TENNESSEE COMPTROLLER OF THE TREASURY

PERFORMANCE AUDIT REPORT

Tennessee Bureau of Investigation

October 2024

Jason E. Mumpower
Comptroller of the Treasury

DIVISION OF STATE AUDIT

Katherine J. Stickel, CPA, CGFM, *Director*

TENNESSEE COMPTROLLER OF THE TREASURY

JASON E. MUMPOWER
Comptroller

October 14, 2024

The Honorable Randy McNally
  Speaker of the Senate
The Honorable Cameron Sexton
  Speaker of the House of Representatives
The Honorable Kerry Roberts, Chair
  Senate Committee on Government Operations
The Honorable John D. Ragan, Chair
  House Committee on Government Operations
          and
Members of the General Assembly
State Capitol
Nashville, Tennessee 37243

                  and
Mr. David B. Rausch, Director
Tennessee Bureau of Investigation
901 R.S. Gass Boulevard
Nashville, Tennessee 37216

Ladies and Gentlemen:

We have conducted a performance audit of selected programs and activities of the Tennessee Bureau of Investigation for the period June 1, 2020, through April 30, 2024. This audit was conducted pursuant to the requirements of the Tennessee Governmental Entity Review Law, Section 4-29-111, *Tennessee Code Annotated.*

Our audit disclosed a finding, observations, a matter for legislative consideration, an emerging issue, conclusions, and recommendations in this report. Management was given the opportunity to respond, and we have included their responses in the respective sections of the report. We will follow up the audit to examine management's corrective actions.

This report is intended to aid the Joint Government Operations Committee in its review to determine whether the Tennessee Bureau of Investigation should be continued, restructured, or terminated.

Sincerely,

Katherine J. Stickel, CPA, CGFM, Director
Division of State Audit

KJS/jc/jw
24/031

TENNESSEE BUREAU OF INVESTIGATION

AUDIT HIGHLIGHTS

Source: Corporate+ images.

MISSION

That guilt shall not escape nor innocence suffer

AUDIT PERIOD

June 1, 2020, through April 30, 2024

Scheduled Termination Date

June 30, 2025

Key Audit Conclusions

Finding: Although the bureau has taken steps to resolve one area, it did not provide adequate internal controls in one remaining area involving two conditions that have been repeated in previous audits and one new condition (page 38).

Observation 1: Although bureau management has taken action to address evidence processing backlogs and turnaround times by hiring, training, and equipping more staff, management must continue to address the backlogs and new challenges related to space and network capacity (page 13).

Observation 2: While the bureau has reduced forensic evidence testing backlogs for sexual assault kits, management is aware and is working to ensure that prioritizing one backlog does not create or worsen backlogs related to violent and non-violent cases (page 20).

Observation 3: Despite staffing challenges and a sharp increase in requests for firearms testing, the bureau has made progress in reducing the backlog of requests and should continue its efforts (page 22).

Observation 4: Bureau management has the opportunity to use systems to track evidence testing milestones in granular detail and identify potential process inefficiencies (page 24).

Observation 5: Cybertips related to internet crimes against children will likely continue to rise in Tennessee, creating a backlog and overburdening the bureau's limited investigative resources (page 32).

Emerging Issue: The bureau is facing challenges with investigating cases with child sexual abuse materials due to artificial intelligence and end-to-end encryption,[1] which may also impact the bureau's staffing resources (page 35).

Matter for Legislative Consideration: Bureau management should seek assistance from the Department of Finance and Administration and/or the General Assembly to be relieved from the bureau's role in accepting and depositing the state's portion of the Sex Offender Registry fees received from registering agencies (page 42).

---

1. End-to-end encryption is a security measure that ensures only the sender and recipient can access the contents of their messages.

Contents

Audit Authority

This performance audit of the Tennessee Bureau of Investigation (the bureau) was conducted pursuant to the Tennessee Governmental Entity Review Law, Title 4, Chapter 29, *Tennessee Code Annotated.* Under Section 4-29-246, the bureau is scheduled to terminate June 30, 2025. The Comptroller of the Treasury is authorized under Section 4-29-111 to conduct a limited program review audit of the agency and to report to the Joint Government Operations Committee of the General Assembly. This audit is intended to aid the committee in determining whether the bureau should be continued, restructured, or terminated.

Background

In March 1951, the Tennessee Bureau of Criminal Identification was established within the Department of Safety. The organization was renamed the Tennessee Bureau of Investigation (the bureau) and positioned as an independent agency in 1980. The bureau has original jurisdiction[2] to investigate the following crimes: illegal narcotics, cybercrimes targeting children, human trafficking, fugitives, public corruption, official misconduct, organized crime, domestic terrorism, arson, gambling, Medicaid fraud, and patient abuse. Additionally, Tennessee law grants the bureau the authority to investigate any criminal violation at the request of the District Attorney General from the judicial district where the offense occurred. The bureau has eight divisions as shown in **Figure 1** below.

Figure 1: Divisions of the Tennessee Bureau of Investigation

Source: Tennessee Bureau of Investigation organization chart.

---

2. Section 38-6-102, *Tennessee Code Annotated*, grants the bureau original jurisdiction for certain offenses, which authorizes the bureau to investigate without a request from the district attorney general.

The bureau also manages the TBI's Most Wanted list, the AMBER Alert program, the Silver Alert program, the statewide Sex Offender Registry, the Drug Offender Registry, the state Human Trafficking Advisory Council, and the Tennessee Dangerous Drugs Task Force. Additionally, the bureau houses the state's Fusion Center, which collects, analyzes, and shares information related to terrorism and other criminal activity between the bureau and federal, state, and local law enforcement agencies to identify crime trends and assist with criminal investigations. See **Appendix 2** for the bureau's organizational chart and additional information on bureau operations.

Field Offices

The bureau has seven offices across the state, including the headquarters in Nashville. See **Figure 2** for the office locations and the divisions/operations at each location.

Figure 2: Map of Bureau Offices and Functions
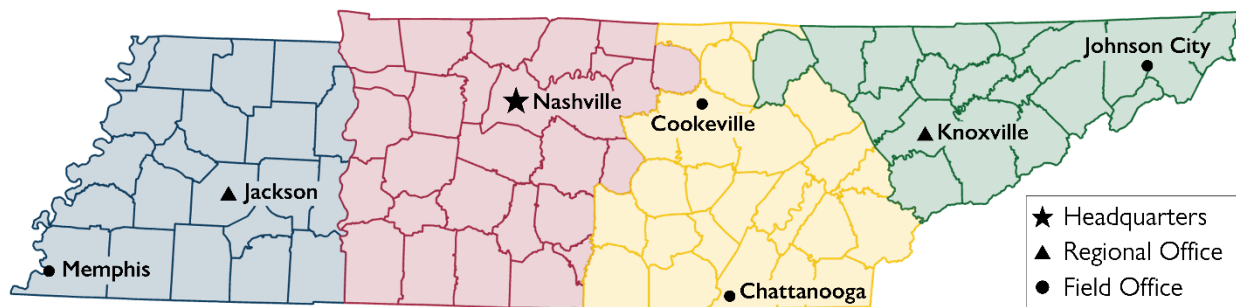
West Region	Middle Region	East Region	Upper East Region
Jackson Regional Office	**Nashville (Headquarters)**	**Cookeville Field Office**	**Knoxville Regional Office**
Administrative Services*	Administrative Services	Criminal Investigation	Administrative Services*
Criminal Investigation	Criminal Investigation	Drug Investigation	Criminal Investigation
Criminal Justice Information Services	Criminal Justice Information Services	Medicaid Fraud Control	Criminal Justice Information Services
Drug Investigation	Drug Investigation	Technology and Innovation	Drug Investigation
Forensic Services	Forensic Services		Forensic Services
Medicaid Fraud Control	Medicaid Fraud Control	**Chattanooga Field Office**	Medicaid Fraud Control
Technology and Innovation	Technology and Innovation	Criminal Investigation	Technology and Innovation
Training	Training	Drug Investigation	
		Medicaid Fraud Control	**Johnson City Field Office**
Memphis Field Office		Technology and Innovation	Criminal Investigation
Criminal Investigation			Drug Investigation
Drug Investigation			Medicaid Fraud Control
Medicaid Fraud Control			
Technology and Innovation			

Source: Created by auditor based on information on the bureau's website.
* These locations have police officers only, which are a part of the Administrative Services Division.

Accreditations

Bureau-wide Accreditations

The bureau is accredited by the Commission on Accreditation for Law Enforcement Agencies, Inc. (CALEA). The accreditation focuses on ensuring the bureau has adopted standards related to life, health, and safety procedures. CALEA conducts on-site assessments every four years; the bureau was reaccredited in 2023. In 2016 and 2020, the bureau also received accreditation from the Tennessee Law Enforcement Accreditation Program, which supports the continued improvement of law enforcement by establishing professional standards of accountability, management, and operations. During our audit, the bureau was reaccredited in April 2024.

Accreditation Applicable Only to the Forensic Services Division

The Forensic Services Division holds accreditation by the American National Standards Institute National Accreditation Board (ANAB) in all forensic testing disciplines, crime scene processing, and breath alcohol calibration. This accreditation demonstrates a lab's commitment to competence, impartiality, and consistent operation by conforming to internationally recognized standards. ANAB conducts reassessments every four years; the division was last reassessed in 2023 and was reaccredited in 2024. The bureau had no findings in ANAB's last assessment.

Audit Scope

We have audited the Tennessee Bureau of Investigation (the bureau) for the period June 1, 2020, through April 30, 2024. Our audit scope included prospective analysis, assessments of program effectiveness and efficiency, internal control, and compliance with provisions of law, regulations, accreditation standards, contracts, policies, and procedures in the following areas:

- the bureau management's collection and analysis of forensic and digital evidence, including management's ability to turn around evidence and the nature of any backlogs;

- management's investigations of internet crimes against children; and

- management's implementation of information systems controls.

Our work involved reviewing management's data to validate backlog and turnaround times for processing and testing evidence. Due to the confidentiality of the bureau's investigative files under Section 10-7-504(a)(2), *Tennessee Code Annotated,* we were limited in what information we could obtain and validate. As a result, management provided some of the data presented in this report, but we did not audit it; that data is identified as such. For the full details of our review, see the Data Reliability Review Methodology in **Appendix 1**.

Additionally, our audit scope included follow-up on prior audit findings in the following areas:

- management's changes to standard operating procedures for the Drug Offender Registry and the Sex Offender Registry;

- management's notification to the National Association of Drug Diversion Investigators when it removed drug offenders from the state registry as required by state statute; and

- the bureau's implementation of internal controls in two specific areas.

The information for our follow-up on prior audit findings can be found in the **Prior Audit Findings** section. We present more detailed information about our audit objectives, conclusions, and methodologies in **Appendix 1** of this report.

For any sample designs applied in this audit, we used nonstatistical audit sampling, which was the most appropriate and cost-effective method for concluding on our audit objectives. Based on our professional judgment, review of authoritative sampling guidance, and careful consideration of underlying statistical concepts, we believe that nonstatistical sampling provides sufficient appropriate audit evidence to support the conclusions in our report. Although our sample results provide reasonable bases for drawing conclusions, the errors identified in these samples cannot be used to make statistically valid projections to the original populations.

We conducted our 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.

The bureau's management is responsible for establishing and maintaining effective internal controls and for complying with applicable laws, regulations, policies, procedures, and provisions of contracts and grant agreements.

Report of Action Taken on Prior Audit Findings

Section 8-4-109(c), *Tennessee Code Annotated*, requires that each state department, agency, or institution report to the Comptroller of the Treasury the action taken to implement the recommendations in the prior audit report. The prior audit report was dated September 2020 and contained three findings. The Tennessee Bureau of Investigation (the bureau) filed its report with the Comptroller of the Treasury on March 12, 2021. We conducted a follow-up of the prior audit findings as part of the current audit.

> **TBI's Audit Findings**
>
> September 2020 Audit:
> 3 findings
> (2 resolved and 1 partially resolved)
>
> Current Audit:
> 1 repeat finding,
> 5 observations, 1 emerging issue,
> and 1 matter for legislative
> consideration

Resolved Audit Findings

The current audit disclosed that the bureau resolved two previous audit findings. Management updated their standard operating procedures for the Drug Offender Registry and the Sex Offender Registry, including notifying the National Association of Drug Diversion Investigators when they removed an individual from the state registry.

Partially Resolved Audit Finding

For one prior finding, we repeated the part of the finding related to the bureau's internal controls in one specific area. See the **Finding**.

Forensic and Digital Evidence

The Tennessee Bureau of Investigation's (the bureau's) mission is "that guilt shall not escape nor innocence suffer." The bureau's Forensic Services Division (forensic evidence) and Digital Forensics Squad (digital evidence) support the bureau's mission by collecting, analyzing, and interpreting evidence that could help judges and juries determine guilt. Both areas have experienced evidence processing backlogs and lengthy turnaround times for approximately 15 years.

Our goal was to examine management's actions to address backlogs and turnaround times for forensic and digital evidence, review the bureau's process for prioritizing evidence testing requests, and review their use of information systems to identify inefficiencies in the evidence testing process. This section is divided into two parts:

In Part 1: Forensic and Digital Evidence Backlogs and Turnaround Time, we found that management has taken action to address turnaround times and clear backlogs through hiring, training, and equipping more staff, but challenges remain with lengthy training times, lack of physical space for expansion, and limited network capacity. See **Observation 1**.

In Part 2:Forensic and Digital Evidence Processing, we evaluated management's processes for prioritizing and processing evidence testing requests for forensic and digital evidence. We found that management faces additional backlog challenges within the Forensic Services Division's Firearms and Toolmark Identification Unit and Forensic Biology Unit. See **Observations 2** and **3.** We also found bureau management could improve their use of existing information systems for data analytic purposes for both forensic and digital evidence to identify inefficiencies in the evidence testing process. See **Observation 4**.

General Background

According to the National Institute of Justice, evidence refers to "information or objects that may be admitted into court for judges and juries to consider when hearing a case." Evidence includes but is not limited to genetic material, fingerprints, weapons, drugs, chemicals, computers, and cell phones. Law enforcement agencies, including the Tennessee Bureau of Investigation (the bureau), play a critical role in collecting, analyzing, and interpreting evidence that could help judges and juries determine whether a suspect is guilty. For our audit, we focused on two areas where the bureau collects and analyzes evidence: the **Forensic Services Division** and the **Digital Forensics Squad** in the Technology and Innovation Division's Cybercrime and Digital Evidence Unit.

Forensic Services Division

Section 38-6-103(b), *Tennessee Code Annotated,* allows the bureau to offer forensic testing services to state and local entities.[3] Each of the bureau's three regional crime labs—located in Jackson, Nashville, and Knoxville—have different testing capabilities to serve Tennessee's three grand divisions. See **Figure 3** for the testing disciplines offered by each laboratory.

Figure 3: Forensic Sciences Disciplines by Location

Discipline	Unit Responsibilities	Jackson	Nashville	Knoxville
Breath Alcohol	Administers and maintains Tennessee's breath alcohol testing program and trains law enforcement.	✔	✔	✔
Combined DNA Index System (CODIS)	Compares evidentiary DNA profiles against the database of convicted offenders and arrestees.*	✔	✔	
Firearms and Toolmark Identification	Analyzes evidence to help law enforcement agencies connect crimes through ballistic data.	✔	✔	
Forensic Biology	Characterizes blood and other body fluids to determine whether they are related to a crime or to persons involved in a crime.	✔	✔	✔
Forensic Chemistry	Analyzes any substance seized in violation of laws regulating the sale, manufacture, distribution, and use of abusive drugs.	✔	✔	✔
Latent Prints	Compares fingerprints and palm prints with suspects' prints using the Automated Fingerprint Identification System (AFIS).		✔	
Microanalysis	Examines and compares trace evidence, such as paint marks, glass, paper, fire debris, and shoe and tire impressions.		✔	
Toxicology	Analyzes blood and other bodily fluids related to DUI and other crimes.	✔	✔	✔

Source: Created by auditor based on information on the bureau's website.

* The Nashville facility manages receipt, outsourced testing, upload, and match management for all statewide CODIS activities. The Jackson facility will perform in-house testing of samples received for the CODIS database to eliminate the need for outsourced testing, with a projected start date of December 1, 2024.

---

3. This includes the state's district attorneys general, the chief medical examiner, all county medical examiners, law enforcement officers, and state departments.

Digital Forensics Squad

According to the Digital Forensics Squad's (squad's) standard operating procedures, its responsibility is "to identify, collect, preserve, analyze, and report on the presence and interpretation of data stored on digital media and technical devices." Its four goals are to

- properly investigate and assist in the prosecution of cases involving digital evidence;

- preserve the integrity of seized digital evidence;

- provide expert testimony in court; [and]

- serve as an educational and training resource for [the bureau], local agencies, and the community [the squad] serves.

The squad's forensic examiners work in four bureau offices across the state: Nashville, Jackson, Chattanooga, and Knoxville. Examiners can extract and analyze data from multiple device types, such as mobile devices, computers, gaming consoles, and vehicle infotainment centers. They can also enhance sound and images from security systems, cameras, and other audiovisual devices. From fiscal year 2021 through 2023, the squad primarily supported death, child exploitation, and drug investigations. See **Chart 7** in **Appendix 5** for more detail about the types of cases the squad works on.

Approximately 70% of evidence the squad processes is submitted by federal, state, and local law enforcement agencies, and the remaining 30% of evidence is processed for the bureau's cases. See **Chart 8** in **Appendix 5** for the percentage of agencies requesting the bureau's digital forensics services for fiscal years 2021 through 2023.

Primary Information Systems for Evidence Processing

The bureau relies on two primary applications to support evidence management and tracking.

The Forensic Services Division uses the **Laboratory Information Management System** to track forensic evidence, generate reports, and document results from forensic testing.

The **Investigations and Evidence System** is the bureau's primary case management system for streamlining case workflows; it tracks digital and forensic evidence, generates reports, monitors case progress, and documents procedures and materials used in investigations. It allows users to track and manage cases from the time they are opened until they are closed.

Within the **Information Systems** section of this report, we also describe the divisions supporting these systems, their role in meeting the bureau's mission, and the importance of protecting these systems. See **Figure 4** for details about these critical applications.

Figure 4: Critical Applications and Application Description Chart

Laboratory Information Management System (LIMS)	Investigations and Evidence System (I+E)*
Implemented in 2004	Implemented in 2010
Approximately 208 users	Approximately 457 users
Management and tracking of forensic evidence, forensics cases, inventories, testing chemicals and expiration dates, and reporting.	Management and tracking of agency-wide cases and reporting, including digital forensics.

Source: Auditor created based on discussions with bureau management.

* In 2012, the bureau overhauled the front end of its 2010 case file management system, Investigative Support Information System, to be more functional and efficient, evolving it into the current system known as I+E.

Evaluating the Bureau's Evidence Processing, Turnaround Times, and Challenges

In Part 1 of this section, we provide information on how the bureau defines backlogs and turnaround times and how training requirements for highly specialized evidence testing impacts evidence processing. We also analyzed the steps bureau management has taken to address backlogs and turnaround times that globally impact all evidence types.

In Part 2, we delve into two types of evidence—forensic biology and firearms—that have not only garnered increased public interest but have also involved some of the lengthiest turnaround times. Part 2 also includes our analysis of the bureau's opportunities to utilize its information systems and data analytics to pinpoint potential inefficiencies in the evidence testing process.

Part 1: Forensic and Digital Evidence Backlogs and Turnaround Time

The bureau is facing challenges in timely processing both forensic and digital evidence, which is critical to ensuring judges and juries have evidence results to determine the guilt of those charged with a crime. Bureau management defines a **backlog** as any evidence that a forensic scientist or forensic examiner has not yet completed testing,[4] and **turnaround time** as the time it takes for the bureau to test evidence and provide results to its clients. According to management, several factors can impact evidence backlogs and testing turnaround times, such as

---

4. The Forensic Services Division quantifies its backlog by requests because one evidentiary item could have multiple requests.

- preexisting backlogs and rush requests;[5]

- the evidence or device type and difficulty of the analysis;

- the volume of evidence submitted to be tested for each request or case;

- extensive training requirements and limited fully trained staff;

- rapidly developing technologies, software, equipment, and testing techniques; and

- network limitations.

We also noted, and management confirmed, that some evidence testing requests may span multiple disciplines, and the evidence must be tested in a specific order (for example, a firearm must be sent for DNA analysis before it can be sent to the Firearms and Toolmark Identification Unit to preserve any biological evidence). As a result, turnaround times vary across disciplines and evidence types. See **Figure 5** for the statuses of backlogs and turnaround times for digital forensics and for select disciplines within the Forensic Services Division. See **Appendix 4** and **Appendix 5** for our complete audit results.

Figure 5: Backlog and Average Turnaround Times (Unaudited) as of April 30, 2024

Forensic Chemistry	Forensic Biology	Firearms Analysis	Digital Evidence
8,345 requests	1,409 requests*	559 requests	417 cases†
5-6 months	6-7 months	16 months	12-18 months
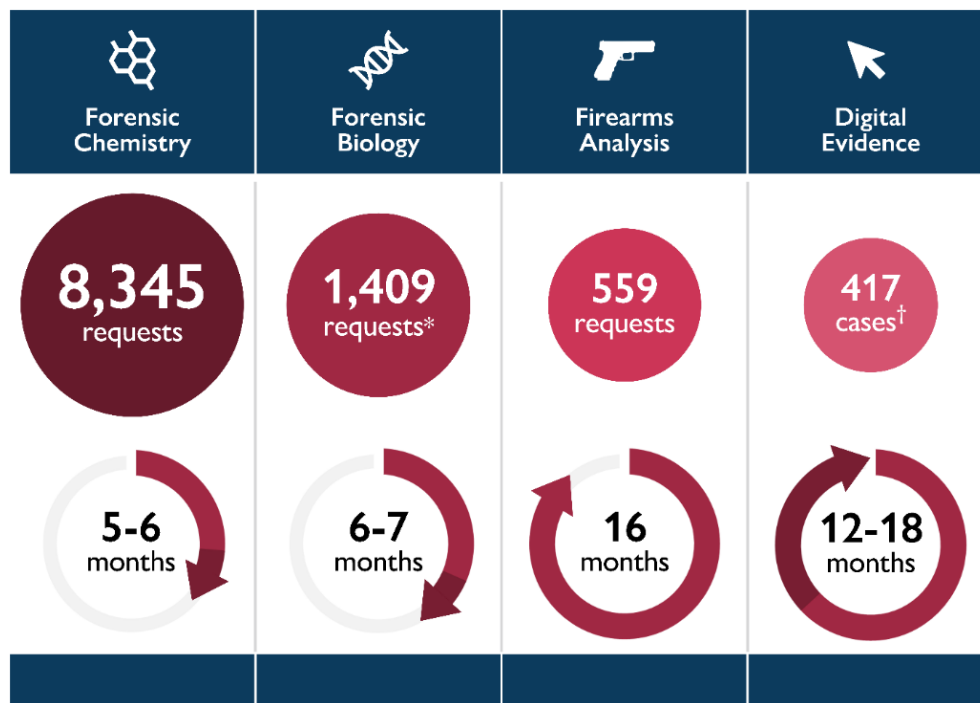
Source: Created by auditor based on unaudited information provided by management.

* The backlog of 1,409 forensic biology requests does not include 181 sexual assault kits that were outsourced to a private lab.

† According to management, these cases may contain multiple evidence requests.

---

5. Forensic scientists and forensic examiners will prioritize evidence testing requests if a law enforcement agency makes a rush request due to extenuating circumstances.

Evidence Backlog

As of April 2024, the Forensic Services Division had a total of 13,537 evidence testing requests yet to be completed, which is fewer than the 18,906 outstanding requests in April 2023. As noted in **Figure 5**, the Digital Forensics Squad had a backlog of 417 cases consisting of multiple devices.

Backlogs and turnaround times can impact justice being served; by clearing backlogs and improving turnaround times, the bureau could help speed up investigations and legal proceedings, prevent future crimes, and enable the exoneration of individuals wrongly accused of a crime.

Impact of Rush Testing for Forensic Evidence

According to management, the bureau generally processes evidence testing on a first-come, first-served basis, except for rush cases. The bureau receives two types of rush case requests. In the first type, there is a threat to public safety, and scientists must stop other testing to only work on that case. For example, management told us the bureau rushes abuse cases involving children under 13 years of age and cases where the elderly are still at risk of being re-victimized because they are living in the same household as the alleged abuser.

In the second type of rush request, cases are asked to be moved up in the queue, often to meet court deadlines, but otherwise do not pose an immediate danger to the public. For these requests, scientists do not have to stop all other testing to work on the rush case.

Even though management appropriately prioritizes these rush cases, rush requests can still impact operations through increased backlogs and turnaround times.

Training Requirements and the Impact on Evidence Processing

In general, all candidates applying for a position within the bureau must undergo a detailed pre-hire background check and are subject to a two-year probationary period after the hire date. Staff must also complete the 16-week special agent training program for candidates applying for commissioned[6] positions. Many of the positions within the bureau are specialized and require a high level of training to ensure evidence is processed properly and is admissible for court proceedings. Once hired, staff must complete the training program specific to their discipline. Depending on the discipline and prior work experience, discipline-specific training can take anywhere from a few months to two years.

Requirements and Training Plan for Forensic Scientists

Forensic scientist positions require a four-year degree in chemistry, natural or physical science, or forensic science. Forensic technician positions, such as those in evidence receiving, require a high school diploma. All of the approximately 23 forensic technician positions are non-commissioned; all of the remaining approximately 177 Forensic Services Division employees, including the forensic

---

6. Commissioned employees have arrest powers and the authority to carry firearms.

scientists and the forensic technician supervisor, are commissioned. See **Figure 17** in **Appendix 4** for a breakdown of the number of staff positions by discipline.

New employees work as apprentices for one or more fully trained scientists in their unit. In addition to conducting scientific testing, employees must be able to testify in court about the results of their evidence analysis. To gain experience, employees participate in mock trials that culminate in a final mock trial to complete their training. Employees in all disciplines except evidence receiving must also complete proficiency testing annually.

Requirements and Training Plan for Digital Forensics Examiners

Digital forensic examiner positions have the basic four-year degree requirement for all criminal investigator positions with a preference for experience and training in the area. All of the positions are commissioned.[7] First, examiners must attend the bureau's 16-week Special Agent Academy, which includes training in conducting criminal investigations. To become a digital forensics examiner, employees must undergo an additional 18-to-24-month training process to become fully certified to independently work on different device types. Once they have completed the academy, the examiners receive training in digital forensics, which includes mobile device and computer preservation, recovery, and analysis, as well as any other specialized disciplines that reside under the Digital Forensics Squad. Additional advanced disciplines include but are not limited to audio enhancement, video enhancement, vehicle infotainment extraction/examination, or countersurveillance detection, in which an agent may be trained on one or more of the disciplines. First, they receive training on mobile device examinations, such as mobile phones and tablets. Once examiners successfully complete their training on mobile devices, they can work independently on them. Next, they begin training in computer examinations. Examiners must successfully complete three mock computer test cases in-house in addition to the required training courses before they can independently work on computers.

Current Audit

We examined bureau management's plans to address the evidence backlogs and turnaround times, including impacts of rush requests and training, for both forensic and digital evidence. See **Observation 1**. See **Appendix 1** for our detailed audit objectives, conclusions, and methodologies.

---

7. The Digital Forensics Squad currently has one non-commissioned employee, a retired Special Agent who was hired back as a civilian.

Observation 1: Although bureau management has taken action to address evidence processing backlogs and turnaround times by hiring, training, and equipping more staff, management must continue to address the backlogs and new challenges related to space and network capacity

Management's overall approach to address evidence processing backlogs and turnaround times has been to hire and train new staff. To accommodate the new staff, management continues to work toward training, expanding laboratory space, and improving the network to enhance the Digital Forensics Squad's capabilities to perform their work. Management has also prioritized testing sexual assault kits, including outsourcing some kits, to address the backlog.

The bureau has added 50 new forensic scientists and 5 new digital forensics examiner positions to help reduce backlogs and turnaround times

After significant increases in backlogs and turnaround times of forensic testing requests between 2011 and 2020, and digital forensic cases from 2007 to 2022, management determined that the bureau needed additional personnel. In November 2021, the bureau requested 50 new positions within the Forensic Services Division and 2 digital forensic examiner positions to help alleviate backlogs and turnaround times. The General Assembly approved 1 digital forensic examiner position, and, over the next 2 years, the General Assembly approved funding for all 50 Forensic Services Division positions. As of February 2024, management had 1 digital forensic examiner position vacant in Jackson. As of April 2024, the bureau has filled 49 of the 50 Forensic Services positions, with 1 Forensic Chemistry position in Knoxville remaining vacant. For fiscal year 2025, the bureau requested and received 4 new digital forensic examiner positions, which it began working to fill on July 1, 2024.

See **Figure 6** for a timeline of when the bureau requested and filled these positions. For full details on the hiring status of the 50 new Forensic Services Division positions, see **Figure 18** in **Appendix 4**.

Figure 6: Timeline of Added Positions

	2021	2022	2023	2024	2025
Forensic Services Division	50 new lab positions requested	25 new lab positions authorized	25 more new lab positions authorized	49 of 50 new lab positions filled as of April 2024	
Digital Forensics Squad	2 new digital positions requested	1 new digital position authorized		4 new digital positions requested	4 new digital positions authorized for 2025

Source: Auditors created using the bureau's 4th Quarter Report to the General Assembly and discussions with bureau management.

The bureau is making efforts to address training challenges for both forensic and digital forensics staff; however, extensive training requirements impact the efficiency of new and existing staff

Management faces continued training challenges when hiring new staff given the length of time it takes to train new employees and the required involvement of existing staff in the new hire training process. Training for employees in both the Forensic Services Division and the Digital Forensics Squad in the Technology and Innovation Division's Cybercrime and Digital Evidence Unit is highly specialized and can take anywhere from a few months to approximately two years, depending on the type and level of training. See **Figure 15** in **Appendix 4** and **Figure 19** in **Appendix 5** for training lengths by discipline.

Until staff are fully trained, they cannot complete actual cases and reduce existing workloads or improve the evidence processing backlogs and turnaround times. Staff in both areas can only perform work related to what they have been trained to do, so they cannot assist with testing across disciplines. Staff in the Forensic Services Division provide the training for new hires, while the Digital Forensics Squad uses a combination of outside and in-house training. According to management, this approach to training devotes approximately half of the existing staff's time to training new employees, which reduces the time they have to contribute to testing evidence. See **Figure 16** in **Appendix 4** for more information on the number of forensic scientists available to test evidence as of March 18, 2024. While the Forensic Services Division cannot do much to reduce the length of training in its area, the Digital Forensics Squad is exploring more options for its outside training due to lengthy waitlists for some of

the classes. See **Figure 20** in **Appendix 5** for more information on the number of fully trained digital forensic examiners.

The bureau is making efforts to hire more staff to increase the number of staff available to work cases; however, management is still facing the potential for increased backlogs due to the delays in having enough fully trained staff available. Without a sufficient number of fully trained staff, management may experience longer wait times for the testing of evidence and possible delays in courts delivering justice for those found guilty or exoneration for individuals who are wrongly accused of a crime. While the length of time it takes to train is not always within the bureau's control, the bureau should continue to look for ways to expedite training and to retain its existing, fully trained employees.

To help reduce the backlog of sexual assault kits, management outsourced 908 kits to a private lab in Florida

In 2023, the bureau completed outsourced testing of 908 sexual assault kits. In 2024, the bureau plans to send an additional 192 kits for outsourced testing to be completed by September 30. According to multiple bureau lab managers, outsourcing sexual assault kits helps reduce the number of kits in the labs but does not instantly clear the backlog. Because the outsourced lab only accepts kits for processing, the bureau is responsible for testing additional items related to that kit, like clothing and bedding, which can be time intensive and add months to the processing turnaround times. Additionally, the bureau is responsible for reviewing the work the outsourced lab conducted, in addition to standard technical and administrative reviews, and for entering the data into the Federal Bureau of Investigation's Combined DNA Index System. Laboratory management told us that outsourcing helps some, but the outsourced lab is only responsible for conducting the simplest task in the testing process.

In February 2024, Forensic Services management began transferring cases between the bureau's labs to help lower the request backlog of the Knoxville Forensic Chemistry Unit

Management explained that due to requests from agencies within the region, the Knoxville lab has the most forensic chemistry requests per capita in the state, but as of March 18, 2024, 3 of the unit's 14 Forensic Scientist positions were vacant. Because of staffing challenges and the high volume of requests in the Knoxville lab's Forensic Chemistry Unit, in February 2024, management began transferring cases between the labs to help reduce Knoxville's backlog.

As of June 14, 2024, approximately 1,800 cases had been transferred from Knoxville to Nashville, and approximately 600 cases had been transferred from Nashville to Jackson. Management explained that because the scientist who performs the testing may have to testify in a trial, staggering cases in this manner was more efficient than transferring cases from Knoxville to Jackson directly. For example, it would be more efficient for a scientist in Jackson to testify in a case in Middle Tennessee versus East Tennessee. Management also stated that these transfers have been beneficial; the Knoxville lab's Forensic Chemistry Unit's backlog decreased from 6,631 requests in January 2024 to 3,695 as of May 2024. The Knoxville lab's Forensic Chemistry Unit's turnaround times have also continued to decline since these transfers began, without affecting the turnaround times for the Nashville or Jackson labs.

The bureau's next biggest challenge in the Forensic Services Division is workspace expansion

Management indicated that space concerns will be the next biggest challenge for the Forensic Services Division because adding any more staff means that they also need to have the space to accommodate them.

In 2023 and 2024, the bureau renovated the Nashville lab to increase desk space for 10 new employees in the Forensic Biology, Forensic Chemistry, and Firearms and Toolmark Identification Units. The reconfiguration, however, did not increase the square footage, and the workstations were not fully equipped. The Knoxville lab also reconfigured office spaces in 2023 and 2024 to accommodate 11 new employees in the Forensic Biology, Toxicology, and Forensic Chemistry Units. The Jackson lab is reconfiguring its current lab space to accommodate 6 new employees. The contract for this project has been awarded, and management expects construction to start in mid-2025.

The bureau has also contracted with a private consulting company to assess future expansion needs. As of April 30, 2024, the results of this assessment were still pending.

The bureau is also working to improve its network to enhance the capabilities of digital forensics examination

The bureau faced a rise in the volume and complexity of digital evidence in 2020, contributing to increased backlogs and longer turnaround times. To address these issues, the bureau began exploring new technologies to enhance efficiency, including automating some digital forensics processes. The automated workflows implemented in 2020, however, were not optimized for the bureau's decentralized structure due to network capacity[8] constraints.

Based on our discussions with management, we learned that management implemented the current process and automation tools in a manner that does not allow examiners to take full advantage of automation due to the network constraints between the remote locations—Chattanooga, Jackson, and Knoxville. Specifically, the limited network capacity could not keep up with the growing demand of digital forensics requests due to the increase in cyber-related crimes and the expanding file sizes of devices. Staffing and training challenges further hindered efficient evidence processing and use of resources.

Given the high costs and limitations of increasing bandwidth on existing lines, management proposed a stand-alone, high-level bandwidth connection to provide a faster and less restrictive network. In early 2024, the bureau and the Department of Finance and Administration's Strategic Technology Solutions began a pilot project to enhance network capabilities and offer a secure, consistent connection between the remote locations. This network improvement initiative is expected to be

---

8. Network capacity is the total information handling ability of a network, considering all connections and resources. It includes network bandwidth, which is the maximum amount of information that can be sent over a network in a certain amount of time. Higher bandwidth generally allows for faster network speeds.

completed by the end of 2024 and is part of a larger effort to reduce digital evidence processing backlogs and improve turnaround times.

Conclusion

In summary, bureau management has taken action to address evidence processing and turnaround times across all disciplines by hiring and training new staff, outsourcing sexual assault kits, expanding laboratory workspace, and piloting ways to improve network capacity. Management should continue to look for opportunities to improve backlogs and turnaround times for forensic and digital evidence.

Management's Comment

We concur. Turnaround times will continue to decrease as the more recently hired forensic scientists complete their training. However, to further reduce turnaround times after that point, additional staff, space, equipment, and network capacity will be needed. These additions must be coordinated and thoughtfully planned. Additional facility space is likely the first step that must be addressed before additional personnel and equipment can be contemplated. We are working with the Administration and the Department of General Services on long term plans related to facility space needs.

Part 2: Forensic and Digital Evidence Processing

The Tennessee Bureau of Investigation's (the bureau's) forensic and digital evidence processing is critical to the bureau's mission. The bureau runs the only statewide crime laboratory for forensic evidence. The Metro Nashville Police Crime Laboratory is the only other public crime lab in Tennessee. The bureau does not complete laboratory testing for areas under the jurisdiction of the Metro Nashville Police Department. Even though some larger Tennessee law enforcement agencies have their own digital forensic testing capabilities, the bureau accepts digital evidence testing requests from all entities. In this part, we reviewed the information systems that support evidence processing and the bureau's processes for prioritizing and working on forensic and digital evidence testing requests. We also focused our review on the bureau's Forensic Biology and Firearms and Toolmark Identification Units because of their lengthy turnaround times and the heightened public interest in sexual assault kits and firearm analysis.

Information Systems that Support Forensic and Digital Evidence Processing

As mentioned in the background of this section, the bureau's two primary information systems that support evidence management and tracking are the Laboratory Information Management System for forensic evidence and the Investigations and Evidence System for digital evidence. The bureau's customers submit evidence and identify the type of testing requested. Depending on the submitting agency's needs, each case may have one or more pieces of evidence requiring one or more types of testing. See **Figure 7** for an overview of the testing process and **Figure 8** for how the Forensic Services Division and the Digital Forensics Squad structure requests and cases within their information systems.

Figure 7: Overview of the Evidence Testing Process

	Forensic Evidence	Digital Evidence
Receiving	Law enforcement agencies submit evidence for testing to the Evidence Receiving Unit.	Law enforcement agencies submit evidence for testing at the nearest regional office.
Storage	Receiving technican secures the evidence in a vault.	Receiving agent secures the evidence in a holding locker.
Logging	Receiving technician logs the evidence into Laboratory Information Management System (LIMS).	Digital Forensics Squad member creates a pending case in Investigations and Evidence (I+E).
Assignment	Evidence is queued or assigned to a forensic scientist based on lab and unit protocols.	Squad supervisor reviews, approves, and assigns the case to an examiner in I+E.
Testing	Forensic scientist conducts testing and documents results in a report.	Examiner updates I+E case status to In-Progress and conducts analysis, documenting the results in a report.
Review	Supervisor reviews the report for completeness and accuracy.	Examiner routes the report to supervisor for review and approval, and updates I+E case status to Completed.
Reporting	Forensic scientist releases the final report to the requesting agency.	Examiner releases the final report to the requesting agency.

Source: Created by auditor based on discussions with bureau management.

Figure 8: Case Structures
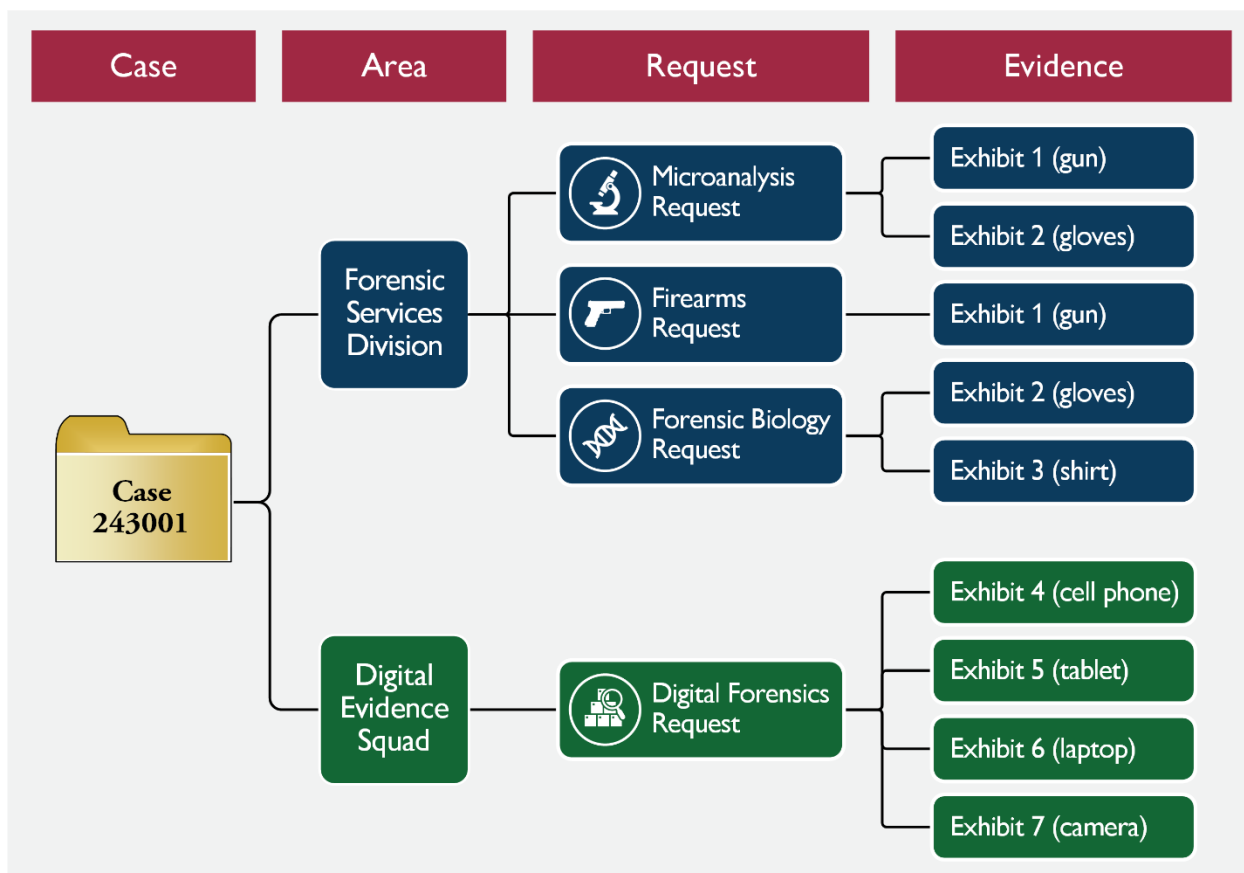
Source: Auditor created based on discussions with bureau management.

Forensic Biology Unit

Forensic biology is an important part of solving crimes because analyzing biological evidence like blood, bodily fluids, and tissues can help identify suspects and victims and help link crimes together. The bureau breaks down forensic biology requests into three different types. Violent requests include homicides and assaults, while non-violent requests may include burglaries and other property crimes. While sexual assaults are considered violent crimes, bureau management tracks them as their own category of testing requests.

> DNA from non-violent crimes can help identify perpetrators of violent crime.

All types of forensic biology requests can be important for linking individuals to crimes and generating investigative leads. Non-violent offenses can often be precursors to violent crimes. According to a 2018 publication by the United States Sentencing Commission, **73%** of federal offenders sentenced in fiscal year 2016 had been convicted of a prior offense. Public order (non-violent) offenses made up **44%** of those prior convictions. Fulfilling requests for non-violent cases, such

as property crimes, can be valuable for the state. A 2010 article published by the National Institute of Justice, titled "Using DNA to Solve Property Crimes," states,

> Based on information in [state and national DNA] databases—and other research on criminal careers—researchers have found that many of those who commit property offenses do not "specialize," that is, they do not limit their activities to crimes against property and may commit other offenses, including violent crimes and drug deals. For example, a Florida study revealed that 52 percent of that state's DNA database "hits" against murder and sexual assault cases matched individuals who were originally placed in the database for burglary convictions.

Current Audit

We focused our review on the bureau's lengthy turnaround times in the Forensic Biology and Firearms and Toolmark Identification Units. See **Observations 2** and **3**. We also focused on bureau management's use of information systems for evidence processing. See **Observation 4**. See **Appendix 1** for our detailed audit objectives, conclusions, and methodologies.

Observation 2: While the bureau has reduced forensic evidence testing backlogs for sexual assault kits, management is aware and is working to ensure that prioritizing one backlog does not create or worsen backlogs related to violent and non-violent cases

Management directed the Forensic Biology Unit to prioritize sexual assault kit testing

According to the bureau's standard operating procedure for Forensic Biology, "Priority should be given to violent cases, such as homicides and sexual assaults. Non-violent cases, such as burglaries and other property crimes, can be tested alongside violent cases as time permits." However, the bureau began prioritizing the testing of sexual assault kits over other violent and non-violent requests in 2022 due to increased public and legislative interest related to a case in Memphis, Tennessee. This led to all three labs prioritizing testing sexual assault kits over violent and non-violent requests to reduce the number of untested sexual assault kits. Between 2020 and 2023, sexual assault kit requests made up more than half of all forensic biology requests, indicating an area of testing with frequent requests. While focusing almost exclusively on testing sexual assault kits in 2023, the bureau's backlogs and turnaround times of other violent and non-violent requests rose. See **Chart 1.**

Chart 1: Statewide Average Turnaround Times for Forensic Biology Requests (Unaudited) Calendar Year Quarters January 2022 to March 2024
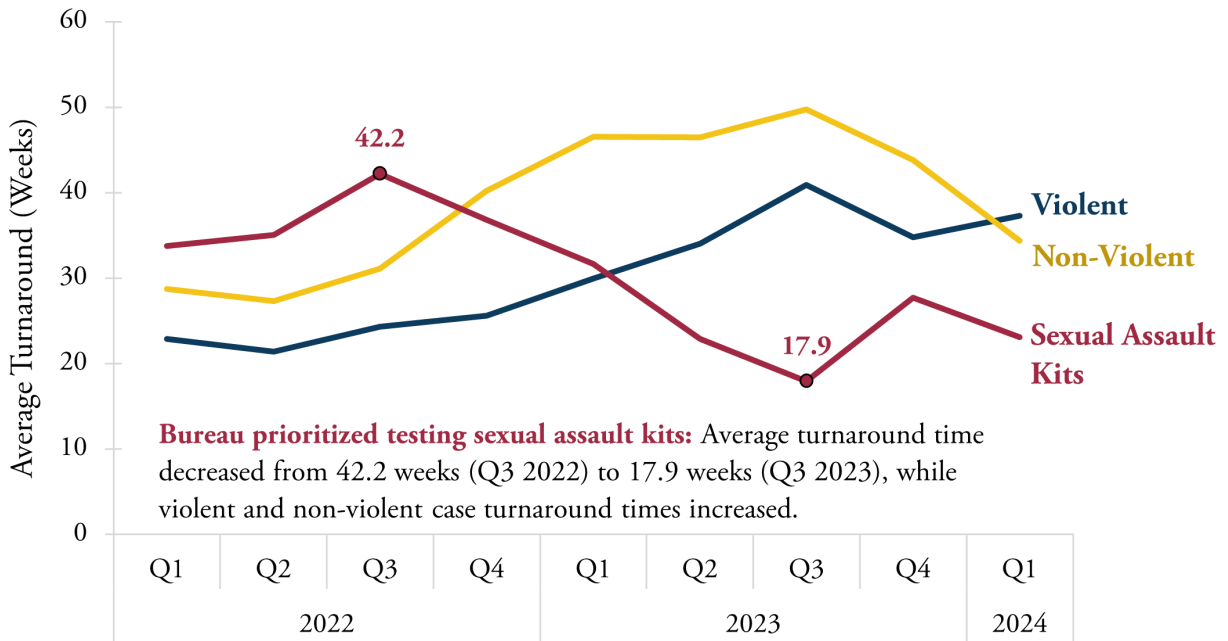
Source: Auditor created based on the Assistant Director's monthly statistical spreadsheet.

In April 2023, Section 38-6-113(e),[9] *Tennessee Code Annotated*, was modified to require the bureau to report to the legislature the average amount of time it takes forensic scientists to analyze evidence pertaining to sexual offenses. This increased focus led management to outsource the testing of 908 sexual assault kits in March, July, and December of 2023, as mentioned in **Observation 1**. According to Forensic Biology Unit management, it is common for testing priorities to shift based on bureau and regional needs.

By prioritizing testing sexual assault kits, management created bottlenecks in violent and non-violent cases. Management stated that they are aware of the effects of prioritizing sexual assault kits over other types of requests and the impact that can have on backlogs. As the quarter one data for 2024 in **Chart 1** indicates, management has begun to transition back toward working on all types concurrently. Management indicated that their overall goal is an 8-to-12-week turnaround time for all forensic biology requests and that they will continue to work on all three types of requests concurrently.

Management's Comment

We concur. Prioritization was shifted towards sexual assault kits due to the lengthy turnaround times. As we relayed to the General Assembly, the turnaround time issue was not confined to sexual assault kits. The problem persisted across disciplines. Thanks to the General Assembly and Governor, personnel were added to allow TBI to address the whole problem. As our newly hired scientists

---

9. This statute requires the bureau to provide quarterly reports to the legislature until January 1, 2025.

complete training, we should continue to see a reduction in turnaround times across disciplines. Now that additional staff are in place, DNA testing on violent crimes will no longer suffer as a result of mitigating testing on sexual crimes.

Firearm and Toolmark Identification Unit

Firearm analysis can help investigators generate leads, assess gun crime trends, and provide evidence in court. The Firearm and Toolmark Identification Unit's main function is to determine if a bullet, cartridge case,[10] or other ammunition component was fired from a particular weapon. This analysis is important because it can identify whether a particular weapon was used and can be used as evidence in court. Firearm analysis also provides information to help investigators understand trends in gun crimes, track illegal firearm movement, and create investigative leads for cases.

The unit also houses the National Integrated Ballistics Identification Network (NIBIN), which is a federal Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) database that allows individual characteristics from cartridge cases to be searched against a database and connect crimes that otherwise might never have been associated. The ATF's minimum required operating standards require staff to enter eligible items within 20 business days but note that the ideal time of entry is within 2 business days.

> **Observation 3:** Despite staffing challenges and a sharp increase in requests for firearms testing, the bureau has made progress in reducing the backlog of requests and should continue its efforts

The bureau saw a significant increase in firearm analysis requests between 2020 and 2022

The bureau's Firearm and Toolmark Identification Unit saw a dramatic increase in firearm analysis requests during the COVID-19 pandemic; an average of 46 requests per month before the pandemic[11] increased to an average of 81 requests per month between April 2020 and 2021. In addition to this increase, multiple scientists left the unit. Management explained that these separations affected the Nashville and Jackson labs' productivity. Scientists and supervisors in the Nashville lab frequently traveled to the Jackson lab to complete cases and help train new employees. Due to the 24-month training time required of new staff, scientists leaving the department have a significant effect on overall productivity, which we explain further in **Observation 1**. These factors have impacted the unit's ability to quickly complete cases and have resulted in increases in evidence processing turnaround time.

However, management is optimistic about its ability to reduce its backlogs for firearm analysis and NIBIN entry. As shown in **Figure 9**, the Firearms and Toolmark Identification Unit's request backlog decreased between April 2022 and April 2024, although turnaround time did not improve. Management explained

---

10. A cartridge is a unit of ammunition, made up of a cartridge case, primer, powder, and bullet. The cartridge case is the container for all the other components that comprise a cartridge.
11. This was calculated based on requests per month for July 2019 through March 2020.

that the unit has focused on working on the oldest cases and clearing its backlog. Because of this focus, turnaround times offer less insight into operations and have not seen a substantial improvement.

Figure 9: Backlog and Turnaround Information for Firearms Analysis Testing and NIBIN Entry, for the Month of April in 2022, 2023, and 2024 (Unaudited)
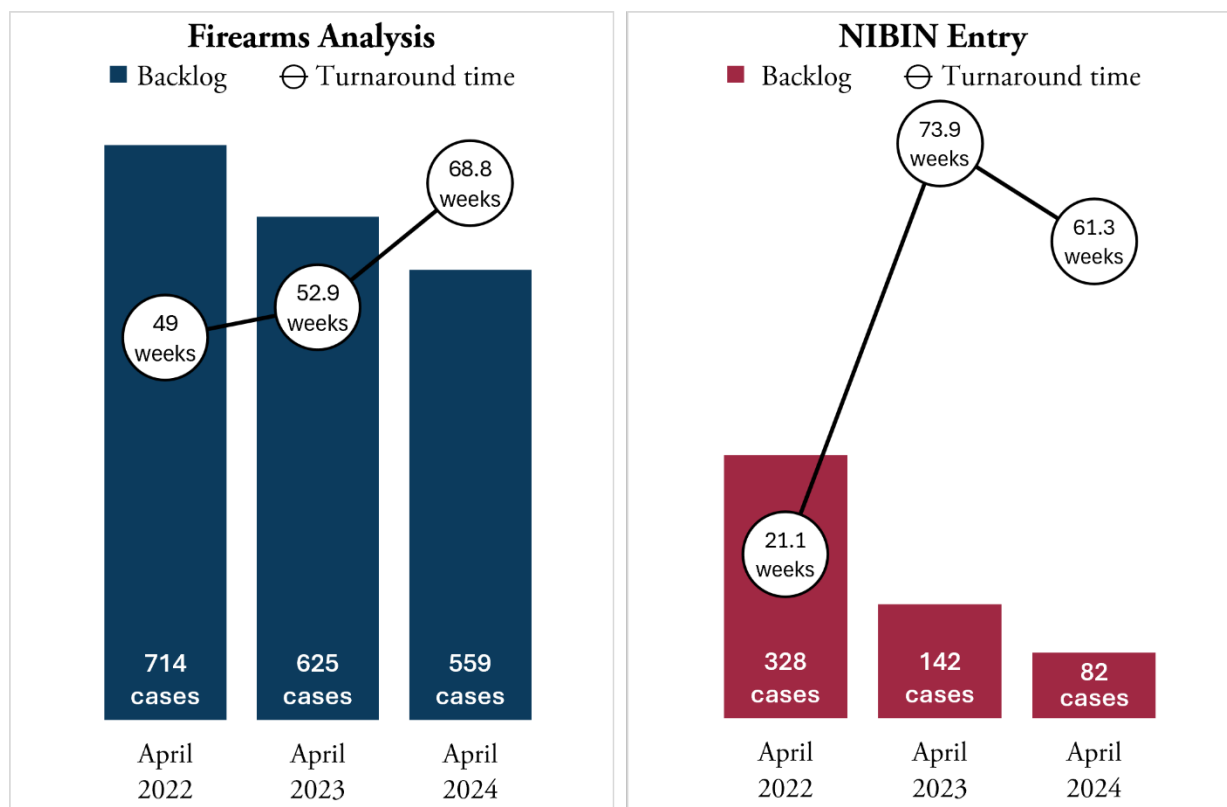
Source: Created by auditor based on information provided by bureau management.

Although NIBIN entry turnaround time was 21.1 weeks in April 2022, the weighted average for the quarter (April, May, and June 2022) was 60.8 weeks, which is more consistent with monthly average turnaround times for NIBIN entry. Management has explained that in units that complete fewer yet more complex cases per month, such as firearms, monthly turnaround times can be skewed depending on the factors of the case or rush requests. Additionally, during this time, the unit tried different strategies to determine new ways to increase efficiency.

As part of the additional 50 positions for the Forensic Services Division (as detailed in **Observation 1**), 4 were allocated to the Firearms and Toolmark Identification Unit, with 2 scientists and 1 technician to the Nashville lab and 1 scientist to the Jackson lab.[12] In March 2024, 3 scientists in the unit were still in training with expected completion dates between April and July 2025. Management expects

---

12. As reported in the bureau's quarterly report to the legislature on July 1, 2024, 1 position within the Jackson lab's Forensic Chemistry Unit has been reallocated to the Firearms and Toolmark Identification Unit. The position is vacant, and management expects training to take 24 months once the scientist is hired.

productivity to increase as the additional staff complete training and hopes to significantly reduce its backlog of requests within the next year.

Management should continue working to reduce the number of pending requests so that evidence can be promptly tested and returned to agencies and those cases can continue in the judicial process.

Management's Comment

We concur.

Opportunities to Use Existing Systems to Improve Processes

As mentioned previously, the bureau's Forensic Services Division uses the Laboratory Information Management System for forensic evidence tracking, and the Digital Forensics Squad uses the Investigations and Evidence System for digital evidence tracking. Our goal was to review bureau management's use of information systems to identify areas where management could better use the systems to highlight areas of inefficiency within the evidence testing process. We also focused on how the Forensic Services Division uses its system to track rush testing requests due to their potential to disrupt the evidence testing workflow.

Observation 4: Bureau management has the opportunity to use systems to track evidence testing milestones in granular detail and identify potential process inefficiencies

We reviewed the Forensic Services Division and the Digital Forensics Squad, within the Technology and Innovation Division,[13] and specifically looked at their processes for prioritizing testing requests and assigning those requests to forensic scientists and forensic examiners, respectively. Based on discussions with management and laboratory staff and a review of the division's standard operating procedures, we found inconsistencies in how labs and disciplines enter rush and case assignment information in the Laboratory Information Management System (LIMS). Because LIMS provides transparency, adaptability, and tracking capabilities, when used consistently, the system can be used to objectively identify inefficiencies. Data from LIMS can also be used to evaluate performance goals and help maximize the lab's efficiency and productivity.

Laboratory and unit management do not consistently use the field available to mark rush cases in LIMS, making it difficult to measure the impact of rush cases on the labs' workflows

We observed that within the case information in LIMS, there is a drop-down menu that users can select to indicate when a request is rushed. However, when we spoke with management across different labs and disciplines, only some staff used this drop-down feature for rush requests. Others added a text

---

13. The Digital Forensics Squad is part of the division's Cybercrime and Digital Evidence Unit.

comment within LIMS to indicate rushes or relied on a manual rush tracking spreadsheet. Staff often used a mixture of two or more of these processes. See **Table 7** in **Appendix 4** for a list of which offices used which methods. If staff across all labs and disciplines consistently used the drop-down menu feature in LIMS to mark rush cases, then management could create a report that quickly shows the volume and turnaround time of rush requests versus non-rush requests and more easily monitor the status of these cases.

The National Institute of Justice explains in its *National Best Practices for Improving DNA Laboratory Process Efficiency*, Recommendation #54,

> By using a LIMS to track case prioritization, managers can ensure that priority levels are effectively communicated to all applicable staff. The ability to classify a case as expedited in a LIMS should extend beyond assigning a target turnaround time; laboratories should be able to query the status of all open rush cases. All staff working on a rush item should be aware of the case status to aid in bench-level decision-making.

According to management, rush requests are necessary for public safety and the greater good, but they do have the potential to disrupt the flow of casework because forensic scientists may need to slow or stop their work in progress to work on a rush case. Due to their urgency and potential to disrupt the regular workflow, management may wish to consider fully implementing the use of the drop-down feature in LIMS to mark rush cases across all labs and disciplines to allow for expanded querying and analytic capabilities.

Each division may assign cases to forensic scientists in LIMS at different times, limiting management's ability to take a closer look at potential delays in the testing process

LIMS maintains a milestone report that captures date and timestamp information for each step in the testing process for any given request. See **Figure 10** for the steps the milestone report captures.

Figure 10: LIMS Milestones*
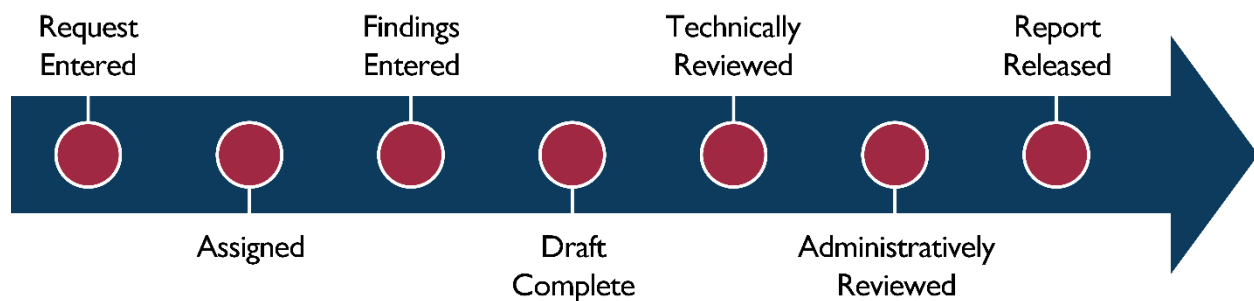
Source: Auditor created based on discussions with bureau management.
* "Requests entered" is the date the request was entered into LIMS, "assigned" is when the case was assigned for testing in LIMS, "findings entered" is the date the scientist enters a result in LIMS, "draft complete" is when all findings have been entered and all analyses are complete, "technically reviewed" is when the first review is completed, "administratively reviewed" is when the second review is completed, and "report released" is when the final report is delivered to the customer.

We discussed the request assignment process with each lab and discipline and found that each discipline has the flexibility to assign requests whichever way works best for them. However, not all labs and disciplines enter request assignments in LIMS at the same time. Some labs and disciplines make the assignment when it is assigned to the scientist, while others may wait until after testing has been completed to enter assignment information in LIMS. See **Table 8** in **Appendix 4** for more information on the case assignment processes by lab and discipline.

The bureau primarily uses LIMS for evidence management and results reporting. According to management, the case assignment function in LIMS simply serves as a prerequisite field that must be completed for an employee to enter findings into the system. By not having all labs and disciplines enter case assignments at the same point in the testing process, management is limited in their ability to run a detailed report that shows turnaround times for all phases of the testing process and thus sheds light on potential areas of improvement. Management may wish to consider having staff use the case assignment function in LIMS to its fullest so that the data in LIMS is a more accurate reflection of current processes and so that management may monitor each phase of the testing process in aggregate to compare individual, discipline, or regional lab performance throughout each phase of testing.

LIMS has standardized reports, including the milestone report, as well as the ability to create customized reports and queries to enhance data analytics capabilities

In gaining our understanding of LIMS and management's use of LIMS in the evidence testing process, management stated that they do not use all available LIMS features. Bureau management further explained that a "one-size-fits-all" approach to evidence processing across all disciplines and all labs was not practical and could hamper efficiency because the workflow in LIMS does not dictate the labs' testing procedures. By exploring ways to further utilize the LIMS features, however, management may increase its data analytic capabilities within all disciplines. Additionally, with the significant increase in new staff within the division, management should ensure that it has a documented plan for continually monitoring quality and growth and avoiding declines in efficiency. To produce long-lasting results, management must maintain and build upon effective processes and target workflow inefficiencies earlier to minimize their impact.

Digital Forensics management should ensure that the new case management system allows for tracking evidence workflow at the granular level to identify potential inefficiencies in the process

The bureau's investigative divisions use the Investigations and Evidence System (I+E) to document and track the status of cases they are responsible for investigating. We reviewed the Digital Forensics Squad's process to track evidence it receives from the point of receipt to the completion of the examiner's forensic work and how this process is documented in I+E. We found that management can track the status of its devices at the case level in I+E, instead of the device level, making it difficult for bureau leadership to know where a specific device is in the workflow and to determine their evidence backlog. For example, if a local law enforcement agency submits five devices to the bureau for analysis, digital forensic staff enter the five devices as one case in I+E. If a digital forensic examiner completes the analysis for four devices, while staff are processing the fifth device, the status in I+E will show that all five devices are processing. According to bureau management, I+E is not granular enough to allow for device tracking.

The Assistant Special Agent in Charge oversees staff at four offices across the state. The ability to track processes at the device level may help management identify bottlenecks and redirect resources as needed so that the agencies that submitted these devices can use the results and proceed with prosecution.

The bureau is in the process of procuring a new case management system. Digital Forensics management should ensure they align the new system's functionality with their practices and workflow elements needed for project management, decision making, and external reporting purposes.

Management's Comment

We concur in part.

We concur that I+E does not have the capability to give us a more granular detail to assist in case process progression. With the implementation of our new case management system, that analysis will be produced automatically.

We do not concur with the information presented in regard to the Laboratory Information Management System (LIMS). The Laboratory Information Management System is used as a repository for case demographic information, to maintain and track chain of custody, for scientists to create and review reports, and to generate and distribute reports to our customers. The current LIMS system was installed in 2004. Prior to 2004, two different LIMS systems were used, and LIMS is one of many software tools used by the laboratory. LIMS is a commercial product, used by many laboratories, and does not dictate the laboratory's workflow. LIMS does have the capacity for case and review assignments. However, all cases are different, and these differences may not be evident at the time of LIMS assignment. It is more effective to distribute case and review assignments based upon scientist availability and expertise, rather than arbitrarily assigning these tasks in LIMS immediately upon receipt of the cases. We do use LIMS to provide reports on case and employee statistics after case completion.

Reducing case backlog inventory is workforce dependent and is a function of staffing, hiring, and training scientists. The inventory of backlogged requests was 19,587 on September 1, 2023. The inventory of backlogged request was 10,173 on September 1, 2024—a reduction of 48%. This reduction is directly related to the hiring and training staff.

The LIMS software product does not come "off the shelf" with rush case flagging. We have customized LIMS to add rush case flagging, and this flagging is used by some supervisors. Again, all cases are different, and these differences may not be evident at the time of LIMS assignment. It is more effective to distribute case assignments (including rush case assignments) based upon scientist availability and expertise, rather than arbitrarily assigning these tasks in LIMS immediately upon case receipt. Flagging a case as "rush" in LIMS does not improve the expeditiousness of case completion, and documentation of the rush case is stored separately in each case file.

Auditor's Comment

We reviewed the observation and considered management's comments. We agree that management should have the flexibility to assign cases in the best manner for each discipline. It was not our intent to recommend that management change their case assignment process but instead look for ways to use LIMS's capabilities to capture additional data and identify inefficiencies in their workflow. Increased data analytic opportunities could help management make better, data-driven decisions in support of their efforts to reduce backlogs and turnaround times. We offer these recommendations as best practices for continued improvement of the bureau's systems and processes to better serve Tennesseans.

Internet Crimes Against Children

> The Tennessee Bureau of Investigation (the bureau) is one of 62 Tennessee law enforcement agencies charged with investigating cybertips (tips) involving child sexual abuse materials. Cybertip reporting incidents that involve children will continue to increase, especially as generative artificial intelligence becomes more advanced and more widely available. Our goal was to examine the bureau's process to prioritize and investigate these tips. See **Observation 5** and the **Emerging Issue**.

General Background

Created in 2007, the bureau's Internet Crimes Against Children (ICAC) Squad is responsible for investigating all incidents of producing, manufacturing, and distributing child sexual abuse materials (CSAM) and child sexual abuse involving technology. These incidents are called cybertips (tips).

The squad consists of one Assistant Special Agent in Charge (ASAC) and four agents. The ASAC and two agents are located in Nashville, one agent and the electronic detection K-9 are in Jackson, and one agent is in Cookeville.

Cybertip Sources

National Center for Missing and Exploited Children – Transmitted Tips

When an individual, a social media company, or an electronic service provider (such as Instagram, Snapchat, Google, and Yahoo) observes CSAM, solicitation, and/or exploitation of a minor on an internet platform, they can report it to the National Center for Missing and Exploited Children (NCMEC),[14] a private, nonprofit corporation dedicated to finding missing children, reducing child

---

14. https://report.cybertip.org/.

sexual exploitation, and preventing child victimization. In response, NCMEC creates a cybertip and assigns a priority based on a scale (see **Table 1).**

Table 1: Cybertip Priority Scale and Descriptions

Scale	Description
1	A tip that appears to contain newly produced CSAM and/or the victim is in imminent danger.
2	A tip where a child may not actively be in danger but could be in danger in the immediate future.
3	A tip that comes directly from the public that may contain limited information.
E	A tip from electronic service providers generally concerning simple possession of CSAM.

Source: Auditor prepared based on information from the Knoxville Police Department and bureau management.

Once the tip is prioritized, NCMEC electronically transmits the tip in the ICAC Database System[15] to a state ICAC Commander, the state's designated individual responsible for ICAC, based on the area where NCMEC believes the victim and/or potential perpetrator is located.

In Tennessee, the ICAC Commander works at the Knoxville Police Department (Knoxville police). Knoxville police will then triage the tip, using the same priority scale, and transmit the tip in the ICAC Database System to the affiliate in the geographical area identified in the tip. An affiliate is a local law enforcement agency that agrees to investigate ICAC tips in their jurisdiction. As of March 1, 2024, there are 62 affiliates in Tennessee. If a county or city does not have an affiliate, Knoxville police assign the tip to the bureau, which is also classified as an affiliate agency. See **Figure 11** for the locations in the state that fall under the bureau's responsibility. See **Appendix 7** for a more detailed map of jurisdictional responsibility.

Figure 11: The Bureau's ICAC Affiliate Coverage for 2023
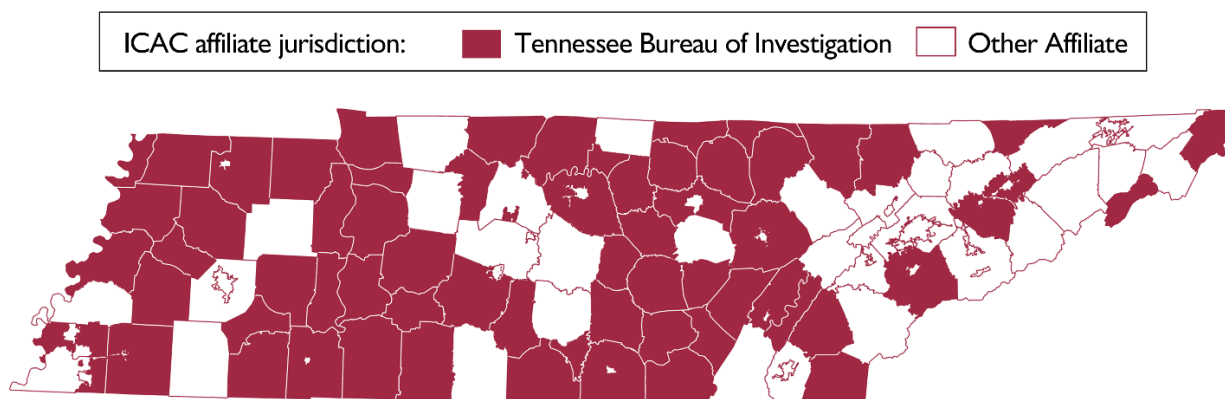
Source: Auditor created based on information provided by the State ICAC Commander.

---

15. All NCMEC taskforces and affiliates use this system to securely transfer and process tips related to internet crimes against children.

Once a cybertip is assigned to the bureau, the bureau's Investigations and Evidence System (I+E) creates an electronic case by uploading the information submitted in the cybertip from the ICAC Database System. The bureau collaborated with NCMEC personnel to develop software and procedures to automatically transfer cybertip information into I+E. This automation process greatly reduced the time it took to create a case file and to upload submitted information. In addition, the automation software queries I+E to determine any possible hits in previously submitted cybertips or existing investigations. Any hits elevate the priority assigned to the cybertip. The bureau is the only ICAC affiliate in the country implementing this process.

ICAC agents view the tip and prioritize it again using the same scale. According to management, they are notified immediately if a tip is labeled a priority 1. The ICAC Commander informed us that Tennessee received 14,190 cybertips in fiscal year 2023, and bureau management was notified of 1,741 during the same fiscal year. From June 1, 2020, through March 31, 2024, the top 10 sources of these tips comprised mostly social media companies. See **Table 2**.

Table 2: Top 10 Reporting Sources of the Bureau's Cybertips
June 1, 2020, Through March 31, 2024

Cybertip Reporting Source	Number of Cybertips Reported
Snapchat	427
Facebook	326
Google	290
Microsoft	270
Discord*	258
MediaLab/Kik*	227
No source reported	204
Synchronoss†	202
Dropbox	160
Instagram	130

Source: Auditor prepared using the bureau's data.
* Instant messaging service.
† A cloud platform solutions provider.

Non-NCMEC–Transmitted Tips

When an outside source, such as a citizen or local law enforcement agency, contacts the bureau[16] directly to report allegations of cybercrimes, designated staff in the Cybercrime and Digital Evidence Unit review the tips. If the bureau receives a tip involving CSAM, staff automatically assign it to the

---

16. While this section focuses on reports of cyber-related crimes involving children, the public can report allegations of any criminal activity to the bureau by calling 1.800.TBI.FIND or emailing TipstoTBI@tbi.tn.gov.

ICAC Squad for investigation. Based on discussions with management, if the agents determine that the tip involves criminal activity, they create and prioritize the case in I+E. From June 1, 2020, through March 31, 2024, the bureau received 187 tips from non-NCMEC sources.

Backlog of Cybertips

ICAC management defines a backlog as a cybertip labeled with an "active hold" status in I+E. According to management, they use the active hold status until an agent becomes available to review the cybertip. As of April 1, 2024, management had a backlog of 2,543 cases. **Chart 2** shows the cybertip cases management opened from June 1, 2020, through March 31, 2024, that were added to the backlog.

**Chart 2: New Cybertips Added to the Internet Crimes Against Children Squad's Backlog
June 1, 2020, Through March 31, 2024**
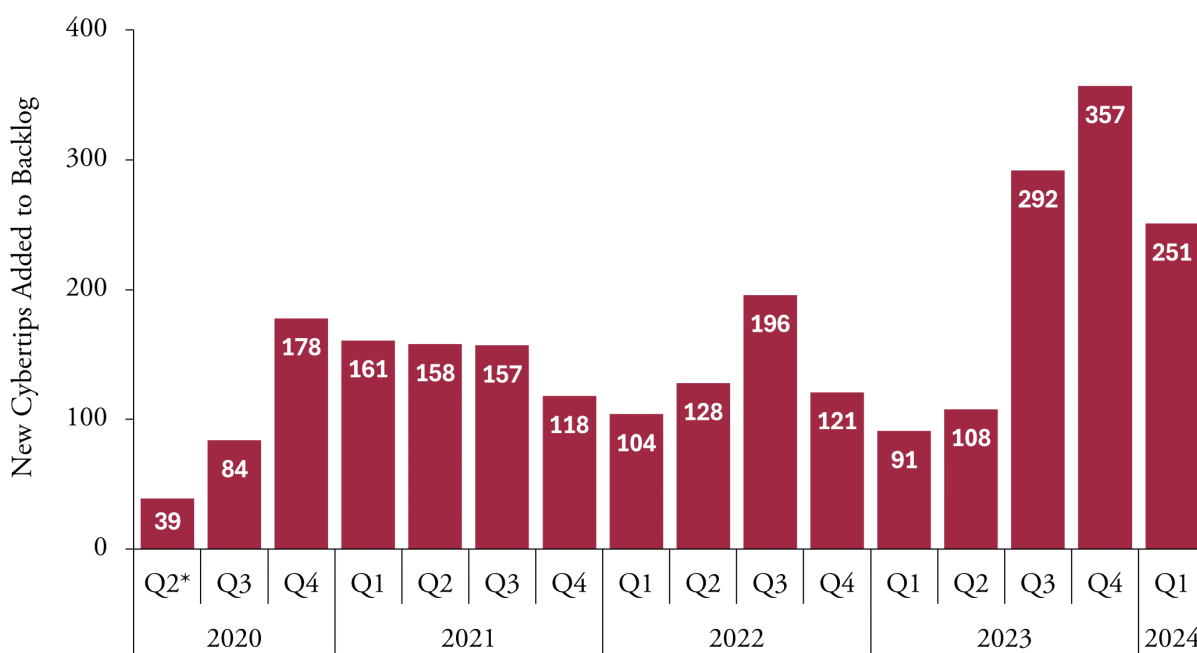
Source: Auditor prepared using ICAC cybertip case data provided by management.
* We only examined new cybertips for June in Q2 of 2020 (the beginning of our audit scope period).

Cybertip Investigation Process

According to Section 38-6-102(b), *Tennessee Code Annotated*,

> Investigators of the bureau of investigation are authorized, without a request from the district attorney general, to make investigations in connection with any matters pertaining to . . . [v]ictimization of children by means of a computer or other electronic communications device.

When the bureau receives cybertips, ICAC agents review each one to determine if a crime was committed or if the tip can be investigated and potentially prosecuted based on the information

provided. If an ICAC agent determines the cybertip can be investigated, they mark it as such in I+E. To begin an investigation on an ICAC tip, the agent reviews all the information related to the tip, including the tip's priority and all attached child sexual abuse materials (CSAM), and may revise the priority based on the CSAM. After verifying the priority, the agent begins the investigation.

Case Tracking in I+E

Agents track the status of each case in the bureau's case management system. While the case created from the tip goes through the legal process, it remains open in the bureau's system. When agents complete the legal process for the case, management closes the case in the system. When the case is closed, management destroys[17] the devices at the district attorney's request if they contain CSAM.

Current Audit

We examined the ICAC Squad's process to prioritize and investigate cybertips. We also examined management's plan to address the cybertip backlog. See **Observation 5**. Furthermore, we examined an emerging issue related to the evolving trends in using artificial intelligence (AI) technology to create CSAM; if AI-generated CSAM continues to increase and be reported to law enforcement agencies, this could impact the bureau's resources. See the **Emerging Issue**. See **Appendix 1** for our detailed audit objectives, conclusions, and methodologies.

> **Observation 5:** Cybertips related to internet crimes against children will likely continue to rise in Tennessee, creating a backlog and overburdening the bureau's limited investigative resources

The Internet Crimes Against Children Squad's staffing levels have not kept pace with the growing backlog of cybertips

According to management, even with the increasing number of cybertips, the squad has had the same 4 agent positions since its inception in 2007, when the number of cybertips they received was much lower. In fiscal year 2023, management received 12% of all cybertips in the state and assisted other affiliates' investigations. Based on our data analysis, bureau management opened 3,044 cases related to tips involving child sexual abuse materials (CSAM) from June 1, 2020, through March 31, 2024. Of those cases, **84%** contributed to the backlog. Our analysis also revealed that 90% of them involved allegations of child exploitation.[18] See **Table 3** for details related to the type of crimes alleged from the cybertips.

---

17. According to management, they either incinerate it or use a hydraulic crusher to destroy a device's hard drive.

18. Child exploitation occurs when an individual uses a child for personal or financial purposes.

Table 3: Types of Crimes Alleged on the Bureau's Cybertips
June 1, 2020, Through March 31, 2024[19]

Alleged Crime Noted	Case In Progress	Case Not Started	Case Completed	Total Cybertips Received
Child Exploitation	128	2,357	262	**2,747**
Enticement	6	135	22	**163**
Child Sexual Molestation	3	33	21	**57**
Crime Not Identified*	7	3	20	**30**
Other Crimes Against Children	3	7	7	**17**
Child Sex Trafficking	0	10	1	**11**
Solicitation	3	0	8	**11**
Multiple Crimes†	6	0	2	**8**
Total	**156**	**2,545**	**343**	**3,044**

Source: Auditor prepared using bureau data.
* The data analyzed did not list an alleged crime for these cybertips.
† These cybertips contained several alleged crimes.

Based on our review, we believe the squad is managing the backlog as best as they can with the current staff. Compared to other affiliates in Tennessee, the Memphis Police Department has 5 investigators and received 486 cybertips in fiscal year 2023 and 562 in fiscal year 2024. The Knoxville Police Department has 3 investigators and received 248 cybertips in fiscal year 2023 and 296 in fiscal year 2024. **Table 4** compares the number of staff the bureau designates for internet crimes against children (ICAC) to the staffing at certain affiliates in Tennessee (for the full list of affiliates, see **Appendix 6**). Staff designated for ICAC are categorized as investigators, forensics, prosecutors, or educators, but none of the affiliates listed in **Table 4** had designated educator staff.

---

19. For completed cases, it took agents an average of 27 weeks to review and close cases that had insufficient evidence to warrant prosecution and 85 weeks to close the cases they investigated and pursued prosecution. As stated previously, bureau management closes investigations when the cases have completed the judicial process.

Table 4: Local Law Enforcement Agencies with the Largest Number of Staff Designated for Internet Crimes Against Children as of 2023

ICAC Affiliate	Number of Designated Staff			
	Investigators	Forensics	Prosecutors	Total
Tennessee Bureau of Investigation	●●●●	●●●●		8.00
Knoxville Police Department	●●●	●●●	●●	8.00
Memphis Police Department	●●●●●	●		6.00
Cookeville Police Department	●● ◗	●		3.50
Jackson Police Department	●● ◗	◖		3.25
Madison County Sheriff's Office	●● ◗	◗		3.00
Tipton County Sheriff's Office	●● ◖			2.75

Percentage of staff member's full-time hours designated to ICAC: ● 100% ◗ 75% ◗ 50%

Source: Auditor prepared using information from the State ICAC Commander.

The number of cybertips ICAC receives will continue to grow each year

The bureau's ICAC Squad is facing an increasing number of cybertips involving crimes against children. According to management, the bureau received approximately 5,500 child sexual abuse tips during fiscal years 2016 through 2023. They also stated that they received an increase in tips during the COVID-19 pandemic and, as of February 1, 2024, continued to receive approximately 120 tips or more a day. See **Chart 3** for the number of tips the bureau has received since 2016 and is projected to receive through fiscal year 2029.

Chart 3: Cybertips Received and Projected, Fiscal Years 2016 Through 2029

■ Cybertips Received
□ Projected Cybertips

Year	Value
2016	120
2017	240
2018	292
2019	482
2020	843
2021	918
2022	1,381
2023	1,741
2024	1,955
2025	2,185
2026	2,414
2027	2,644
2028	2,874
2029	3,103
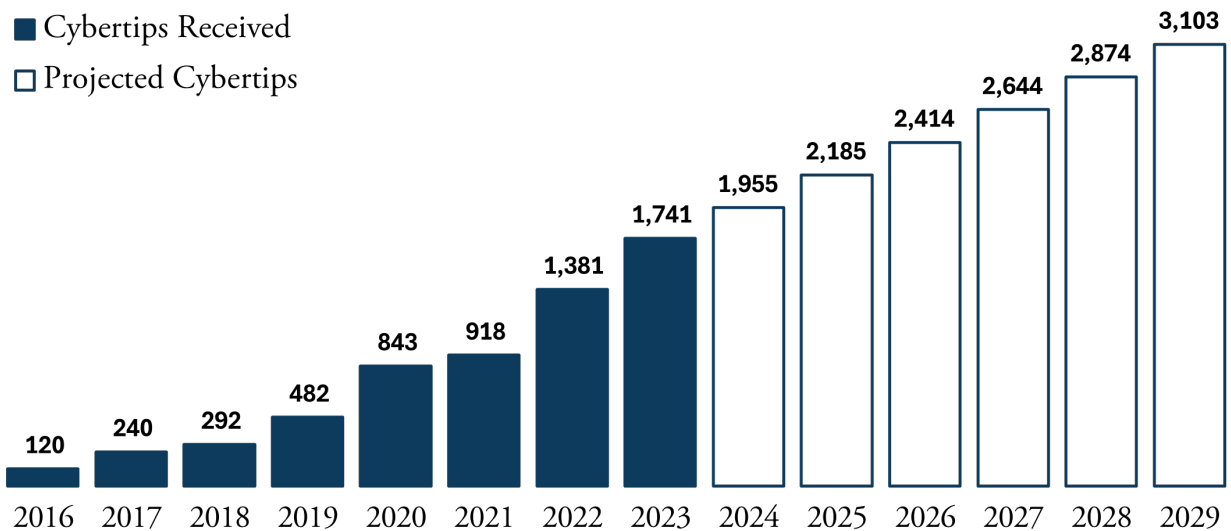
Source: Created by auditor based on information provided by bureau management.

As technology advances, including the increased use of generative artificial intelligence to create CSAM (see the **Emerging Issue**), the number of cybertips the bureau receives may continue to grow, resulting in more time needed to close cases and hold people accountable for their crimes. Management must take proactive steps to ensure that staffing levels are adequate for the current and future demand to investigate cybertips related to internet crimes against children. Ensuring adequate staffing levels for ICAC would also help reduce the backlog that would otherwise continue to grow.

Management's Comment

We concur. TBI will continue to seek additional positions in order to help with the growing number of cases involving Internet Crimes Against Children throughout Tennessee.

Emerging Issue: The bureau is facing challenges with investigating cases with child sexual abuse materials due to artificial intelligence and end-to-end encryption, which may also impact the bureau's staffing resources

Technology, whether devices or applications, is becoming more advanced and widely accessible to individuals, including those who use this technology to commit crimes. While artificial intelligence (AI) has been around for decades, generative AI was introduced to the public in the late 2000s. According to the "Science & Tech Spotlight: Generative AI," issued by the U.S. Government Accountability Office in 2023, generative AI is a form of AI technology "that can create content, including text, images, audio, or video" when a user enters a text prompt in a generative AI app on a computer or mobile device. Users can use generative AI to create a variety of documents, such as papers, realistic images, and other types of artwork.

National agencies are concerned about the impact of generative AI on the number of cybertips needing investigation

According to a summary of federal legislation called the DEFIANCE Act of 2024,[20] as generative AI becomes more available, one of its most popular uses is to create deepfakes[21] and child sexual abuse materials (CSAM). According to the National Center for Missing and Exploited Children (NCMEC), in 2023, they received 36 million cyber tipline reports, 4,700 of which were generative AI CSAM and sexually exploitative content. NCMEC also stated it is concerned that generative AI CSAM will lead to even more dramatic increases in tipline reports as generative AI apps become more technologically advanced, thereby putting more strain on the law enforcement community. As previously noted, the bureau is one of the 62 affiliates in Tennessee responsible for investigating cybertips reported to

---

20. DEFIANCE stands for Disrupt Explicit Forged Images and Non-Consensual Edits. The legislation seeks to protect individuals from sexual exploitation through the use of generative AI.
21. Deepfakes are AI-created images or videos, typically of people, that look realistic.

NCMEC, including tips about CSAM created by generative AI, if the victim and/or perpetrator resides in Tennessee.

According to bureau management, their concerns related to generative AI involve trouble distinguishing a real child from a child created by generative AI, which will complicate their ability to determine if a real child is in danger. Furthermore, the bureau is working with federal and international organizations to develop offensive measures that protect an individual's images. They are currently working on ways to confuse the generative AI technology and allow people to protect their images. Bureau staff have encountered one suspected case of generative AI CSAM, but management is extremely confident that they will start to encounter more material. The biggest issues resulting from generative AI are the inability to identify what is real and how quickly the technology of generative AI is evolving.

If cybertips continue to rise as expected, then management may face an increased need for additional resources devoted to investigating AI-related CSAM cases. The bureau should continue to monitor AI and generative AI advancements and their use in crimes. Management should develop policies to address AI and generative AI as guidance from the federal government becomes available. Bureau leadership should also continue to seek training on AI and generative AI technology for staff as it becomes available.

Social media and instant messaging companies' decision to implement end-to-end encryption across their platforms endangers the largest source of cybertips

During the course of our audit, management stated that the rising threat posed by AI-generated CSAM is compounded by social media and instant messaging companies' decision to bring end-to-end encryption, a security method that ensures messages remain private even to the platform owner, to all their platforms. By doing so, the companies blind themselves to harmful content and compromise the largest source of cybertips to the National Center for Missing and Exploited Children. If these companies cannot make content for their tips available to the bureau's Internet Crimes Against Children investigators, the investigators will be forced to explore extremely time-intensive and inefficient investigative strategies, such as conducting cold interviews without legal process or waiting for someone to accidentally discover and report CSAM.

In response to these companies' decision to enact end-to-end encryption, the bureau has told us they intend to continue to advocate against unregulated encryption on their platforms. In the meantime, management believes it will take more agents doing more digital detective work to mitigate the impact of these companies' decision. Management should enhance its process for prioritizing cybertips by using other data sources to make the best of limited information. To make the most of the evidence that remains, they should also stay current with new tools and techniques through national participation and research.

Management's Comment

Management agrees that search warrant-proof encryption and AI-generated CSAM will increase the burden on Internet Crimes Against Children investigators, making cases more complex and impeding

turnaround times for processing CyberTips. In order to meet these challenges, TBI is pursuing a variety of strategies to mitigate the impact of provider encryption and AI CSAM. First, as noted, TBI participates actively in national efforts for a legislative approach that will appropriately balance user privacy with the need to protect children online. Second, TBI has invested significant time and effort to enrich the data available during CyberTip processing, creating a highly advanced system for CyberTip triage that leverages technology and the investigative experience of ICAC agents. Third, TBI is participating in a variety of national committees and the Tennessee Artificial Intelligence Advisory Council in an effort to ensure that our response to the threat of AI CSAM is best in class as the threat evolves. These steps will not completely compensate for the growth of the problems, however, and TBI agrees that more staffing for the ICAC Squad will be necessary to keep pace with the CyberTip workload and ensure that these vulnerable victims are protected.

Information Systems

> The Tennessee Bureau of Investigation's (the bureau's) information systems store and process a significant amount of confidential and sensitive information protected by federal and state policies. The bureau uses information systems to accomplish law enforcement activities and is responsible for safeguarding confidential and sensitive information. Our goal was to determine whether bureau management designed and implemented internal controls over information systems to safeguard sensitive and protected information and to evaluate whether management corrected the conditions reported in the prior audit. See the **Finding**.

General Background

The bureau relies on information systems—including the Laboratory Information Management System and the Investigations and Evidence System mentioned throughout this report—to access, store, and process a significant amount of private, confidential, and personal information belonging to individuals, including Tennessee citizens, to support its day-to-day activities.

Within the bureau, the Technology and Innovation Division's information systems staff provide information technology and desktop support to the bureau's staff and serve as the primary responsible party for managing and securing the bureau's computer systems and network, which allows employees and the bureau's law enforcement partners access to the bureau's data. Though the bureau primarily manages its own information technology (IT) infrastructure internally, the Department of Finance and Administration's Division of Strategic Technology Solutions (STS) also provides IT support to the bureau through infrastructure, technical direction, project planning, and network monitoring.

Information Systems Controls to Protect Sensitive Data

Robust internal controls over information systems are paramount to protect the information that the bureau collects from its law enforcement activities. As a criminal justice agency, bureau management must adhere to stringent compliance policies and guidelines because it manages criminal justice information[22] and other sensitive data. They must operate in accordance with the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Policy, which is enforced by the FBI's CJIS Division.[23] In addition, STS developed the state's *Enterprise Information Security Policy*, which applies to all state agencies and establishes safeguards to protect systems and data from security threats, ensuring minimum protections against unauthorized access, use, and disclosure of criminal justice information and other sensitive information.

Results of the Prior Audit

In the bureau's September 2020 performance audit, we found that the bureau did not follow state information system policies and industry best practices regarding information systems controls in two areas. The details of these conditions are confidential pursuant to Section 10-7-504(i), *Tennessee Code Annotated*. Bureau management concurred with the finding and stated that they would address the issues through policy changes, additional procedures, and new applications.

Current Audit

We focused our review on determining whether bureau management established relevant internal controls related to information systems. We also evaluated whether management corrected the conditions reported in the prior audit finding. See the **Finding**. See **Appendix 1** for our detailed audit objectives, conclusions, and methodologies.

Finding: Although the bureau has taken steps to resolve one area, it did not provide adequate internal controls in one remaining area involving two conditions that have been repeated in previous audits and one new condition

Although management did resolve one area from the prior audit, we found that management did not effectively design and monitor internal controls in the remaining area, which includes conditions noted as far back as the prior three audits. We reported one condition in the prior three audits and one other

---

22. Criminal justice information refers to all the FBI's Criminal Justice Information Services-provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

23. The FBI's CJIS Division ensures that criminal justice agencies handling this sensitive data comply with the CJIS security policy by conducting audits every three years and special audit reviews as resources allow. Noncompliance carries severe penalties, including criminal charges, denial of FBI database/CJIS system access, fines, formal disciplinary action, and suspension or revocation of criminal justice information access.

condition in the prior two audits. We also identified one new condition. For these conditions, we found internal control deficiencies related to the bureau's systems because the bureau did not adhere to state policies and industry best practices. While these internal control deficiencies increase the risk to the bureau's information technology operations, we did not identify any instances when the bureau was unable to safeguard confidential and sensitive information.

Pursuant to Standard 9.61 of the U.S. Government Accountability Office's *Government Auditing Standards,* we omitted details from this finding because they are confidential under the provisions of Section 10-7-504(i), *Tennessee Code Annotated.* We provided bureau management with detailed information regarding the specific conditions we identified, as well as the related criteria, causes, and our specific recommendations for improvement.

Recommendation: Bureau management should correct these conditions by promptly developing and consistently implementing internal controls. Management should implement effective controls to ensure compliance with applicable requirements, assign staff to be responsible for ongoing monitoring of the risks and mitigating controls, and take action if deficiencies occur.

Management's Comment

We concur in part. We have provided the Comptroller's Office with a Corrective Action Plan to include expected implementation dates.

Auditor's Comment

We have evaluated the finding and considered management's comment, and we stand by our original assessment that controls were not adequately designed in one area. This area involves two conditions that have been repeated in previous audits and one new condition identified in the current audit.

Bureau Management Oversight

> In order to meet the Tennessee Bureau of Investigation's (the bureau's) mission, bureau management develop and implement internal controls to ensure staff properly carry out duties and provide management with procedures to oversee their staff. Our goal was to evaluate management's processes and internal controls over their operational areas.

General Background

To carry out the bureau's responsibilities, the Director and the management team must establish adequate internal controls to provide reasonable assurance that the bureau can achieve objectives related to its operations, as well as that it complies with laws, regulations, and policies. Effective internal controls mitigate the risks of noncompliance, errors, fraud, waste, and abuse.

Policies and Procedures

The U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government* (Green Book) provides a comprehensive framework for internal control practices in federal agencies and serves as a best practice for other government agencies, including state agencies. According to Green Book OV1.03,

> Internal control comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the entity. Internal control serves as the first line of defense in safeguarding assets. In short, internal control helps managers achieve desired results through effective stewardship of public resources.

In addition, the bureau is accredited by the Commission on Accreditation for Law Enforcement Agencies, Inc. The accreditation focuses on ensuring the bureau has adopted standards related to life, health, and safety procedures. Policies and procedures describe management's day-to-day operations in order to deliver services to its customers.

Current Audit

We focused our review on determining whether bureau management established relevant internal controls related to their oversight responsibilities. Our review did not result in any findings or observations. See **Appendix 1** for our detailed audit objectives, conclusions, and methodologies.

Remittance of Sex Offender Registry Fees to the State

> Law enforcement entities are required to register convicted sex offenders on the state's Sex Offender Registry and obtain a $150 fee from the offenders when they initially register and annually thereafter; the state receives $50 of the fee. Prior to 2020, the Tennessee Bureau of Investigation (the bureau) was explicitly required by state statute to collect the fees. Our goal was to review the process to collect the fees since the statute changed in 2020. See the **Matter for Legislative Consideration**.

General Background

Bureau management uses the electronic sex offender database to maintain the registration of all sexual offenders within the state. The Sex Offender Registry section within the bureau's Criminal Intelligence Unit is responsible for maintaining the database.

However, the bureau does not have the authority to enforce sex offender registration. According to Section 40-39-205, *Tennessee Code Annotated*, that responsibility falls to the registering agencies across the state. Registering agencies include sheriff's offices, municipal police departments, metropolitan police departments, campus law enforcement agencies, the Department of Correction, the Tennessee Board of Parole, and any private contractor with the Department of Correction.

Prior to 2020, Section 40-39-201(b)(7) and Section 40-39-204(b) and (c), *Tennessee Code Annotated*, required any individual convicted of a sexual offense to report to a registering agency periodically and pay an annual administrative fee of $150.[24] The registering agencies were responsible for collecting it and remitting $50 from each fee to the bureau for the maintenance of the Sex Offender Registry. In April 2020, the statute changed and redirected this portion of the fees from the bureau to the General Fund. The updated statute, however, did not explicitly state which entity the registering agencies should sent the $50 state portion to for deposit into the state's General Fund. As a result, the Department of Finance and Administration directed the bureau to continue to accept the fees and deposit them. From April 1, 2020, through May 31, 2024, bureau management deposited $1,815,812 in Sex Offender Registry fees.

---

24. According to management, the registering agencies are responsible for determining an offender's ability to pay. If an agency determines that an offender is indigent, the offender is exempt from paying the fee.

Current Audit

We reviewed the bureau's role in accepting Sex Offender Registry fees since the statute changed in 2020. See the **Matter for Legislative Consideration.** See **Appendix 1** for our detailed audit objectives, conclusions, and methodologies.

> **Matter for Legislative Consideration:** Bureau management should seek assistance from the Department of Finance and Administration and/or the General Assembly to be relieved from the bureau's role in accepting and depositing the state's portion of the Sex Offender Registry fees received from registering agencies

Through the passage of Public Chapter 668 in 2020, which amended Section 40-39-201(b)(7) and Section 40-39-204(b) and (c), *Tennessee Code Annotated*, registering agencies were still required to remit $50 of an offender's Sexual Offender Registry fees to the state for deposit into the state's General Fund; however, the law did not specify where the fees should be sent.

Based on our research and according to the bureau's Fiscal Services Division's standard operating procedures, the Department of Finance and Administration instructed the bureau in March 2021 to continue accepting the state's portion of the fees from the registering agents, even though the law did not specify the state entity responsible to receive and deposit the state's $50 portion into the state's General Fund. According to management, the bureau is a law enforcement agency focused on public safety and not an agency that deals in business transactions. As such, management stated they believe the fee depositing function should be transferred to a state agency that specializes in fee receipt and deposit.

Given management's preference to be removed from this fee process, management should seek assistance from the Department of Finance and Administration and/or the General Assembly to assist them in this matter.

Management's Comment

We concur. The Bureau was previously tasked with the acceptance of the state's portion of sex offender registry (SOR) fees, but various problems persisted with that duty, which resulted in past findings/observations from the Comptroller. The TBI's expertise lies in criminal investigation, not in fee collection. TBI does not have the proper personnel or infrastructure to adequately manage acquisition of SOR fees from all the supervising agencies across the state. It would also not be cost effective, nor efficient to provide the TBI those personnel, as we are not the authority for ensuring proper payment of the fees. That responsibility resides with the registering agencies. Beyond the Bureau's belief that it is not the appropriate agency to manage collections, we would defer to the will of the General Assembly and the Administration on which possible solution is most appropriate.

Appendices

Appendix 1: Objectives, Conclusions, and Methodologies

Prior Audit Findings

Standard Operating Procedures

Audit Objective: In response to the prior audit finding, did Tennessee Bureau of Investigation (bureau) management have sufficient written policies and standard operating procedures for the Drug Offender Registry and the Sex Offender Registry, including the collection of Sex Offender Registry fees?

Conclusion: Based on our review, bureau management developed and incorporated relevant policy and procedures into their standard operating procedures for the Drug Offender Registry and the Sex Offender Registry. This finding is resolved. We also found that a 2020 change in state statute failed to include the state entity responsible for collecting $50 of the Sex Offender Registry fees from registering agencies for deposit into the state treasury. The Department of Finance and Administration notified bureau management that they should continue to collect and deposit these fees. To provide clarity to all registering agencies regarding fee submission, the General Assembly may wish to add the bureau as the responsible state agency. See the **Matter for Legislative Consideration**.

Methodology to Address the Audit Objective

To address the audit objective, which included gaining an understanding of management's process to update their standard operating procedures related to the Sex Offender Registry and Drug Offender Registry and assessing management's design and implementation of internal control significant to our audit objective, we interviewed the Fiscal Director, CJIS[25] Support Analyst, the Special Agent in Charge of the Drug Investigation Division, the Intelligence Analyst of the Drug Investigation Division, and the Assistant Special Agent in Charge of the Central Intelligence Unit. We reviewed the

- 2020 Tennessee Bureau of Investigation performance report;

- management's report of actions taken to correct the prior audit findings;

- the bureau's 2021 Criminal Intelligence Unit Sex Offender Registry Standard Operating Procedures;

- Section 40-39-201, *Tennessee Code Annotated;*

---

25. CJIS stands for criminal justice information service.

- Section 40-39-204, *Tennessee Code Annotated;*

- the bureau's 2020, 2023, and 2024 Drug Offender Registry Standard Operating Procedures; and

- the bureau's 2021 Fiscal Services Standard Operating Procedures.

Drug Offender Registry

Audit Objective: Did bureau management notify the National Association of Drug Diversion Investigators (NADDI) when they removed offenders from the Drug Offender Registry, as required by Section 39-17-431(l)(1), *Tennessee Code Annotated?*

Conclusion: Based on our testwork, with the exception of one email that management could not locate, we found that management notified NADDI when they removed offenders from the Drug Offender Registry. This finding is resolved.

Methodology to Address the Audit Objective

To address the audit objective, which includes gaining an understanding of management's notification process to inform NADDI of Drug Offender Registry deletions and assessing management's design and implementation of internal control significant to our audit objective, we interviewed the CJIS Support Analyst and the Intelligence Analyst for the Drug Investigation Division that oversees Drug Offender Registry deletions. Additionally, we reviewed

- Section 39-17-436(e), *Tennessee Code Annotated*;

- Section 39-17-431, *Tennessee Code Annotated*; and

- the bureau's 2020, 2023, and 2024 Drug Offender Registry Standard Operating Procedures.

To determine operating effectiveness and management's compliance with state statute, we obtained a list of 3,186 individuals that bureau management deleted from the Drug Offender Registry from June 1, 2020, through February 22, 2024. The U.S. Government Accountability Office, whose standards we are statutorily obligated to follow, requires us to assess the sufficiency and appropriateness of computer-processed information we use to support our findings, conclusions, and recommendations. To determine the population's reliability, we examined the data to identify duplicate or invalid records for completeness and accuracy. We determined that the data was sufficiently reliable for the purpose of this report. From our population, we selected a nonstatistical, random sample of 60 individuals deleted from the Drug Offender Registry and requested the emails management sent to NADDI.

Current Audit Objectives

Forensic and Digital Evidence

1. Audit Objective: Has management developed plans to address the backlogs and turnaround times related to evidence processing requests?

    Conclusion: **Forensic Services Division**: Based on our review, management added 50 new laboratory positions, began training new staff, added new workspaces, outsourced some sexual assault kit testing, and redistributed some requests for testing across the labs to address the backlog and turnaround times of cases and requests. Additionally, the lengthy training programs for forensic scientists pose temporary productivity challenges for the bureau. See **Observation 1**.

    Digital Forensics Squad: Based on our review, management added one new digital forensics examiner position in fiscal year 2023 and received approval for four more for fiscal year 2025 to address the backlog and turnaround time of digital forensics evidence requests. Additionally, the lengthy training programs for digital forensic examiners pose temporary productivity challenges for the bureau. See **Observation 1**.

2. Audit Objective: Does management have a process to prioritize and analyze evidence requests?

    Conclusion: **Forensic Services Division:** Based on our review, management has a process to prioritize and analyze cases and requests that varies slightly depending on the unit. However, we noted that priorities can shift depending on the public's and the bureau's needs, resulting in longer turnaround times for cases with lower priority, such as non-expedited firearms requests or violent and non-violent forensic biology requests. See **Observations 2** and **3**.

    Digital Forensics Squad: Based on our review, we found that management should work to improve its network capabilities to improve their ability to process large-scale devices to reduce delays in analyzing digital evidence. See **Observation 1**.

3. Audit Objective: Can management better use their information systems to look for ways to improve the efficiency of the evidence testing process?

    Conclusion: **Forensic Services Division:** Based on our review, management has the opportunity to use their information system to consistently track requests, yielding more accurate information for their reports. See **Observation 4**.

Digital Forensics Squad: Based on our review, we found that digital forensics management has a process in place to prioritize and process digital evidence. We also noted, however, that management could use their case management system to track device workflow and break down evidence milestones to look for inefficiencies in their process. See **Observation 4**.

Methodology to Address the Audit Objectives

Forensic Services Division: To address our audit objectives, which includes assessing the design and implementation of management's internal controls, we interviewed

- the Forensic Services Division's Assistant Director, Quality Assurance Manager, and Information Technology Manager;

- the bureau's Fiscal Director;

- the Regional Administrators for the Jackson, Nashville, and Knoxville laboratories;

- the unit managers and/or supervisors in each regional laboratory over Forensic Biology, Forensic Chemistry, Toxicology, Firearms and Toolmark Identification, the Combined DNA Index System (CODIS), Latent Prints, and Microanalysis; and

- the Nashville laboratory's Evidence Receiving staff.

We observed management's operations to gain an understanding of the laboratories' processes to receive, prioritize, and analyze forensic evidence and report results, as well as to hire and train forensic laboratory staff. We also reviewed

- *Tennessee Code Annotated,* bureau and laboratory accreditation standards,[26] Federal Bureau of Investigation compliance reviews for the CODIS Unit, standard operating procedures, and quality assurance manuals for the Forensic Services Division;

- the National Institute of Justice's best practices and recommendations for forensic laboratories;

- the bureau's quarterly reports to the legislature from July 2023 to April 2024, annual reports for fiscal years 2021, 2022, and 2023, and risk assessment for fiscal year 2024;

- budget requests and hearings, staffing proposals, and salary studies from fiscal year 2021 to 2025 for the Forensic Services Division;

- backlog and turnaround time reports for all disciplines from June 2020 to May 2024, generated from the Laboratory Information Management System;

- the Assistant Director of Forensic Services' backlog and turnaround time statistical tracking spreadsheet from July 2019 to May 2024; and

---

26. The Commission on Accreditation for Law Enforcement Agencies, Inc. and the American National Standards Institute National Accreditation Board.

- examples of Forensic Services staff training records and proficiency testing results.

We attempted to perform a data reliability assessment of the backlog and turnaround time reports provided by management by requesting the underlying data and code used to generate the reports but were unable to assess data reliability due to management's assertions of statutory confidentiality restrictions. (See the Data Reliability Review Methodology section below for additional information.) As a result, all backlog and turnaround time information in the report was provided by management and is presented as unaudited data.

Digital Forensics Squad: To address our audit objectives, which includes assessing the design and implementation of management's internal controls, we interviewed

- the Assistant Director of the Technology and Innovation Division,
- the Special Agent in Charge of the Cybercrime and Digital Evidence Unit,
- the Assistant Special Agent in Charge of the Digital Forensics Squad,
- the Business Intelligence Specialist, and
- Strategic Technology Solutions' Network Architect.

We observed management's operations to gain an understanding of the Digital Forensics Squad's process to receive, prioritize, and analyze digital evidence and approve the results. We reviewed

- the Digital Forensics Squad's standard operating procedures;
- the bureau's policies;
- the bureau's annual reports for fiscal years 2021, 2022, and 2023;
- budget requests and hearings and staffing proposals from fiscal years 2021 to 2025 for the Technology and Innovation Division; and
- the bureau's Information System Plan.

To determine operating effectiveness for audit objective 2, we obtained a population of 1,848 cases, consisting of 4,139 digital evidence items, that the bureau opened from June 1, 2020, through April 30, 2024, to assess the status of each case and to calculate backlog and turnaround time statistics.

Data Reliability Review Methodology

The U.S. Government Accountability Office (GAO), whose standards we are statutorily obligated to follow, requires us to assess the sufficiency and appropriateness of computer-processed information we use to support our findings, conclusions, and recommendations. We attempted to perform procedures to assess the sufficiency and appropriateness of backlog and turnaround time data from information systems for both the Forensic Services Division and the Digital Forensics Squad.

Forensic Services Division

To evaluate management's evidence processing backlog and turnaround time reports, we requested a data extract from the Laboratory Information Management System (LIMS) of all evidence testing requests from June 1, 2020, to February 29, 2024, that included data points on each milestone[27] of the testing process. We discussed the request with bureau management and indicated that we did not need any case-specific information as part of the request; however, bureau management stated that all data in LIMS, even if no case-specific information was included, was confidential pursuant to Section 10-7-504(a)(2)(A), *Tennessee Code Annotated,* which states "[a]ll investigative records of the Tennessee bureau of investigation . . . shall be treated as confidential and shall not be open to inspection by members of the public." According to the Assistant Director of Forensic Services, "TCA 10-7-504, [laboratory] accreditation requirements, and laboratory policy do not permit . . . laboratory [management] to share specific information from the LIMS database/case files."

Because we were prohibited from obtaining the underlying data supporting the Forensic Services Division's backlog and turnaround time reports, we were unable to determine the reliability of the data. Internal control weaknesses that we identified further complicated using the data related to our planned audit objectives. As such, we concluded that this data is of undetermined reliability in accordance with GAO's *Applied Research and Methods: Assessing Data Reliability.*

Management did provide us with aggregate backlog and turnaround time reports from June 2020 to February 2024 and the Assistant Director's trend spreadsheets that covered the same time. We matched the Assistant Director's spreadsheet to the backlog and turnaround time reports. We did not note any discrepancies. In consultation with bureau management, we decided to use management's trend spreadsheet in the report to provide contextual information on backlog and turnaround times with a disclaimer that the data was provided by management (unaudited) and the underlying data is of undetermined reliability.

Digital Forensics Squad

We requested data from the Investigations and Evidence (I+E) system related to digital forensics evidence to calculate and assess backlog and turnaround time statistics for the period June 2020 through March 2024. We met with management to discuss the request and indicated that we did not need any case-specific information as part of the request. We assessed information systems controls for the system that produced the data. Management was able to provide a redacted extract of the data; however, due to limitations in I+E, management could not provide the tracking details related to how each piece of evidence moves through the forensic analysis process. According to management, the evidence tracking details are embedded with case information. I+E can only provide high-level tracking details for cases. Management also stated that pursuant to Section 10-7-504(a)(2)(A), "[a]ll investigative records of the Tennessee bureau of investigation . . . shall be treated as confidential and shall not be open to inspection by members of the public," and could not provide the evidence-level

---

27. As explained in **Observation 4** of this report, milestones refer to each major step of the testing process, beginning with the date the request was received and ending with the date the final results report was generated.

tracking details we requested. Given that we could not obtain evidence-level details, we had to use the high-level case tracking to complete our work.

Because we could not obtain the evidence-level tracking data to calculate the squad's backlog and turnaround times and due to internal control weaknesses we identified through our work, we were unable to determine the reliability of the data related to our planned audit objectives. As such, we concluded that this data is of undetermined reliability in accordance with GAO's *Applied Research and Methods: Assessing Data Reliability.*

In summary, we are required by Section 10-7-504(a)(22), *Tennessee Code Annotated,* to protect all confidential records when performing our audits. Furthermore, as members of the Office of the Comptroller of the Treasury's Division of State Audit, we are not members of the public; however, due to time constraints, we conceded to management's request to not turn over the data we requested. We were able to obtain limited backlog and turnaround time data from management to support our observations and conclusions.

Internet Crimes Against Children

1. **Audit Objective:** Did management in the Internet Crimes Against Children (ICAC) Squad have a process to prioritize and investigate the cybertips it received?

   Conclusion: Based on our review, we found that ICAC management has a multi-level prioritization review process in place that helps the squad prioritize and investigate submitted ICAC tips.

2. **Audit Objective:** Has management in the ICAC Squad developed plans to address the backlogs of tips received?

   Conclusion: Based on our review, we found that the ICAC Squad has a backlog of 2,543 tips and has requested additional personnel to assist in reducing the backlog. See **Observation 5**.

3. **Audit Objective:** What does the bureau see as potential emerging issues related to child sexual abuse materials involving artificial intelligence (AI)?

   Conclusion: Based on our review, as of March 28, 2024, management has identified child sexual abuse materials created using generative AI as an emerging issue that could affect the bureau's operations due to the potential growth in generative AI-created child sexual abuse materials and nonconsensual sexual abuse materials. Management is also aware there is a lack of current offensive measures to protect individuals against AI and believes the state will experience an increase in these types of crimes. Furthermore, management has identified

the use of end-to-end encryption as another emerging issue affecting investigations of child sexual abuse materials. See the **Emerging Issue**.

Methodology to Address the Audit Objectives

To address audit objectives 1 and 2 and assess management's design and implementation of internal controls, we interviewed the Special Agent in Charge of the Cybercrime and Digital Evidence Unit, the Assistant Special Agent in Charge of the ICAC Squad, the Assistant Special Agent in Charge of the Cybercrime Investigations Squad, the unit's Business Intelligence Analyst, and the state's ICAC Commander to determine the bureau's process to receive, prioritize, and investigate cases involving child sexual abuse materials and observed management's operations. We reviewed ICAC statistics and data for ICAC related to the bureau and other affiliates for our audit period, as well as management's January 2024 ICAC status report. Finally, we reviewed a redacted example of a cybertip received by the National Center of Missing and Exploited Children, as well as the corresponding case from the bureau's case management system.

To determine operating effectiveness, we obtained a population of 3,044 cases assigned to the ICAC Squad from June 1, 2020, through March 31, 2024, to assess the status of each case and to calculate backlog and turnaround time statistics. The U.S. Government Accountability Office, whose standards we are statutorily obligated to follow, requires us to assess the sufficiency and appropriateness of computer-processed information we use to support our findings, conclusions, and recommendations. We assessed the reliability of the data by (1) performing electronic testing, (2) reviewing existing information about the data and the system that produced them, and (3) interviewing bureau personnel knowledgeable about the data.

To address audit objective 3, we interviewed

- the Special Agent in Charge of the Cyber Crime and Digital Evidence Unit,

- the Assistant Special Agent in Charge of the Cyber Crime Squad, and

- the Assistant Special Agent in Charge of the Digital Forensics Squad.

We reviewed

- the ICAC grant agreement with the Knoxville Police Department;

- testimony presented before the U.S. House Committee on Oversight and Accountability Subcommittee on Cybersecurity, Information Technology, and Government Innovation on November 8, 2023, and March 1, 2024;

- the U.S. Government Accountability Office's *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities* and "Science & Tech Spotlight: Generative AI";

- news articles concerning AI and generative AI;

- articles and press releases concerning end-to-end encryption published by the Federal Bureau of Investigation, the U.S. Department of Justice, and the National Center for Missing and Exploited Children;

- the 2022 and 2023 CyberTipline Reports published by the National Center for Missing and Exploited Children; and

- legislation filed during the 113th Legislative Session of the Tennessee General Assembly.

Information Systems

Audit Objective:	Has bureau management implemented information systems controls to safeguard the bureau's sensitive and confidential information?
Conclusion:	Based on our interviews with management, observation of processes, and tests of selected controls, we found that, except for one area, bureau management designed and implemented effective internal controls over critical information systems. One condition was repeated from the prior three audits, and another condition was repeated from the prior two audits. We also identified one new condition. Our work in this area is considered confidential, or for limited official use, according to Section 10-7-504(i), *Tennessee Code Annotated.* Therefore, we will not list specific details in this report. See the **Finding**.

Methodology to Address the Audit Objective

To address our audit objective and to assess the design and implementation of relevant internal controls, we interviewed key personnel from the bureau and Strategic Technology Solutions (STS). These personnel included the bureau's Assistant Director for the Technology and Innovation Division, the Security and Compliance Manager, application system administrators, and bureau and STS IT Managers. We also reviewed the bureau's policies and procedures, inspected the bureau's most recent risk assessments and applicable information systems plans, completed an information system controls questionnaire, and performed walkthroughs to gain an understanding of how management designed and implemented relevant internal controls. We observed selected information systems controls and settings on key systems, and we inspected evidence demonstrating how the bureau configured information systems controls for compliance with the state's *Enterprise Information Security Policy*. We performed testwork to evaluate the operating effectiveness of selected internal controls.

Bureau Management Oversight

Audit Objective:	Did bureau management implement relevant internal controls related to their oversight responsibilities?

Conclusion: Based on our interviews with management and observation of processes, we found that bureau management designed and implemented effective internal controls related to oversight.

Methodology to Address the Audit Objective

To address our audit objective and to assess the design and implementation of relevant internal controls, we interviewed key bureau personnel. We also reviewed the bureau's policies and procedures, inspected the bureau's most recent risk assessments, and performed walkthroughs and observed evidence to gain an understanding of how management designed and implemented relevant internal controls.

Appendix 2: Bureau's Organizational Chart and Structure

Chart 4: Tennessee Bureau of Investigation Organizational Chart as of April 16, 2024

Director

- General Counsel
  - Professional Standards
- Policy Director
- Internal Audit
- Deputy Director
- Accreditation
- Communications
  - Public Affairs

Criminal Investigation Division AD
- West SAC
- Middle SAC
- East SAC
- Upper East SAC

Drug Investigation Division AD
- West SAC
- Middle SAC
- East SAC
- Upper East SAC
- TDDTF SAC

Medicaid Fraud Control Division AD
- West SAC
- Middle SAC
- East SAC
- Medicaid Fraud Manager
- Associate Counsel

CJIS Division AD
- FBI CJIS Systems Officer
- CJIS Support Center
- Law Enforcement Support Unit
- TICS Unit
- Biometrics Unit
- CJIS Special Projects
- TIES

Administrative Services Division AD
- Protective Services
- Human Resources
- Fiscal Services
- Support Services
- Special Projects

Forensic Services Division AD
- Jackson Lab Administrator
- Nashville Lab Administrator
- Knoxville Lab Administrator
- Quality Assurance Manager
- Forensic IT Manager

Technology and Innovation Division AD
- Information Systems
- Criminal Intelligence SAC
- CDEU SAC

Training Division AD
- Associate Counsel
- Training SAC

Aviation

Acronyms
AD – Assistant Director
CDEU – Cybercrime and Digital Evidence Unit
CJIS – Criminal Justice Information Services
SAC – Special Agent in Charge
TDDTF – Tennessee Dangerous Drugs Task Force
TICS – Tennessee Instant Check System
TIES – Tennessee Information Enforcement System

Source: Tennessee Bureau of Investigation management.

Tennessee Bureau of Investigation Organizational Structure

Led by the Director of the Tennessee Bureau of Investigation, the bureau consists of six offices/units and eight divisions. The deputy director oversees the divisions.

The **Internal Audit Office** is responsible for providing value to the bureau by conducting independent, objective, and consulting activity in order to review the bureau's operations to assess risk management, internal controls, compliance, efficiency, and process improvement.

The **Accreditation Office** ensures that the bureau maintains its compliance with accreditation standards from the Commission on Accreditation for Law Enforcement Agencies, Inc. and the Tennessee Law Enforcement Accreditation program.

The **Communications Office** handles communications between the bureau and the public, including all media requests. The staff also maintain the bureau's website and produce video content and promotional materials related to the bureau.

The **General Counsel's Office and Professional Standards Unit** is responsible for legal functions, including contracts, internal affairs, and public records.

The **Policy Office** is responsible for any legislative initiatives, including tracking legislation, advising the Director and Deputy Director on legislation that affects the bureau, and updating bureau personnel on statute changes. Staff also represent the bureau before the General Assembly, lobbyists, the Governor's Office, and other state agencies. The office also assists with the bureau's annual budget request and presentation.

The **Aviation Unit** operates the bureau's aircraft that support their investigations and assists federal, state, and local law enforcement agencies. This unit transports critical personnel, gathers intelligence, and provides officer safety overwatch.

The **Criminal Investigation Division** conducts criminal investigations and assists local law enforcement with their investigations. This division is composed of the following:

- The **Field Investigation Unit** investigates violent and white-collar crimes and provides independent examinations of officers' use of force. It is divided into four geographic regions: west, middle, east, and upper east.

- The **Human Trafficking Unit** investigates cases of adult and minor commercial sex and labor trafficking and is heavily involved in recovering trafficking victims.

- The **Fire Investigations Unit** responds to statewide incidents of fire that destroy property or result in fatalities. Unit staff work closely with local jurisdictions to determine the cause, origin, and circumstances of fires. The investigators use a team of K-9s trained in sniffing out evidence at fire scenes. Staff also operate the 24-hour Arson Hotline,[28] where the public can report

---

28. More information about the Arson Hotline (1.800.762.3017) is available at http://tnarson.org/.

information about suspicious and incendiary fires. Support for the hotline is the result of an ongoing partnership between the bureau and the Tennessee Advisory Committee on Arson.[29]

- The **Victim Services Unit** ensures the victims and witnesses involved in bureau investigations know their rights, the bureau's investigative process, and the criminal justice process, as required by federal and state law. The unit also provides access to multiple support services, such as crisis intervention and counseling, advocacy, education, and information and referrals for victims of crime and trauma.

- The **Polygraph Unit** conducts polygraph examinations regarding allegations of criminal conduct at the request of local, state, and federal law enforcement agencies. The unit also conducts pre-employment polygraph examinations for potential bureau employees.

- The **TBI Overdose and Violent Crime Task Force** consists of local enforcement officers from across the state whose parent agencies allow the bureau to use them as needed for at least a year. In return, the officers receive elite training and equipment from the bureau that they would not otherwise have available. This allows the bureau to use local law enforcement officers to help combat major issues of overdose deaths and violent crime.

The **Medicaid Fraud Control Division** investigates and prosecutes Medicaid provider fraud, patient abuse and neglect, and abuse or neglect of residents in nursing homes and "board and care" facilities.[30]

The **Drug Investigation Division** investigates, gathers evidence, and assists in prosecuting "criminal offenses involving controlled substances, controlled substance analogues, narcotics, and other drugs," and it has "original jurisdiction over the investigation of all drugs" as outlined in Section 38-6-202, *Tennessee Code Annotated*. The division cooperates with local, state, and federal law enforcement agencies such as the Drug Enforcement Administration, the Federal Bureau of Investigation, and Tennessee's United States Attorney's offices. The division includes two task forces:

- The **Tennessee Dangerous Drugs Task Force** is a collaboration between federal, state, and local agencies to reduce the availability and illegal use of harmful scheduled drugs, including methamphetamine, marijuana, prescription drug diversion, heroin, cocaine, fentanyl, and others.

- The **Tennessee Alliance for Drug-Endangered Children** taskforce is composed of federal, local, and state agencies that, according to the bureau's website, work to "prevent drug related harm to children and rescue, shelter, and support Tennessee's children who suffer physical and psychological harm caused by the manufacture, distribution, sale, and abuse of prescription drugs and alcohol."

This division maintains the statewide Drug Offender Registry. It also has a leadership role in several programs that are integral to Tennessee's drug enforcement community: the Appalachia High-

---

29. The Tennessee Advisory Committee on Arson is led by a board of directors consisting of 9 officers and 12 directors elected from its membership. The committee's purpose is to foster relationships between public and private fire investigators, provide continuing education to its members, and support arson prevention and prosecution through the state's Arson Hotline.

30. "Board and care" facilities are assisted care living facilities that provide room, board, and other services to individuals who cannot live independently but do not need the constant supervision that a nursing home provides.

Intensity Drug Trafficking Areas (HIDTA) task force, the Middle Tennessee HIDTA task force, the Gulf Coast HIDTA task force, and the Governor's Task Force on Marijuana Eradication.

The **Forensic Services Division** provides forensic science services for every law enforcement agency[31] and medical examiner in Tennessee. The division has a central laboratory in Nashville and regional laboratories in Jackson and Knoxville. The following units/teams comprise the division:

- The **Evidence Receiving Unit** receives, inventories, distributes, and stores all evidence submitted to the laboratory.

- The **Forensic Chemistry Unit** analyzes any substance seized in violation of laws regulating the sale, manufacture, distribution, and use of abusive drugs.

- The **Toxicology Unit** analyzes blood and other body fluids for alcohol, drug, or poison related to traffic charges, such as driving under the influence, and other crimes.

- The **Breath Alcohol Unit** administers and maintains Tennessee's breath alcohol testing program, certifies and calibrates breath alcohol instruments, and trains law enforcement personnel on how to operate the instruments.

- The **Latent Print Examination Unit** analyzes fingerprints and palm prints and compares them with suspects' prints. This unit contains the Automated Fingerprint Identification System, which allows staff to compare unidentified prints against a database of fingerprint records.

- The **Firearms and Toolmark Identification Unit** determines if a bullet, cartridge case, or other ammunition was fired from a particular weapon. This unit houses the National Integrated Ballistics Identification Network, which allows individual characteristics from cartridge cases and weapons to be searched against a database to connect crimes.

- The **Microanalysis Unit** examines and compares evidence involving fire debris; shoe, tire, and paper impressions; explosive residue; paint; glass; fiber; tape; and gunshot residue.

- The **Forensic Biology Unit** identifies and characterizes blood and other body fluids to determine whether they are related to a crime or to persons involved in a crime.

- The **Combined DNA Index System Unit** enables evidentiary DNA profiles to be searched against the database of convicted offenders and arrestees.

- The **Violent Crime Response Team** includes special agents with expertise in forensic science. They travel in three regionally located vehicles equipped with advanced forensic equipment for homicide crime scenes.

The **Technology and Innovation Division's** units deliver the following services to the bureau's other divisions, as well as to local, state, and federal criminal justice agencies and to the public:

---

31. The bureau does not complete laboratory testing for areas under the jurisdiction of the Metro Nashville Police Department; these requests are tested by the Metro Nashville Police Crime Laboratory.

- The **Information Systems Unit** runs the bureau's data center and business technology; manages critical communications; and creates, deploys, and maintains systems for bureau personnel and external customers.

- The **Cybercrime and Digital Evidence Unit** investigates a range of online harms, including internet crimes against children, life-threatening communications, cyber-enabled fraud, and computer intrusions. The unit performs digital forensic analysis and uses tools to obtain communications and geolocation evidence for the bureau's special agents and local law enforcement. It also assists with mobile command and radio communications. The unit includes an electronics detection K-9.

- The **Criminal Intelligence Unit** is responsible for compiling, analyzing, and sharing statewide criminal intelligence, with an emphasis on organized crime, fugitives, terrorists, gang activity, missing children, sex offenders, and human trafficking. The employees assigned to this unit manage Tennessee's Fusion Center, the state's missing persons alert programs, the Tennessee Sex Offender Registry, and the bureau's Most Wanted Program.

The **Criminal Justice Information Services (CJIS) Division** provides support and services for the bureau's divisions, as well as state, local, and federal criminal justice agencies. The division houses the state repository of criminal history records, supports criminal justice information traffic, conducts background checks, and performs the following other duties:

- The **Tennessee Instant Check System Unit** processes legally required point-of-sale background checks for firearm purchases by accessing state and federal databases.

- The **Law Enforcement Support Unit** provides state and local law enforcement with information from the National Crime Information Center[32] through Tennessee's Information Enforcement System (TIES) and provides technical support and training for TIES. This unit also houses the Tennessee Crime Information Center and assumes emergency communications responsibilities within the bureau after hours and on weekends.

- The **Criminal Justice Information Services Support Center** collects and reports a variety of crime data. This unit includes the Tennessee Incident Based Reporting System, which captures details on every crime incident, as well as systems that collect data on law enforcement-related deaths. The unit also manages Tennessee's participation in the National Data Exchange System, which provides law enforcement officers with immediate access to criminal justice records from agencies across the country. In addition, this unit is responsible for the bureau's annual report and other publications related to crime in Tennessee.

- The **Biometric Services Section** houses three units:

---

32. The National Crime Information Center maintains files on various types of stolen property; files related to persons including those on supervised release, missing persons, unidentified persons, foreign fugitives, gang members, terrorists, wanted persons, immigration violators, protection orders, and the National Sex Offender Registry; and image files to help identify people and property.

- o The **Fee Programs Unit** processes and maintains the fingerprint-based criminal records database. This includes the Tennessee Application Process System, which provides nationwide criminal histories to employers based on applicants' fingerprints, and Tennessee Open Records Information Services,[33] which allows the bureau to provide third-party vendors with Tennessee criminal history for background checks.

- o The **Criminal Records Unit** processes orders from judges to expunge, or remove, criminal history information and enters final court dispositions into the state repository.

- o The **Data Quality Unit** receives fingerprint submissions and maintains the Automated Fingerprint Identification System database.

- The **State of Tennessee FBI CJIS Systems Officer** monitors system use, enforces system discipline, and ensures users follow proper operating procedures. This individual also serves on policy boards and serves as a liaison with other justice information systems groups.

- The **CJIS Special Projects Unit** acts as a quality control consultant and oversees special projects chosen specifically by the CJIS Assistant Director.

The **Administrative Services Division** provides technical and administrative support to all areas of the bureau and includes the following:

- **Human Resources** provides services in recruitment, onboarding, employee relations, leave and attendance, performance management, and classification and compensation. The unit also provides technical support for processing payroll, benefits, worker's compensation, and other employment matters. The unit is responsible for compliance with the Family Medical Leave Act; the Americans with Disabilities Act; the Fair Labor Standards Act; and Titles VI, VII, and IX of the Civil Rights Act of 1964.

- **Fiscal Services** supports the bureau by preparing the budget, monitoring expenditures and revenues, processing accounts receivable and payable transactions, purchasing goods and services, and maintaining grants.

- **Special Projects** implements special projects and programs that enhance and expand bureau services to its employees and to external customers by routinely assessing work culture and processes and through collaborative efforts. The Special Projects Manager also oversees naloxone[34] distribution.

- **Protective Services** consists primarily of police officers who are responsible for the physical security of the bureau's facilities, personnel, and all guests at the facilities. Additional duties include conducting background investigations for full-time and temporary employees, interns, contract personnel, vendors, certain Tennessee Education Lottery employees, and all Governor

---

33. Tennessee Open Records Information Services background checks are only name-based checks; they provide Tennessee criminal history information to the requestor and do not involve the submission of fingerprints.
34. Naloxone is a medicine that rapidly reverses an opioid overdose.

appointments. The officers also handle investigations based on public-submitted complaints of alleged misconduct by bureau employees.

- **Fleet and Procurement** handles the purchasing of all goods and services necessary for effective operations, manages all bureau vehicles and transportation equipment, and conducts a biennial inventory of all the bureau's state-tagged equipment.

The **Training Division** provides effective, evidence-based training to bureau employees and law enforcement personnel across the state. The division is also responsible for maintaining training records for all criminal investigators in the bureau. In addition, the division oversees the bureau's signature academies and programs, including the following:

- The **Internship Program** gives college juniors and seniors and postgraduate students an inside look at the bureau's work across the state and its place in the criminal justice system.

- The **TBI Special Agent Academy** is an intensive 16-week training course that all newly hired commissioned special agents must attend. The new agents learn how to conduct criminal investigations of all kinds and develop skills to protect themselves and others.

- The **TBI State Academy Leadership Development Experience** provides leadership training for law enforcement leaders from local agencies across the state.

- The **TBI Criminal Investigation Academy** provides investigators from local law enforcement agencies across the state with hands-on training in areas such as interviews and interrogations, search warrant writing, photography, and crime scene processing.

- The **TBI Director's Academy** provides the bureau's future leaders with pre-supervisory leadership training.

- The **TBI Citizens' Academy** was designed to provide the public with a better understanding and awareness of the bureau by offering a peek at the bureau's work.

- The **TBI Criminal Justice Forensic Academy** is a college-student-only, one-week residential program that provides learning experiences for students interested in criminal investigations or forensic science.

- The **TBI Cares Program** trains and allows bureau staff to obtain certification in critical incident stress debriefing, peer support, and health and wellness. CARES Peer Support members provide debriefing services following critical incidents. They also provide ongoing peer support and wellness assistance for employees who need it. The bureau partnered with the Tennessee Public Safety Network to create this program.[35]

---

35. For more information on the program, see https://www.tnpsn.org/.

Where did the bureau's money come from?

Figure 12: Sources of the Bureau's Funding

Federal

Department of Justice grants

Public Safety Partnership and Community Policing
DNA Backlog Reduction Program
Support for Adam Walsh Act Implementation Grant Program
Services for Trafficking Victims
Opioid Affected Youth Initiative
National Sexual Assault Kit Initiative
National Institute of Justice Research, Evaluation, and
    Development Project Grants
Crime Victim Assistance Discretionary Grants
State Justice Statistics Program for Statistical Analysis Centers

Department of Health and Human Services grant

State Medicaid Fraud Control Unit

Office of National Drug Control Policy grant

High-Intensity Drug Trafficking Areas Program

State

General state appropriations

Pass-Through

Criminal court cash bond forfeitures

Defendant diversion and expungement request fees

Fines for convictions

Sex offender registration fees

Other

Fees for services to law enforcement agencies

Criminal background check fees

Firearm permit and background check fees

Training fees

Interdepartmental transfers

Interest and investment income

Source: Auditor analysis of Edison revenue data for fiscal years 2021 to 2024.

Figure 13: Bureau's Budget by Funding Source, Fiscal Year (FY) 2020 to 2025

Federal
$10.37 M
11%

State
$56.78 M
63%

FY 2020

Other
$23.56 M
26%

Total:
$90.70 M

Federal
$10.98 M
12%

State
$52.97 M
59%

FY 2021

Other
$25.75 M
29%

Total:
$89.70 M

Federal
$12.49 M
12%

State
$62.87 M
62%

FY 2022

Other
$26.47 M
26%

Total:
$101.84 M

Federal
$13.18 M
10%

State
$81.71 M
66%

FY 2023

Other
$29.39 M
24%

Total:
$124.27 M

Federal
$13.42 M
8%

State
$117.54 M
74%

FY 2024*

Other
$28.87 M
18%

Total:
$159.83 M

Federal
$13.40 M
9%

State
$110.24 M
74%

FY 2025†

Other
$24.62 M
17%

Total:
$148.25 M

Source: State of Tennessee Budget publications for fiscal years 2022 through 2025.

* FY 2024 amounts represent the estimated budget as of February 5, 2024.

† FY 2025 amounts represent the recommended budget as of February 5, 2024.

How much did the bureau spend at the division level?

Figure 14: Bureau's Spending by Division and State Fiscal Year, FY 2020 to 2024*

Administrative Services

Year	Amount
2020	$12.4 M
2021	$12.8 M
2022	$15.2 M
2023	$24.8 M
2024	$17.8 M

Criminal Investigation

Year	Amount
2020	$21.9 M
2021	$21.3 M
2022	$24.3 M
2023	$24.6 M
2024	$24.7 M

Criminal Justice Information Services

Year	Amount
2020	$11.2 M
2021	$10.8 M
2022	$12.9 M
2023	$16.5 M
2024	$11.6 M

Drug Investigation

Year	Amount
2020	$12.6 M
2021	$13.0 M
2022	$14.7 M
2023	$16.7 M
2024	$16.2 M

Forensic Services

Year	Amount
2020	$20.8 M
2021	$19.2 M
2022	$21.1 M
2023	$26.5 M
2024	$29.5 M

Medicaid Fraud Control

Year	Amount
2020	$5.4 M
2021	$7.0 M
2022	$7.4 M
2023	$7.7 M
2024	$7.9 M

Technology and Innovation

Year	Amount
2020	$3.8 M
2021	$3.8 M
2022	$5.0 M
2023	$5.7 M
2024	$9.6 M

Training

Year	Amount
2020	$2.8 M
2021	$1.9 M
2022	$2.2 M
2023	$2.6 M
2024	$2.3 M

Source: Auditor analysis of Edison data.
* FY 2024 spending is as of May 15, 2024.

Appendix 4: Forensic Services Audit Results

Forensic Services Division Training Requirements

The visuals in this section provide information on the length of the training programs for forensic scientists, as well as information on the number of scientists available for casework.

Figure 15: Length of Forensic Services Training Programs
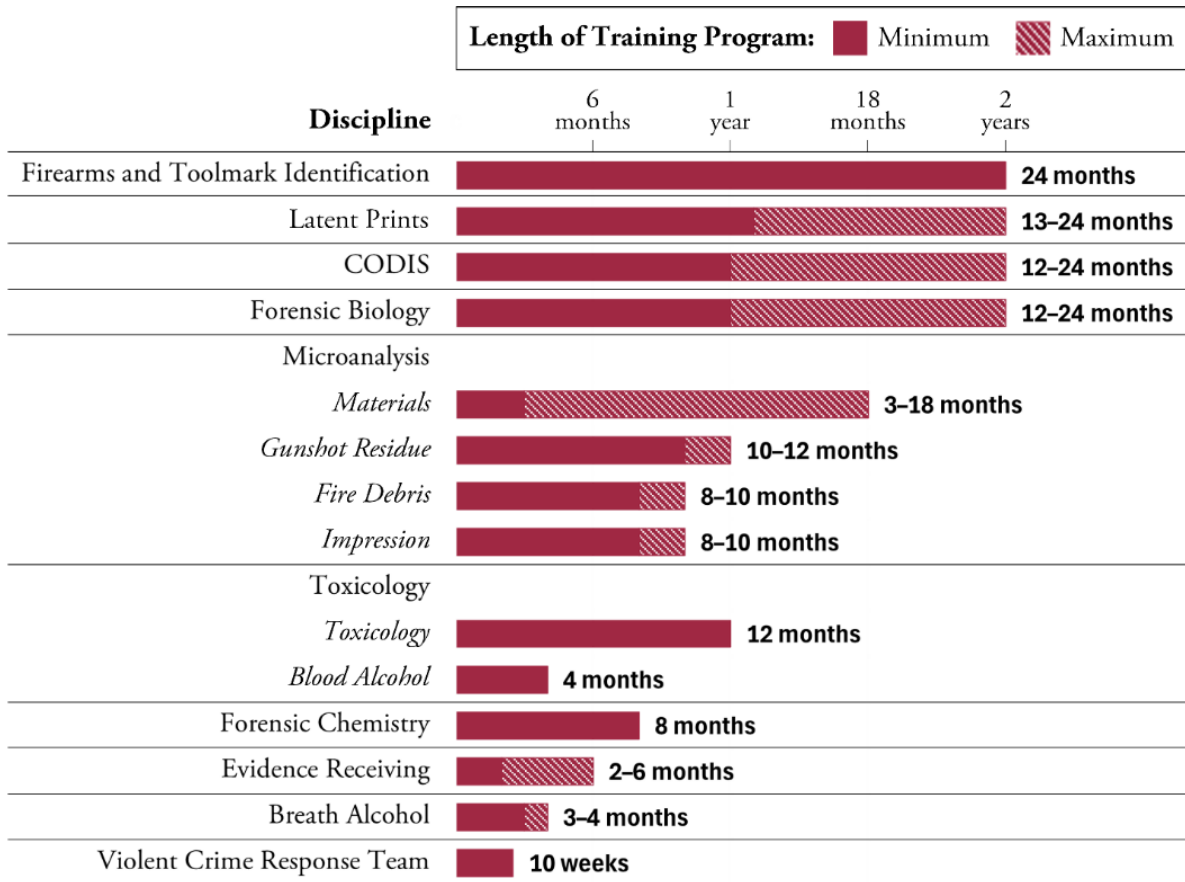
Source: The bureau's Forensic Services Division Quality Assurance Manual.

Figure 16: Full-Time Forensic Services Staff Available for Casework as of March 18, 2024

Discipline	Total Staff	Available Staff*	Percentage of Staff Available for Casework	
Forensic Chemistry	38	34		89%
Latent Prints	13	11		85%
Forensic Biology	43	21		49%
Toxicology	28	12		43%
Firearm Analysis	15	6		40%
Microanalysis	7	1		14%
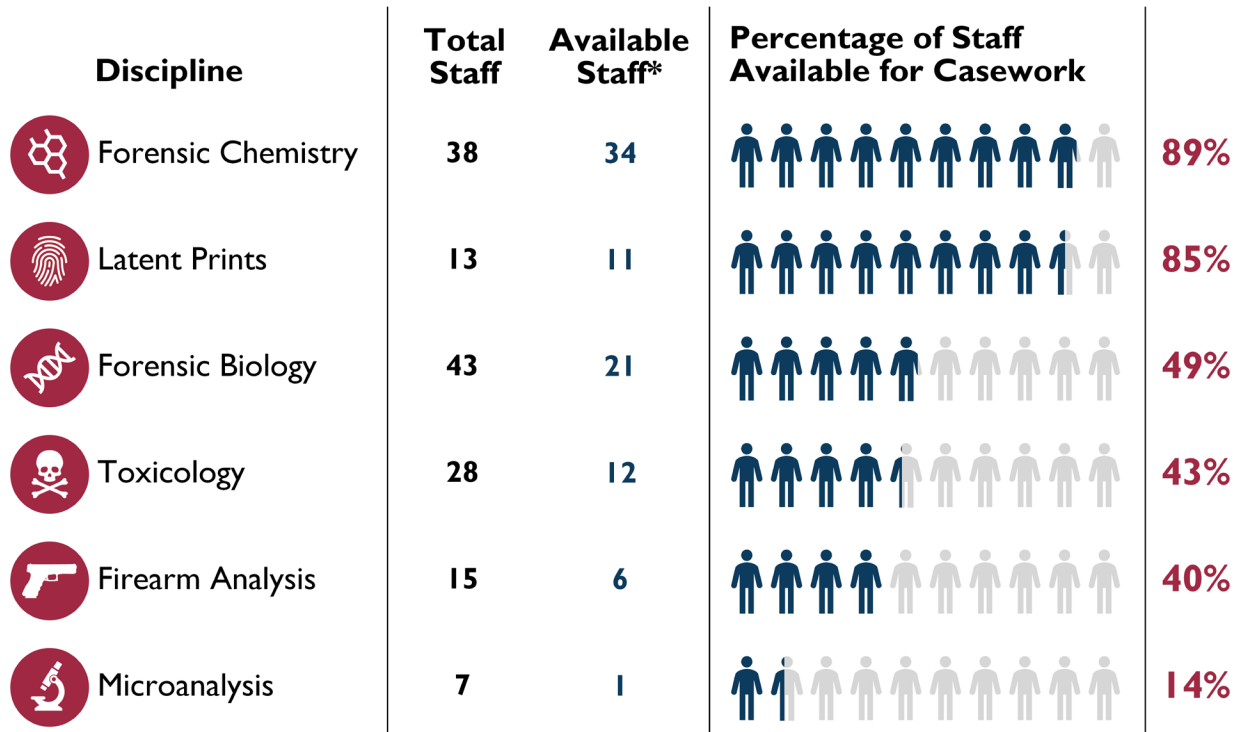
Source: Prepared by auditor from information provided by bureau management.

* Indicates the number of fully trained staff and does not include vacant positions.

Forensic Services Testing Requests and Backlog Information

The visuals in this section provide information on the number of requests for testing and backlogs for each laboratory and discipline. **Table 5** indicates the number of testing requests each laboratory received by forensic discipline from January 1, 2020, to December 31, 2023.

Table 5: Testing Requests by Forensic Discipline and Laboratory, 2020 to 2023 (Unaudited)

Lab Location	Number of Requests			
	2020	2021	2022	2023
Nashville				
Firearms and Toolmark Identification	788	602	540	410
Forensic Biology	969	983	926	919
Forensic Chemistry	11,761	12,722	9,783	10,147
Latent Prints	1,194	1,138	1,067	1,003
Microanalysis	514	480	503	459
NIBIN Entry	308	329	125	72
Toxicology	14,179	15,365	13,754	14,190
Knoxville				
Firearms and Toolmark Identification	*	*	*	*
Forensic Biology	701	772	822	795
Forensic Chemistry	10,952	12,608	9,323	9,341
Latent Prints	*	*	*	*
Microanalysis	*	*	*	*
NIBIN Entry	*	*	*	*
Toxicology	6,758	7,955	6,765	7,650
Jackson				
Firearms and Toolmark Identification	131	108	129	112
Forensic Biology	685	602	617	865
Forensic Chemistry	2,879	3,166	2,979	3,314
Latent Prints	*	*	*	*
Microanalysis	*	*	*	*
NIBIN Entry	21	0	0	0
Toxicology	2,998	2,270	2,776	2,639
Statewide Total Requests	**54,838**	**59,100**	**50,109**	**51,916**

Source: Created by auditor based on data provided by bureau management.
* This lab does not conduct this type of testing.

Table 6 shows the percent change in the backlogs from April 2023 to April 2024. The table also includes turnaround times as of April 2024. This information is presented for each laboratory, statewide, and by discipline.

Table 6: Percentage Change in Backlogs Between April 2023 and April 2024 and Turnaround Time in April 2024 (Unaudited)

Lab Location	Backlog April 2023	Backlog April 2024	▲/▼ % change in Backlog	Turnaround in Weeks as of April 2024
Statewide				
Toxicology – Alcohol	1,824	1,248	▼ 32%	4.3
Toxicology – Drug	1,740	1,362	▼ 22%	13.1
Forensic Chemistry	12,294	8,345	▼ 32%	24.8
Forensic Biology (FB) – Violent	491	532	▲ 8%	38.8
FB – Non-Violent	383	483	▲ 26%	49.8
FB – Sex Offense – Kit Only	-	154	-	8.8
FB – Sex Offense – Kit Plus Additional Items	392	240	▼ 39%	28.0
FB – Outsourced Kit	550	181	▼ 67%	44.3
Firearms Analysis	625	559	▼ 11%	68.8
Firearms NIBIN Entry	142	82	▼ 42%	61.3
Latent Prints	274	230	▼ 16%	13.0
Microanalysis	191	121	▼ 37%	22.3
Nashville				
Toxicology – Alcohol	1,161	595	▼ 49%	4.3
Toxicology – Drug	1,080	534	▼ 51%	11.3
Forensic Chemistry	3,992	2,929	▼ 27%	20.3
Forensic Biology (FB) – Violent	252	316	▲ 25%	28.6
FB – Non-Violent	176	300	▲ 70%	11.3
FB – Sex Offense – Kit Only	-	29	-	11.8
FB – Sex Offense – Kit Plus Additional Items	124	74	▼ 40%	24.4
FB – Outsourced Kit	50	52	▲ 4%	45.2
Firearms Analysis	501	396	▼ 21%	74.8
Firearms NIBIN Entry	142	82	▼ 42%	61.3
Latent Prints – Violent	55	58	▲ 5%	11.2
Latent Prints – Non-Violent	219	172	▼ 21%	13.7
Microanalysis – Arson	23	14	▼ 39%	5.4
Microanalysis – Gunshot Residue	156	92	▼ 41%	31
Microanalysis – Other Testing	12	15	▲ 25%	7.9
Knoxville				
Toxicology – Alcohol	559	490	▼ 12%	4.4
Toxicology – Drug	480	715	▲ 49%	17.4
Forensic Chemistry	7,183	4,538	▼ 37%	35.5
Forensic Biology (FB) – Violent	129	126	▼ 2%	47.0
FB – Non-Violent	147	131	▼ 11%	59.4
FB – Sex Offense – Kit Only	-	31	-	7.8
FB – Sex Offense – Kit Plus Additional Items	123	70	▼ 43%	12.4
FB – Outsourced Kit	248	20	▼ 92%	2.0

Jackson				
Toxicology – Alcohol	104	163	▲ 57%	3.9
Toxicology – Drug	180	113	▼ 37%	10.2
Forensic Chemistry	1,119	878	▼ 22%	11.3
Forensic Biology (FB) – Violent	110	90	▼ 18%	38.9
FB – Non-Violent	60	52	▼ 13%	35.0
FB – Sex Offense – Kit Only	-	94	-	7.9
FB – Sex Offense – Kit Plus Additional Items	145	96	▼ 34%	39.1
FB – Outsourced Kit	252	109	▼ 57%	45.2
Firearms Analysis	124	163	▲ 31%	58.7

Source: Auditor created based on data provided by bureau management.

Chart 5 shows the trend in the number of backlogged requests the regional labs had since 2022.

Based on the chart, the Jackson office has the lowest backlog of requests. All three regions saw a decrease in the backlog over the last two years. Although all labs have been impacted by the time it takes to hire and train new staff, management indicated that the Knoxville lab has had the most challenges hiring and training new staff.

Chart 5: Backlog of Requests for Calendar Year 2022 Through April 2024 (Unaudited)
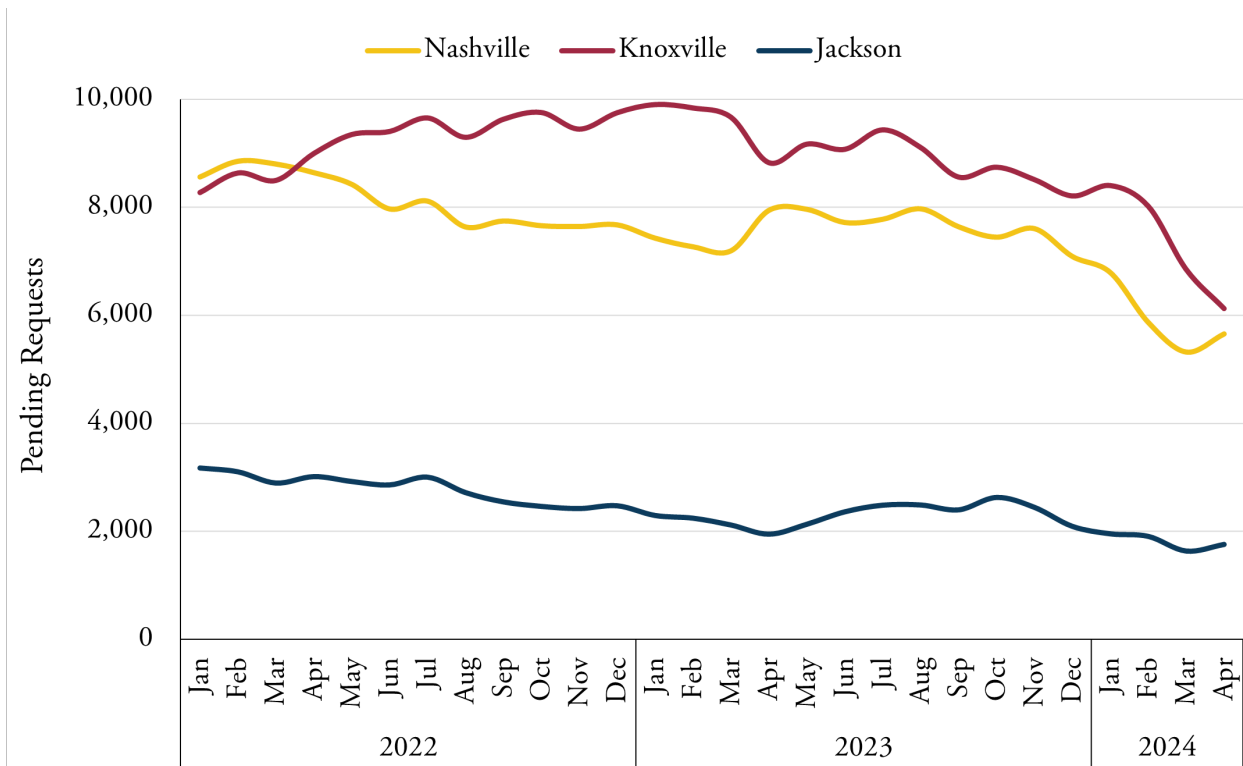
Source: Auditor prepared based on data provided by bureau management.

Figure 17 shows the number of Forensic Services Division staff by discipline at each of the bureau's three regional laboratories as of March 31, 2024.

Figure 17: Lab Positions per Discipline as of March 2024

|	Nashville Lab		Knoxville Lab		Jackson Lab	
Forensic Chemistry	●●●●● ●●●●● ●●●●● ●●●	18	●●●●● ●●●●● ●●●●● ○○○	18	●●●●●	5
Forensic Biology	●●●●● ●●●●● ●●●●● ●	16	●●●●● ●●●●● ●●●○	14	●●●●● ●●●●● ●●●●○	15
Toxicology	●●●●● ●●●●● ●●●○	14	●●●●● ●●●●●	10	●●●●●	5
Latent Prints	●●●●● ●●●●● ●●●	13		-		-
Firearm and Toolmark Identification	●●●●● ●●●●● ●●	12		-	●●●●	4
CODIS	●●●●● ●●●●●	10		-	●●●●○ ○	6
Microanalysis	●●●●● ●●	7		-		-
Evidence Receiving	●●●●● ●○	7	●●●●● ○	6	●●●○	4
Breath Alcohol	●●	2	●	1	●	1
Total		**99**		**49**		**40**

● represents 1 lab staff member   ○ represents 1 vacant lab position

Source: Created by auditors from staffing data provided by management.

We reviewed the Forensic Services Division's quarterly reports to the General Assembly from July 2023 to April 2024 and obtained updated information from management regarding the hiring status of the 50 positions added since 2022. **Figure 18** indicates the hiring status of the 50 new Forensic Services Division positions as of April 30, 2024.

Figure 18: Hiring Status of New Positions as of April 30, 2024
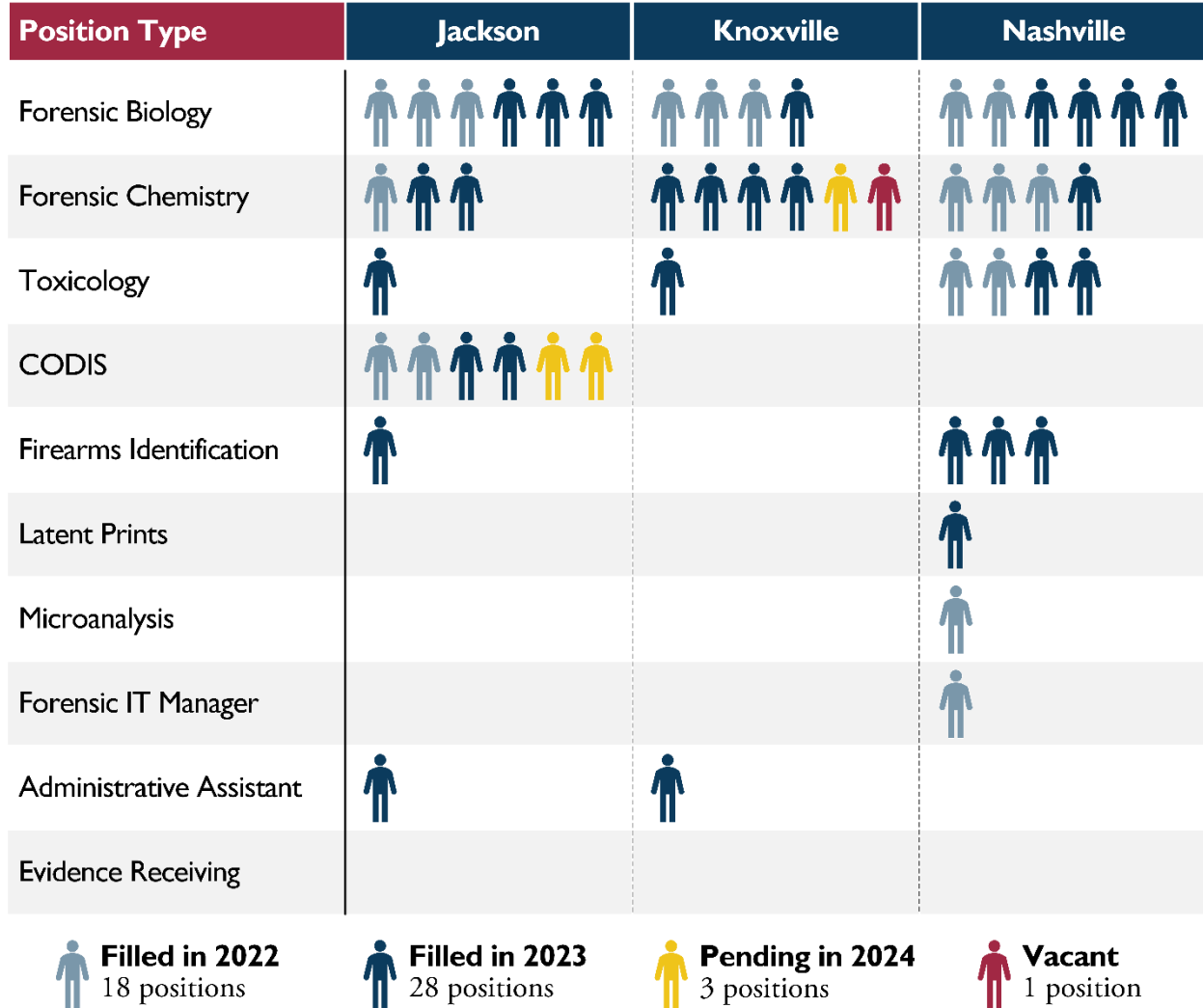
Source: The bureau's fourth quarterly report to the General Assembly, released April 2024, and follow-up discussions with bureau management.

We reviewed the Forensic Services Division's processes for approving and tracking rush testing requests. **Table 7** outlines the rush case approval and tracking processes at each regional laboratory.

Table 7: Rush Case Documentation

Regional Lab	Rush Case Approval and Tracking Process
Jackson	• The approved rush case request is signed by a supervisor and added to the case file. • The Regional Crime Lab Administrator maintains an Excel spreadsheet where rush case requests are tracked. • The Regional Crime Lab Administrator marks the case as rushed within LIMS and assigns a due date within LIMS via the drop-down reasons tab.
Nashville	• The approved rush case request is signed by a supervisor and added to the case file. • Lab personnel add a comment in LIMS in the comment box that the case is rushed. • The lab places rush folders in a separate case file holder.
Knoxville	• The approved rush case request is signed by a supervisor and added to the case file. • Unit supervisors mark the case as rushed within LIMS via the drop-down reasons tab.

Source: Created by auditors based on interviews with regional lab management.

We reviewed the Forensic Services Division's processes for assigning testing requests to forensic scientists in LIMS. **Table 8** outlines how each discipline and each regional laboratory assigns cases and requests to forensic services for testing.

Table 8: Case Assignment (LIMS)

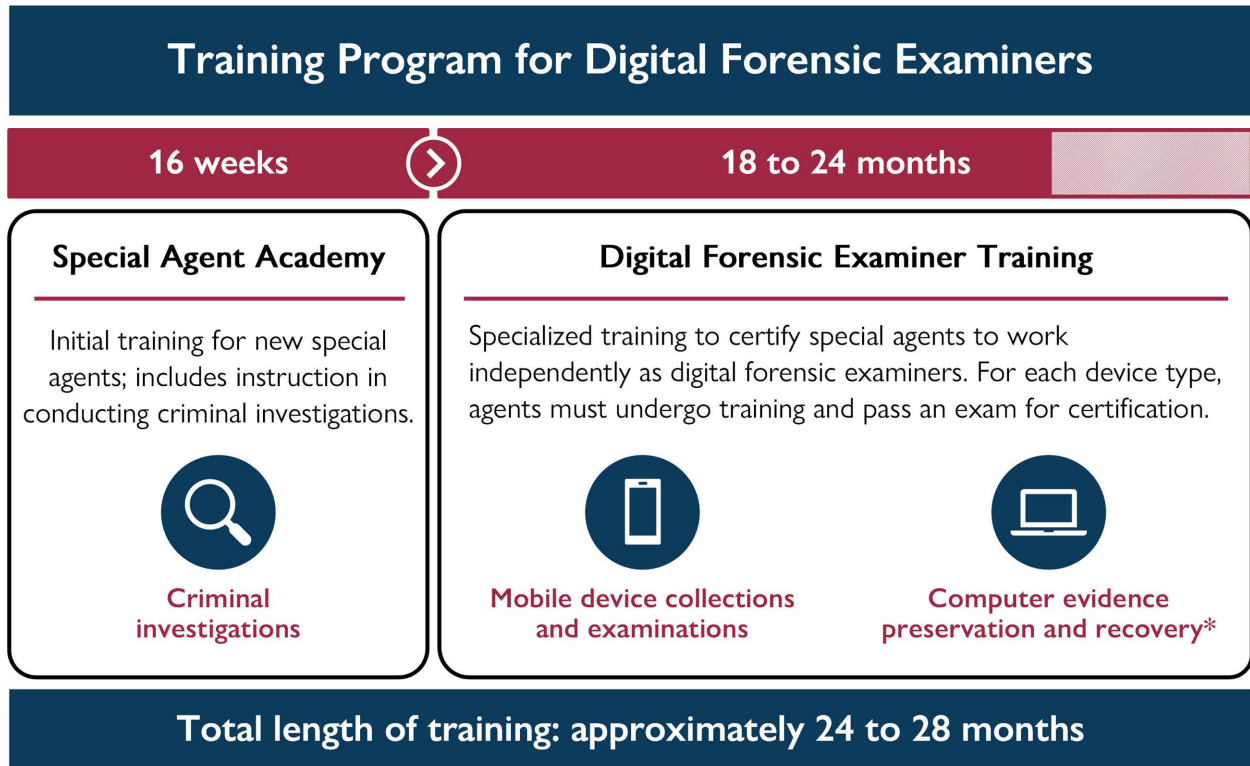| Regional Lab	Latent Prints & Micro	Toxicology	Forensic Chem	Firearms	Forensic Bio
Jackson	N/A	Scientists select cases and assign themselves in LIMS.	Scientists select cases and assign themselves in LIMS.	Unit supervisor assigns cases and balances out more complex cases.	Unit manager gives case files to each scientist and the scientist or unit supervisor assigns in LIMS.
Nashville	Micro: Scientists assign the cases in LIMS. Latent: Either the unit manager, supervisor, or forensic technician assigns cases to scientists.	Scientists can assign themselves cases from a batch of 30 to 40 test requests.	Scientists can assign themselves cases from a batch of 30 to 40 test requests.	Unit supervisor assigns cases and balances out more complex cases.	Scientists select cases and assign themselves in LIMS.
Knoxville	N/A	Cases are assigned by the unit supervisor or staff in evidence receiving.	Cases are assigned by the unit supervisor or staff in evidence receiving.	N/A	Scientists select cases and assign cases to themselves in LIMS.

Source: Information provided by laboratory personnel.

Appendix 5: Digital Forensics Audit Results

Digital Forensics Training Information

The visuals in this section provide information on the length of the training programs for digital examiners, as well as information on the number of examiners by region.

Figure 19: Training Program Lengths for Digital Examiners

Training Program for Digital Forensic Examiners

16 weeks › **18 to 24 months**

Special Agent Academy

Initial training for new special agents; includes instruction in conducting criminal investigations.

Criminal investigations

Digital Forensic Examiner Training

Specialized training to certify special agents to work independently as digital forensic examiners. For each device type, agents must undergo training and pass an exam for certification.

Mobile device collections and examinations

Computer evidence preservation and recovery*

**Total length of training: approximately 24 to 28 months**

Source: Created by auditor based on data provided by bureau management.

* For computer evidence preservation and recovery, an examiner must successfully complete three mock test cases in-house in addition to the required training course.

Figure 20: Digital Forensic Examiners by Region and Training Status as of February 2024
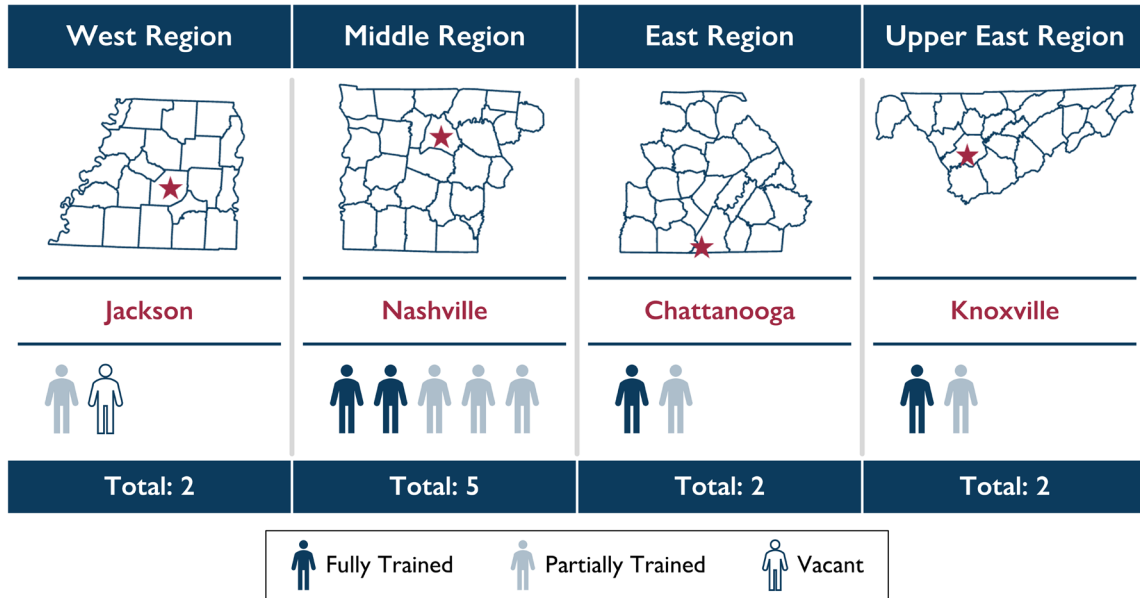

Source: Created by auditor based on data provided by bureau management.

Digital Forensics Testing Submissions

The visuals in this section provide information on the number of cases and pieces of evidence submitted for testing for each type of device, requesting agency, and investigation. As shown in **Chart 6**, digital forensics management has seen consistently high numbers in evidence submission for the past three years. Even though the number of cases reduced in 2023, with the reliance on and use of technology, the evidence numbers remained somewhat consistent with prior years.

Chart 6: Number of Cases and Evidence Items Submitted to Digital Forensics Fiscal Years 2021 Through 2023
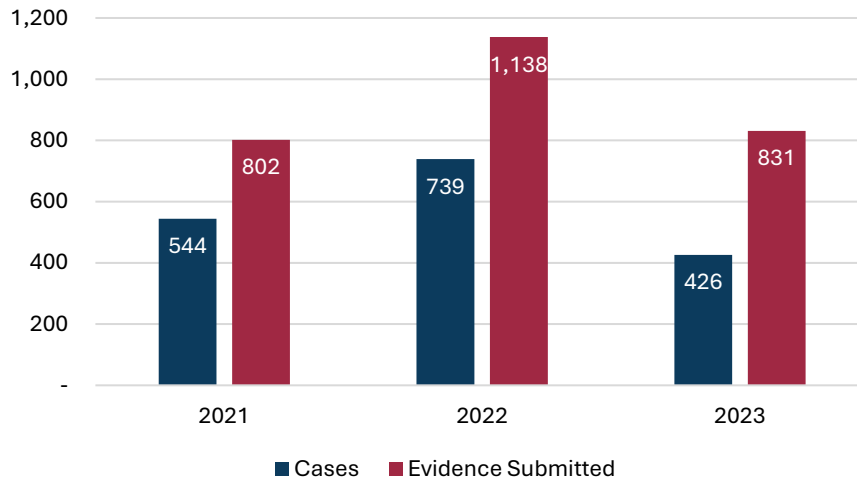
Source: The bureau's annual reports for 2020–2021 and 2021–2022 and bureau management.

See **Table 9** for the number of device types submitted to bureau management for analysis for fiscal years 2021 through 2023. The majority of Digital Forensics' evidence consisted of mobile devices since 2020.

Table 9: Number of Devices Received by Digital Forensics for Fiscal Years 2021 Through 2023

Fiscal Year	Mobile Devices	Computers	Other*	Total
2021	442	60	300	802
2022	607	77	454	1,138
2023	331	41	459	831

Source: Bureau's annual reports for 2020–2021 and 2021–2022 and bureau management.
* Other device types include audiovisual enhancements, vehicle infotainment systems, and devices obtained with the squad K-9.

Chart 7 shows the types of investigations that the Digital Forensics Squad has worked on for fiscal years 2021 through 2023.

Chart 7: Distribution of Digital Forensics' Work by Type of Investigation Supported Fiscal Years 2021 Through 2023
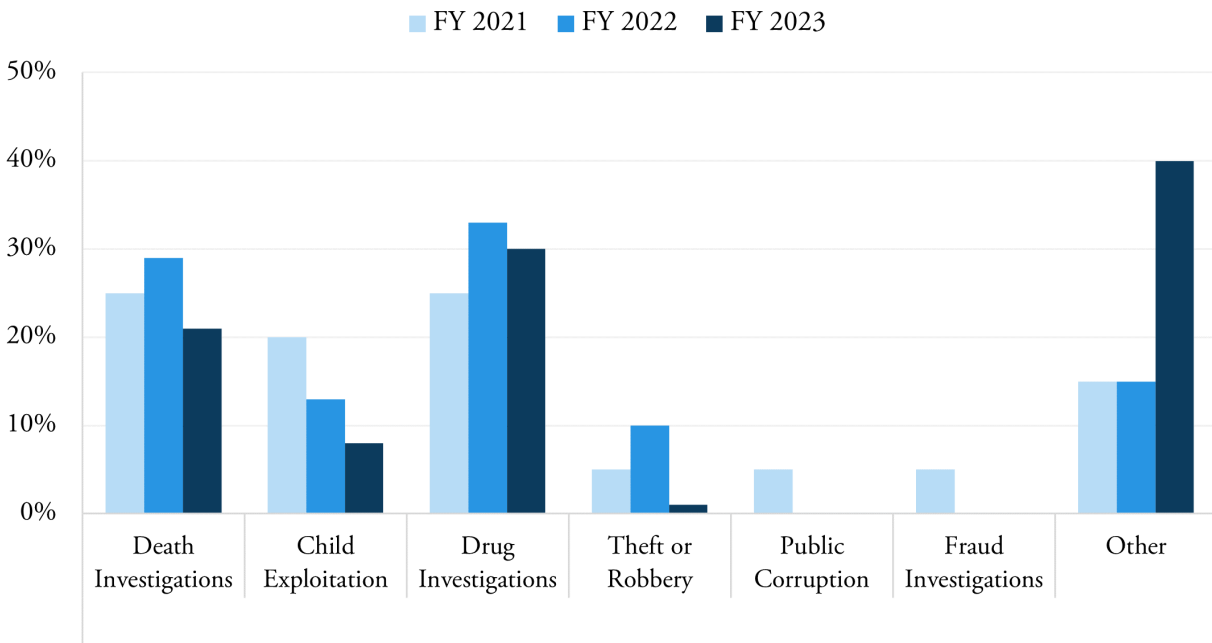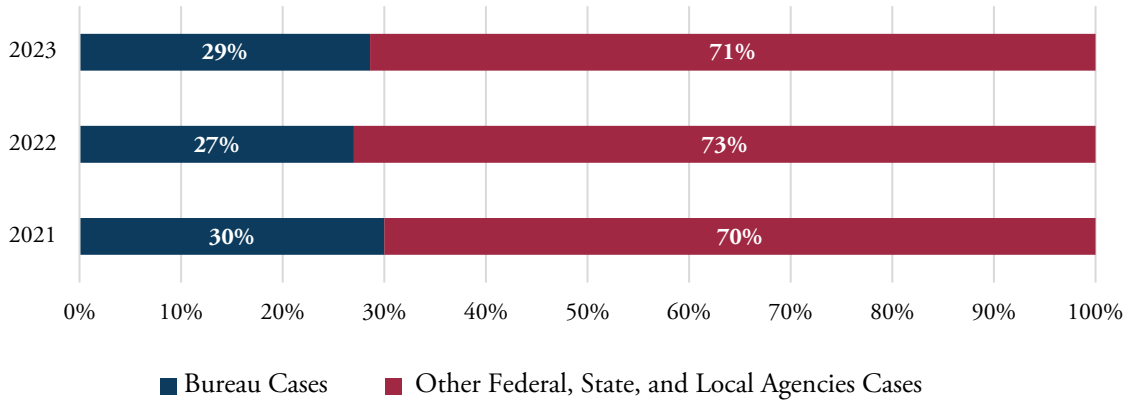

Source: Bureau's annual reports for 2020–2021 and 2021–2022 and bureau management.

Chart 8 shows that the Digital Forensics Squad's work consists of approximately 70% for other federal, state, and local agencies' cases, and the remaining 30% is processed for the bureau's cases.

Chart 8: Source of Digital Evidence Requests for Fiscal Years 2021 Through 2023

	Bureau Cases	Other Federal, State, and Local Agencies Cases
2023	29%	71%
2022	27%	73%
2021	30%	70%

Source: Bureau's annual reports for 2020–2021 and 2021–2022 and bureau management.

Digital Forensics Turnaround Times

The visuals in this section provide information on digital forensics turnaround times by case, device type, and location. From June 1, 2020, through April 30, 2024, the Digital Forensics Squad opened 1,848 cases associated with 4,139 pieces of evidence and closed 212 of these cases (11%), associated with 432 pieces of evidence, during this time period. As shown in **Table 10**, with the exception of general technical assistance, it has taken digital forensics staff at least a year and a half to process devices. **Table 11** shows device turnaround time by office location.

Table 10: Digital Forensic Turnaround Time by Case

Device	Average Weeks
Audio Enhancement	88
Computer	109
General Technical Assistance*	35
Mobile Device	88
Video Enhancement	82

Source: Auditor prepared using bureau data.

* According to management, general technical assistance consists of an informal request to digital forensics to perform a minor task on a device for an agency or a colleague.

Table 11: Turnaround Time (in Weeks) by Device Type and Laboratory Location
June 1, 2022, Through April 30, 2024

Device Type	Chattanooga	Jackson	Knoxville	Nashville
Audio Enhancement	-	-	88	-
Computer	60	143	176	98
General Technical Assistance	-	-	77	32
Mobile Device	45	64	115	84
Video Enhancement	-	–	148	72

Source: Auditor prepared using bureau data.

Appendix 6: Internet Crimes Against Children Affiliate Staffing

Table 12: 2023 ICAC Affiliate Staffing

ICAC Affiliate	Number of Designated Staff*			
	Investigators	Forensics	Prosecutors	Total
Anderson County Sheriff's Office	0.50	0.00	0.00	0.50
Bartlett Police Department	1.00	0.00	0.00	1.00
Bedford County Sheriff's Office	1.00	0.00	0.00	1.00
Bradley County Sheriff's Office	1.50	0.00	0.00	1.50
Carroll County District Attorney	1.00	0.00	0.00	1.00
Carter County Sheriff's Office	0.75	0.00	0.00	0.75
Claiborne County Sheriff's Office	0.75	0.00	0.00	0.75
Cleveland Police Department	0.75	0.00	0.00	0.75
Clinton Police Department	0.50	0.00	0.00	0.50
Cocke County Sheriff's Office	0.50	0.00	0.00	0.50
Cookeville Police Department	2.50	1.00	0.00	3.50
Crossville Police Department	0.50	0.00	0.00	0.50
Dayton Police Department	0.25	0.50	0.00	0.75
Dickson County Sheriff's Office	0.50	0.50	0.00	1.00
Gatlinburg Police Department	0.25	0.00	0.00	0.25
Germantown Police Department	1.00	0.25	0.00	1.25
Giles County Sheriff's Office	1.50	0.50	0.00	2.00
Grainger County Sheriff's Office	0.25	0.00	0.00	0.25
Greene County Sheriff's Office	0.75	0.00	0.00	0.75
Hamilton County Sheriff's Office	2.00	0.00	0.00	2.00
Hardeman County Sheriff's Office	0.25	0.00	0.00	0.25
Hawkins County Sheriff's Office	0.75	0.00	0.00	0.75
Jackson Police Department	2.50	0.75	0.00	3.25
Jefferson City Police Department	1.00	0.00	0.00	1.00
Kingsport Police Department	1.75	0.50	0.00	2.25
Knox County Sheriff's Office	2.00	0.50	0.00	2.50
Knoxville Police Department	3.00	3.00	2.00	8.00
Lebanon Police Department	0.50	0.00	0.00	0.50
Lenoir City Police Department	0.75	0.00	0.00	0.75
Loudon County Sheriff's Office	0.50	0.00	0.00	0.50
Macon County Sheriff's Office	0.25	0.00	0.00	0.25
Madison County Sheriff's Office	2.50	0.50	0.00	3.00

Table 12 (Continued): 2023 ICAC Affiliate Staffing

ICAC Affiliate	Number of Designated Staff*			
	Investigators	Forensics	Prosecutors	Total
Martin Police Department	1.25	0.25	0.00	1.50
Maryville Police Department	0.50	0.00	0.00	0.50
Memphis Police Department	5.00	1.00	0.00	6.00
Metropolitan Nashville Police Department	2.00	1.00	0.00	3.00
Millington Police Department	0.50	0.00	0.00	0.50
Monroe County Sheriff's Office	0.50	0.50	0.00	1.00
Montgomery County Sheriff's Office	1.00	0.00	0.00	1.00
Morgan County Sheriff's Office	0.50	0.00	0.00	0.50
Morristown Police Department	2.00	1.00	0.00	3.00
Nolensville Police Department	0.75	0.00	0.00	0.75
Oak Ridge Police Department	0.50	0.00	0.00	0.50
Oakland Police Department	0.25	0.00	0.00	0.25
Roane County District Attorney	0.75	0.50	0.75	2.00
Rutherford County Sheriff's Office	1.00	0.00	0.00	1.00
Savannah Police Department	0.25	0.00	0.00	0.25
Sevier County Sheriff's Office	0.50	0.00	0.00	0.50
Sevierville Police Department	0.50	0.00	0.00	0.50
Spring Hill Police Department	2.00	0.00	0.00	2.00
Sullivan County Sheriff's Office	1.50	1.00	0.00	2.50
Tennessee Bureau of Investigation	**4.00**	**4.00**	**0.00**	**8.00**
Tipton County Sheriff's Office	2.75	0.00	0.00	2.75
Union County Sheriff's Office	0.25	0.25	0.00	0.50
Washington County Sheriff's Office	0.75	0.00	0.00	0.75
White County Sheriff's Office	0.50	0.00	0.00	0.50
Williamson County Sheriff's Office	1.75	0.75	0.00	2.50
Winchester Police Department	1.00	1.00	0.00	2.00
Total	**65.75**	**19.25**	**2.75**	**87.75**

Source: State ICAC Commander.

* Staff designated for ICAC are categorized as investigators, forensics, prosecutors, or educators, but none of the listed ICAC affiliates had designated staff in the educators category.

Appendix 7: Map of Internet Crimes Against Children Affiliates

Figure 21: Map of ICAC Affiliates for 2023

ICAC Affiliate Jurisdiction
- Tennessee Bureau of Investigation
- Other Affiliate
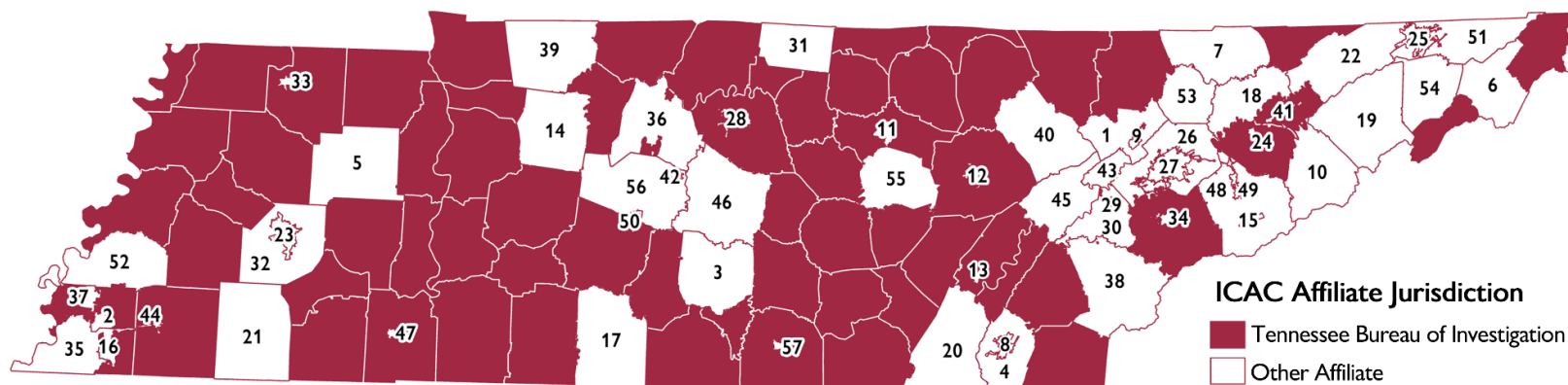
List of Other Affiliates

1 Anderson County Sheriff's Office	16 Germantown Police Department	31 Macon County Sheriff's Office	46 Rutherford County Sheriff's Office
2 Bartlett Police Department	17 Giles County Sheriff's Office	32 Madison County Sheriff's Office	47 Savannah Police Department
3 Bedford County Sheriff's Office	18 Grainger County Sheriff's Office	33 Martin Police Department	48 Sevier County Sheriff's Office
4 Bradley County Sheriff's Office	19 Greene County Sheriff's Office	34 Maryville Police Department	49 Sevierville Police Department
5 Carroll County District Attorney	20 Hamilton County Sheriff's Office	35 Memphis Police Department	50 Spring Hill Police Department
6 Carter County Sheriff's Office	21 Hardeman County Sheriff's Office	36 Metropolitan Nashville Police Department	51 Sullivan County Sheriff's Office
7 Claiborne County Sheriff's Office	22 Hawkins County Sheriff's Office	37 Millington Police Department	52 Tipton County Sheriff's Office
8 Cleveland Police Department	23 Jackson Police Department	38 Monroe County Sheriff's Office	53 Union County Sheriff's Office
9 Clinton Police Department	24 Jefferson City Police Department	39 Montgomery County Sheriff's Office	54 Washington County Sheriff's Office
10 Cocke County Sheriff's Office	25 Kingsport Police Department	40 Morgan County Sheriff's Office	55 White County Sheriff's Office
11 Cookeville Police Department	26 Knox County Sheriff's Office	41 Morristown Police Department	56 Williamson County Sheriff's Office
12 Crossville Police Department	27 Knoxville Police Department	42 Nolensville Police Department	57 Winchester Police Department
13 Dayton Police Department	28 Lebanon Police Department	43 Oak Ridge Police Department	
14 Dickson County Sheriff's Office	29 Lenoir City Police Department	44 Oakland Police Department	
15 Gatlinburg Police Department	30 Loudon County Sheriff's Office	45 Roane County District Attorney	

Source: Created by auditor based on a list of ICAC affiliates obtained from the State ICAC Commander.