Publication/ Revision Date:	Chapter Number:	Chapter Title:
December 30, 2020	1.0	Child Support Basics
	Section Number: 1.23	Section Title: Cooperative Reimbursement Program (CRP) Agreements (Contracts)

Table of Contents

Exhibit 1.23E3: County-Managed Purchases of Imaging Systems
Exhibit 1.23E4: Information Technology (IT) Purchasing Checklist
Exhibit 1.23E5: Appropriate Allocation of Data-Processing Costs
Exhibit 1.23E6: Independent Security Audit Guidance
Exhibit 1.23E7: OCS Analysis of the OCSE Security Agreement Controls and Their Use in the Independent Security Audit
Exhibit 1.23E8: OCSE Security Agreement
Exhibit 1.23E9: OCSE Security Addendum

1. Introduction

The Cooperative Reimbursement Program (CRP) is a contract that county offices enter into with the Michigan Department of Health and Human Services (MDHHS) Office of Child Support (OCS) to receive reimbursement for the net expenditures of providing services for the Title IV-D child support enforcement program.

All phases of the CRP agreement process, including the original application through agreement signatures, line-item transfers, and amendments, are completed in the web-based Electronic Grants Administration & Management System (EGrAMS).

CRP policy that does not appear in this manual section remains in previously published Action Transmittals (ATs) and IV-D Memorandums. Links to these documents and other CRP-related materials are found on mi-support.[1]

Within this manual section and its exhibits, responsibilities assigned to unspecified or undefined representatives within local county offices will be the responsibility of the Prosecuting Attorney (PA) and Friend of the Court (FOC) IV-D office directors or their designees.

2. Information Technology (IT) Support Options for County IV-D Offices and the Billing Process for IT Services

This subsection describes the information technology (IT) support options available to county FOC, PA and combined IV-D offices that began fiscal year (FY) 2016 and the process for billing IT hardware, software and county-supplied data-processing services. The IT hardware, software and county-supplied data-processing services discussed throughout this manual section and its exhibits are reimbursable via Title IV-D funds only if they are:

- Needed to provide IV-D services to IV-D customers pursuant to OCS policies; or
- Authorized under other federal Title IV-D guidance or law.

For the purposes of this manual section, data processing is defined as “access to or use of a computer-based system(s).” Included in data-processing costs are

[1] Ref: the mi-support pages 1.23 Cooperative Reimbursement Program (CRP) Agreements (Contracts) and Contracts – Cooperative Reimbursement Program (CRP).

hardware and software and the cost of IT support staff. Office supplies (e.g., printer paper, toner, etc.) are excluded from the definition of data-processing costs.

2.1 Overview of IT Support Models: State-Managed and County-Managed

As of the beginning of FY 2016, each FOC, PA or combined IV-D office selected either a state-managed or a county-managed IT support model. Each IT model is described below.

IT Support Model	Description
State-Managed	• FOC or PA offices log into a DTMB-provided[2] central server for the purposes of automated virus update distribution, automated operating system patch distribution, general software updates, remote desktop troubleshooting and resolution, Internet access, state email use, and user login. • The hardware resides on the DTMB-provided local area network (LAN). • DTMB provides the personal computers (PCs)/laptops. • The county provides the printers, scanners, monitors and other peripherals such as keyboards and mice. Without prior approval, FOC and PA offices may purchase printers, scanners, monitors and other peripherals such as keyboards and mice through their own procurement processes, and reimbursement of any eligible costs for these items will be through the CRP agreement. • No access to the county network is provided. Any county-based IV-D child support applications (e.g., an imaging system) and county business applications (e.g., county email, timekeeping, etc.) are provided separately through county-provided computer hardware and software. These applications are supported by the county IT staff and are county-managed.
County-Managed	• Local FOC or PA offices log into a county-provided central server for the purposes of automated virus update distribution, automated operating system patch distribution, general software updates, remote desktop troubleshooting and resolution, file and print services, Internet access, user login, and email. • The hardware resides on the county LAN. • The county provides the PCs/laptops. FOCs and PAs may purchase, with prior OCS approval, PCs or laptops in accordance with the county's PC replacement policy that applies to all county departments

[2] DTMB is the Department of Technology, Management & Budget.

IT Support Model	Description
	and is in accordance with the OCS PC allocation guidelines. • The county provides the printers, scanners, monitors and other peripherals such as keyboards and mice. Without prior approval, FOCs and PAs may purchase printers, scanners, monitors and other peripherals such as keyboards and mice, and reimbursement of any eligible costs for these items will be through the CRP agreement. • Access to the county network, county-based IV-D child support applications (e.g., an imaging system) and county business applications (e.g., county email, timekeeping, etc.) may be included in the services provided and supported by the county IT staff.

Each county FOC or PA office may choose its own IT support model. However, in most counties, both the FOC and PA office have chosen the same IT support model.

2.2 Elements Common to Both IT Support Models

2.2.1 Problem Resolution Through the DTMB Client Services Center

A. Service Hours and Contact Information

The DTMB Client Services Center will provide assistance only for DTMB-provided hardware or software. It is available to facilitate problem resolution for hardware, IV-D software, and network issues Monday through Friday, from 7:30 a.m. until 5 p.m. IV-D staff may contact the DTMB Client Services Center by:

- Calling 1-800-968-2644; or
- Entering a self-service request at www.michigan.gov/itsm-remedy.

Note: To ensure proper routing of requests, FOCs and PAs should identify themselves as from a county FOC or PA office and not from an MDHHS local office.

County IT staff will provide DTMB the names of contact people from the FOC, PA and county IT staff who are authorized to contact the DTMB Client Services Center. The county FOC, PA or IT contact person(s) will notify the DTMB Client Services Center to resolve any hardware, software or network communication issues related to the Michigan Child Support Enforcement System (MiCSES). If the DTMB Client Services Center is unable to resolve the issue, DTMB staff members will immediately notify the appropriate technical staff who

will work directly with the FOC, PA or county IT staff to resolve the issue.

The DTMB Client Services Center will email communications only to those individuals identified as Local Project Coordinators.[3] The Local Project Coordinators are responsible for distributing information to the appropriate FOC and PA end-users.

DTMB staff and the FOC, PA or IT contact person will schedule service calls that require DTMB staff to access any hardware at county FOC or PA offices.

B. Process for Problem Resolution

It is highly desirable for individuals closest to problem situations to resolve them in a timely manner. In the event that county IT and DTMB staff are unable to reach an agreement on who is responsible for correcting a network, hardware or software problem, the county IT and/or DTMB staff will escalate the issue to the county IT director and the DTMB-MDHHS Business Relationship Manager. If these two individuals are unable to reach an agreement within one business day, one or both individuals will escalate the issue to the Program Leadership Group (PLG) for resolution.

Depending on the nature of the problem, the PLG will consider the issue at its next regularly scheduled meeting or through an immediate conference call. The county IT director and the DTMB-MDHHS Business Relationship Manager will each submit to the PLG a written description of the problem, a description of attempts to resolve the problem, and a recommendation for resolution. County IT and DTMB staff will make knowledgeable representatives available to discuss the issue with the PLG.

2.2.2 Purchase of Printers, Scanners, Monitors and Other Peripherals Such as Keyboards and Mice

Without prior OCS approval, both state-managed and county-managed FOC and PA offices may purchase printers, scanners, monitors and other peripherals such as keyboards and mice and may request reimbursement through the CRP contract. Requesters must charge these purchases to the Data Processing line item on the *Title IV-D Cooperative Reimbursement Actual Expenditure Report* (DHS-286) and follow the procurement, purchasing and expensing practices that apply to all county departments.

[3] A county's Local Project Coordinator is the individual listed as the "LPC" in the county's contact information that is accessible from the mi-support Partner Contact Information page.

2.2.3 Confidentiality/Security

Both state-managed and county-managed offices must comply with the provisions of Section 1.10, "Confidentiality/Security," of the *Michigan IV-D Child Support Manual*. Section 1.10 covers IT security requirements and includes a subsection on computer system security.

Also, the terms and conditions of the FOC and PA CRP agreements contain data security and confidentiality information (sections 4.31 to 4.33 of the FY 2017 agreement). In section 4.33, there are references to IT security; for example, section 4.33(a)(6) requires documents to be provided to an office's IT provider, and section 4.33(a)(8) refers to DTMB Technical Policies, Standards and Procedures. There is also the requirement in section 4.33(b) to obtain an Independent Security Audit. FOC and PA offices should refer to Subsection 3 of this manual section for guidance on the Independent Security Audit.

2.2.4 Moving DTMB-Provided Network Hardware and/or PCs/Laptops

County FOC, PA or IT staff may move DTMB-provided network hardware and/or PCs/laptops within the confines of the county offices. If hardware is being moved to a location that will require new networking and wiring, staff must notify the MiCSES Help Desk at least eight weeks in advance of the move. DTMB will help coordinate the move with the county IT staff.

2.2.5 Number of PCs/Laptops

Exhibit 1.23E1 discusses the number of PCs/laptops provided to state-managed offices and the number that may be purchased by county-managed offices.

2.2.6 Change in Support Model

If an FOC or PA office wants to change their IT support model, they must obtain prior written approval from OCS Financial Management. The FOC or PA office will follow the procedure outlined in Exhibit 1.23E2. If the support model change is from state-managed to county-managed, the office must return all PCs/laptops to DTMB.

2.3 Elements Specific to the State-Managed IT Support Model

2.3.1 Hardware and Software

DTMB will provide the PCs/laptops and related software that access the IV-D applications. Refer to Exhibit 1.23E1 for the number of PCs/laptops that will be provided. The county, however, will provide the printers,

scanners, monitors and other peripherals such as keyboards and mice. DTMB will not provide these items.

DTMB will provide all network hardware, including the router connecting the LAN to the state's wide area network (WAN). The PCs/laptops will reside on the state LAN.

Only DTMB-provided equipment other than the items noted above and required to be provided by the county may be attached to the DTMB-provided PCs/laptops or the state LAN.

Only DTMB-provided software may reside on and/or be installed on a DTMB PC/laptop.

No county applications may reside on and/or be installed on a DTMB PC/laptop or the state LAN.

2.3.2 Support

DTMB will provide all routine maintenance, repair or replacement for the PCs/laptops and related software. DTMB-provided PCs/laptops that need to be replaced due to obsolescence[4] will be replaced in accordance with state replacement policies, depending on budget and resource availability.

DTMB will provide all routine and emergency services/maintenance for LAN and WAN network hardware, including the router connecting the state LAN to the state WAN.

The county will provide support for printers, scanners, monitors and other peripherals such as keyboards and mice.

Note: Maintenance does not cover accidental damage such as dropped hardware, coffee/soft drink spills, damage caused by the site's negligence to protect against computer viruses, or installation of hardware or software by unauthorized personnel. Costs incurred to repair damage resulting from these items will be the responsibility of the FOC or PA and/or the county.

DTMB will be responsible for the implementation of any software or hardware upgrades or changes. DTMB will distribute information about any upgrades or changes, including the potential impact and implementation date, as soon as information is available.

[4] For the purposes of this manual section, "obsolescence" means that the PC/laptop is unable to provide the functionality necessary for the users to perform their assigned IV-D tasks and/or fulfill their IV-D responsibilities as described in the CRP agreement in effect at the time.

2.3.3 Funding of IT Purchases

As described in Subsection 2.2.2 of this manual section, a state-managed office can bill and be reimbursed for printers, scanners, monitors and other peripherals such as keyboards and mice without prior approval from OCS. The county cannot bill for any other costs unless OCS Financial Management has provided pre-approval for the specific items.

2.3.4 Confidentiality/Security

As described in Subsection 2.2.3 of this manual section, state-managed offices must comply with the provisions of Section 1.10 of the *Michigan IV-D Child Support Manual*. As stated in Subsection 3.3.1 of this manual section, a state-managed office does not need to obtain an Independent Security Audit.

2.3.5 Disposal of PCs/Laptops Provided by DTMB

All PCs/laptops or any equipment provided by DTMB (other than as described in the note below) must be returned to DTMB when it is no longer being used.

Note: Any failing DTMB-provided printers, monitors and peripheral devices that are being replaced should be disposed of in accordance with the county's disposal policy. The county will return this equipment to DTMB only if the county's policy does not ensure that any data/memory is overwritten or erased prior to disposal.

2.4 Elements Specific to the County-Managed IT Support Model

2.4.1 Hardware and Software

County staff[5] will provide PCs/laptops and related software that access the IV-D applications. Refer to Exhibit 1.23E1 on the number of PCs/laptops that can be purchased. The county will also provide the printers, scanners, monitors and other peripherals such as keyboards and mice.

The county will provide all network hardware and associated software up to the router connecting the county LAN to the state WAN. The PCs/laptops will reside on the county LAN.

[5] County staff may include vendor IT staff.

County applications that provide services to computer users across the county may reside on or be installed on the county-provided PCs/laptops.

The county may use an imaging system in the performance of IV-D child support duties and may bill the appropriate amounts for the imaging system to the IV-D program; refer to Exhibit 1.23E3. IV-D data provided to an imaging system cannot be used or viewed by non-IV-D staff.[6]

2.4.2 Support

The county will provide all routine maintenance, repair or replacement for the county-provided PCs/laptops and related software. County-provided PCs/laptops that need to be replaced must be replaced in accordance with county replacement policies that, absent any unusual circumstances that have been communicated to and approved by OCS, apply to all county departments.

The county will provide all routine and emergency service/maintenance for the county's LAN hardware. DTMB will provide all routine and emergency service/maintenance for the state WAN hardware, including the router connecting the county LAN to the state WAN.

The county will provide support for printers, scanners, monitors and other peripherals such as keyboards and mice.

DTMB staff will notify the county FOC or PA office Local Project Coordinator of any minimum system technical requirements that are needed to ensure that IV-D applications function properly on the county-provided PCs/laptops. DTMB staff will distribute information about DTMB application upgrades or changes, including the potential impact and implementation date, as soon as information is available. It will be the county's responsibility to implement any necessary upgrades or changes to its PCs/laptops, network, etc. in a timely manner.

2.4.3 Funding of IT Purchases

As described in Subsection 2.2.2 of this manual section, a county-managed office can bill and be reimbursed for printers, scanners, monitors and other peripherals such as keyboards and mice without prior approval from OCS. The county can bill and be reimbursed for other costs as described in Exhibit 1.23E2 of this manual section.

[6] Ref: Section 1.10 of the *Michigan IV-D Child Support Manual* for additional information on the security of IV-D data.

2.4.4 Confidentiality/Security

As described in Subsection 2.2.3 of this manual section, county-managed offices must comply with the provisions of Section 1.10 of the *Michigan IV-D Child Support Manual*. As stated in Subsection 3.3.2 of this manual section, county-managed offices must obtain an Independent Security Audit.

2.4.5 Disposal of IT Hardware

Any hardware no longer being used, including any failing DTMB-provided printers, monitors and peripheral devices that are being replaced, should be disposed of in accordance with the county's disposal policy. The county's disposal policy must ensure that any data/memory is overwritten or erased prior to disposal.

Note: The county will return any DTMB-provided printers, monitors and peripheral devices to DTMB only if the county's policy does not ensure that any data/memory is overwritten or erased prior to disposal.

3. Independent Security Audit Requirement in the Cooperative Reimbursement Program (CRP) Agreement

This subsection explains how OCS will implement the Independent Security Audit requirement contained in the CRP agreement.[7] It also provides guidance related to the items that must be reviewed in an Independent Security Audit and supporting documentation for the security standards.

Detailed information for OCS offices regarding the audit is provided in:

- Exhibit 1.23E6, Independent Security Audit Guidance; and
- Exhibit 1.23E7, OCS Analysis of the OCSE Security Agreement Controls and Their Use in the Independent Security Audit.

3.1 Overview

The CRP agreement contains the following requirement:

> ***Independent Security Audit***
> At least once every three years, the Grantee must obtain an independent security audit that evaluates its compliance with the management, operational, and technical controls required by the OCSE Security Agreement,[8] *Internal Revenue Service*

[7] In the current (FY 2017) CRP agreement, this provision can be found in Section 4.33(b).
[8] Ref: Exhibit 1.23E8. OCSE is the federal Office of Child Support Enforcement.

(IRS) Publication 1075, DTMB Technical Policies, Standards, and Procedures, and MDHHS-OCS security and confidentiality policies. The audit must be conducted by an unbiased, independent entity. The entity must issue an audit report that includes detailed findings and recommendations to improve the Grantee's procedures, practices and systems in order to meet the control requirements. The Grantee must provide the report to MDHHS.

The following audits will meet this requirement:

- An IRS Safeguards Review conducted by the IRS; or
- A review conducted by an independent auditing/security review firm.

Under the current IT support models, a biennial MDHHS-OCS IRS Internal Inspection site visit meets this requirement for state-managed offices, but does not completely meet this requirement for county-managed offices. The biennial MDHHS-OCS IRS Internal Inspection site visits only review business/office procedures and processes; they do not review the IT infrastructure, personal computers (PCs)/laptops/devices, and county systems that contain IV-D data (e.g., imaging systems, file shares). However, the IT infrastructure and PCs/laptops/devices for state-managed offices are reviewed at the state level by the IRS; therefore, everything is audited. The IT infrastructure, PCs/laptops/devices, and county systems that contain IV-D data (e.g., imaging systems, file shares) at county-managed offices are not reviewed at the state level; therefore, everything is not audited. This is summarized in the following table.

	State-Managed Offices	**County-Managed Offices**
Business/Office Procedures and Processes	Reviewed in biennial MDHHS-OCS IRS Internal Inspection site visit.	Reviewed in biennial MDHHS-OCS IRS Internal Inspection site visit.
IT Infrastructure, PCs/Laptops/Devices, and County Systems That Contain IV-D Data (e.g., Imaging Systems, File Shares)	Reviewed at state level by IRS.	Reviewed in an Independent Security Audit.

3.2 Analysis of the Independent Security Audit Requirement Between the Different IT Support Models

An Independent Security Audit, as it is written in the CRP agreement, refers to more than just IT security; it covers all management, operational and technical controls over handling, storing and using confidential data. For the purposes of

this manual section and what needs to be done in an Independent Security Audit, the management, operational and technical controls over handling, storing and using confidential data are divided into:

- The business/office procedures and process controls; and
- The controls over the IT infrastructure, PCs/laptops/devices, and county systems (e.g., imaging systems, file shares) that contain IV-D data.

For the purposes of this manual section, references to "county systems that contain IV-D data" will include imaging systems and file shares that contain IV-D data.

Note: Section 4.33(a)(8) of the FY 2017 CRP agreement refers to DTMB Technical Policies, Standards and Procedures; however, because of the comprehensive nature of the OCSE Security Agreement and IRS *Publication 1075*, DTMB Technical Policies, Standards and Procedures do not need to be considered at this time, and no action needs to be taken related to those requirements.

3.2.1 State-Managed Offices

At state-managed offices, responsibility for the management, operational and technical controls over handling, storing and using confidential data are split between the state and the county office. The business/office procedures and process controls are managed by the county office, but the IT infrastructure and PCs/laptops/devices are managed by the state.

Note: There should not be any IV-D county systems or file shares at state-managed sites.

The biennial MDHHS-OCS IRS Internal Inspection site visits fully meet the audit requirement for state-managed offices because OCS reviews the business/office procedures and process controls during the site visits. Although OCS does not review the controls related to the IT infrastructure and PCs/laptops/devices, those controls are reviewed at the state level (e.g., by the IRS).

3.2.2 County-Managed Offices

At county-managed offices, the county has the entire responsibility for the management, operational and technical controls over handling, storing and using confidential data. The county manages the business/office procedures and process controls as well as the controls over the IT infrastructure and PCs/laptops/devices and any county system that contains IV-D data. OCS reviews the business/office procedures and process controls during its biennial IRS Internal Inspection site visits, but OCS does not review the IT infrastructure,

PCs/laptops/devices, and county systems that contain IV-D data. Neither DTMB nor the IRS review these items at the state level. Therefore, county-managed offices need an Independent Security Audit that covers the IT infrastructure, PCs/laptops/devices, and any county system that contains IV-D data.

Note: The IRS may choose to audit a county-managed office during an audit of OCS.

The CRP agreement requires an Independent Security Audit once every three years. The effective date of the FY 2017 CRP agreement was October 1, 2016, and the county-managed offices completed their first audit by September 30, 2019. Therefore, the due dates for the next four audits are as follows:

- September 30, 2022;
- September 30, 2025;
- September 30, 2028; and
- September 30, 2031.

OCS Financial Management staff will issue reminders to county-managed offices approximately 11 months before the end of a three-year cycle. However, those offices should not rely solely on that reminder for initiating appropriate steps in advance of the deadline.

County offices must bill the cost of the audit in accordance with Subsection 2 of this manual section. When charging for the cost of the audit, they will use the same method they used to charge for the IT services that are the subject of the audit.

3.3 Compliance With the Independent Security Audit Requirement

3.3.1 State-Managed Offices

State-managed offices do not need to have an Independent Security Audit.

3.3.2 County-Managed Offices

County-managed offices need to complete an Independent Security Audit.

County-managed offices must do the following:

A. Identify if they have confidential IV-D data[9] that is contained in a county system or file share and determine if any of the data is federal tax information (FTI) (e.g., MiCSES tax-offset information, MiCSES IRS addresses).[10]

B. Contact their county administrator and/or county IT department; refer them to IRS *Publication 1075* Section 9 and the IRS Office of Safeguards website (https://www.irs.gov/uac/safeguards-program); and provide them with the CRP agreement language, copies of Exhibits 1.23E6 and 1.23E7 (guidance documents), the OCSE Security Agreement (Exhibit 1.23E8), and the OCSE Security Addendum (Exhibit 1.23E9).

C. Inform the county administrator and/or county IT department that the IT infrastructure and PCs/laptops/devices that **access** the state systems must be assessed against IRS *Publication 1075* Section 9 as outlined in Exhibit 1.23E6.

D. Inform the county administrator and/or county IT department that if there is FTI stored on a county system or file share that contains IV-D data, that system must also be assessed against IRS *Publication 1075* Section 9 as outlined in Exhibit 1.23E6. If there is no FTI on the system that contains IV-D data, the system only needs to be assessed against the OCSE Security Agreement as outlined in Exhibits 1.23E6 and 1.23E7.

E. Complete the assessment, compile the findings, remediate the findings (especially significant and critical findings within 30 days of the report date) and submit the Independent Security Audit Report along with the Corrective Action Plan to the county's assigned OCS contract manager by September 30. The plan should include the findings, plan of action, major milestones, and remediation completion date for all findings.

3.4 Additional Information

Based upon a discussion with the Michigan State Police, OCS has determined that a Law Enforcement Information Network (LEIN) audit does not meet the requirements for an independent security review/audit.

[9] "IV-D data" or "child support *program* information" is data or information obtained in connection with the performance of IV-D functions; this information may or may not be stored in a IV-D data system. "Confidential information" is defined in Section 1.10 of the *Michigan IV-D Child Support Manual*.
[10] Ref: Section 1.10 of the *Michigan IV-D Child Support Manual* for a definition of IRS data. Also refer to IV-D Memorandum 2017-001, *Commingling of Federal Tax Information (FTI) With Non-FTI, and the Independent Verification of FTI Addresses*.

If the county needs an example of an Independent Security Audit contract, as of the publication of this manual section, the state has a contract with Cyber Defense Technologies, LLC (Contract No. 071B6600012) to provide various vulnerability assessment services to the state. The contract is also available for use by counties under the MiDeal Extended Purchasing Program.[11]

The federal OCSE issued Information Memorandum (IM)-17-01, *Independent Security Assessors and Baseline Security Controls*, for tribal agencies. This memorandum discusses identifying independent security assessors and gives examples of minimum baseline security controls. It may provide valuable guidance in the selection of an independent auditing/security review firm.

In addition, OCSE IM-17-01 contains the definition of an acceptable auditor for purposes of the Independent Security Audit: "a competent, independent, and unbiased evaluator who has expertise in information assurance and IT cybersecurity technology, processes, and methodology to validate existing security controls and make a determination of a general security posture of an IT system."

SUPPORTING REFERENCES:

Federal
2 Code of Federal Regulations (CFR) Part 200
45 CFR 74.40–74.46
45 CFR Parts 75 and 95
45 CFR 92.25
45 CFR 92.36
45 CFR 95.613

State
None

REVISION HISTORY:

IV-D Memorandum 2020-036
IV-D Memorandum 2020-009

[11] The state's contract for this service may be terminated or revised subsequent to the publication of this manual section. If this example is unavailable, office managers may contact the OCS Financial Management office for assistance.