STATE OF MICHIGAN
GRETCHEN WHITMER
GOVERNOR
DEPARTMENT OF HEALTH AND HUMAN SERVICES
LANSING
ELIZABETH HERTEL
DIRECTOR

IV-D MEMORANDUM 2022-001

TO: All Prosecuting Attorney (PA) Office Directors
All Friend of the Court (FOC) Office Directors

FROM: Erin P. Frisch, Director
Office of Child Support (OCS)

DATE: January 7, 2022

UPDATE(S):

☐ Manual

☐ Form(s)

SUBJECT: OCS Procurement of Vendor for Independent Security Audit in County-Managed Offices

ACTION DUE: None

POLICY EFFECTIVE DATE: None

PURPOSE:

County-managed offices in the Cooperative Reimbursement Program (CRP) complete Independent Information Technology (IT) Security Audits every three years. For the audit due by September 30, 2022, OCS is procuring the vendor that will conduct the audit.[1] This vendor will:

- Audit the county-managed offices' IT infrastructure, workstations, and county systems that process or store IV-D data;
- Provide the county office and OCS an audit report (including findings, if any);
- Assist the county in preparing a Plan of Action and Milestones (POAM) as a result of the findings, and offer guidance regarding cybersecurity improvements; and
- Provide OCS with a summary of county findings in a statewide risk assessment.

In concert with DTMB,[2] OCS has recently finalized a contract with Dewpoint, Inc. and will provide more information to county-managed offices as it becomes available. OCS

[1] This was first announced in the September 8, 2021 email notification *Reminder: FOC and PA ACTION REQUIRED – Due Date: 9/30/2022 – County-Managed Offices Must Submit Independent Security Audit Findings to OCS As Required by the CRP Contract; OCS-Selected Vendor to Perform the Independent Security Audits*.

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

asks county-managed offices to share this IV-D Memorandum with their IT provider leadership.

OCS will update Section 1.23, "Cooperative Reimbursement Program (CRP) Agreements (Contracts)," of the *Michigan IV-D Child Support Manual* after all audit-related processes are finalized.

DISCUSSION:

Background

September 30, 2022 is the due date for the completion of the second cycle of the Independent IT Security Audit.[3] The first audit, which was due September 30, 2019, was completed by vendors that the county-managed offices procured. Each county office then submitted their audit report and POAM to OCS. County offices were asked to address all critical and high-level risks and provide updates on the resolution of the risks.

Upon receiving the counties' audit reports, OCS noticed significant variability in the structure and content of the reports. As a result, OCS was unable to prepare a statewide assessment of the cybersecurity risks for all the county-managed offices.

OCS Procurement of Vendor for Audit Due September 30, 2022

For the audit, audit reports, and POAMs due on September 30, 2022, OCS has procured Dewpoint to perform the audit work for all county-managed offices. OCS, in concert with the Michigan DTMB Cybersecurity & Agency Services Offices, developed a Request for Proposal (RFP) and released it on September 1, 2021. The RFP was developed with the goal to have one vendor (or a prime vendor with subcontractors) do the following:

- Perform audits at all county-managed offices;
- Prepare and deliver a county audit report with findings to the county office and OCS;
- Summarize county findings into a statewide risk assessment; and
- Periodically monitor and update the POAM and remediation activities, including periodic coaching for offices as necessary.

Preparing for the Audit Process

OCS will work with Dewpoint to develop a comprehensive plan for the audit process. The individual local office audit process will include preparatory steps in which Dewpoint

[3] The Independent IT Security Audit that is due September 30, 2022 was first announced in IV-D Memorandum 2020-036, *Implementation of the Independent Security Audit Requirement Contained in the Cooperative Reimbursement Program (CRP) Agreement*.

will contact the identified IT staff and create a plan. This will include gathering IT environment information, obtaining an understanding of IT assets involving child support data, and requesting access to IT environments. Dewpoint will also provide, as necessary, coaching and information on the specific audit steps based on the size and IT environment of the office.

The process being considered will include the following steps:

1. Meetings with county-managed FOC and PA office and IT management staff.

   Note: OCS contract managers are currently contacting counties to confirm each county's IT management representatives.

2. The Center for Internet Security (CIS) Controls[4] cybersecurity framework (version 8) will be used to perform the assessments, including penetration testing similar to Internal Revenue Service security reviews.

3. Dewpoint will provide the results of the assessment and identified risks, if any, in an audit report to the county IT and FOC/PA staff.

4. If risks are identified, within a month of completion of the audit, county staff will develop a POAM to address the risks and submit it to OCS.

   Note: As part of the contract, Dewpoint will provide coaching as necessary during the audit and monthly thereafter based on the findings of the audit. These sessions are intended to assist county staff in understanding the audit process, the identified risks, and available cybersecurity improvements based on the county IT environment. Dewpoint will also provide guidance on developing the POAM and implementing improvements.

5. After completing all the county audit reports, Dewpoint will compile a statewide report using general, non-identifying data from the county findings. This information will identify overall cybersecurity risks to child support data in county-managed offices. OCS intends to use the statewide report to focus on child support program security risks and determine opportunities for improvements. The report may also be used for developing and improving safeguarding policies.

Additional Information

To begin the process, OCS and Dewpoint will identify a few offices that will be in the first group of assessments and will reach out to those offices and IT contacts. OCS will share a comprehensive schedule of office assessments when it is finalized. Also, OCS

[4] CIS Controls are cybersecurity-prioritized best practices that assess the current level of safeguards to help improve an organization's cyber defense program.

will provide additional information to county-managed offices as necessary via email notifications, webinars, or other means.

NECESSARY ACTION:

Share this IV-D Memorandum with your IT provider leadership. County-managed offices will participate in the audit by Dewpoint and complete and submit a POAM within one month of the completion of their audit.

REVIEW PARTICIPANTS:

Program Leadership Group

CONTACT PERSON:

Sonya Butler
OCS Financial Management Unit
Butlers2@michigan.gov
517-241-7728

CC:

All FOC Staff
All PA Staff
All OCS offices
State Court Administrative Office (SCAO) Friend of the Court Bureau

ATTACHMENTS:

None

EPF/STB