Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

Official Audit Report – Issued November 8, 2021

Office of the Commissioner of Probation

For the period July 1, 2018 through June 30, 2020

Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

November 8, 2021

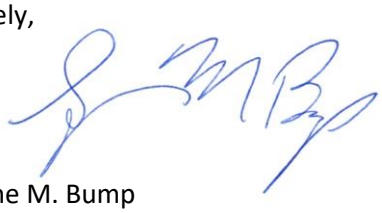
Mr. Edward J. Dolan, Commissioner
Office of the Commissioner of Probation
1 Ashburton Place, Room 405
Boston, MA 02108

Dear Commissioner Dolan:

I am pleased to provide this performance audit of the Office of the Commissioner of Probation. This report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2018 through June 30, 2020. My audit staff discussed the contents of this report with management of the agency, whose comments are reflected in this report.

I would also like to express my appreciation to the Office of the Commissioner of Probation for the cooperation and assistance provided to my staff during the audit.

Sincerely,



Suzanne M. Bump
Auditor of the Commonwealth

cc: The Honorable Paula M. Carey, Chief Justice of the Trial Court

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AFI	Automated Facial Intelligence
CORI	Criminal Offender Record Information
ELMO	electronic monitoring
EM	event monitor
EOTSS	Executive Office of Technology Services and Security
GPS	global positioning system
HR	human resources
ISMS	information security management system
MPS	Massachusetts Probation Service
OCP	Office of the Commissioner of Probation
SCRAM	Secure Continuous Remote Alcohol Monitoring
WMTD	Wearable Miniature Tracking Device
WMU	Warrant Management Unit

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 the Office of the Commissioner of Probation (OCP) for the period July 1, 2018 through June 30, 2020. In this performance audit, we determined whether OCP enrolled participants in the Electronic Monitoring Program in accordance with court-ordered parameters, monitored the participants in accordance with OCP policies and procedures, and ensured that participants' juvenile probation records were accessed by police officials in accordance with Section 90 of Chapter 276 of the General Laws.

Our audit revealed no significant instances of noncompliance by OCP that must be reported under generally accepted government auditing standards. However, we did identify a number of information technology control issues we believe warrant OCP's attention, which we have disclosed in the "Other Matters" section of this report.

OVERVIEW OF AUDITED ENTITY

The Office of the Commissioner of Probation (OCP) is part of the Massachusetts Trial Court system. The system is overseen by the Chief Justice of the Trial Court and the Court Administrator, who report to the Chief Justice of the Supreme Judicial Court. According to the Massachusetts Probation Service's (MPS's) website,

> *The Commissioner of Probation, Edward J. Dolan, and his office oversee the Massachusetts Probation Service and the Office of the Community Corrections, which includes 105 probation departments and 18 community corrections centers, the Electronic Monitoring Center, and the Trial Court Community Service Program. Probation officers working in adult criminal courts (Superior Court, Boston Municipal Court, and District Court) supervise pre-trial and post-disposition cases.*

The Commissioner administers MPS in conjunction with the Chief Justice of the Trial Court and the Court Administrator, who make final decisions on a number of matters. According to its website,

> *The Massachusetts Probation Service's mission is to increase community safety, reduce recidivism, contribute to the fair and equitable administration of justice, support victims and survivors, and assist individuals and families in achieving long term positive change.*

OCP is located at 1 Ashburton Place in Boston. As of June 30, 2020, the office had 1,778 employees. Its operating budget was $156,133,131 for fiscal year 2019 and $163,055,581 for fiscal year 2020.

According to MPS's website,

> *The Massachusetts Probation Service's Electronic Monitoring (ELMO) Program was first established in April 2001 as an alternative to incarceration and to provide structure, control, and accountability for probationers who were sentenced to house arrest by a judge.*

In addition to supervision of probationers, the program includes supervision of parolees and litigants. The program's core functions include enrolling program participants, handling program alerts, and responding to phone calls. Electronic Monitoring (ELMO) Program employees also call courts to gather information, resolve problems, and follow up on warrants. The primary tools the ELMO Program uses to monitor participants are global positioning system (GPS) devices—specifically, electronic bracelets that provide participants' locations via GPS—and Secure Continuous Remote Alcohol Monitoring (SCRAM) remote breath devices, which provide participants' real-time breath alcohol test results and locations via GPS.

The ELMO Center, home of ELMO Program operations, is in Clinton, and its daily operations are managed by a statewide manager from OCP. The center is open 24 hours a day all year. During our audit period, the ELMO Program monitored 19,960 probationers, parolees, and litigants: 14,073 with GPS devices only, 4,803 with SCRAM devices only, and 1,084 with both GPS and SCRAM devices.

The ELMO Center is staffed by a team of 64 MPS employees who collaborate with probation officers throughout the state to monitor participants. According to the ELMO Center's website,

> *GPS devices are used to enforce court-mandated curfews and court orders, including house arrest. The remote breath alcohol monitoring device is used to monitor people who are court-ordered to not drink alcohol.*

The ELMO Program uses two external software systems to manage enrollment and monitoring. The software system used for managing GPS monitoring of participants is called Attenti Event Monitor (EM) Manager. This system is owned by the Attenti Group, a company with operations in over 30 countries. The company's United States headquarters is in Odessa, Florida. The software system used for managing SCRAM participants is called SCRAMNET. This software is owned by SCRAM Systems, which also operates in a number of other countries and has its global headquarters in Littleton, Colorado.

ELMO Program Enrollment Process

For each new participant with a GPS or SCRAM device, a probation officer or parole officer, or an officer's designee, must complete an enrollment packet. The probation officer or parole officer assigned to the new participant emails the enrollment packet information to the ELMO Center. An ELMO Center employee electronically tags the email to indicate that the employee is working on the enrollment; prints the enrollment packet; places the packet in a folder; and attaches a label indicating whether the packet is for a participant with a GPS device, a SCRAM device, or both. The packet is placed with those of other enrollments that occurred that day; an overnight team reviews the packets for accuracy. Each GPS enrollment packet includes court-ordered parameters[1] in the following documents: (1) an Enrollment Form; (2) a Weekly Itinerary Form; (3) a Zone Form, if the participant is subject to a court-ordered exclusion or inclusion zone (i.e., an area the participant is not allowed to enter or leave); (4) a Victim Information Form, if there is a victim; and (5) a signed Order of GPS Supervision Conditions Form. A sixth form, the Pre-Trial Conditions of Release Form, is not required for new enrollments but is kept on file if

1. Court-ordered parameters are critical supervisory directives from the court that must be adhered to and enforced. These include conditions of supervision such as exclusion and inclusion zones, remote breath testing schedules, and victim notification requirements.

received. Each SCRAM enrollment packet includes (1) an Enrollment Form; (2) an Alcohol Monitoring Device Weekly Itinerary Form; and (3) a Victim Information Form, if applicable. A Pre-Trial Conditions of Release Form is not required for new enrollments but is kept on file if received. The ELMO Center employee enters the information from enrollment packets in Attenti EM Manager for participants with GPS devices and SCRAMNET for participants with SCRAM devices. This employee then contacts the probation officer who is responsible for supervising each participant to activate the monitoring equipment. A participant is considered enrolled once the monitoring equipment is activated.

According to OCP management, during our audit period the ELMO Center began a transition to a new paperless case filing system using MassCourts.[2] The goal of transitioning to the new system was to streamline operations, reduce redundancy, and increase efficiency in enforcing court orders. For this new system, once a court orders an individual to use a GPS and/or SCRAM device, a probation officer, or an officer's designee, enters information about the individual in MassCourts. This information may include special conditions, inclusion and/or exclusion zones, and curfews. The probation officer completes an enrollment packet in MassCourts, as well as an Order of GPS Supervision Conditions Form if the individual will be monitored with a GPS device, and emails the ELMO Center a notification that a new enrollment has been uploaded. An ELMO Center employee then accesses the enrollment packet in MassCourts and processes the new participant's enrollment. After the enrollment is processed, the ELMO Center employee emails the probation officer to indicate that the monitoring equipment is ready to be activated.

ELMO Program Alert Process

GPS Monitoring

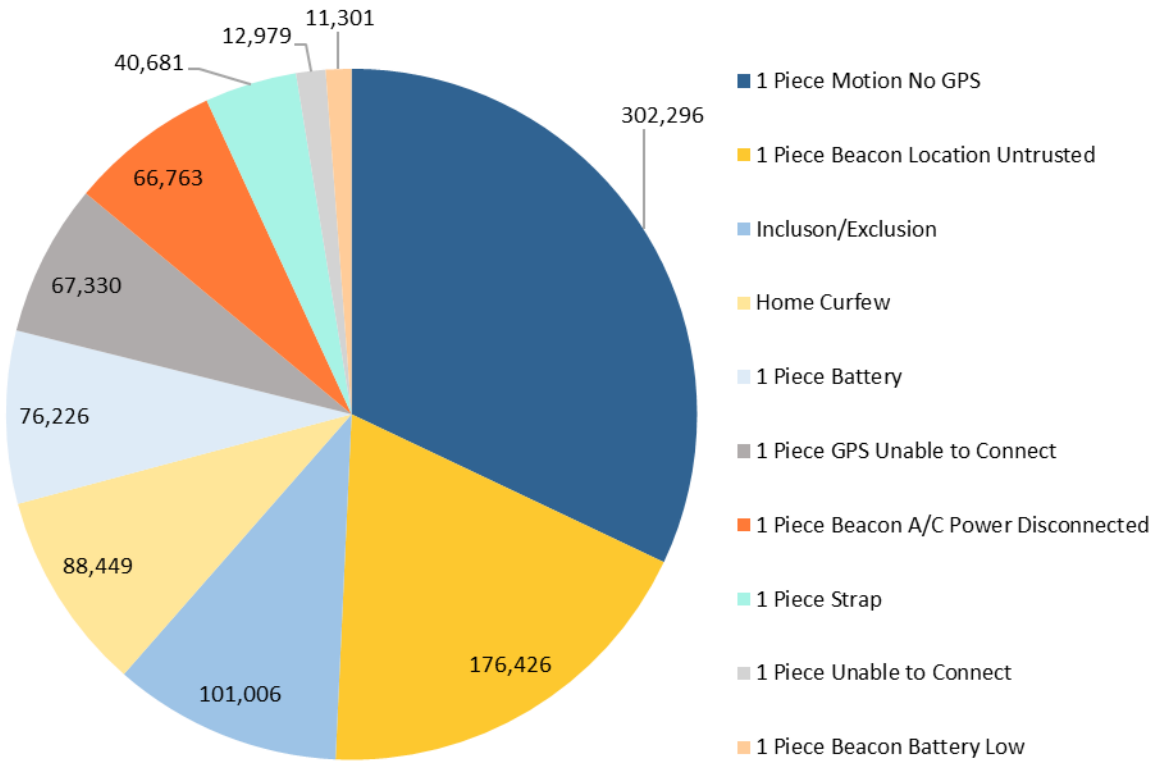
GPS device malfunctions, tampering with or removal of GPS devices, and violations of exclusion and/or inclusion zones and curfews cause GPS alerts. The ELMO Center receives approximately 2,300 alerts a day. Alerts are categorized as Tier 1, Tier 2, or Tier 3. (See Appendix A for a description of alerts by tier.) Tier 1 alerts are the most serious and Tier 3 the least. Tier 1 and Tier 2 alerts can involve deliberate tampering with or removal of equipment, as well as violation of exclusion and/or inclusion zones and curfews. Tier 3 alerts are more technical and generally involve other variables, including low battery, lack of GPS coverage, or power disconnection.

2. According to the Massachusetts Court System's website, MassCourts is "the central case management application used by all of the Trial Court departments and the Massachusetts Probation Service."

If an alert occurs during court hours, an ELMO Center employee attempts to contact the participant to determine what caused it and/or sends a notification to the participant's device. The ELMO Center employee investigates information provided by the participant, reviews the participant's itinerary and any special circumstances (e.g., releases for medical treatment or court appearances), and checks for any other pertinent notes. If there is no documentation of special circumstances, the ELMO Center employee contacts the participant's probation officer to discuss the alert and what response is appropriate. If the employee cannot contact the probation officer, the employee contacts the assistant chief probation officer or chief probation officer in any court where the participant is being supervised. ELMO Center employees must record all actions in Attenti EM Manager or SCRAMNET case notes.

If an alert occurs after court hours, ELMO Center employees follow the initial steps outlined above to resolve it. If these steps do not resolve the alert, an ELMO Center employee informs an ELMO supervisor/manager and, if directed to do so, the ELMO Center's Warrant Management Unit (WMU).[3] WMU is provided with all information available for the case, including Court Activity Record Information,[4] charges, any history of failing to respond to summonses or complaints within the required timeframe, all communications with the participant, and the participant's history of alerts. If a WMU employee cannot resolve the alert, s/he issues a warrant, and an ELMO Center employee fills out the warrant and a Warrant Information Form, notifies the police, and emails the warrant and form to the probation officer and chief probation officer in any court where the participant is being supervised. If there is a Victim Notification Form in the participant's folder that indicates that a victim wants to be notified after hours, the victim must be notified of the warrant. Additionally, if there is a victim, the ELMO Center employee copies an OCP victim services coordinator on the email with the warrant. On the next business day, if the warrant has not been resolved, WMU contacts the probation officer, assistant chief probation officer, and chief probation officer in any court where the participant is being supervised to see what additional steps need to be taken to resolve the alert and warrant. During the audit period, 958,384 GPS alerts were received. The top 10 alert types were as follows.

3. WMU consists of a chief probation officer and five assistant chief probation officers who also work at the ELMO Center and authorize warrants.
4. According to the Probate and Family Court's Standing Order 1-11, "[Court Activity Record Information] includes Criminal Offender Record Information (CORI), juvenile records and civil restraining order information."



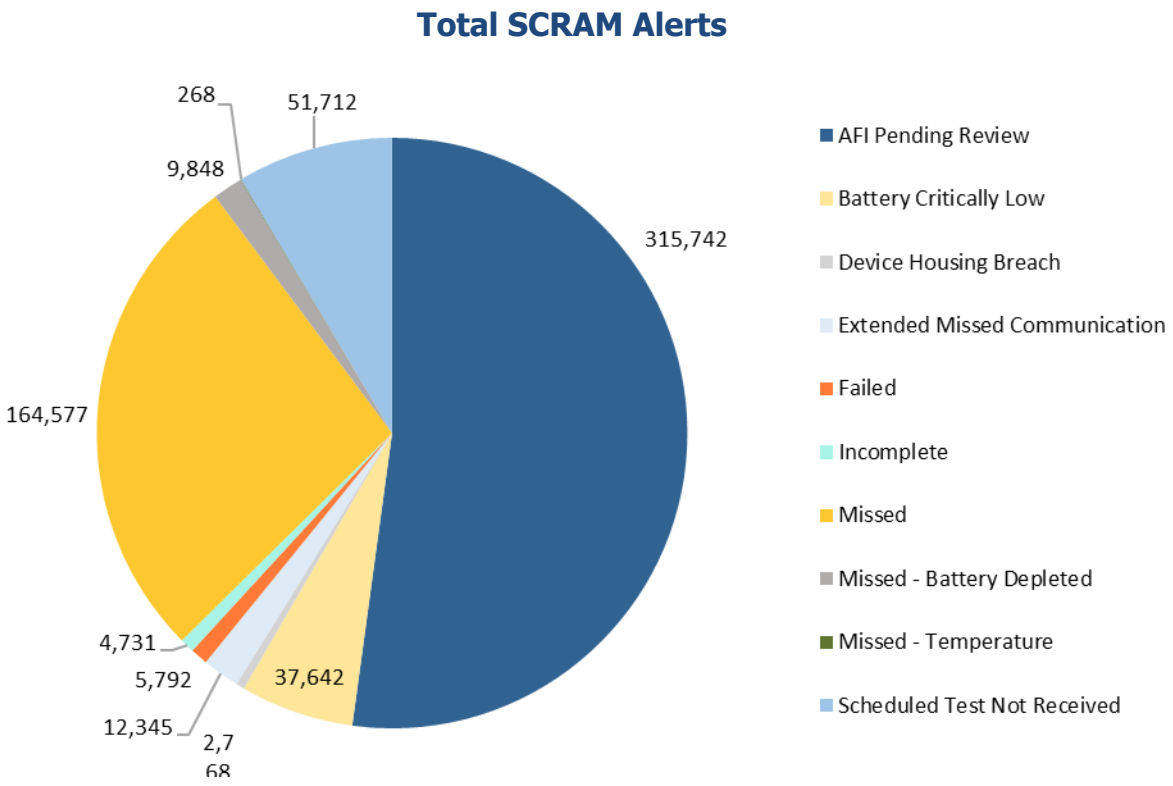
SCRAM Monitoring

Causes of SCRAM alerts include scheduled breath alcohol tests being missed; test results not being received within 90 minutes after a scheduled test; tests being failed (i.e., showing a breath alcohol concentration level above the acceptable threshold); and Automated Facial Intelligence (AFI) pending review alerts (which occur when the breath test for a participant is passed, but the photograph of the person tested does not match the initial enrollment photograph of the participant in SCRAM Systems' AFI software, or when a circumvention of the breath test is identified).

SCRAM alerts are generally handled in the order in which they are received. There are different categories of alerts, and each has its own response protocol. (See Appendix B for SCRAM alert categories.) For example, when a missed-test alert is received, an ELMO Center employee calls the participant to determine why the test was missed. The ELMO Center employee may request that the

participant take an on-demand test. Tests can be missed for various reasons, such as the SCRAM device malfunctioning or the participant not having charged the battery. If an alert is not resolved during office hours, an ELMO Center employee contacts the participant's probation officer to explain the situation. When an alert is generated after business hours, an ELMO Center employee follows a protocol similar to the protocol for handling after-hours GPS alerts. In both protocols, an ELMO supervisor/manager (and possibly WMU) is notified. As with GPS alerts, if the alert has not been resolved after initial protocol is followed, a warrant is issued and sent to the relevant authorities with jurisdiction over the participant's case.

There were 605,425 SCRAM alerts during the audit period, as shown below.



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 the Office of the Commissioner of Probation (OCP) for the period July 1, 2018 through June 30, 2020.

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 and the conclusion we reached regarding each objective.

Objective	Conclusion
1. Does OCP ensure that court-ordered parameter information is entered correctly in the global positioning system (GPS) and Secure Continuous Remote Alcohol Monitoring (SCRAM) systems in accordance with Sections B(1)(c) and B(5) of the Massachusetts Probation Service Electronic Monitoring (ELMO) Center's "GPS Standards Policy No. 02.07.01"?	**Yes**
2. Does OCP monitor GPS Tier 1 and Tier 2 alerts in accordance with the ELMO Center's "GPS Standards Policy No. 02.07.01" and the ELMO Program's "GPS Protocol"?	**Yes**
3. Does OCP monitor SCRAM alerts in accordance with the Trial Court's *Electronic Monitoring SCRAM Remote Breath Program (SCRAM) Procedures*?	**Yes**
4. Does OCP ensure that it obtains consent from a court justice before allowing police officials to access juvenile records, as required by Section 90 of Chapter 276 of the General Laws?	**Yes**

To achieve our audit objectives, we conducted interviews with OCP's staff and management and reviewed agency policies and procedures to gain an understanding of internal controls that were relevant to the objectives. In addition, we performed the following procedures to obtain sufficient, appropriate audit evidence to address the objectives.

Enrollment of GPS and SCRAM Participants

To determine whether OCP correctly entered information related to court-ordered parameters for GPS enrollment, we selected a random, statistical sample of 60 of 11,262 GPS participants who were enrolled or reenrolled during our audit period, with a confidence level of 95%, a tolerable error rate of 5%, and an expected error rate of 0%. We compared the most recent information in each participant's enrollment packet to information in the GPS tracking system, Attenti Event Monitor (EM) Manager. We reviewed the following sections of the various GPS enrollment packet forms: "Enrollee Information," "Enrollee Employment Information," "Offense and Supervision Information," "Victim Information," "Assigned Monitoring Equipment," "Victim Notification," and "Conditions of Supervision."

To determine whether OCP correctly entered information about court-ordered parameters for SCRAM enrollment, we selected a random, statistical sample of 60 of 4,253 SCRAM participants whose equipment was activated during our audit period, with a confidence level of 95%, a tolerable error rate of 5%, and an expected error rate of 0%. We compared the most recent information in each participant's enrollment packet to information in the SCRAM tracking system, SCRAMNET. We reviewed the following sections of the various SCRAM enrollment packet forms: "Enrollee Information," "Enrollee Employment Information," "Offense and Supervision Information," "Victim Information," "Assigned Monitoring Equipment," "Victim Notification," and "Alcohol Monitoring Device Weekly Itinerary Form."

Monitoring of GPS Alerts

To determine whether OCP monitored its GPS Tier 1 and 2 alerts in accordance with the ELMO Center's "GPS Standards Policy No. 02.07.01" and the ELMO Program's "GPS Protocol," we obtained a list of all 958,384 GPS alerts that the ELMO Center handled during our audit period. We grouped the alerts according to the category the ELMO Center had assigned to each one: Tier 1, Tier 2, or Tier 3. The total population of GPS Tier 1 and Tier 2 alerts during our audit period was 392,971.

We selected a random, statistical sample of 60 of these 392,971 alerts, with a confidence level of 95%, a tolerable error rate of 5%, and an expected error rate of 0%, and reviewed each alert to determine whether the ELMO Center followed pertinent and measurable steps specified in the ELMO Center's "GPS Standards Policy No. 02.07.01" and the ELMO Program's "GPS Protocol." To review each alert in our sample, we logged into Attenti EM Manager and reviewed the case notes and GPS alert history for each alert to verify that an ELMO Center employee had followed the required steps. Depending on the type

of alert, these steps could include contacting the participant, the participant's probation officer during business hours, or the Warrant Management Unit after hours and/or clearing the alert if applicable.

Monitoring of SCRAM Alerts

To determine whether OCP monitored SCRAM alerts in accordance with the Trial Court's *Electronic Monitoring SCRAM Remote Breath Program (SCRAM) Procedures*, we selected a random, statistical sample of 60 from the total population of 605,425 SCRAM alerts during our audit period that were not coded as "passed" (e.g., the test was not taken or indicated a higher-than-acceptable breath alcohol concentration), with a confidence level of 95%, a tolerable error rate of 5%, and an expected error rate of 0%. To review each alert, we logged on to SCRAMNET and reviewed the case notes and SCRAM device message history for each record to verify that an ELMO Center employee had adhered to the required steps. These steps could include contacting the participant, the participant's probation officer, or an OCP regional supervisor; requesting that the participant take an on-demand test; and/or clearing the alert.

Review of Juvenile Record Requests

To determine whether OCP ensured that it obtained consent from a court justice before allowing police officials to access participants' juvenile records as required by Section 90 of Chapter 276 of the General Laws, we selected a random, nonstatistical sample of 60 from the total population of 812 juvenile GPS participants who were monitored during the audit period. We determined whether there was a court justice's signature on the Order of GPS Supervision Conditions Form for each juvenile GPS participant and whether the relevant information in the "Conditions" paragraph[5] had been altered.

When using nonstatistical sampling, we could not project the results to the entire population.

Data Reliability

To determine the reliability of the Attenti reports of the population of GPS participants who were enrolled or reenrolled during the audit period (provided by OCP management), we checked for duplicate records and verified that all enrollment and reenrollment dates were within the audit period. ELMO management demonstrated for us Attenti EM Manager application controls designed to ensure the integrity of data entry by validating certain fields (e.g., ZIP code, county, and address) before allowing an

5. This paragraph states, "Coordinates and other data related to your physical location while on GPS are recorded and may be shared with the court, probation, parole, attorneys and law enforcement. Data generated by GPS equipment assigned to you is not private and confidential."

enrollment to continue. Based on these procedures, we determined that the GPS participant population obtained was sufficiently reliable for the purposes of this audit.

To determine the reliability of the list of SCRAM participants who were monitored during the audit period (provided by OCP management), we compared participant totals on the list to a spreadsheet we downloaded from SCRAMNET. We checked the list for duplicate records, hidden rows, and hidden columns and verified that entry dates were within the audit period. ELMO management demonstrated for us SCRAMNET application controls designed to ensure the integrity of data entry by validating certain fields (e.g., remote breath alcohol schedule not completed) before allowing an enrollment to continue. Based on these procedures, we determined that the SCRAM participant population obtained was sufficiently reliable for the purposes of this audit.

To determine the reliability of the alert population in the SCRAM alert resolution reports provided by OCP management, we verified that the reports contained the total number of SCRAM alerts that were resolved during the audit period. Additionally, we selected a sample of 20 SCRAM alerts and verified that the participants associated with them were monitored in SCRAMNET during the audit period. Based on these procedures, we determined that the SCRAM alert population obtained was sufficiently reliable for the purposes of this audit.

From Attenti EM Manager, we downloaded Total Alert Action Reports, which listed all GPS alerts for the audit period. To determine the reliability of these reports, we selected a sample of 20 alerts and verified that the participants associated with them were monitored in Attenti EM Manager during our audit period. Based on the analyses conducted, we determined that the GPS alert population obtained was sufficiently reliable for the purposes of this audit.

We assessed the reliability of the data obtained from Attenti EM Manager and SCRAMNET systems by reviewing policies for security management; interviewing OCP personnel who were knowledgeable about the systems; and testing certain information system general controls, including access controls, security awareness training, and personnel screening, for both Attenti EM Manager and SCRAMNET. Based on our understanding and testing of information system general and application controls, we determined that both Attenti EM Manager and SCRAMNET were reliable for the purposes of this audit. However, we did identify a number of issues, which we address in the “Other Matters” section of this report.

OTHER MATTERS

The Office of the Commissioner of Probation needs to strengthen information technology general controls.

During our review of Attenti Event Monitor (EM) Manager and SCRAMNET information technology general controls, we identified a number of issues that warrant attention from the Office of the Commissioner of Probation (OCP). These issues concern (1) incomplete or missing system approval documentation (e.g., lack of an Access Request Form[6] for SCRAMNET), (2) user access rights that were inconsistent with employees' job functions, (3) employees not completing cybersecurity awareness training, (4) missing evidence of Criminal Offender Record Information (CORI) checks, and (5) terminated employees not having their system access removed in accordance with state or vendor policies. (See Appendix C for a summary of issues found.)

We selected 50 current active users and 5 new active users out of a population of 1,074 employees who used Attenti EM Manager, SCRAMNET, or both during the audit period. Current users are OCP employees hired before the audit period, and new users are OCP employees hired during the audit period. Because the auditee uses two systems, we chose two unique lists of 25 employees, one list for each system, who were identified in the system as active users throughout the entire audit period. For the new-user test, we chose 5 employees who had access to both systems during audit period.

1. Evidence of Access Rights Approval

To determine whether employees' access rights were properly authorized, we requested the Access Request Forms for our sample of 55 employees. This constituted a request for 60 Access Request Forms, because 5 of the employees in our sample received access to both Attenti EM Manager and SCRAMNET. In our review, we found that in 54 of 60 instances, an Access Request Form was missing or did not contain the required OCP and/or vendor signatures authorizing the requested access.

Section 6.1.4.3 of the Executive Office of Technology Services and Security's (EOTSS's) "Access Management Standard" states, "User access requests shall be recorded (paper or tool-based) and approved by the requestor's supervisor." This standard applies to any Commonwealth entity that voluntarily uses, or participates in services provided by, EOTSS, such as mass.gov.

6 An Access Request Form is a form OCP submits to one of its vendors to ask it to grant a user access to a system (Attenti EM Manager, in this case). It is also used to request modification or termination of a user's access rights.

Section 1.5.7 of OCP's internal control plan states, "Department heads must limit access to resources and records to authorized individuals."

OCP management stated that Access Request Forms and signatures were missing for Attenti EM Manager because of a lack of management oversight and that the Attenti EM Manager Access Request Form was outdated and in the process of being replaced. They also stated that the reason there were missing Access Request Forms for SCRAMNET was that OCP had implemented SCRAMNET in November 2015 and no Access Request Form had been created for this system. Finally, OCP management told us they were considering a new combined Access Request Form for Attenti EM Manager and SCRAMNET.

Not having adequate access controls could compromise the security and integrity of sensitive OCP case data. OCP should update its forms and ensure that all necessary signatures and approvals from OCP and its vendor appear on these documents.

2. Evidence of Appropriate User Permission Rights

In 3 of the 60 instances we reviewed where employees were granted access to Attenti EM Manager, SCRAMNET, or both, user permission rights did not correspond with the system access level appropriate to the employees' positions.

Section 6.1.5.1 of EOTSS's "Access Management Standard" states,

> *The **Information Owner** or **Information Custodian** shall verify that the type of access requested is required for the user's role and responsibilities.*

This standard applies to any Commonwealth entity that voluntarily uses, or participates in services provided by, EOTSS, such as mass.gov.

The Attenti Group's "Access Control Policies and Procedures" states,

> *Customers [in this case, OCP] submit an "Access Request Form." Account representatives [at the Attenti Group] will approve these forms for the creation, modification, and [termination of customer user accounts]. Those forms are sent to the Monitoring Center, who will create/modify/[terminate] the [customer user accounts]. Only permissions requested are granted, based on the review by the account representative.*

Section 3.1 of SCRAM Systems' "Access Control Policy ([Information Security Management System, or ISMS])" states,

> *A request for access to the organization's network and computer systems shall first be submitted to the [SCRAM Systems information technology] Service Desk for approval. All requests will be processed according to a formal procedure that ensures that appropriate security checks are carried out and correct authorisation is obtained prior to user account creation.*

OCP management told us that the reason for two of these instances was poor internal communications and that in the third instance, management did not update an employee's permission rights to reflect that person's new positon at OCP.

Inappropriate permission rights could compromise the security and integrity of OCP data. OCP should ensure that user permission rights correspond to the system access level appropriate to each employee's position.

3. Evidence of Annual Security Awareness Training

OCP only began conducting cybersecurity awareness training in March 2020, and 7 of 55 users tested had not completed it as of the end of our audit period.

Section 6.2.4 of EOTSS's "Information Security Risk Management Standard" states, "All personnel will be required to complete Annual Security Awareness Training." This standard applies to any Commonwealth entity that voluntarily uses, or participates in services provided by, EOTSS, such as mass.gov.

OCP management told us that EOTSS training standards did not apply to OCP. However, OCP management told us that the Trial Court had implemented online security awareness courses that all judges and court staff members must complete. Based on training records provided by OCP, these courses were first provided to OCP employees on March 6, 2020.

Insufficient cybersecurity awareness training may lead to user error and compromise the integrity and security of protected information at OCP. OCP should ensure that all employees who use Attenti EM Manager and SCRAMNET take annual cybersecurity awareness training.

4. Evidence of Background Check

For 20 of 55 users tested, there was no evidence of a completed CORI check. The *Trial Court Personnel Policies and Procedures Manual* contains the following requirements:

A. General Requirements

1. The Human Resources Department will conduct a criminal record check on the final candidate(s) for appointment as a new hire to any Trial Court position. . . .

B. Record Keeping Requirements . . .

2. CORI check results and CORI request forms shall be kept for the duration of employment and no more than seven years from the last date of employment.

OCP told us that it had no control over the CORI check process performed by the Trial Court's Human Resources (HR) Department. Although the HR Department could not locate the CORI checks, OCP management did state that only employees who pass required CORI checks are hired.

Not completing CORI checks could cause OCP to give individuals with serious convictions access to personally identifiable information as well as probation monitoring information that is crucial to public safety. OCP management should work with the Trial Court to ensure that all completed CORI checks are filed accurately and are easily accessible if needed.

5. Evidence of Promptly Terminated Access Privileges

Nine user accounts, out of a total of 125 accounts belonging to employees who were terminated during the audit period, were still coded as "enabled" in Attenti EM Manager and/or "active" in SCRAMNET. OCP could not explain specifically why the accounts were not deactivated or provide exact dates when they were deactivated. EOTSS's document "Enterprise Access Control Security Standards" states, "Terminated employment status must be reflected in the users' access privileges immediately upon termination being carried out." It also states,

This standard applies to . . . any entity that uses [EOTSS]-controlled resources to access the Commonwealth's wide area network ([Massachusetts Access to Government Network]). . . . Other Commonwealth entities are encouraged to adopt this or a similar standard.

OCP's vendors, the Attenti Group and SCRAM Systems, also have standards for termination of user access privileges. According to the Attenti Group's "Access Control Policies and Procedures,"

Customers [in this case, OCP] are trained to inform Attenti for the removal of terminated users immediately, or within 5 business days for voluntary termination or change of responsibilities. . . .

For departing users [at OCP], HR creates a ticket with the date of the end of employment. This is done within 5 business days for voluntary end of employment, or on the same day for termination.

SCRAM Systems' "Access Control Policy (ISMS)" states,

> *When an employee leaves the organization under normal circumstances, their access to computer systems and data shall be suspended at the close of business on the employee's last working day.*

Not deactivating terminated employees' access rights in a timely manner increases the risk of terminated employees improperly accessing offender and victim information, including personal and location information. This could lead to public safety risk if information is passed to unauthorized parties. OCP should revoke employees' access to its systems in accordance with the timelines in Attenti Group's and SCRAM Systems' access control policies.

Additionally, OCP should update its internal control plan to incorporate an information system control section to reduce the risk of these issues occurring.

Auditee's Response

> *The following addresses the information technology control issues identified in the "Other Matters" section of the report and provides detail as to how the Office of the Commissioner of Probation / [Electronic Monitoring, or ELMO] has since strengthened its information technology general controls.*
>
> *To address the issues of (1) incomplete or missing system approval documentation and (2) user access rights that were inconsistent with employees' job functions, we created and now use the [Global Positioning System, or GPS] and Remote Alcohol Monitoring Software Access Form. This form must accompany the ELMO System Access User Agreement and is an updated form that is used to request electronic access to the Massachusetts Probation Service's [MPS's] GPS and Remote Alcohol Monitoring case management platforms or to request a change in one's current access level. These forms are located within the Courtyard, the Trial Court's intranet site, which is used to share news, updates, memos, transmittals, resources, and other information. Completed forms are submitted via e-mail attachment. . . . The form is then reviewed by the ELMO Systems Manager and the Attenti Account Representative. This updated form and process helps ensure sensitive case data is secure and user access rights are consistent with employees' job functions.*
>
> *To further ensure user access rights are consistent with employees' job functions, ELMO receives a termination list from the Office of the Commissioner of Probation's Personnel Department on a weekly basis. This list contains the names and positions of all terminated employees and we cross-reference it and update the ELMO Terminated Account Access Log to ensure employees that are no longer working for the MPS have their ELMO software accounts deactivated, which resolves the issue of (5) terminated employees not having their system access removed in accordance with state or vendor policies. This process is conducted by the Statewide Manager of ELMO, the Attenti Account Representatives, and the ELMO Administrative Coordinator. In addition, the Office of the Commissioner of Probation devised the Massachusetts Probation*

Service Personnel Security Policy, which consists of steps Department Heads shall take to ensure employees' access to confidential information, available through a variety of sources, is promptly suspended or terminated when appropriate.

To address the issue of (3) employees not completing cybersecurity awareness training, MPS employees had to complete the mandatory online security awareness courses that were introduced by the Trial Court in March 2020. In June 2021, the Judiciary implemented a policy requiring annual information security training that included suspension of digital access for those that did not comply within the allotted training window.

Last, to address the issue of (4) missing evidence of Criminal Offender Record Information (CORI) checks, the Office of the Commissioner of Probation is now creating and filing its own copies of the CORI completion/compliance forms, which are typically kept at the Office of Court Management. This will help ensure all completed CORI checks are filed accurately and are easily accessible.

In sum, the Office of the Commissioner of Probation / ELMO has since strengthened its information technology general controls.

Auditor's Reply

Based on its response, OCP is taking measures to address our concerns on this matter. OCP should also update its internal control plan to incorporate an information system control section to reduce the risk of issues associated with access controls and permission rights, ensure that cybersecurity training is conducted, and ensure that CORI checks are completed in accordance with its policies and procedures.

APPENDIX A

Global Positioning System Monitoring Alerts[7]

Alert	Description
Tier 1—One-Piece Wearable Miniature Tracking Device (WMTD)* Alerts	
Exclusion Zone	*The offender has violated a Zone set up by the courts. . . . Exclusion zones are a geographic area used to define off-limits to the offender.*
Strap†	*The strap has been compromised, or removed, by the offender. This may also be due to a new installation or equipment change or deletion.*
Tamper	*The 1 Piece (WMTD) has been compromised in some form.*
Tier 1—Two-Piece XT‡/ Bracelet Alerts	
Bracelet§ Gone	*Occurs when the offender is out of range of the [2 Piece XT] or Bracelet Battery dies.*
Bracelet Strap	*The strap has been compromised, or removed, by the offender.*
Exclusion Zone	*The offender has violated a Zone set up by the courts. . . . Exclusion zones are a geographic area used to define off-limits to the offender.*
Tamper	*The [2 Piece XT] has been compromised and/or tampered with.*
Tier 2—One-Piece Alerts	
Battery	*The battery is getting low and the device needs to be charged.*
Home Curfew‖	*If the 1 Piece (WMTD) has a home schedule set and the 1 Piece (WMTD) is not in range of the Beacon during this time, a curfew violation will be generated.*
Inclusion Zone	*The offender has violated a Zone set up by the courts. . . . Inclusion zones are areas like home, work or school where the offender is confined during a defined schedule.*
Unable to Connect	*The 1 Piece (WMTD) has a defined call-in interval, every hour. If the 1 Piece (WMTD) is unable to call in at its defined call-in interval, a default 90 minute grace period will go into effect. If the default 90 minute grace period expires and the 1 Piece (WMTD) has still not called in, a violation will appear on the event monitor.*

7. The alert definitions in this table are quoted from the Electronic Monitoring Program's "GPS Protocol."

Alert	Description
Tier 2—Two-Piece Alerts	
In Charger	*The [2 Piece XT] is **NOT** in the assigned Base Unit or attached to the wall charger when the In Charger schedule is in effect.*
Inclusion Zone	*The offender has violated a Zone set up by the courts. . . . Inclusion zones are areas like home, work or school where the offender is confined during a defined schedule.*
Unable to Connect	*The [2 Piece XT] has a defined call-in interval of one hour. If the [2 Piece XT] is unable to call [the Attenti Group] at its defined call-in interval, a default 90 minute grace period will go into effect. If the default 90 minute grace period expires and the [2 Piece XT] has still not called in, the [Attenti Group] database will create this alarm.*
XT Battery	*The [2 Piece XT] battery is low and needs to be charged.*
Tier 3—One-Piece Alerts	
Beacon Battery Low	*The backup battery in the Beacon is designed to last 24 hours. This alarm will be generated when the battery is getting low.*
Beacon Power Disconnected	*A Beacon . . . Power Disconnect alarm will be generated if the Beacon is disconnected from or loses power.*
Beacon Location Untrusted	*The Beacon Location Un-Trusted alarm will be generated if any of the following conditions occur:* • *If the . . . power is lost in conjunction with motion detection* • *If the Beacon detects excessive motion, whether or not it has . . . power* • *If the Beacon detects loss of power for over one hour* • *If the Beacon backup battery dies*
Motion No Global Positioning System (GPS)	*Occurs when the 1 piece (WMTD) has accumulated 20 minutes of motion in a 60-minute period without receiving a signal from the GPS satellites.*
Tier 3—Two-Piece Alerts	
Base Unit A/C Power Disconnected	*The base unit has lost A/C power and is running on the battery back-up.*
Base Unit Battery	*The Base Unit has been running on the back-up battery and is about to lose power.*
Base Unit Phone Line Disconnected	*The phone line has been removed from the Base Unit.*
Base Unit Tamper	*The Base Unit has been compromised and/or tampered with.*
Base Unit Unable to Connect	*The Base Unit has not called out in over 6.5 hours. The Base Unit calls the server 4 times a day at six hour intervals.*

Alert	Description
Bracelet Battery	*The Bracelet battery is getting low; the **bracelet must be replaced** within 5 days.*
Phone Number Caller ID	*Signals the offender may have moved the Base Unit to a new phone line or home.*
XT Motion No GPS	*Occurs when the [2 Piece XT] has accumulated 10 minutes of motion in a 60-minute period without receiving a signal from the GPS satellites.*

* This is a device that uses GPS satellites to establish an offender's location.
† The strap attaches a GPS device to an offender's ankle.
‡ This is a handheld device that receives information from GPS satellites and an ankle bracelet and then uses its modem to transmit information to Attenti Event Monitor Manager using a cellular network.
§ This is a GPS device worn on an offender's ankle.
|| The beacon that triggers this alert is a unit placed in an offender's home that communicates with a one-piece tracking device through radio frequency.

APPENDIX B

Secure Continuous Remote Alcohol Monitoring Alerts[8]

Alert	Description
Automated Facial Intelligence Pending Review	*Generated when SCRAMNET receives a test with a passed [breath alcohol concentration level, or BrAC] level but the facial recognition does not match.*
Device Battery Critically Low	*Generated when the battery in a SCRAM Remote Breath device has reached a level that requires immediate charging.*
Device Battery Low	*Generated when the battery in a SCRAM Remote Breath device is at a level that requires charging.*
Device Housing Breach	*Generated when the battery door is removed from a SCRAM Remote Breath device.*
Extended Missed Communication	*Generated when a [Secure Continuous Remote Alcohol Monitoring, or SCRAM] Remote Breath Device has not communicated with SCRAMNET for 24 hours. This alert would only come after multiple* ***Scheduled Test Not Received Alerts****.*
Failed Test	*Generated when a client provides a positive air sample with a BrAC above the acceptable threshold (.020).*
Incomplete Test	*Generated when a client does complete a scheduled test. ie; did not blow long enough, did not blow into straw correctly.*
Missed Test	*Generated when a client does not take a scheduled test.*
Scheduled Test Not Received	*Generated when SCRAMNET does NOT receive a test result within 90 minutes of the scheduled time test.*

8. The alert definitions in this table are quoted from the Trial Court's *Electronic Monitoring SCRAM Remote Breath Program (SCRAM) Procedures*.

APPENDIX C

Summary of Information Technology General Control Issues in SCRAMNET and Attenti Event Monitor Manager

	Yes	No	Total
SCRAMNET Current Users			
Access Level Approval	0	25	25
Appropriate System Access Rights	25	0	25
Security Awareness Training	21	4	25
Background Check	14	11	25
Total	60	40	100
Attenti Event Monitor (EM) Manager Current Users			
Access Level Approval	6	19	25
Appropriate System Access Rights	24	1	25
Security Awareness Training	23	2	25
Background Check	17	8	25
Total	70	30	100
SCRAMNET / Attenti EM Manager New Users			
Access Level Approval	0	10	10
Appropriate System Access Rights	8	2	10
Security Awareness Training	4	1	5
Background Check	4	1	5
Total	16	14	30
Total (By Category)			
Access Level Approval	6	54	60
Appropriate System Access Rights	57	3	60
Security Awareness Training	48	7	55
Background Check	35	20	55

Terminated Users' Account Statuses

System	Deactivated	Active	Total
SCRAMNET	79	7	86
Attenti EM Manager	37	2	39
Total	116	9	125