewater does not comply with certain elements of the Gramm-Leach-Bliley Act (GLBA) related to its information security program. Public Law 106-102, known as the GLBA, classifies institutions of higher education as financial institutions due to their involvement in financial assistance programs. Related regulations in 16 CFR §§ 314.3 and 314.4 require organizations to develop, implement, and maintain an information security program to safeguard customer information. Specifically, Tidewater does not comply with the following GLBA requirements:

- Although Tidewater's information security program requires the college to base the information security program on a risk assessment, Tidewater does not perform an annual review and update of three previously completed risk assessments as required by its information security program. As a result, Tidewater does not have up to date risk assessment information to evaluate and adjust its information security program. GLBA requires that Tidewater base its information security program on a risk assessment that "identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks." GLBA also requires Tidewater to adjust its information security program based on the results of the risk assessment. By not maintaining current risk assessments, Tidewater may not identify risks that pose a threat to the college's sensitive customer data and update its information security program accordingly.

- Tidewater does not have documented and approved policies and procedures requiring the design and implementation of specific safeguards as part of its information security program to control or mitigate risks to customer information. GLBA requires Tidewater to develop, implement, and maintain a comprehensive information security program that includes certain minimum safeguards. Without having documented and approved policies and procedures, Tidewater is unable to ensure it implements safeguards as expected to protect customer information within its information technology (IT) environment. Specifically, Tidewater does not have policies and procedures including the following safeguards that GLBA requires:

    - Conduct a periodic inventory of data, noting where it's collected, stored, or transmitted;

    - Encrypt customer information on the college's systems at rest and in transit;

    - Adopt secure development practices for applications developed by the college utilized for transmitting, accessing, or storing customer information;

- Implement multi-factor authentication for anyone accessing customer information on the college's systems;
- Dispose of customer information securely based on the college's data retention policy;
- Implement change management for information systems and network components;
- Log and monitor access and activity to customer information;
- Regularly test and monitor the effectiveness of implemented safeguards, such as vulnerability management and penetration testing;
- Oversee third-party service providers; and
- Conduct and document review, revisions, and approvals for the college's information security program, including its IT policies and procedures.

While Tidewater designates an individual to be responsible for the information security program, a lack of the necessary staff and resources to maintain the information security program resulted in out of date risk assessments and inadequately documented and approved policies and procedures.

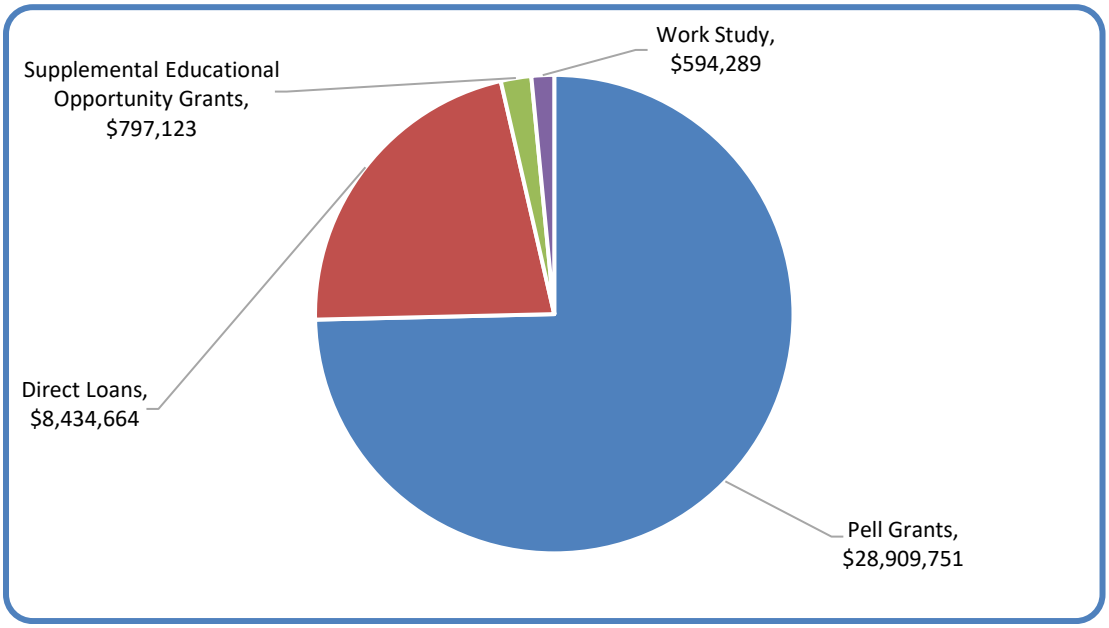
Tidewater should allocate the necessary resources to document and approve policies and procedures and review and update its risk assessments to identify potential risks to customer information. Additionally, Tidewater should develop and revise its information security program to ensure it includes all safeguards required by GLBA and is based on the results of the updated risk assessments. Compliance with GLBA requirements will assist Tidewater in evaluating its information security practices and ensuring the confidentiality, integrity, and availability of customer information.

AUDIT SCOPE OVERVIEW

Tidewater is part of the Virginia Community College System and serves South Hampton Roads with four campuses in Chesapeake, Norfolk, Portsmouth and Virginia Beach and six regional centers. Tidewater provides federal financial assistance through Direct Loans, Pell Grants, Supplemental Educational Opportunity Grants, and Work-Study programs. Chart 1 below shows the amounts comprising the Student Financial Assistance Cluster of federal programs at Tidewater.

Student Financial Assistance Cluster Federal Program Awards
Fiscal Year 2025

Chart 1



For our audit covering the fiscal year ended June 30, 2025, we performed procedures over the Student Financial Assistance Cluster of federal programs in accordance with U.S. Office of Management and Budget Compliance Supplement Part 5 Student Financial Assistance Programs. In addition, we reviewed the accuracy of the Schedule of Expenditures of Federal Awards attachment information submitted to the Department of Accounts.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

August 4, 2026

The Honorable Abigail D. Spanberger
Governor of Virginia

Joint Legislative Audit
and Review Commission

State Board for Community Colleges
Virginia Community College System

David Doré
Chancellor, Virginia Community College System

Marcia Conston
President, Tidewater Community College

We have audited **Tidewater Community College's** (Tidewater) compliance over the Student Financial Assistance Cluster of federal programs for the year ended June 30, 2025. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Objectives

Our audit's primary objective was to audit the Student Financial Assistance Cluster of federal programs. In support of this objective, we evaluated the accuracy of recorded transactions in Tidewater's accounting and financial reporting system, U.S. Department of Education's federal student financial assistance systems, and the federal attachment submitted to the Department of Accounts (Accounts); reviewed the adequacy of Tidewater's internal controls; and tested compliance with applicable laws, regulations, contracts, and grant agreements; and reviewed corrective actions with respect to previously unresolved audit findings and recommendations from prior reports. See the Findings Summary included in the Appendix for a listing of prior audit findings and the status of follow-up on management's corrective action.

Audit Scope and Methodology

Tidewater's management has responsibility for establishing and maintaining internal control and complying with applicable laws, regulations, contracts, and grant agreements. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws, regulations, contracts, and grant agreements.

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered significance and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following applicable Student Financial Assistance Cluster of federal programs compliance requirements:

- Cash management
- Enrollment reporting
- Financial reporting
- Gramm-Leach-Bliley Act
- Institutional eligibility
- Return of Title IV funds
- Student eligibility
- System access
- Title IV disbursements
- Verification

We performed audit tests to determine whether Tidewater's controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, contracts, and grant agreements. Our audit procedures included inquiries of appropriate personnel, inspection of documents and records, and observation of Tidewater's operations. We performed analytical procedures and tested details of transactions to achieve our objectives.

A nonstatistical sampling approach was used. Our samples were designed to support conclusions about our audit objectives. An appropriate sampling methodology was used to ensure the samples selected were representative of the population and provided sufficient, appropriate evidence. We identified specific attributes for testing each of the samples and when appropriate, we projected our results to the population.

Conclusions

We found that Tidewater has properly stated, in all material respects, the amounts recorded and reported in its financial system and the U.S. Department of Education’s federal student financial assistance systems for the Student Financial Assistance Cluster of federal programs.

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, contracts, and grant agreements that require management's attention and corrective action. These matters are described in the section titled "Audit Findings and Recommendations."

We determined that Tidewater has not fully implemented corrective action with respect to a prior year audit finding as identified in the section titled Findings Summary.

Exit Conference and Report Distribution

We discussed this report with management on July 31, 2026. Management's response to the findings identified in our audit is included in the section titled "College Response." We did not audit management's response and, accordingly, we express no opinion on it.

This report is intended for the information and use of the Governor and General Assembly, Tidewater Community College management, the Virginia Community College System Chancellor, the State Board for Community Colleges, and the citizens of the Commonwealth of Virginia and is a public record.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

DLR/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Improve Reporting to National Student Loan Data System	Ongoing	2018
Implement Information Security Program Requirements for the Gramm-Leach-Bliley Act **	Ongoing	2020

* A status of **Ongoing** indicates existing findings that require management's corrective action as of fiscal year end.

** Prior finding title was Perform Risk Assessment as Required by Gramm-Leach-Bliley Act.

TIDEWATER COMMUNITY COLLEGE
From here, go anywhere.™

DISTRICT ADMINISTRATION

September 2, 2026

Ms. Staci Henshaw
Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw:

In response to the 2025 Student Financial Aid Reaccreditation Audit recommendations, Tidewater Community College (TCC) accepts and concurs. The following outlines the APA recommendations and management's response with appropriate corrective action to address and resolve.

MP #02: IMPROVE REPORTING TO NATIONAL STUDENT LOAN DATA SYSTEM

Tidewater Community College (Tidewater) Registrar's Office staff did not report accurate and timely enrollment data to the National Student Loan Data System (NSLDS) for students that graduated, withdrew or changed enrollment levels. Management did not establish effective monitoring controls and clearly defined communication procedures between the Financial Aid Office and Registrar's Office to ensure staff follow established enrollment reporting procedures. As a result, we identified the following instances of noncompliance within a sample of 50 students:

- Tidewater reported an inaccurate enrollment status for three students (6%);
- Tidewater reported an inaccurate effective date for nine students (18%);
- Tidewater staff did not report enrollment status changes timely for nine students (18%); and
- Tidewater inaccurately reported at least one campus or program-level field deemed critical for 10 students (20%).

In accordance with Title 34 Code of Federal Regulations (CFR) §685.309 an institution shall submit, in accordance with deadline dates established by the Secretary of Education (Secretary), other reports and information the Secretary requires and shall comply with the procedures the Secretary finds necessary to ensure the reports are correct. As further outlined in Education's NSLDS Enrollment Guide, institutions are required to certify enrollment every 60 days. The accuracy of Title IV enrollment data depends heavily on information reported by institutions. Tidewater's inaccurate and untimely enrollment data submissions to NSLDS can affect Education's reliance on the system for monitoring purposes. Noncompliance may also impact an institution's participation in Title IV programs.

Tidewater management should strengthen supervision and enhance monitoring controls to consistently adhere to the federal reporting requirements by reporting accurate and timely student enrollment status changes to NSLDS. Management should also consider implementing a quality control review process to monitor the accuracy of campus and program-level batch submissions.

CHESAPEAKE NORFOLK PORTSMOUTH SUFFOLK VIRGINIA BEACH

121 College Place Norfolk Virginia 23510 • Telephone: 757-822-1122 • www.tcc.edu

TCC Response

Tidewater Community College (TCC) recognizes the importance of timely and accurate enrollment reporting to the National Student Loan Data System (NSLDS), including enrollment information submitted through the National Student Clearinghouse. TCC will strengthen its enrollment reporting controls and monitoring processes to support compliance with applicable federal reporting requirements and improve the accuracy and timeliness of enrollment data.

In addition to the corrective actions described below, the Office of the College Registrar will implement a documented quality-control review of enrollment reporting. Identified discrepancies will be reviewed and corrected within applicable reporting and correction timeframes. Management will monitor the process to support sustained compliance.

Tidewater reported an inaccurate enrollment status for three students (6%);

The Office of the College Registrar will review enrollment records, including applicable F grades, to identify records requiring evaluation to ensure accurate enrollment status reporting. Admissions and Enrollment will process approved grade changes when appropriate.

Tidewater reported an inaccurate effective date for nine students (18%);

The Office of the College Registrar will receive a weekly list of student withdrawals and review the associated effective dates for accuracy and alignment with the academic calendar and applicable NSLDS reporting requirements. Any discrepancies or missing reports identified through this review will be addressed and corrected within applicable reporting and correction timeframes.

Tidewater staff did not report enrollment status changes timely for nine students (18%); and

During Spring 2026, the Virginia Community College System (VCCS) updated the SIS enrollment extract logic to address identified issues affecting enrollment status and effective-date calculations. TCC will continue to monitor enrollment reporting following implementation of the updated logic and review identified exceptions to verify that enrollment status changes and effective dates are reported accurately and in a timely manner.

Tidewater inaccurately reported at least one campus or program-level field deemed critical for 10 students (20%).

TCC reviewed its reporting practices for students who complete an eligible credential while remaining enrolled in an active parent program. TCC revised its reporting practice so that students who complete an eligible credential are reported using the appropriate graduation status, consistent with applicable reporting requirements.

TCC also reviewed the Classification of Instructional Programs (CIP) codes associated with applicable academic programs and corrected identified discrepancies. The Office of the College Registrar will incorporate a review of applicable program and CIP information into its enrollment reporting quality-control process to support continued reporting accuracy.

TCC will continue to monitor the effectiveness of these corrective actions and make additional adjustments as needed to support accurate and timely enrollment reporting to NSLDS.

MP # 03: IMPLEMENT INFORMATION SECURITY PROGRAM REQUIREMENTS FOR THE GRAMM-LEACH BLILEY ACT

Tidewater Community College (Tidewater) does not comply with certain elements of the Gramm-Leach-Bliley Act (GLBA) related to its information security program. Public Law 106-102, known as the GLBA, classifies institutions of higher education as financial institutions due to their involvement in financial assistance programs. Related regulations in Title 16 of the Code of Federal Regulations (CFR)

§§ 314.3 and 314.4 require organizations to develop, implement, and maintain an information security program to safeguard customer information. Specifically, Tidewater does not comply with the following GLBA requirements:

- While Tidewater's information security program requires the college to base the information security program on a risk assessment, Tidewater does not annually review and update three completed risk assessments used to identify security risks to customer information. As a result, Tidewater is unable to evaluate and adjust its information security program based on the results of the risk assessments. GLBA requires that Tidewater base its information security programs on a risk assessment that "identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks." GLBA also requires that Tidewater adjust its information security program based on the results of the risk assessment. By not maintaining current risk assessments, Tidewater may not identify risks that pose a threat to the college's sensitive customer data and update its information security program accordingly (*16 C.F.R. § 314.4(b) and 314.4(g)*).

- Tidewater does not have documented and approved policies and procedures to design and implement specific safeguards as part of its information security program to control or mitigate risks to customer information. GLBA requires Tidewater to develop, implement, and maintain a comprehensive information security program that includes certain elements at a minimum. Without having documented and approved policies and procedures, Tidewater is unable to ensure it implements safeguards as expected to protect customer information within its information technology (IT) environment. The elements Tidewater is missing from its information security program include:
  - Conduct a periodic inventory of data, noting where it's collected, stored, or transmitted (*16 C.F.R. § 314.4(c)(2)*).
  - Encrypt customer information on the college's systems at rest and in transit (*16 C.F.R. § 314.4(c)(3)*).
  - Adopt secure development practices for applications developed by the college utilized for transmitting, accessing, or storing customer information (*16 C.F.R. § 314.4(c)(4)*).
  - Implement multi-factor authentication for anyone accessing customer information on the college's systems (*16 C.F.R. § 314.4(c)(5)*).
  - Dispose of customer information securely based on the college's data retention policy (*16 C.F.R. § 314.4(c)(6)*).
  - Implement change management for information systems and network components (*16 C.F.R. § 314.4(c)(7)*).
  - Log and monitor access and activity to customer information (*16 C.F.R. § 314.4(c)(8)*).
  - Regularly test and monitor the effectiveness of implemented safeguards, such as vulnerability management and penetration testing (*16 C.F.R. § 314.4(d)*).
  - Oversee third-party service providers (*16 C.F.R. § 314.4(f)*).
  - Conduct and document its review, revisions, and approvals for the college's information security program, including its IT policies and procedures (*16 C.F.R. § 314.4(g)*).

While Tidewater designates an individual to be responsible for the information security program, a lack of the necessary staff and resources to maintain the information security program caused Tidewater to not update its risk assessments nor have documented and approved policies and procedures as required.

Tidewater should allocate the necessary resources to review and update its risk assessments to identify potential risks to customer information. Additionally, Tidewater should develop and revise its information security program to ensure it includes all elements required by GLBA and is based on the results of the updated risk assessments. Compliance with GLBA requirements will assist Tidewater in evaluating its information security practices and ensuring the confidentiality, integrity, and availability of customer information within its environment.

TCC Response

The College concurs with the recommendations and has worked with staff to provide documentation addressing mitigating factors. Information Technology will continue to provide and maintain current documentation and records demonstrating approved policies for the technology systems used at TCC.

Please note that we also utilize systems provided by the VCCS and the Commonwealth of Virginia, which we do not maintain and over which we do not have oversight. Additionally, we will continue requiring staff with Financial Aid access to complete GLBA training to help ensure awareness of requirements and safeguards for protecting data. The College will implement a phased remediation strategy beginning in 2026 to establish a fully compliant GLBA Information Security Program.

The plan includes: 1) annual review of the enterprise risk assessments for AIS, HCM, and SIS completed by the VCCS and adjustment of our information security program based on the results of the risk assessment, and 2) review of all current documented and approved security policies and modify and/or develop policies and procedures to include mission components.

Sincerely,

Heather Hardiman

Heather Hardiman
Executive Vice President and CFO

cc:
Dr. Marcia Conston, President
Dr. Karen Campbell, Vice President for Student Affairs
Dr. Misty Lyon, Dean of Enrollment Management
Nicole Wilson, College Registrar
Andrea Etheridge, Director of Information Technology and CIO
Taniya LeGrand, Director of Central Financial Aid