OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

Official Audit Report – Issued July 1, 2025

Cape Cod Community College

For the period January 1, 2021 through December 31, 2023

State House Room 230 ■ Boston, MA 02133 ■ auditor@massauditor.gov ■ www.mass.gov/auditor

OFFICE OF THE STATE AUDITOR

DIANA DIZOGLIO

July 1, 2025

Dr. John Cox, President
Cape Cod Community College
2240 Iyannough Road
West Barnstable, MA 02668

Dear President Cox:

I am pleased to provide to you the results of the enclosed performance audit of Cape Cod Community College. As is typically the case, this report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, January 1, 2021 through December 31, 2023. As you know, my audit team discussed the contents of this report with college managers. This report reflects those comments.

I appreciate you and all your efforts at Cape Cod Community College. The cooperation and assistance provided to my staff during the audit went a long way toward a smooth process. Thank you for encouraging and making available your team. I am available to discuss this audit if you or your team has any questions.

Best regards,

Diana DiZoglio
Auditor of the Commonwealth

cc: Tammy Glivinski-Saben, Chair of the Cape Cod Community College Board of Trustees

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ASR	annual security report
CCCC	Cape Cod Community College
CFR	Code of Federal Regulations
Clery Act	Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act
CSA	campus security authority
EOTSS	Executive Office of Technology Services and Security
NIST	National Institute of Standards and Technology

EXECUTIVE SUMMARY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of certain activities of Cape Cod Community College (CCCC) for the period January 1, 2021 through December 31, 2023.

In this performance audit, we examined CCCC's compliance with certain aspects of the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (Clery Act), as amended. The Clery Act was enacted in 1990 to ensure that colleges and universities maintain transparency and accountability about crime prevention and response on their campuses. It requires educational institutions participating in federal student aid programs to publish an annual security report (ASR) that discloses campus crime statistics and security information. In addition, we reviewed CCCC's cybersecurity awareness training program for employees.

The purpose of our audit was to determine the following:

- whether CCCC included all required policies, procedures, and statements in its ASR, in accordance with the Clery Act (Section 668.46[b–h] of Title 34 of the Code of Federal Regulations [CFR]);
- whether CCCC recorded all crimes within its Clery geography in a daily crime log and accurately reported these crimes to the US Department of Education (US DOE) and in its ASR in accordance with the Clery Act (34 CFR 668.46[c][1] and [f][1]);
- whether CCCC had a process in place to ensure that it identified campus security authorities (CSAs) and that these employees completed training on their responsibilities as CSAs, in accordance with the Clery Act (34 CFR 668.46[a]); and
- whether CCCC ensured that its employees completed cybersecurity awareness training, in accordance with its "Cyber / Information Security Awareness Training" policy; Section 6.2.3 of the Executive Office of Technology Services and Security's (EOTSS's) Information Security Risk Standard IS.010; and Section AT-3 of Revision 5 of the National Institute of Standards and Technology's Special Publication 800-53.

Below is a summary of our findings, the effects of those findings, and our recommendations, with hyperlinks to each page listed.

Finding 1 **Page 17**	CCCC did not accurately report all required crime statistics in its ASR and to US DOE.

Effect	If CCCC inaccurately reports its Clery Act crime statistics, then current and prospective students, CCCC employees, and members of the public may draw incorrect conclusions about campus safety. Additionally, not complying with the Clery Act's ASR reporting requirements may result in CCCC having to pay fines to US DOE.
Recommendation Page 20	CCCC must make certain that all Clery Act crimes that occur within its Clery geography are accurately recorded in CCCC's daily crime log and its ASR by establishing policies and procedures to ensure that the following occur: • cases are recorded accurately in CCCC's daily crime log, and are also identified as Clery Act crimes where applicable; • Clery Act crimes are accurately documented in CCCC's disciplinary action records management system and reported to CCCC's Department of Public Safety so that they can be properly investigated and included in CCCC's ASR; • a verification process is developed, documented, and implemented by CCCC that includes supervisory review and sign-off of the disciplinary action records on a regular basis; • Clery Act crime data is accurately reported to US DOE; and • as required by law, all supporting documentation for CCCC's Clery Act crime statistics is retained by CCCC's Department of Public Safety, including the daily crime log statistics, student disciplinary action log statistics, and any other records used to complete CCCC's ASR for at least three years.
Finding 2 Page 22	CCCC did not properly identify and train campus security authorities (CSAs) in their duties as CSAs.
Effect	If CCCC does not properly designate and train all CSAs, then CCCC's ability to compile and report accurate annual crime statistics is limited, and, with inaccurately reported crime statistics, current and prospective students, CCCC employees, and members of the public may be misinformed or draw incorrect conclusions about campus safety.
Recommendations Page 24	1. CCCC should establish a process for its Human Resources Department and Department of Public Safety to identify individuals who meet the definition of a CSA. 2. CCCC should maintain and regularly update a list of identified CSAs. 3. CCCC should notify identified CSAs and train them on their responsibilities as CSAs at least annually and retain records of training completion for all CSAs.
Finding 3 Page 25	CCCC did not ensure that all of its employees completed cybersecurity awareness training.
Effect	If CCCC does not ensure that all of its employees complete cybersecurity awareness training, then CCCC exposes itself to an increased risk of cybersecurity attacks, and financial and/or reputational losses.
Recommendation Page 27	CCCC should develop and implement monitoring controls to ensure that all employees are enrolled in and complete initial and annual refresher cybersecurity awareness training.

OVERVIEW OF AUDITED ENTITY

Cape Cod Community College (CCCC) was established by Section 5 of Chapter 15A of the Massachusetts General Laws and operates under the direction of an eleven-member board of trustees, the members of which are appointed by the Governor. The board of trustees is responsible for overseeing long-term planning, managing financial resources, and determining organizational structure.

According to CCCC's website,

> *CCCC delivers educational programs and services to meet the diverse needs of the residents of Cape Cod, the Greater Plymouth Area, Martha's Vineyard, and Nantucket, across the Southeastern Coastal Region of Massachusetts. [CCCC] is the only comprehensive college on Cape Cod offering Associate of Arts, Associate of Science, Associate of Applied Science degrees, and academic certificate programs in a wide variety of areas.*

CCCC is a member of the Massachusetts public higher education system, which consists of 15 community colleges, nine state universities, and five University of Massachusetts campuses. The main campus is located in West Barnstable.

According to CCCC's 2022–2023 Academic Catalog, each semester, approximately 2,500 students enroll at the college, with 85% pursuing degree or certificate programs. Approximately 69% of students attend part-time. The college employs 61 full-time faculty members and over 220 part-time adjunct faculty.

In fiscal year 2022, CCCC's operating revenue (i.e., tuition; fees; federal, state, and private grants; and contracts) was $17,251,790 and its nonoperating revenue (i.e., state appropriation, federal assistance, and interest income) was $33,569,768. In fiscal year 2023, CCCC's operating revenue was $20,670,710 and its nonoperating revenue was $22,893,508.

Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act

As a participant in federal student financial aid programs under Title IV of the Higher Education Act of 1965, CCCC is required to comply with the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (Clery Act). The Clery Act is a federal law that requires institutions to disclose campus crime statistics and other related security information in the form of an annual security report (ASR) to

students and the public.[1] The Clery Act was initially enacted as Title II of the Crime Awareness and Campus Security Act of 1990, which was signed into law as an amendment to the Higher Education Act of 1965. In 1998, this law was amended and renamed the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act in memory of a student who was raped and murdered in her dormitory at Lehigh University. In 2013, the act was amended to include statistics, policies, and programs related to domestic violence, dating violence, sexual assault, and stalking. The purpose of the Clery Act is to improve transparency and accountability in campus safety. Institutions covered by the Clery Act must comply with specific requirements outlined in the Clery Act Appendix of the *Federal Student Aid Handbook*,[2] including those listed in the table below.

Clery Act Requirements—The Basics

• Collect, classify, and count crime reports and statistics	
• Issue campus alerts and warning notices	• Publish an Annual Security Report (Due date: October 1)
• Disclose missing student notification procedures, when applicable	• Submit crime and fire statistics to the [US Department of Education], when applicable
• Disclose procedures for institutional disciplinary actions	• Provide educational programs and campaigns
• Keep a daily crime log, when applicable	• Disclose fire safety information, when applicable

Source: The Clery Act Appendix of the *Federal Student Aid Handbook*

The US Department of Education (US DOE) conducts compliance reviews and audits to ensure that all higher education institutions receiving federal funds adhere to the Clery Act; it also imposes fines on institutions that do not comply.

Daily Crime Log

All institutions of higher education with campus security or police departments, and which are subject to the Clery Act, must maintain a daily crime log of all crimes reported to them and any crimes that have occurred within an institution's Clery geography. Clery geography includes buildings and property that are

1. The Clery Act requires institutions to report crimes that have been reported to them but does not necessarily require that those crimes be adjudicated before they are included in the statistics. Therefore, for the purposes of this report, Clery Act crimes refer to alleged crimes.
2. The *Federal Student Aid Handbook* is a guide from the Federal Student Aid office published in individual volumes with information specific for students, their parents and/or guardians, and their institutions of higher education on eligibility, statutory, and regulatory requirements.

part of an institution's campus (e.g., classroom buildings or cafeterias); an institution's non-campus buildings and property (e.g., institution-owned bookstores located off campus, apartment buildings owned or controlled by the institution, and sorority- and fraternity-owned chapter houses); and public property within or immediately adjacent to and accessible from an institution's campus (e.g., public streets, sidewalks, and parking lots). The CCCC Department of Public Safety maintains, controls, and monitors CCCC's daily crime log.

According to the Clery Act, "The institution must make the crime log for the most recent 60-day period open to public inspection during normal business hours . . . [and] make any portion of the log older than 60 days available within two business days of a request for public inspection."

Clery Act crimes fall into four categories: (1) criminal offenses, such as murder, rape, statutory rape, robbery, or arson; (2) arrests and disciplinary action referrals for liquor law violations, drug law violations, or illegal weapon possession; (3) hate crimes, such as intimidation or simple assault motivated by bias; and (4) Violence Against Women Act offenses, which include domestic violence, dating violence, and stalking. (See the Appendix for more information.) These crimes must be recorded based on the Clery geography categories of on-campus, non-campus buildings or property, or public property. CCCC students, employees, and visitors report crimes that occur within CCCC's Clery geography to CCCC's Department of Public Safety or a campus security authority (CSA). (See the "Crime Reporting" section of this report for more information.)

CSAs

According to Number 202 of Volume 79 of the *Federal Register*, dated October 20, 2014, CSA is a term that refers to "an official of an institution who has significant responsibility for student and campus activities, including, but not limited to, student housing, student discipline, and campus judicial proceedings." CSAs are required to report any Clery Act crimes to their campus security or police department,[3] such as CCCC's Department of Public Safety, regardless of whether the victim or witness decides to report it.

3. Unlike campus security departments, campus police departments employ sworn officers certified by the Massachusetts Police Officer Standards and Training Commission.

According to Section 668.46(a) of Title 34 of the Code of Federal Regulations, the following individuals meet the CSA criteria:

(i) A campus police department or a campus security department of an institution.

(ii) Any individual who has responsibility for campus security but does not constitute a campus police or a campus security department . . . such as an individual who is responsible for monitoring entrance into institutional property.

(iii) Any individual or organization specified in an institution's statement of campus security policy as an individual or organization to which students and employees should report criminal offenses.

(iv) An official of an institution who has significant responsibility for student and campus activities, including, but not limited to, student housing, student discipline, and campus judicial proceedings.

CCCC's Department of Public Safety is responsible for identifying CSAs, notifying CSAs of their responsibilities on an ongoing basis, and training CSAs annually. During the audit period, CCCC did not have an established process for identifying, notifying, and training CSAs.

ASR

Institutions of higher education subject to the Clery Act are required to publish an ASR that provides accurate information on campus crime statistics and security-related details for the three most recent calendar years. Institutions of higher education compile the crime statistics in accordance with definitions provided by the Federal Bureau of Investigation for use in the Uniform Crime Reporting Program. The table below details information that institutions of higher education must include in their ASRs in accordance with the Clery Act.

Required Contents of the ASR

1.	Policies regarding alcoholic beverages and underage drinking laws	7.	Policies regarding missing student notifications
2.	Policies regarding illegal drugs and applicable federal and state drug laws	8.	Campus crime statistics
3.	Programs on substance [use]	9.	Policies regarding procedures for reporting criminal actions or other emergencies on campus
4.	Programs to prevent dating and domestic violence, sexual assault, and stalking, and the procedures institutions will follow when such crimes are reported	10.	Policies on the security of and access to campus facilities

5. Information regarding sex offenders	11. Policies on enforcement authority of security personnel; working relationship of campus security personnel with State and local police agencies; accurate and prompt reporting of crimes; pastoral and professional counselors
6. Descriptions of emergency response and evacuation procedures	12. Programs on campus security procedures and practices

Source: The Clery Act Appendix of the *Federal Student Aid Handbook*

This report must be distributed to the entire campus community, including employees and current and prospective students, by October 1 of each year. The campus safety survey administrator must also submit the Clery Act crime statistics within the ASR to US DOE annually. CCCC electronically submits campus crime statistics to US DOE, publishes its ASR on its website, and notifies CCCC's campus community of the report through email annually.

Crime Reporting

CCCC students, employees, and visitors may report alleged incidents, suspicious activities, or emergencies by contacting CCCC's Department of Public Safety in person or by telephone, or by reporting them to a different CSA. According to the Clery Act, a crime is considered reported when any person, including the victim, a witness, a third party, or an offender brings it to the attention of CCCC's Department of Public Safety, a different CSA, or a local law enforcement agency.

According to CCCC's website,

> *The Cape Cod Community College Department of Public Safety is here to protect and serve the campus community. The College employs [Peace Officer Standards and Training]-certified police officers and security officers to provide public safety and emergency services. Additionally, there are partnerships with the Massachusetts State Police, Barnstable County Sheriff's Office and the West Barnstable Fire Department to support operations and campus officers have direct radio communication with Barnstable Police in an emergency.*

CCCC management explained that there was turnover in the chief of police and public safety position during the audit period. Currently, CCCC's Department of Public Safety comprises a director of public safety, who also serves as CCCC's chief of police and public safety, and an investigator. Both the director of public safety and the investigator are sworn officers commissioned in accordance with Section 63 of Chapter 22C of the General Laws, and they meet the standards set by the Commonwealth of Massachusetts Peace Officer Standards and Training Commission. They can make arrests, carry firearms, and investigate crimes on campus. Additionally, CCCC's Department of Public Safety has three security

officers and additional contracted security personnel members who are uniformed public safety professionals authorized to enforce campus rules and regulations. These security officers do not carry firearms or make arrests.

According to the director of public safety, during the audit period, most reports of alleged incidents were made through telephone calls to CCCC's Department of Public Safety. Once received, the alleged incidents were entered into the Department of Public Safety's daily crime log within CCCC's case management system. All security officers had access to enter incidents into this log. During the audit period, the former chief of police and public safety was responsible for reviewing the daily crime log for completeness and accuracy. The daily crime log was then published on CCCC's website each week.

During the audit period, if an individual who was a CSA witnessed or received a report of an incident related to prohibited conduct (which may or may not be related to a crime), then they were required to report the incident using the Code of Conduct Incident Report Form found on CCCC's website. The report needed to include the reporter's contact information, along with the date, time, and location of the alleged incident; information about the parties involved and the type of alleged prohibited conduct; and details of the alleged incident. Once the form was submitted, the information was recorded in CCCC's student disciplinary action records management system, which sent an email notification to the applicable CCCC office (Student Conduct, Title IX,[4] or Wellness) responsible for addressing the type of alleged incident.

During the audit period, on an annual basis, the former chief of public safety would review the daily crime log for Clery Act crimes and reach out to CCCC's associate dean of students to obtain any student disciplinary actions that were required by the Clery Act to be included in CCCC's ASR. CCCC published its completed ASR on its website annually. According to CCCC's 2023 ASR, "An email notification is made to all enrolled students, faculty, and staff on how to access the Annual Security Report both on-line and in printed form."

Additionally, CCCC must submit crime statistics for the three most recent calendar years to US DOE annually.

4. According to US DOE's website, "Title IX prohibits discrimination based on sex in education programs or activities that receive federal financial assistance."

Cybersecurity Awareness Training

CCCC's "Cyber / Information Security Awareness Training" policy requires all information system users to complete cybersecurity awareness training upon hire and at least annually thereafter. This aligns with Section AT-3 of Revision 5 of the National Institute of Standards and Technology's Special Publication 800-53, a best practice for information system security, which advocates for providing cybersecurity awareness training to system users as part of initial training and at a frequency defined by the organization thereafter.

Additionally, the Executive Office of Technology Services and Security (EOTSS) has established policies and procedures that apply to all Commonwealth agencies within the executive branch. EOTSS recommends, but does not require, non-executive branch state agencies to follow these policies and procedures. Section 6.2.3 of EOTSS's Information Security Risk Management Standard IS.010[5] requires that all newly hired employees complete an initial cybersecurity awareness training course within 30 days of their orientation. Since CCCC's policy does not specify a timeframe for this initial training, we used EOTSS's standard as a best practice to measure CCCC's performance during the audit period in this area.

During the audit period, CCCC's chief information officer assigned an email address to all employees, thereby classifying them as information system users. According to CCCC management, it recommended but did not mandate that all information system users complete initial training (which included cybersecurity awareness training) and annual refresher cybersecurity awareness training thereafter. CCCC used a third-party, web-based training program to provide and track CCCC's cybersecurity awareness training during the audit period.

5. EOTSS updated the titles and numbers of at least some of its policies and standards between the end of the audit period and the publication of this report. In this report, we reference the titles and numbers of EOTSS's policies and/or standards as they were documented during the audit period (unless stated otherwise).

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of certain activities of Cape Cod Community College (CCCC) for the period January 1, 2021 through December 31, 2023.

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.

Below is a list of our audit objectives, indicating each question we intended our audit to answer; the conclusion we reached regarding each objective; and, if applicable, where each objective is discussed in the audit findings.

Objective	Conclusion
1. Did CCCC include all required policies, procedures, and statements in its annual security report (ASR) in accordance with the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (Clery Act) (Section 668.46[b–h] of Title 34 of the Code of Federal Regulations [CFR])?	**Yes**
2. Did CCCC record all crimes within its Clery geography in a daily crime log and accurately report these crimes to the US Department of Education (US DOE) and in its ASR, in accordance with the Clery Act (34 CFR 668.46[c][1] and [f][1])?	**No; see Finding 1**
3. Did CCCC have a process in place to ensure that it identified campus security authorities (CSAs) and that these employees completed training on their responsibilities as CSAs, in accordance with the Clery Act (34 CFR 668.46[a])?	**No; see Finding 2**
4. Did CCCC ensure that its employees completed cybersecurity awareness training, in accordance with its "Cyber / Information Security Awareness Training" policy; Section 6.2.3 of the Executive Office of Technology Services and Security's (EOTSS's) Information Security Risk Standard IS.010; and Section AT-3 of Revision 5 of the National Institute of Standards and Technology's (NIST's) Special Publication 800-53?	**No; see Finding 3**

To accomplish our audit objectives, we gained an understanding of CCCC's internal control environment relevant to our objectives by reviewing applicable policies and procedures and by interviewing CCCC officials. We evaluated the design and implementation of the internal controls related to our audit objectives. In addition, to obtain sufficient, appropriate evidence to address our audit objectives, we performed the procedures described below.

ASR-Required Policies, Procedures, and Statements

To determine whether CCCC included all required policies, procedures, and statements in its ASR, in accordance with the Clery Act (34 CFR 668.46[b-h]), we inspected CCCC's published ASRs for calendar years 2021, 2022, and 2023 (the audit period). These ASRs included the Clery Act–required policies, procedures, and statements for the period[6] January 1, 2020 through December 31, 2023.

We noted no exceptions in our testing. Therefore, we concluded that CCCC included all required policies, procedures, and statements in its ASRs.

ASR Clery Act Crime Statistics

To determine whether CCCC recorded all crimes within its Clery geography in a daily crime log and accurately reported these crimes to US DOE and in its ASR, in accordance with the Clery Act (34 CFR 668.46[c][1] and [f][1]), we took the actions described below.

We inspected CCCC's 2023 ASR and CCCC's electronic submission to US DOE, which included Clery Act crime statistics for calendar years 2020 through 2022. We compared the Clery Act crime statistics published in CCCC's 2023 ASR to those that CCCC submitted to US DOE to ensure that they matched.

To ensure that all cases from the daily crime log required by the Clery Act were reported in CCCC's 2023 ASR, we took the following actions.

- We inspected a list of all 178 cases from the daily crime log we obtained from CCCC's director of public safety and attempted to identify the total number of cases that fell within each of the four categories of Clery Act crimes (as described in the "Daily Crime Log" section of this report).
- We attempted to compare the total number of cases we identified as Clery Act crimes to the total number of Clery Act crimes CCCC included in its daily crime log and its 2023 ASR. However, we were unable to do so because the crime categories in CCCC's daily crime log did not correspond directly to those in the ASR, making a direct comparison impossible.
- We followed up with CCCC to ask about any variances we identified (i.e., crimes reported in CCCC's ASR that were not on the daily crime log, and crimes that were only reportable if they were hate crimes).

6. CCCC's 2021, 2022, and 2023 ASRs were listed on CCCC's website, and each ASR included CCCC's current policies for that year and Clery Act crime statistics for the previous three calendar years. For example, CCCC's 2023 ASR included CCCC's 2023 policies and Clery Act crime statistics for 2020, 2021, and 2022. Therefore, CCCC's 2021, 2022, and 2023 ASRs collectively reflect CCCC's policies for 2021 through 2023 and Clery Act crime statistics for 2018 through 2022. CCCC's 2024 ASR, which would have included Clery Act crime statistics for 2023 (the final year of the audit period), was published after our audit commenced and, therefore, was not included in the scope of this audit.

To ensure that all incidents from CCCC's disciplinary action record management system that must be reported under the Clery Act were included in the daily crime log and CCCC's 2023 ASR, we took the following actions.

- We inspected a list of all 82 incidents from the disciplinary action record management system we obtained from CCCC's dean of students and CCCC's associate dean of students and attempted to identify the total number of incidents that fell within each of the four categories of Clery Act crimes (as described in the "Daily Crime Log" section of this report).
- We attempted to compare the total number of incidents we identified as Clery Act crimes to the total number of Clery Act crimes CCCC included in its daily crime log and its 2023 ASR. However, we were unable to do so because the crime categories in CCCC's disciplinary action record management system did not correspond directly to those in the ASR, making a direct comparison impossible.
- We followed up with CCCC to ask about any variances we identified (i.e., Clery Act crimes that were reported in CCCC's ASR but not in CCCC's disciplinary action record management system and vice versa).

Based on the results of our testing, we determined that, during the audit period, CCCC did not accurately report all required crime statistics in its ASR and to the US DOE. See Finding 1 for more information.

CSAs

To determine whether CCCC had a process in place to ensure that it identified CSAs and that these employees completed training on their responsibilities as CSAs, in accordance with the Clery Act (34 CFR 668.46[a]), we took the actions described below.

- We interviewed CCCC's vice president of finance and operations and CCCC's director of public safety to determine how CCCC identified CSAs and trained them on their responsibilities. We were informed that, during the audit period, the former chief of police and public safety conducted some informal training for CSAs. However, CCCC could not provide documentation confirming that any training, informal or formal, was provided to employees identified as CSAs.
- We obtained a list of six CCCC employees who were identified as CSAs during the audit period.
- We compared the job titles of these six CCCC employees to the Clery Act definition of a CSA and CCCC's definition of CSAs published in its 2021, 2022, and 2023 ASRs.
- Additionally, we reviewed the list of 571 CCCC employees provided by CCCC to determine whether there were other potential employees, based on their job titles, who met the criteria for a CSA.

Based on the results of our testing, we determined that, during the audit period, CCCC did not properly identify and train campus security authorities See Finding 2 for more information.

Cybersecurity Awareness Training

To determine whether CCCC ensured that its employees completed cybersecurity awareness training, in accordance with its "Cyber / Information Security Awareness Training" policy; Section 6.2.3 of the Executive Office of Technology Services and Security's Information Security Risk Standard IS.010; and Section AT-3 of Revision 5 of NIST's Special Publication 800-53, we took the actions described below.

We obtained from CCCC's vice president of finance and operations a list of 571 employees who were employed by CCCC during the audit period. We grouped these 571 CCCC employees into the following two categories: 239 CCCC employees with hire dates during the audit period (i.e., newly hired employees)—who were therefore required to complete initial cybersecurity awareness training—and 332 CCCC employees with hire dates before the audit period (i.e., existing employees)—who were therefore required to complete annual refresher cybersecurity awareness training.

We selected a random, nonstatistical[7] sample of 35 newly hired employees from the population of 239 and another random, nonstatistical sample of 40 existing employees from the population of 332.

To determine whether CCCC ensured that its employees from our two samples completed cybersecurity awareness training—the initial training for our sample of 35 newly hired employees and the annual refresher training for our sample of 40 existing employees—we took the actions described below for each sample.

We obtained a report of all cybersecurity awareness training activity for the audit period from CCCC's cybersecurity awareness training system. This report contained CCCC employee email addresses, training campaign names, content name (description of the training), enrollment dates, and completion dates. According to CCCC management, this is the only record of enrollment and completion of cybersecurity awareness training for CCCC employees. We inspected this report for each of the CCCC employees in both of our samples (both newly hired and existing employees) to determine whether they enrolled in and completed cybersecurity awareness training.

Additionally, for the newly hired employees in our sample, we compared their date of hire (from the CCCC employee list) to their listed completion date of initial cybersecurity awareness training (from the report

7. Auditors use nonstatistical sampling to select items for audit testing when a population is very small, the population items are not similar enough, or there are specific items in the population that the auditors want to review.

of all cybersecurity awareness training activity from the audit period). We calculated the number of days it took each of the newly hired employees to complete the initial cybersecurity awareness training to determine whether the number of days for each newly hired employee was within 30 days of their hire date.

Based on the results of our testing, we determined that, during the audit period, CCCC did not ensure that all employees completed cybersecurity awareness training. See Finding 3 for more information.

We used a nonstatistical sampling method for testing and therefore did not project the results of our testing to the corresponding populations.

Data Reliability Assessment

Daily Crime Log

To determine the reliability of the daily crime log data maintained in CCCC's case management system, we interviewed CCCC employees who were knowledgeable about the daily crime log data. We also tested certain general information system controls (including security management, access controls, configuration management, and contingency planning for CCCC's case management system). We observed the director of public safety query CCCC's case management system and extract 178 cases that were made during the audit period. The director of public safety then provided us with a list of these 178 cases in a Microsoft Excel file. We also conducted a date range analysis on the list of 178 cases that we received to ensure that the dates for these cases were within the audit period. We inspected the list of 178 cases for duplicate case numbers, for embedded data, for hidden rows and columns, and for gaps in the sequential case numbers to determine whether cases were missing or deleted from the dataset. We followed up with CCCC regarding any gaps and determined that there were valid reasons for the gaps.

Student Disciplinary Action Log

To determine the reliability of the student disciplinary action log data, we interviewed CCCC employees who were knowledgeable about the data. We observed CCCC's dean of student affairs and student retention query CCCC's student disciplinary action record management system and extract 82 student disciplinary actions that were made during the audit period. The dean of student affairs and student retention then provided us with a list of these 82 student disciplinary actions in a

Microsoft Excel file. We conducted a date range analysis on the list of 82 student disciplinary actions that we received to ensure that the dates for these student disciplinary actions were within the audit period. Additionally, we inspected the list of 82 student disciplinary actions for duplicate file identification numbers, embedded data, and hidden rows and columns.

Cybersecurity Awareness Training

To determine the reliability of the cybersecurity awareness training data obtained from CCCC's cybersecurity awareness training system, we interviewed CCCC employees who were knowledgeable about the data. We also tested certain general information system controls (including security management, access controls, configuration management, and contingency planning for CCCC's cybersecurity awareness training system). We obtained a list of all 5,351 cybersecurity awareness trainings from the audit period that CCCC's chief information officer generated from CCCC's cybersecurity awareness training system. We conducted a date range analysis on the list of 5,351 cybersecurity awareness trainings that we received to ensure that the dates for these trainings were within the audit period. Additionally, we inspected the list of 5,351 cybersecurity awareness trainings for embedded data and hidden rows and columns. According to CCCC management, this is the only record of enrollment and completion of cybersecurity awareness training for CCCC employees.

We obtained from CCCC's vice president of operations a list of all 571 CCCC employees who were employed by CCCC during the audit period. To determine the reliability of the list of 571 CCCC employees, we compared the employee names and employee identification numbers for each of the 571 CCCC employees to a list of individuals who were actively employed during the audit period, which we generated independently from the Commonwealth's Human Resources Compensation Management system, the Commonwealth's official payroll system. We also selected a random sample of 20 CCCC employees from the list of 571 CCCC employees that we received and verified their employment status with CCCC by tracing employee information (e.g., employee identification number, employee name, start date, union code, and employee title) to the employee information in the employee personnel files maintained by CCCC's Human Resources Department. We conducted a date range analysis on the list of 571 CCCC employees to check for dates outside the audit period. We inspected the list of 571 CCCC employees for duplicate employee identification numbers, embedded data, and hidden rows and columns.

Based on the results of the data reliability assessment procedures described above, we determined that the information we obtained was sufficiently reliable for the purposes of our audit.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. Cape Cod Community College did not accurately report all required crime statistics in its annual security report and to the US Department of Education.

Cape Cod Community College (CCCC) did not accurately report some statistics for Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (Clery Act) crimes that were allegedly committed within CCCC's Clery geography during calendar years 2020 through 2022 to the US Department of Education (US DOE). In addition, we were unable to cross-reference the Clery Act crimes reported in CCCC's 2023 annual security report (ASR) with the data in CCCC's daily crime log and student disciplinary action log. This was because of discrepancies in how the crime categories are recorded in each system, which made a direct comparison impossible.

There was a total of 24 Clery Act crime categories listed on CCCC's 2023 ASR. We inspected all 24 Clery Act crime categories and identified 9 with variances between what was reported in CCCC's 2023 ASR and what was reported to US DOE. Of these 9 categories with variances, 6 had more crimes reported to US DOE than what was reflected in CCCC's 2023 ASR, and 2 had fewer crimes reported to US DOE. For example, CCCC reported 4 rapes for calendar year 2022 in its 2023 ASR but reported 12 rapes to US DOE. Additionally, CCCC reported 1 motor vehicle theft for calendar year 2022 in its 2023 ASR, which was not reported to US DOE.

See the table below for a comparison of what CCCC reported in its 2023 ASR and to US DOE.

Calendar Year	2020		2021		2022	
Clery Act Crime Category	Reported in 2023 ASR	Reported to US DOE	Reported in 2023 ASR	Reported to US DOE	Reported in 2023 ASR	Reported to US DOE
Sex Offenses / Violence Against Women Act Offense Rape	1†	1	4†	4	4†	12
Fondling	0	0	2†	2	4†	11
Robbery	0	0	0	0	1†	2
Burglary	0	0	0	0	1	2
Motor Vehicle Theft	0	0	0	0	1	0
Domestic Violence (Violence Against Women Act Offense)	0	0	1*	1	0	0
Dating Violence (Violence Against Women Act Offense)	0	0	0	0	3†	8
Stalking (Violence Against Women Act Offense)	8†	8	2‡	2	11†	22
Hate Crime (Intimidation, Bias—Race)	1**†	0	0	0	0	0

* This Domestic Violence (Violence Against Women Act Offense) incident was reported in CCCC's 2023 ASR under the total column for calendar year 2021 but was not reported in the applicable location (the On Campus Non-Campus Public Property column).

** According to CCCC's director of public safety, this Hate Crime (Intimidation, Bias—Race) was not a hate crime and should not have been reported.

† According to CCCC's 2023 ASR, these crimes occurred in or on non-campus properties associated with CCCC, not on the main campus itself.

‡ According to CCCC's 2023 ASR, one of these crimes occurred on campus and one occurred on non-campus property.

In addition to the above variances, we identified at least one disciplinary referral for drug use noted in CCCC's student disciplinary action log that was not reported either in CCCC's ASR or to US DOE.

If CCCC inaccurately reports its Clery Act crime statistics, then current and prospective students, CCCC employees, and members of the public may draw incorrect conclusions about campus safety. Additionally, not complying with the Clery Act's ASR reporting requirements may result in CCCC having to pay fines to US DOE.

Authoritative Guidance

According to Section 668.46(c) of Title 34 of the Code of Federal Regulations (CFR),

*(1) **Crimes that must be reported and disclosed**. An institution must report to the [US DOE] and disclose in its annual security report statistics for the three most recent calendar years concerning the number of each of the following crimes that occurred on or within its Clery geography and that are reported to local police agencies or to a campus security authority:*

(i) Primary crimes, including . . .

(B) Sex offenses:

(1) Rape;

(2) Fondling . . .

(C) Robbery . . .

(E) Burglary.

(F) Motor vehicle theft . . .

(ii) Arrests and referrals for disciplinary actions, including—

(A) Arrests for liquor law violations, drug law violations, and illegal weapons possession . . .

(iii) Hate crimes, including—

(A) The number of each type of crime in paragraph (c)(1)(i) of this section that are determined to be hate crimes; and

(B) The number of the following crimes that are determined to be hate crimes:

(1) Larceny-theft.

(2) Simple assault.

(3) Intimidation.

(4) Destruction/damage/vandalism of property.

(iv) Dating violence, domestic violence, and stalking. . . .

(2) All reported crimes must be recorded. . . .

(3) Crimes must be recorded by calendar year.

(i) An institution must record a crime statistic for the calendar year in which the crime was reported to local police agencies or to a campus security authority.

(ii) When recording crimes of stalking by calendar year, an institution must follow the requirements in paragraph (c)(6) of this section.

> ***(4) Hate crimes must be recorded by category of bias.*** *For each hate crime recorded under paragraph (c)(1)(iii) of this section, an institution must identify the category of bias that motivated the crime. For the purposes of this paragraph, the categories of bias include the victim's actual or perceived—*
>
> *(i) Race.*

According to US DOE's *Handbook for Campus Safety and Security Reporting*, CCCC must "retain the annual security report and all supporting records used in compiling the report for three years." This includes the supporting records from CCCC's daily crime log, CCCC's student disciplinary action log, and any other records that were used to report the Clery Act crime statistics in CCCC's 2023 ASR.

Reasons for Issue

According to CCCC management, there was turnover in the position of chief of police and public safety during the audit period, which led to issues with accurate recordkeeping and reporting. The former chief of police and public safety was responsible for reporting CCCC's Clery Act crime statistics in CCCC's ASR and to US DOE accurately and in a timely manner. CCCC management also told us that the inconsistencies between what was reported in the ASR and what was reported to US DOE may be because of subjective interpretations of reporting requirements as it relates to Clery geography. Additionally, user interpretation, generalization, and poor supervisory oversight contributed to issues in identifying allegations of Clery Act–reportable crimes within CCCC's daily crime log and CCCC's student disciplinary action log as well as the proper reporting of these allegations in CCCC's ASR and to US DOE.

CCCC management did not provide a reason why the former chief of police and public safety did not retain all the supporting documentation used to complete CCCC's 2023 ASR.

Recommendation

CCCC must make certain that all Clery Act crimes that occur within its Clery geography are accurately recorded in CCCC's daily crime log and its ASR by establishing policies and procedures to ensure that the following occur:

- cases are recorded accurately in CCCC's daily crime log, and are also identified as Clery Act crimes where applicable;
- Clery Act crimes are accurately documented in CCCC's disciplinary action records management system and reported to CCCC's Department of Public Safety so that they can be properly investigated and included in CCCC's ASR;

- a verification process is developed, documented, and implemented by CCCC that includes supervisory review and sign-off of the disciplinary action records on a regular basis;
- Clery Act crime data is accurately reported to US DOE; and
- as required by law, all supporting documentation for CCCC's Clery Act crime statistics is retained by CCCC's Department of Public Safety, including the daily crime log statistics, student disciplinary action log statistics, and any other records used to complete CCCC's ASR for at least three years.

Auditee's Response

Cape Cod Community College (the College) takes seriously its role in reporting crimes as required under federal and state laws, while acknowledging changes in those laws and ambiguities in reporting standards. The dramatic impact of the COVID-19 pandemic, implementation of the Massachusetts Police Officer Standards & Training (POST) reforms, and changes in leadership has resulted in changes and evolution of the College's Public Safety/Police Department (Department) throughout the reporting period (Calendar years 2020, 2021 & 2022) to present day. Just as reporting standards evolve or become more fine-tuned, different persons doing the reporting may result in differences in interpretation as to counting or not counting certain events in reports. For example, student conduct issues which are not traditionally understood as crimes—especially when the result of a misunderstanding by a student and the mistaken over-reporting of an incident by a public safety officer—reasonably results in differences in emphasis, enlargement of statistics, and differences between Annual Security Report (ASR) and U.S. Department of Education (DOE) reporting which have since been corrected.

Presently, the College's Chief of Police/Director of Public Safety is one of two sworn police officer positions and the sole administrator/manager for the Department. This level of staffing is commensurate with the low occurrence of crime on the College's campus. The 2022 variation between the statistics reported in the ASR and those reported to DOE is, in part, related to recording redundant data from three sites which resulted in an overcount. In support of this it is significant to note that:

1. *The DOE Campus Security Survey requires users to identify Clery Geography within a "Yes" or "No" type framework.*

2. *The DOE Campus Security Survey reports data in aggregate.*

For example, if a College maintains two separate programs (Satellite Campus) on another institution's property (Host Campus), and if each of those discrete programs meet the federal definition of a "campus," then the crime statistics for the Host Campus must be assimilated by each Satellite Campus. While the ASR can explain that the crimes reported at each Satellite Campus actually occurred on the Host Campus, and that these crimes (for example two burglaries) are the same, the Campus Security Survey counts in the aggregate and reports four, instead of two, burglaries. The College has an affiliation with Bridgewater State University (BSU), and it is important for [the Office of the State Auditor (OSA)] to note the location of crime data, whether it occurred on the campus of BSU or the College's West Barnstable campus. Indeed, in September 2024, the College consulted with DOE's Clery HelpDesk to ensure it was reporting crimes correctly

and based on that conversation, revised the College's Clery geography. This explains why it appeared to OSA that there were 12 rapes as four rapes counted on the College's individual site reports and counted in the aggregate when in fact there were a total of four rapes and none of these occurred at the College but rather at BSU.

The recommendations suggested in the preliminary report of OSA will allow the College to continue to make improvements to its ASR reporting process in addition to those reforms already instituted. CSA training has been one such measure. Much of the reporting that was subject of the audit of public safety cases was the tendency of report writers to classify events as "criminal" when they were not. This over-reporting of incidents resulted in skewing ASR reportable incidents. Going forward, such incident reporting will be forwarded and reviewed by the Chief for applicability to ASR and then entered into the College's [case management system] that is the clearinghouse for all Department reports.

The [case management system] captures all reportable events for the Department; this includes crimes, emergency medical response, and other relevant incidents (e.g. property damage, accidents). The current Chief publishes a crime log which is inclusive of Clery crimes and other calls for service as identified above and is available to the public which meets the requirement of both the Clery Act and Code of Massachusetts Regulations for police department reporting.

In summary, the College views this audit finding as an aberration of the confluence of multiple circumstances and ambiguities in reporting standards rather than a pattern of conduct. Further, it is reasonable to infer that ambiguity in Clery geography related to the College campuses and to Host campuses contributed to the inconsistent [campus security survey] reporting detected by the OSA.

Auditor's Reply

We acknowledge that the discrepancies in crime reporting may have been influenced by staffing changes and uncertainty around how to properly classify and count certain incidents—particularly those related to Clery geography and potential duplication across locations. We believe it is essential for CCCC to implement effective policies and procedures to ensure accurate and consistent reporting of crime statistics. We strongly encourage CCCC to fully implement our recommendations, as doing so will help ensure compliance and improve the reliability of CCCC's crime data.

Based on its response, CCCC is taking measures to address our concerns regarding this matter. As part of our post-audit review process, we will follow up on this matter in approximately six months.

2. Cape Cod Community College did not properly identify and train campus security authorities in their duties as campus security authorities.

CCCC did not have a formal process in place to determine which employees met the definition of a campus security authority (CSA) or to ensure that these employees were notified of and trained on their

responsibilities. Although CCCC provided us with a list of six employees, each of whom it determined as meeting the definition of a CSA during the audit period, CCCC could not demonstrate the process used to make this determination or that these employees had received training on their responsibilities as CSAs.

If CCCC does not properly designate and train all CSAs, then CCCC's ability to compile and report accurate annual crime statistics is limited, and, with inaccurately reported crime statistics, current and prospective students, CCCC employees, and members of the public may be misinformed or draw incorrect conclusions about campus safety.

Authoritative Guidance

According to 34 CFR 668.46(a), a CSA is defined as the following:

> *(i) A campus police department or a campus security department of an institution.*
>
> *(ii) Any individual or individuals who have responsibility for campus security but who do not constitute a campus police department or a campus security department . . . such as an individual who is responsible for monitoring entrance into institutional property.*
>
> *(iii) Any individual or organization specified in an institution's statement of campus security policy as an individual or organization to which students and employees should report criminal offenses.*
>
> *(iv) An official of an institution who has significant responsibility for student and campus activities, including, but not limited to, student housing, student discipline, and campus judicial proceedings. If such an official is a pastoral or professional counselor . . . the official is not considered a campus security authority when acting as a pastoral or professional counselor.*

According to the Clery Act Appendix of the *Federal Student Aid Handbook*,

> *The Department [of Education] will defer to an institution's designation of CSAs as authoritative and provide any technical assistance necessary to work with institutions to help ensure proper identification and notification of CSAs consistent with the regulations.*

According to CCCC's 2023 ASR, examples of individuals who are considered CSAs include the following:

> *CCCC CSA's include student services personnel, the College's affirmative action officer/Title IX coordinator, weekend/evening administrators, satellite campus managers, employees who monitor building access (i.e. designated Fitness Center personnel), and may include others whom CCCC recognizes as having a "significant responsibility for student and campus activities" as part of their regular duties.*

Reasons for Issue

CCCC management could not explain why a formal process had not been established to determine which employees met the definition of a CSA and to train those employees. According to CCCC management, the six individuals who were CSAs during the audit period were identified by the former chief of police and public safety based upon this official's experience.

CCCC did not have policies and procedures in place to ensure that all CSAs were trained in their responsibilities and that records of completion of this training were retained.

Recommendations

1. CCCC should establish a process for its Human Resources Department and Department of Public Safety to identify individuals who meet the definition of a CSA.
2. CCCC should maintain and regularly update a list of identified CSAs.
3. CCCC should notify identified CSAs and train them on their responsibilities as CSAs at least annually and retain records of training completion for all CSAs.

Auditee's Response

Cape Cod Community College (the College) acknowledges that, previously the College could not fully authenticate training delivered to Campus Security Authorities (CSAs) which although not required by Clery is best practice. The College is also currently improving the training and identification of the CSAs throughout the organization. Effective August 2024, the College partnered with an outside vendor to provide an array of necessary trainings for a core group of employees identified as CSAs. In 2025, this core group of CSAs was expanded. Additionally, the current Chief has formal training in the foundations of the Clery Act. The College has also established an ad hoc Clery Team to review the ASR. The College agrees with the recommendation that Human Resources and the Department coordinate on the identification and incorporation of the duties of CSA.

Learning from the audit findings, the College is moving forward with the following framework to ensure that the process behind the ASR is more robust.

1. *Identify multidisciplinary senior level representatives to comprise a Clery (compliance) Team.*
2. *Designate an administrative assistant and/or compliance coordinator to support CSA recordkeeping, including CSA identification and training.*
3. *Ensure that Clery Compliance team members have an adequate understanding of Clery regulations.*
4. *Incorporate . . . CSA reporting form on College website.*

Auditor's Reply

Based on its response, CCCC is taking measures to address our concerns regarding this matter. As part of our post-audit review process, we will follow up on this matter in approximately six months.

3. Cape Cod Community College did not ensure that all of its employees completed cybersecurity awareness training.

CCCC did not ensure that all employees (newly hired and existing employees) completed cybersecurity awareness training during the audit period. Regarding the initial cybersecurity awareness training for our sample of 35 newly hired employees, we found the following:

- Out of our sample of 35 newly hired employees, 20 (57%) were never enrolled in initial cybersecurity awareness training and, therefore, never completed the training.
- Out of our sample of 35 newly hired employees, 8 (23%) were enrolled in initial cybersecurity awareness training but never completed the training.
- Out of our sample of 35 newly hired employees, 1 (3%) completed initial cybersecurity awareness training 350 days late.

Regarding the annual refresher cybersecurity awareness training, from our sample of 40 existing employees, we found the following:

- For the 2021 annual refresher cybersecurity awareness training:
  - Out of our sample of 40 existing employees, 5 (13%) were never enrolled in the annual refresher cybersecurity awareness training, and, therefore, never completed the training.
  - Out of our sample of 40 existing employees, 8 (20%) were enrolled in the annual refresher cybersecurity awareness training but did not complete the training.
- CCCC did not provide annual refresher cybersecurity awareness training to CCCC's employees in calendar year 2022.
- For the 2023 annual refresher cybersecurity awareness training:
  - Out of our sample of 40 existing employees, 5 (13%) were never enrolled in the annual refresher cybersecurity awareness training and, therefore, never completed the training.
  - Out of our sample of 40 existing employees, 19 (48%) were enrolled in the annual refresher cybersecurity awareness training but did not complete the training.

If CCCC does not ensure that all of its employees complete cybersecurity awareness training, then CCCC exposes itself to an increased risk of cybersecurity attacks, and financial and/or reputational losses.

Authoritative Guidance

According to CCCC's "Cyber / Information Security Awareness Training" policy,

> *All users of CCCC information resources will complete security awareness training with respect to CCCC information security policies and procedures upon hire and subsequently at least annually. Human Resources is responsible for notifying the Chief Information and Technology Officer (CITO) of a new hire immediately so that the workforce member can be trained in a timely manner. Employees will receive documentation of completion upon successfully finishing the training indicating that they understand the basis of cybersecurity and information protection. After the training has been conducted, CCCC will maintain such records, as it deems appropriate, to confirm that an employee or contractor received such training.*

According to Section 6.2.3 of the Executive Office of Technology Services and Security's Information Security Risk Standard IS.010,

> *6.2.3 New Hire Security Awareness Training: All new personnel must complete an Initial Security Awareness Training course . . . The New Hire Security Awareness course must be completed within 30 days of new hire orientation.*

According to Section AT-3 of Revision 5 of the National Institute of Standards and Technology's Special Publication 800-53,

> *ROLE-BASED TRAINING*
>
> *Control:*
>
> *a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: . . .*
>
> *1. Before authorizing access to the system, information, or performing assigned duties, and [at least annually] thereafter.*

Reasons for Issue

CCCC did not have monitoring controls in place during the audit period to ensure that all of its employees were enrolled in and completed the required initial and annual refresher cybersecurity awareness trainings.

According to CCCC management, there was employee turnover in the chief information officer position during calendar year 2022. This position would have been responsible for providing cybersecurity awareness training to CCCC employees. As a result, CCCC did not offer cybersecurity awareness training in calendar year 2022.

Recommendation

CCCC should develop and implement monitoring controls to ensure that all employees are enrolled in and complete initial and annual refresher cybersecurity awareness training.

Auditee's Response

The College recognizes that during the audit period not all employees had completed cybersecurity awareness training, and the tracking of college-wide training completion has not always been complete. While the Community Colleges do not fall under the Executive Office of Technology Services and Security (EOTSS) and its requirements, the College acknowledges [EOTSS] models as best practices.

The College was the victim of a cyber security attack in 2018 that resulted in a significant loss of funds. However, through quick identification of the crime and follow up with law enforcement and bank investigators, most of the funds were recovered. The College worked very closely with the US Attorney for the Southern District of New York in the prosecution and sentencing of three criminals involved in this crime. As a result, the College is hyper-focused on cyber security issues and becoming a standard bearer for excellence in this space both in technology and social engineering awareness training. Cape Cod Community College was the first Community College to introduce Multi-Factor Authentication to verify users. We were one of the first to introduce Managed Detection and Response (MDR) which is software that monitors and detects a potential cyber breach, along with Endpoint Detection and Response (EDR) which isolates and shuts down a computer under the suspicion of a breach.

Attackers do not always attack when staff are in the office. Often, these attacks happen in the middle of the night, so we have safeguards in place that protect our systems 24/7. The College uses [a software platform] as protection services for our hardware and [a member of a third-party company] as a Cyber Security officer. Both services are designed to protect the College in a manner that uses a modern security approach and verifies access request, regardless of where it comes from, to keep our systems and community safe. The College's goal is protecting everyone through smart, adaptive safeguards.

It is noteworthy, that the 2018 cybercrime occurred in a functional area of the College where all users had received cybersecurity training when the actual crime occurred. Noting the sophistication of the social engineering that was utilized, we recognize the continuing need for training our employees to become more familiar with developments in cybersecurity.

The College agrees that education of our employees is important, and we have provided training during Opening Day and Professional Day but have not recorded all the participants. The College has been running weekly Phishing-Email campaigns and "Scam of the week" messages using [third-party, web-based training program]. Also, in October 2024, the College initiated a cyber-training module to all full-time non-unit professional employees (managers) and recorded a 75% completion percentage.

The College's new [chief information officer] will work closely with [human resources] to be sure we increase our percentages of training for new employees within the first 30 days by requiring that the training be completed onsite and give time for new employees to complete, like the Commonwealth does for required state ethics training. The College will link our [student records, accounting, and finance system] to our [third-party, web-based training program] . . . to be able to provide one comprehensive listing. The College has also hired a new Administrative Support personnel who works in both [information technology and human resources] to assist in this type of follow-up that previously was done by the department head.

Auditor's Reply

Based on its response, CCCC is taking measures to address our concerns regarding this matter. As part of our post-audit review process, we will follow up on this matter in approximately six months.

APPENDIX

Below are the crimes that must be reported under the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act, according to Section 668.46(c) of Title 34 of the Code of Federal Regulations.

(1) ***Crimes that must be reported and disclosed.*** *An institution must report to the [US Department of Education] and disclose in its annual security report statistics for the three most recent calendar years concerning the number of each of the following crimes that occurred on or within its Clery geography and that are reported to local police agencies or to a campus security authority:*

(i) Primary crimes, including—

(A) Criminal homicide:

(1) Murder and nonnegligent manslaughter; and

(2) Negligent manslaughter.

(B) Sex offenses:

(1) Rape;

(2) Fondling;

(3) Incest; and

(4) Statutory rape.

(C) Robbery.

(D) Aggravated assault.

(E) Burglary.

(F) Motor vehicle theft.

(G) Arson.

(ii) Arrests and referrals for disciplinary actions, including—

(A) Arrests for liquor law violations, drug law violations, and illegal weapons possession.

(B) Persons not included in paragraph (c)(1)(ii)(A) of this section who were referred for campus disciplinary action for liquor law violations, drug law violations, and illegal weapons possession.

(iii) Hate crimes, including—

(A) The number of each type of crime in paragraph (c)(1)(i) of this section that are determined to be hate crimes; and

(B) The number of the following crimes that are determined to be hate crimes:

(1) Larceny-theft.

(2) Simple assault.

(3) Intimidation.

(4) Destruction/damage/vandalism of property.

(iv) Dating violence, domestic violence, and stalking as defined in paragraph (a) of this section.

*(2) **All reported crimes must be recorded. . . .***

*(3) **Crimes must be recorded by calendar year.***

(i) An institution must record a crime statistic for the calendar year in which the crime was reported to local police agencies or to a campus security authority.

(ii) When recording crimes of stalking by calendar year, an institution must follow the requirements in paragraph (c)(6) of this section.

*(4) **Hate crimes must be recorded by category of bias.** For each hate crime recorded under paragraph (c)(1)(iii) of this section, an institution must identify the category of bias that motivated the crime. For the purposes of this paragraph, the categories of bias include the victim's actual or perceived—*

(i) Race;

(ii) Gender;

(iii) Gender identity;

(iv) Religion;

(v) Sexual orientation;

(vi) Ethnicity;

(vii) National origin; and

(viii) Disability.