Office of the Auditor General
Performance Audit Report

Handling and Safeguarding of Physical Media and Devices

Computer Crimes Unit
Michigan Department of State Police

May 2025

551-0147-24

State of Michigan Auditor General
Doug A. Ringler, CPA, CIA

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

The auditor general may make investigations pertinent to the conduct of audits.

Article IV, Section 53 of the Michigan Constitution

OAG
Office of the Auditor General

Report Summary

Performance Audit
Handling and Safeguarding of Physical Media and Devices
Computer Crimes Unit (CCU)
Michigan Department of State Police (MSP)

Report Number:
551-0147-24

Released:
May 2025

CCU is organizationally located in the Intelligence Operations Division within MSP's State Services Bureau. CCU has eight offices located throughout the State and provides investigative support in the seizure, acquisition, and analysis of digital evidence, including forensic examinations for the law enforcement community. CCU took approximately 14,800 devices into custody for the 29-month period from October 1, 2022 through February 28, 2025 and completed approximately 14,600 digital forensic examinations. CCU's expenditures totaled $11.7 million and $12.8 million for fiscal years 2023 and 2024, respectively, and CCU had 48 employees and 44 affiliates assisting from outside law enforcement agencies as of October 3, 2024.

Audit Objective			Conclusion
Objective: To assess the sufficiency of CCU's efforts to properly handle and safeguard physical media and devices.			Sufficient, with exceptions
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
CCU needs to enhance policies and/or procedures for physical access controls to CCU office workspaces and property rooms, such as performing periodic access reviews and enhancing tracking of individuals with access (Finding 1).		X	Agrees
CCU locations applied varying time frames and methods for destruction of devices no longer needed in an investigation and/or court case (Finding 2).		X	Agrees
CCU office workspace and property rooms had varying fire suppression methods. Five CCU locations had automatic fire suppression systems installed; however, three locations had fire extinguishers to protect CCU property rooms, which require an on-site staff presence and manual intervention to extinguish a fire (Finding 3).		X	Agrees

Findings Related to This Audit Objective *(Continued)*	Material Condition	Reportable Condition	Agency Preliminary Response
Forty-four former MSP employees had active user accounts in the Electronic Automated Incident Capture System for an average of 482 days after their employment or affiliation ended (Finding 4).		X	Agrees
Observations Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
Although this audit focused on CCU's efforts, the recommendations contained in this audit report related to physical access controls, fire suppression systems, and system user access controls can likely be applied more broadly to MSP operations (Observation 1).	Not applicable for observations.		

Obtain Audit Reports

Online: audgen.michigan.gov

Phone: (517) 334-8050

Office of the Auditor General
201 N. Washington Square, Sixth Floor
Lansing, Michigan 48913

Doug A. Ringler, CPA, CIA
Auditor General

Laura J. Hirst, CPA
Deputy Auditor General

OAG
Office of the Auditor General
Doug A. Ringler, CPA, CIA
Auditor General
201 N. Washington Square, Sixth Floor • Lansing, Michigan 48913 • Phone: (517) 334-8050 • audgen.michigan.gov

May 22, 2025

Colonel James F. Grady II, Director
Michigan Department of State Police
7150 Harris Drive
Dimondale, Michigan

Colonel Grady:

This is our performance audit report on Handling and Safeguarding of Physical Media and Devices, Computer Crimes Unit, Michigan Department of State Police.

Your agency provided preliminary responses to the recommendations at the end of our fieldwork. The *Michigan Compiled Laws* and administrative procedures require an audited agency to develop a plan to comply with the recommendations and to submit it to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

We appreciate the courtesy and cooperation extended to us during this audit.

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

HANDLING AND SAFEGUARDING OF PHYSICAL MEDIA AND DEVICES

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

EFFORTS TO PROPERLY HANDLE AND SAFEGUARD PHYSICAL MEDIA AND DEVICES

BACKGROUND

The Computer Crimes Unit (CCU) has eight offices located throughout the State (see Exhibit 1) and is responsible for performing forensic examinations and ensuring proper handling and safeguarding of physical media and devices in its custody. All CCU locations have a designated workspace(s) and property room(s)* to store media and devices such as cell phones, laptops, cameras, tablets, and other electronic storage devices.

The property items in CCU's possession are associated with either a Michigan Department of State Police (MSP) case or an analysis for outside law enforcement agencies*, such as local, other state, and federal agencies. The volume of property stored varies by CCU location, ranging from 1 to approximately 1,000 devices and averaging approximately 275 devices as of August 2024. The devices in each location's possession changes regularly because devices are received from and returned to outside law enforcement agencies, with CCU estimating approximately 70% of its work relates to outside law enforcement agencies (see Exhibit 2).

CCU uses MSP's Electronic Automated Incident Capture System (eAICS), an electronic records management system, to manage its property, perform inventory audits of physical media and devices, and document the results of digital forensic analyses. As part of its recordkeeping, CCU is responsible for maintaining proper documentation regarding the intake, movement, and release or destruction of all property. MSP requires regular inspections of all property rooms to ensure the integrity of its property management programs and proper handling of evidence in its custody.

AUDIT OBJECTIVE

To assess the sufficiency of CCU's efforts to properly handle and safeguard physical media and devices.

CONCLUSION

Sufficient, with exceptions.

FACTORS IMPACTING CONCLUSION

- Our on-site observations of the eight CCU location workspaces and property rooms showed they were neat, clean, and orderly, and we noted no visible or obvious concerns, such as standing water, water or fire damage, mold, or unreasonable temperatures.
- All sampled property items reviewed during our on-site testing were:
    - Appropriately stored in sealed containers, unless the device was too large or actively being worked on.

** See glossary at end of report for definition.*

    - Properly tagged with accurate identification and description information.
    - Physically located at the correct CCU location.

- Nearly all sampled property items were supported by proper intake documentation, when applicable, recording who dropped the device off and an appropriate description of the device.
- CCU maintained an accurate electronic property inventory according to our sample-based review.
- CCU maintained property receipt forms and obtained proper authorization to release the property for 99% of sampled released property items reviewed.
- CCU obtained proper authorization to destroy property items and maintained documentation to support the destruction was witnessed appropriately for 100% of applicable sampled destroyed property items reviewed.
- Nearly all individuals with electronic swipe card access to CCU office workspaces and property rooms were current employees or affiliates*.
- All required property room inspections were timely completed by an appropriate MSP member(s) and all property items we reviewed were included in the applicable property audits.
- Four reportable conditions* related to:
    - Enhanced policies and/or procedures for physical access controls (Finding 1).
    - Development of a specific digital evidence disposition policy (Finding 2).
    - A current evaluation of fire suppression systems (Finding 3).
    - System access control improvements (Finding 4).

** See glossary at end of report for definition.*

FINDING 1

Enhanced policies and/or procedures are needed for physical access to CCU office workspaces and property rooms.

CCU should enhance policies and/or procedures for physical access to CCU office workspaces and property rooms to help ensure property is properly controlled and protected while in CCU's custody.

The Commission on Accreditation for Law Enforcement Agencies* (CALEA) and the International Association of Chiefs of Police* (IACP) require:

- All in-custody and evidentiary property to be stored within designated secure areas with access limited to authorized personnel.
- Development of policies and procedures regarding the safekeeping of items.

CALEA states entry to property rooms should be controlled to prevent alteration, unauthorized removal, theft, or other compromise of property and to maintain the chain of custody.

Individuals with access to CCU locations at the time of our review included CCU employees, a limited number of other MSP employees, and approximately 40 affiliates (employees of outside law enforcement agency assisting CCU in performing forensic examinations). Our on-site visits to the eight CCU locations noted the use of a variety of physical access methods for CCU office workspaces and property rooms as summarized in the following table:

	Physical Access Method(s) Used by CCU Location				
CCU Location	Electronic Swipe Card	Temporary Electronic Swipe Card	Key	Keypad	Combination Lock
1	✓	✓		✓	
2	✓	✓	✓	✓	
3	✓	✓			
4	✓		✓	✓	
5			✓		
6	✓			✓	
7	✓			✓	✓
8				✓	
Total	6	3	3	6	1

MSP has two relevant procedure manuals addressing physical access, with the first providing departmentwide guidelines for storage and security of property and the second providing guidelines for access to MSP facilities located at the Lansing Secondary Complex. Our review of the procedure manuals and our understanding of CCU operations noted CCU should improve physical access controls for CCU locations, including:

- Clarifying guidelines for assigning access privileges to CCU staff, other MSP employees, and affiliates,

** See glossary at end of report for definition.*

particularly as they relate to CCU property rooms or other property storage areas.

IACP states access to evidence and property should be restricted to the fewest number of personnel necessary to perform the required functions. MSP's procedure manual is consistent with this approach; however, our review noted CCU property storage practices resulted in varying applications of this guidance.

- Requiring performance of periodic physical access reviews at all CCU locations, including reviewing the list of individuals with physical access to verify access is still needed and aligns with their job responsibilities.

  MSP's procedure manual requires semiannual audits of facility access at MSP's Lansing Secondary Complex, which is applicable to only the Lansing CCU location. Also, CCU was unable to provide clear evidence to support the required semiannual access audits were completed for the Lansing CCU location.

- Enhancing tracking of individuals granted access to CCU office workspaces and property rooms.

  MSP was able to generate reports listing all individuals granted electronic swipe cards from the card access systems; however, CCU had not implemented a consistent tracking mechanism(s) for assignment of keys, access codes, lock combinations, or temporary electronic swipe cards. MSP's procedure manuals are silent on tracking these access methods, and we noted one CCU location maintained a key log, while others relied on informal tracking methods such as individuals' recollection or temporary notes on a whiteboard.

- Formalizing requirements for regularly changing keypad access codes and lock combinations and clarifying requirements for rekeying locks and replacing lock mechanisms.

  MSP's procedure manual requires work site commanders to consider periodically changing the locks on property rooms at their discretion, and the manual is silent on changing access codes and combinations.

- Clarifying visitor sign-in and escort requirements.

  MSP's procedure manuals require:

  - Visitors to sign in at the public entrance and all non-departmental visitors to be escorted at MSP's Lansing Secondary Complex, which is applicable to only the Lansing CCU location.

- Individuals to be escorted by an authorized key holder in the property room but the manuals are silent on escorting requirements for the office workspace area.

Our review of individuals with CCU electronic swipe card access noted nearly all were current employees or affiliates; however, improved guidance would help CCU promote consistency across its geographically dispersed CCU locations and minimize unintended physical access issues when staffing changes occur. When enhancing its controls, CALEA supports having CCU weigh the importance of the property it is placing in these areas and the consequences if the property is stolen, damaged, or contaminated while in custody.

MSP stated some procedures are informal and not documented and other procedures need additional clarity.

RECOMMENDATION

We recommend CCU enhance policies and/or procedures for physical access to CCU office workspaces and property rooms.

AGENCY PRELIMINARY RESPONSE

MSP provided us with the following response:

MSP agrees with the recommendation. Physical access is controlled through varying levels of physical security prior to access, requirements for non-CCU authorized individuals to be escorted and accompanied at all times in the property room, and property is audited at least semi-annually. MSP follows CALEA policy standards for physical access to property as CALEA accreditation was achieved on March 22, 2025, however, MSP will update policies and procedures for physical access to CCU office workspaces and property rooms.

FINDING 2

A specific digital evidence disposition policy is needed for releasing and destroying physical media and devices.

MSP should develop a policy specific to the disposition of digital evidence, including physical media and devices. Industry best practices support that prompt, authorized property removal prevents an overload on the property management system and reduces the requirement for additional storage space. Policy development would help ensure consistent evidence disposition across MSP's eight CCU locations.

After a device is no longer needed in an investigation and/or court case, the device must be either destroyed or returned to the owner or another authorized individual. CALEA and IACP support development of written procedures for the prompt, final disposition or destruction of found, recovered, and evidentiary property after legal requirements have been satisfied.

Although MSP had general departmental property disposition policies, we noted MSP had not yet developed policies specific to disposition of digital evidence. Best practices support the development of digital evidence policies addressing establishment of time lines to ensure timely decisions are made, consideration of legal and court requirements, and statute of limitations. They also suggest the development of procedures for tracking court dispositions and information from the prosecutor's office indicating a case has been adjudicated.

We noted:

- All CCU locations required consideration of some or all of the following information: appeal periods, written consent, and/or prosecutor authorization prior to disposition.

- More than half of the CCU locations destroyed devices every 6 months, while other locations destroyed media and devices 3 to 4 times per year or when time permitted.

- All CCU locations utilized tools, such as hammers, axes, or sledgehammers, to physically destroy devices, while half reported also using firearms to destroy devices.

Development of a specific digital evidence disposition policy would be consistent with MSP's development of existing property disposition policies for other specialized evidence areas including motor vehicles, controlled substances, firearms, and weapons. MSP stated it had not developed a specific digital evidence disposition policy because it believed digital evidence disposition was inclusive within the general departmental property disposition policies.

RECOMMENDATION

We recommend MSP develop a policy specific to the disposition of digital evidence, including physical media and devices.

AGENCY PRELIMINARY RESPONSE

MSP provided us with the following response:

MSP agrees with the recommendation. MSP will update procedures specific to disposition of digital evidence, including physical media and devices.

FINDING 3

A current evaluation of fire suppression systems is needed.

MSP should perform a current evaluation of its fire suppression systems and take necessary measures to ensure all physical media and devices are best protected from fire, given its fire suppression systems vary at its eight CCU locations.

We conducted on-site visits at MSP's eight CCU locations in October and November 2024 and observed varying fire suppression methods in CCU office workspace and property rooms, ranging from a gas fire suppression system to hand-held fire extinguishers. Specifically, we noted:

- One CCU location had an automatic gas fire suppression system in its property room, while fire extinguishers were used in the office workspace area.
- Two CCU locations had automatic dry foam fire suppression systems covering the office workspace and property rooms.
- Two CCU locations had water sprinkler systems for their office workspace and property rooms.
- Three CCU locations had fire extinguishers for their office workspace and property rooms. We believe it is reasonable to expect protection exceeding that of a fire extinguisher, which requires on-site staff presence and manual intervention to extinguish a fire. CCU indicated two of these property rooms have concrete block walls and steel doors; however, this construction would not control or suppress a fire originating in the property room itself.

CALEA and IACP support it is MSP's responsibility to protect evidence in its custody. In its evaluation, MSP should consider the size and layout of the CCU location, property storage practices, the suppression agent's potential negative impact on property, and whether an automatic or manual activation method is appropriate, among others, for improvements to its fire suppression system where needed. If physical improvements to building infrastructure are not possible or feasible, MSP may consider other solutions such as fireproof safes and/or relocating storage of digital evidence to a location where it can be better protected.

MSP stated it works with the Michigan Department of Technology, Management, and Budget to determine the appropriate fire suppression system(s) which is dependent on a number of factors, including building ownership and management (State owned vs. leased), cost, building codes, size, and necessity.

RECOMMENDATION

We recommend MSP perform a current evaluation of its fire suppression systems and take necessary measures to ensure all physical media and devices are best protected from fire.

AGENCY PRELIMINARY RESPONSE

MSP provided us with the following response:

MSP agrees with the recommendation. At the time of occupancy, building and local code requirements for fire suppression were met per DTMB standards and MSP follows CALEA policy standards for property protection as CALEA accreditation was achieved on March 22, 2025, however, MSP recognizes the opportunity for conducting a reevaluation of fire suppression.

FINDING 4

eAICS user access controls need improvement.

MSP needs to improve user access controls over eAICS. Doing so would increase MSP's assurance that only properly approved individuals can access and/or edit eAICS data, including CCU's electronic inventory of physical media and devices.

CALEA and IACP support implementing a process for maintaining security of its computer systems to prevent unauthorized access. Also, State of Michigan (SOM) Technical Standards 1340.00.020.01 and 1340.00.080.01 establish requirements for granting, reviewing, and removing access; passwords; and disabling inactive user accounts.

CCU uses MSP's eAICS, an electronic records management system, to manage its property and perform inventory audits of physical media and devices, as well as document confidential investigation material including names of victims, individuals under investigation, and the results of digital forensic analysis. eAICS had 315 active user accounts with access to CCU data as of November 25, 2024, and our review of selected eAICS access controls disclosed MSP did not:

a. Establish an automated process to identify and disable inactive eAICS user accounts, as required, and did not always timely remove eAICS access for users who had departed State employment or ended their affiliation with CCU.

   SOM technical standards require MSP to automatically disable inactive user accounts after 60 days and remove user access within 72 hours when access is no longer required.

   Our review determined 93 (30%) of the total 315 active eAICS user accounts had not been accessed in 60 days. Of these 93 users, 44 were no longer MSP employees yet had active user accounts for an average of 482 days after their employment or affiliation ended, ranging from 25 to 2,289 days.

   MSP stated automatic account disabling was not appropriately established. MSP also stated timely notification of departure was not always received because there was no single point of contact to notify eApplication* system administrators of personnel movement.

b. Always maintain sufficient documentation to support assignment of access rights based on an individual's current job responsibilities.

   SOM technical standards require MSP to implement processes to grant access rights based on the principle of least privilege* and require approval for creation of system accounts by an authorized requestor.

** See glossary at end of report for definition.*

We noted an eAICS user access request form existed; however:

(1) The approximately 50 different eAICS user role options were not listed or described on the form, and there were no accompanying instructions to assist in selection of the appropriate role(s). Because of the complexity of assignment of user roles, CCU stated it relied on eApplication system administrators to assign proper user roles based on a description of the users' job responsibilities.

(2) MSP did not require use of the form for 24 (83%) of 29 selected active eAICS users reviewed. For 4 of these users, MSP was unable to provide any documentation supporting the request or approval of system access. For the remaining 20 users, MSP provided various other documentation, such as e-mails and eAICS help desk tickets, to support system access requests; however, those documents did not always include the necessary information to ensure proper access was granted according to the principle of least privilege.

MSP stated historically, access requests were made via various methods, and the eApplication team worked with the requestor to determine appropriate role(s).

c. Perform annual or semiannual reviews of user access, as required.

MSP stated it had previously performed these reviews but ultimately determined to stop due to the complexity of eAICS roles and the resulting time-consuming nature of the access review.

d. Enforce minimum password complexity and change requirements for privileged users, as required. Instead, the passwords were only required to meet the less strict non-privileged user requirements.

MSP stated the password complexity and change requirements were established but did not meet SOM technical standards.

RECOMMENDATION

We recommend MSP improve user access controls over eAICS.

AGENCY PRELIMINARY RESPONSE

MSP provided us with the following response:

MSP agrees with the recommendation to improve user access controls over eAICS. As a compensating control, eAICS is only accessible through designated network locations on a state issued device. Network access and state issued devices are

collected at time of employee departure. MSP will make updates to the eApps access request form and privileged users password complexity requirements. MSP has created an eAICS cleanup plan for CCU to remove users no longer requiring access once the audit is complete. MSP will work with the application vendor to incorporate automated processes for user access controls. MSP will review and update access control policies and procedures.

OBSERVATION 1

Recommendations contained in this audit report can likely be applied more broadly to MSP operations.

Although this audit focused on proper handling and safeguards for CCU physical media and devices, the recommendations contained in this audit report can likely be applied more broadly to MSP operations, including the recommendations reported in:

- Finding 1 related to physical access controls. For example, MSP established requirements for performance of periodic physical access reviews at only the Lansing Secondary Complex. Without a Statewide policy addressing this review, our recommendation is likely to extend to other MSP State-owned or leased buildings, locations, and property rooms throughout the State.

- Finding 3 related to fire suppression systems for protection of property. MSP stores a wide range of property in carrying out its law enforcement and public safety services, including controlled substances, vehicles, money, firearms, weapons, biological material, and electronics, among others. Considering the varying levels of fire protection we observed at the CCU locations and MSP's lack of Statewide policy establishing fire suppression requirements for protecting property, our recommendation likely extends to other MSP property storage locations throughout the State. MSP may need to begin with departmentwide identification and evaluation of fire suppression systems in place for all MSP property storage locations. If needed physical improvements to building infrastructure are not possible or feasible, MSP may need to consider other solutions, such as relocating property.

- Finding 4 related to user access controls for the eAICS module, which is part of MSP's larger eApplication suite. The suite also includes electronic Crash Reporting (eCrash) for capturing traffic crash reporting data, electronic Citation (eCitation) for issuance of tickets, and electronic Daily Activity Report (eDaily) for recording officers' daily activity. Our discussions with eApplication system administrators showed the processes for granting and monitoring eAICS user access are the same for all modules, likely extending our recommendation to the eApplication suite as a whole.

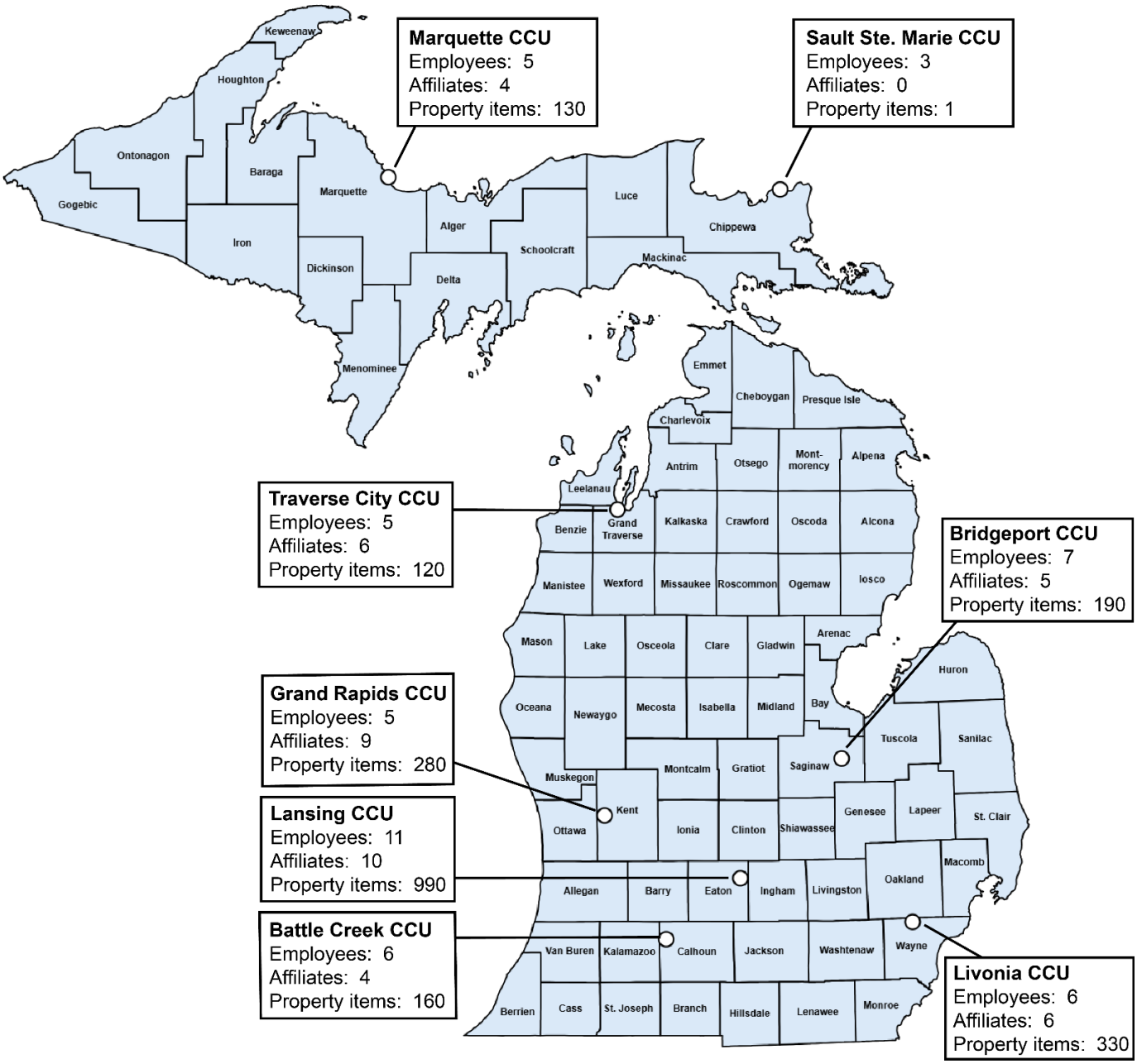
Considering MSP's geographically dispersed operations, clearly defined Statewide expectations and controls would help ensure consistency in operations and appropriate protection of property, among others. We encourage MSP to apply its corrective action more broadly to MSP operations.

SUPPLEMENTAL INFORMATION

UNAUDITED
Exhibit 1

HANDLING AND SAFEGUARDING OF PHYSICAL MEDIA AND DEVICES
Computer Crimes Unit
Michigan Department of State Police

CCU Office Location Map



Source: The OAG prepared this exhibit based on information provided by MSP, including CCU employee and affiliate staffing levels as of October 3, 2024 and CCU property in possession from eAICS as of August 20, 2024 (rounded for all CCU locations except Sault Ste. Marie).

HANDLING AND SAFEGUARDING OF PHYSICAL MEDIA AND DEVICES
Computer Crimes Unit
Michigan Department of State Police

Number of Property Items and Incidents Submitted by Agency by Month and Year
From October 1, 2022 Through February 28, 2025

	Property Items		Incidents* Submitted by Agency		
Month and Year	Devices Taken Into Custody	Examinations Completed	MSP	Outside Agency[1]	Total[2]
October 2022	615	614	138	194	332
November 2022	510	734	109	218	327
December 2022	534	428	112	211	323
January 2023	527	418	148	306	454
February 2023	643	559	148	260	408
March 2023	723	534	214	11	225
April 2023	497	394	88	241	329
May 2023	510	532	93	240	333
June 2023	585	428	124	277	401
July 2023	433	372	84	288	372
August 2023	553	433	109	243	352
September 2023	515	436	133	236	369
October 2023	642	517	109	332	441
November 2023	443	482	62	253	315
December 2023	312	396	35	129	164
January 2024	708	596	124	332	456
February 2024	478	490	93	280	373
March 2024	580	523	104	255	359
April 2024	441	589	67	296	363
May 2024	485	521	68	259	327
June 2024	100	129	23	50	73
July 2024	457	363	64	142	206
August 2024	406	423	80	180	260
September 2024	411	461	63	191	254
October 2024	691	796	101	281	382
November 2024	333	457	64	194	258
December 2024	438	578	62	199	261
January 2025	630	745	96	352	448
February 2025	629	647	89	263	352
Total	14,829	14,595	2,804	6,713	9,517
Monthly Average	511	503	97	231	328

[1] Outside submitting agencies include all non-MSP law enforcement agencies, such as local, other state, and federal agencies.

[2] One incident can have one or more associated devices.

Source: The OAG prepared this exhibit based on statistics contained in MSP's Cyber Section strategic plan.

** See glossary at end of report for definition.*

AGENCY DESCRIPTION

CCU is organizationally located in the Intelligence Operations Division within MSP's State Services Bureau. CCU has eight offices located throughout the State as illustrated in Exhibit 1. CCU provides investigative support in the seizure, acquisition, and analysis of digital evidence which includes forensic examinations for the law enforcement community. CCU also has oversight of the Michigan Internet Crimes Against Children task force which includes federal, State, and local enforcement agencies who collaborate to investigate offenders using the Internet, online communication systems, or computer technology to sexually exploit children. From October 1, 2022 through February 28, 2025, CCU took approximately 14,800 devices into custody and completed approximately 14,600 forensic examinations (see Exhibit 2).

CCU's expenditures totaled $11.7 million and $12.8 million for fiscal years 2023 and 2024, respectively. As of October 3, 2024, CCU had 48 employees and 44 affiliates assisting from outside law enforcement agencies.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the records and processes related to CCU's efforts to properly handle and safeguard physical media and devices. We conducted this performance audit* in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

As part of the audit, we considered the five components of internal control* (control environment, risk assessment, control activities, information and communication, and monitoring activities) relative to the audit objectives and determined all components were significant.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered October 1, 2022 through July 31, 2024. We updated certain data when possible to reflect current information.

METHODOLOGY

We conducted a preliminary survey to gain an understanding of CCU's operations to formulate a basis for establishing the audit objectives, scope, and methodology. During our preliminary survey, we:

- Interviewed CCU management and staff to obtain an understanding of responsibilities and procedures carried out by the unit.
- Reviewed applicable State law and departmental procedure manuals, official orders, and memorandums.
- Analyzed CCU expenditures and revenues from October 1, 2022 through September 30, 2024.
- Reviewed CCU's strategic plan for fiscal years 2022 through 2024.
- Conducted on-site visits at three CCU locations in July 2024 to gain an understanding of CCU operations and to assess the office workspace and property room physical conditions.

** See glossary at end of report for definition.*

- Completed a limited inventory review of property items in possession at two CCU property rooms we visited in July 2024.

OBJECTIVE

To assess the sufficiency of CCU's efforts to properly handle and safeguard physical media and devices.

To accomplish this objective, we:

- Reviewed CALEA standards, IACP's publication titled *Property and Evidence Control*, and MSP policies related to safeguarding property.
- Evaluated applicable MSP policies and procedures for consistency with industry best practices.
- Conducted on-site visits at the eight CCU locations in October and November 2024 and:
    - Based on interviews with management and observations from our on-site tours, we gained an understanding and evaluated processes regarding:
        - Physical access controls.
        - Storage of physical media and devices.
        - Intake, movement, release, and destruction of property.
        - Physical conditions of the CCU office workspaces and property rooms.
    - Performed physical inventory reviews for 103 randomly selected property items from the population of 2,931 property items in CCU's possession at the time of our visits according to the eAICS electronic property inventory to verify:
        - Property was appropriately stored, accurately recorded, and on site at the correct location.
        - Intake forms were properly completed, if applicable, for 101 of the 103 randomly selected property items.
    - Evaluated the completeness and accuracy of eAICS by tracing 30 judgmentally selected property items from property room shelves across six CCU locations to CCU's eAICS electronic property inventory using the unique identification numbers affixed to the property

items and verified the property items were accurately recorded in eAICS, including the proper location, description, and identification number.

- Evaluated MSP's policies regarding applicable physical access requirements in procedure manual 12-03, which provides departmentwide guidelines for storage and security of property, and procedure manual 19-07 regarding access to departmental facilities located at MSP's Lansing Secondary Complex.

- Assessed all individuals with physical access to each of the eight CCU office workspaces and property rooms as of September 2024 through December 2024 (varies based on CCU location) to ensure only authorized individuals had access to CCU office workspaces and property rooms.

- Randomly sampled 75 of 11,728 property items released by CCU from October 1, 2022 through September 24, 2024 to verify proper authorization and documentation of release on a property receipt form, including signature of releasing MSP member and receiving individual.

- Randomly sampled 75 of 917 property items destroyed by CCU from October 1, 2022 through September 13, 2024 to verify proper authorization and evidence that two individuals witnessed the destruction, when applicable.

- Reviewed documentation for all required CCU property room inspections from October 1, 2022 through August 27, 2024 to verify:

    - MSP timely completed and properly documented all required semiannual, annual, headquarter, and change of command or change in property manager inspections, as applicable.

    - Appropriate MSP member(s) completed the inspection.

    - MSP completed partial or full property audits in conjunction with the required inspections, where applicable, and the 103 property items we selected for review (referenced in bullet 3, sub-bullet 2 of this objective) were included in the applicable audits and any identified discrepancies were appropriately resolved.

- Interviewed MSP management and staff regarding its processes for select eAICS user access controls to better understand and evaluate the design and

implementation of its internal control procedures when compared with SOM policy and industry best practices for granting, removing, and recertifying access.

- Determined MSP began requiring eAICS user access forms for new accounts and changed permissions for existing accounts starting October 23, 2018. For accounts requiring completion of the eAICS user access form, we randomly selected 29 of 261 eAICS active user accounts as of November 25, 2024 to determine whether MSP maintained proper documentation to support authorization for granting the individuals' access.

- Analyzed last log-in dates for all eAICS accounts with access to CCU data as of November 25, 2024 to determine if user accounts were being disabled after 60 days of inactivity.

Our random samples were selected to eliminate bias and enable us to project the results to the respective populations. Our judgmental samples were selected based on risk, and we could not project the results to the respective populations.

CONCLUSIONS

We base our conclusions on our audit efforts and any resulting material conditions* or reportable conditions.

When selecting activities or programs for audit, we direct our efforts based on risk and opportunities to improve State government operations. Consequently, we prepare our performance audit reports on an exception basis.

AGENCY RESPONSES

Our audit report contains 4 findings and 4 corresponding recommendations. MSP's preliminary response indicates it agrees with all of the recommendations.

The agency preliminary response following each recommendation in our report was taken from the agency's written comments and oral discussion at the end of our fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 3, Section 100) require an audited agency to develop a plan to comply with the recommendations and to submit it to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

** See glossary at end of report for definition.*

SUPPLEMENTAL INFORMATION

Our audit report includes supplemental information presented as Exhibits 1 and 2. Our audit was not directed toward expressing a conclusion on this information.

GLOSSARY OF ABBREVIATIONS AND TERMS

affiliate	An individual employed by an outside law enforcement agency assisting CCU in performing forensic examinations.
CCU	Computer Crimes Unit.
Commission on Accreditation for Law Enforcement Agencies (CALEA)	Created in 1979 as a credentialing authority through the joint efforts of law enforcement's major executive associations including IACP, the National Organization of Black Law Enforcement Executives, the National Sheriffs' Association, and the Police Executive Research Forum to provide public safety agencies with an opportunity to voluntarily meet an established set of professional standards.
eAICS	Electronic Automated Incident Capture System.
eApplication	An application suite used by MSP composed of four modules including eAICS, eCrash, eCitation, and eDaily.
incident	A record created in eAICS to document every criminal event brought to MSP's attention, allowing MSP the ability to perform case management procedures, track property in its custody, and create reports. An incident is created for MSP cases and for each outside law enforcement agency case when the agency provides digital media and devices to CCU for examination. One incident may have one or more associated digital media and devices.
internal control	The plan, policies, methods, and procedures adopted by management to meet its mission, strategic plan, goals, and objectives. Internal control includes the processes for planning, organizing, directing, and controlling program operations. It also includes the systems for measuring, reporting, and monitoring program performance. Internal control serves as a defense in safeguarding assets and in preventing and detecting errors; fraud; violations of laws, regulations, and provisions of contracts and grant agreements; or abuse.
International Association of Chiefs of Police (IACP)	A professional association for police leaders whose mission is to advance the policing profession through advocacy, research, outreach, and education.
material condition	A matter, in the auditor's judgment, which is more severe than a reportable condition and could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person

	concerning the effectiveness and efficiency of the program. Our assessment of materiality is in relation to the respective audit objective.
MSP	Michigan Department of State Police.
observation	A commentary highlighting certain details or events which may be of interest to users of the report. An observation may not include all of the attributes (condition, effect, criteria, cause, and recommendation) presented in an audit finding.
outside law enforcement agencies	Includes all other law enforcement agencies CCU assists, such as local, county, other states, and federal agencies.
performance audit	An audit which provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision-making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability.
principle of least privilege	The practice of limiting access to the minimal level which will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user access rights they can have and still do their jobs.
property room	A room(s) within each CCU location used to store property and evidence recovered, received, seized, or held in custody.
reportable condition	A matter, in the auditor's judgment, less severe than a material condition and falls within any of the following categories: a deficiency in internal control; noncompliance with provisions of laws, regulations, contracts, or grant agreements; opportunities to improve programs and operations; or fraud.
SOM	State of Michigan.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

Hotline: (517) 334-8070