

APPENDIX E

IV/D (Child Support) SECURITY REQUIREMENTS

Attachments

- E1 - DHS – OCS Action Transmittal 2005-069
- E2 - DHS – OCS Action Transmittal 2004-032 w/Attachments 1 & 2
- E3 - DHS – OCS Transmittal 2004-032 Attachment 3
- E4 – DHS – OCS Action Transmittal 2005-008
- E5 – DHS – OCS Action Transmittal 2004-21
- E6 – DHS – OCS Action Transmittal 2004-21 Attachment 1
- E7 - Child Support Security Cites and References
- E8 - Child Support Obligation Disclosure Form



JENNIFER M. GRANHOLM
GOVERNOR

STATE OF MICHIGAN
DEPARTMENT OF HUMAN SERVICES
LANSING



MARIANNE UDOW
DIRECTOR

MICHIGAN IV-D ACTION TRANSMITTAL 2005-069

TO: All Friends of the Court (FOCs)
All Prosecuting Attorneys (PAs)
All Office of Child Support (OCS) staff

FROM: Marilyn F. Stephen, Director
Office of Child Support

DATE: October 28, 2005

SUBJECT: REVISED: Transmission of Restricted Information via Email

PURPOSE:

This Action Transmittal (AT):

- Replaces AT 2004-040, *Transmission of Restricted Information via Email*;
- Provides a change bar in the left-hand margin of the document to signify procedural changes to the AT;
- Updates each reference to the Family Independence Agency (FIA) and replaces it with the Department of Human Services (DHS);
- Provides the local county offices with an attachment that outlines conversion dates for the name replacement project on existing confidentiality email accounts; and
- Provides guidelines and policy for the transmission of restricted information via email, between OCS, the Michigan Child Support Enforcement System (MiCSES) staff, the Michigan State Disbursement Unit (MiSDU) staff, the child support partners (FOCs and PAs), and customers.

DEFINITIONS:

- **Restricted information** — Information that contains any of the following items:
 - Internal Revenue Service (IRS) information (i.e., any information obtained from the IRS);¹
 - Social Security numbers (SSNs);

¹ IRS information includes any taxpayer identifying information, or any taxpayer identifying information and the refund intercept amount.

- Address/location information when the *Family Violence Indicator* (FVI) is set to "Y" with a specific *Family Violence Type* (FV) code;² and
 - Any list or report³ that contains identifying information⁴ on any case participant.
- **IV-D worker** — Any staff employed or contracted by a IV-D agency doing IV-D work. This includes, but is not limited to, staff of the following offices:
 - FOCs;
 - PAs;
 - MiSDU;
 - MiCSES;
 - OCS;
 - Attorney General's child support unit; and
 - Workers contracted to help in any of these offices.
- **State network** — Any server maintained by the State of Michigan.
 - **michigan.gov email account** — Any email address that ends with michigan.gov (e.g., doej@michigan.gov).
 - **Non-michigan.gov email account** — Any email address that ends with something other than michigan.gov (e.g., doej@county.mi.us).
 - **User name** — Everything to the left of the "@" symbol in an email address. For example, if the email address is doej@michigan.gov, then the user name is doej.
 - **User ID** — The code used to identify a user when (s)he logs into a system and starts a login session. It is used by the system to uniquely identify each user.
 - **Secure** — A transmission where there is little or no likelihood of the communication being intercepted by an unauthorized person.
 - **Firewall** — An electronic blocking mechanism that inhibits unauthorized users from accessing a computer system.

SECURE TRANSMISSION:

An email transmission between two michigan.gov email accounts is secure; both via Novell GroupWise and Novell GroupWise web access. An email transmission between

² The FV codes are: CT – court order; SS – sworn statement; PW – Michigan personal protection order (PPO) with confidential address; FW – Foreign PPO with confidential address; and FP – Federal Parent Locator Service (FPLS).

³ A list or report is defined as a document containing case participant information from multiple cases.

⁴ Identifying information includes any one of the following: name, SSN, address.

a michigan.gov account and a non-michigan.gov account is **not** secure. Even if the county is connected to its own secure server, the transmission between a michigan.gov account and a non-michigan.gov account is **not** secure.

Any IV-D worker using a michigan.gov account **must not**:

- Send restricted information to a non-michigan.gov account; or
- Forward any email containing restricted information to a non-michigan.gov account.

CONFIDENTIAL michigan.gov ACCOUNTS:

For the purposes of transmitting and receiving restricted information, OCS requested that the Department of Information Technology (DIT) create confidential michigan.gov email accounts for all FOC and PA offices.

As a result of the recent name change to DHS, DIT will update the confidential addresses to reflect this new name change. Select county FOC offices have already undergone this transition and are listed as **converted** counties on the provided attachment. The remainder of FOC and PA offices are listed on the attachment with projected dates for the name change to each county's confidential email address account (Ref: Attachment 1).

This name change also affects the user login. At the time the account was created, the user ID naming conventions started each user ID with "FIA." The user of the confidential michigan.gov account must now use DHS instead of FIA when (s)he logs into the account. IV-D staff will continue to use the password that (s)he originally created for the account. In addition, stored email will be retained in the new account.

The FOC office account is designated "DHS-*countyname*-Confidential@michigan.gov" and the PA office account is designated "DHS-PA-*countyname*-CTY-Confidential@michigan.gov."⁵ For example, the Alcona FOC confidential account is DHS-Alcona-Confidential@michigan.gov. The Alcona PA confidential account is DHS-PA-Alcona-CTY-Confidential@michigan.gov. The county office will assign three designated users (one primary user and two alternates) to maintain the confidential michigan.gov account. The county office does not need to identify the designated users to OCS or DIT.

If the designated user is located in a county office that is connected to the state network, (s)he can access the confidential michigan.gov account either via the Novell GroupWise software or the State of Michigan Novell GroupWise web access (<http://gw.state.mi.us>).⁶

⁵ Counties with two-word names must omit the space when logging in (e.g., the Grand Traverse FOC would be DHS-GrandTraverse-Confidential@michigan.gov).

⁶ The designated user must select "Department of Human Services" from the list and must enter the user name and password for the confidential michigan.gov account.

If the designated user is located in a county office that is **not** connected to the state network, (s)he must only access the confidential michigan.gov account via the State of Michigan Novell GroupWise web access.⁷

Each FOC/PA IV-D Contact⁸ will receive a password for the confidential michigan.gov account. The FOC/PA IV-D Contact will send the password to the primary user. Then, the primary user must immediately change the password.

If the primary user accesses the account via Novell GroupWise, then (s)he must:

1. Select "Tools" from the toolbar;
2. Select "Options";
3. Double-click on "Security";
4. Enter the old password;
5. Enter the new password;
6. Confirm the new password; and
7. Click "OK."

If the primary user accesses the account via GroupWise web access, then (s)he must:

1. Select the "options" icon at the top of the page;⁹
2. Enter the new password;
3. Confirm the new password; and
4. Click "Save."

After the password is changed, the primary user must inform the two alternate users of the new password. These three designated users must be the only people with access to the office's confidential michigan.gov account.

GENERAL PROCEDURES:

Receiving Restricted Information From OCS

OCS and DIT will send scheduled (e.g., law enforcement information network (LEIN) validation reports, bonus reports, tax refund offset data) and unscheduled mass distributions of restricted information to confidential michigan.gov accounts, even if the county office uses michigan.gov accounts. This frees OCS and DIT from maintaining statewide distribution lists. If the county office uses michigan.gov accounts, the designated user can forward the restricted information to the appropriate staff. If the county office does not use michigan.gov accounts, the designated user must save the document containing the restricted information to a folder on his/her personal hard drive. Then, the designated user will open his/her county-based email and attach the

⁷ <http://gw.state.mi.us>

⁸ The FOC/PA IV-D Contact was formerly known as the Local Project Coordinator (LPC).

⁹ The "options" icon is denoted by the following symbol at the top of the page: . This is not the same as the "internet options" function from the drop down menus of your internet browser.

document to an email addressed to the appropriate staff within his/her county office. This two-step process using two email accounts behind the same firewall ensures that the information will not be transmitted through an unprotected connection. **The designated user must not forward the email containing restricted information to a non-michigan.gov account.**

When the restricted information is not contained within a mass distribution OCS, MiSDU, and MiCSES staff will only send restricted information to michigan.gov accounts. If the recipient(s) does not use a personal michigan.gov account OCS, MiSDU, or MiCSES staff will send the restricted information to the office's confidential michigan.gov account. The designated user must follow the same guidelines outlined above for disseminating the information to the appropriate staff. If the communication does not contain restricted information, OCS, MiSDU, and MiCSES staff will correspond with the IV-D worker's personal account, including non-michigan.gov email accounts.

Sending Restricted Information to OCS, MiSDU, and MiCSES

County staff must only send restricted information to OCS, MiSDU, and MiCSES from a michigan.gov account. The IV-D worker can either use a personal michigan.gov account or give the information to the designated user of the office's confidential michigan.gov account for him/her to send.

Sending Restricted Information to Customers and Employers

IV-D workers must **not** send restricted information to customers or employers via email. Before sending a response to a customer or employer, the IV-D worker **must**:

- Delete any restricted information from the body of the original email; and
- Not add any additional restricted information.

ADDITIONAL INFORMATION:

If an FOC or PA wants to set up michigan.gov accounts for all staff the FOC/PA IV-D Contact must notify the CSES Hotline.

LEGAL REFERENCES:

Federal
26 United States Code (USC) 6103
42 USC 653
IRS Publication 1075

State
Michigan Compiled Law 400.64

POLICY REFERENCE:

AT 2005-023, **Revised:** *Use of State Make Whole Funds*
AT 2004-018, *Family Violence Indicator (FVI)*

AT MAINTENANCE: Retain until further notice

EFFECTIVE DATE: Upon receipt

REVIEW PARTICIPANTS: Virginia Hambric, MiCSES Project Staff
Jan Isaacs, MiCSES Project Staff
Dave Clagett, Prosecuting Attorneys Association of Michigan
Lynn Davidson, Macomb County FOC
Steve Capps, State Court Administrative Office, Friend of the Court Bureau
Financial Work Improvement Team
Program Leadership Group
Friend of the Court Association Review Board

CONTACT PERSON: Suzy Crittenden
Policy Analyst
Crittendens2@michigan.gov
(517) 241-5083

ENCLOSURE: Attachment 1-*County Conversion Dates for Confidential michigan.gov Email Accounts*

CC: Michigan Attorney General

MFS/SC



STATE OF MICHIGAN
FAMILY INDEPENDENCE AGENCY
LANSING



JENNIFER M. GRANHOLM
GOVERNOR

MARIANNE UDOW
DIRECTOR

MICHIGAN IV-D ACTION TRANSMITTAL 2004-032

TO: Friends of the Court (FOCs)
Prosecuting Attorneys (PAs)
Office of Child Support (OCS) Staff

FROM: Marilyn F. Stephen, Director
Office of Child Support

DATE: October 7, 2004

SUBJECT: Internal Revenue Service (IRS) and State of Michigan Tax Return Information

RESPONSE DUE: December 15, 2004

PURPOSE:

This Action Transmittal (AT) informs all IV-D staff and contractors of the IRS and Michigan Department of Treasury tax return information confidentiality requirements. In addition, it notifies FOCs and PAs of the OCS reporting requirements.

BACKGROUND:

The IRS and the Michigan Department of Treasury provide tax return information to the Michigan Title IV-D program. For purposes of the Michigan Title IV-D program, tax return information is defined as: the receipts in MiCSES that are from an offset to an individual's tax refund, amount and date of offset and any hard copies showing these offsets. All persons who access/use/store this information must keep the tax return information confidential. Personal penalties apply to anyone who discloses confidential tax return information. The IRS and Michigan Department of Treasury prescribe guidelines, procedures and policies that carry out the confidentiality requirements of the Internal Revenue Code (IRC) and Michigan Codified Laws (MCL). All organizations that receive and use tax return information must have safeguards and procedures in line with these requirements. The organization must ensure that staff keep the information confidential and make staff aware of the penalties. County FOC and PA offices must report their safeguards and procedures to OCS. OCS reports to the IRS and Michigan Department of Treasury.

PROGRAM ACTIONS AND POLICY INFORMATION:

I. FOC/PA

Each county FOC and PA must submit an Annual Safeguard Activity Report for 2004 due to OCS by no later than December 15, 2004.

The IRS' guidelines, procedures, and reporting requirements and the consequences of unauthorized disclosure are included in Tax Information Security Guidelines for Federal, State, and Local Agencies (OMB No. 1545-0962) also called the IRS Publication 1075¹. The individual or individuals responsible for the use of tax return information at the FOC/PA must read the publication and be aware of the requirements and penalties. This is necessary to ensure that the organization meets all the physical security, computer system security, and employee awareness requirements. The requirements of the MCL will be met if the IRS requirements are followed and applied to the Michigan Department of Treasury information.

As part of meeting the requirements of IRS Publication 1075 the majority of the FOC/PA offices submitted a Safeguard Procedures Report (refer to section 7.2 of IRS Publication 1075) for the calendar year ended December 31, 2003. (OCS submitted a Safeguard Procedures Report to the IRS in January, 2004, covering that same period.)

A new Safeguard Procedures Report will not be due until January 31, 2010, (six years) unless there have been significant changes in procedures. However, as stated above, each county FOC and PA must submit an Annual Safeguard Activity Report for 2004 due to OCS by no later than December 15, 2004.

In the past, FOC/PA retained these reports. However, with the need to report the system security on a statewide basis, the county staff must submit these reports to OCS. Those counties that did not submit Safeguard Procedures Report for the year ended December 31, 2003, must complete the Safeguard Procedures Report and submit it as soon as possible. FOC/PA staff must then complete the Annual Safeguard Activity Report and submit it, as described above, for the current year.

The FOC/PA staff must pay particular attention to sections 5.6 (Computer Security), 5.7 (Common Criteria), and 7.2 (Safeguard Procedures Report: Computer Security) of IRS Publication 1075. Each FOC/PA must include in the Annual Safeguard Activity Report, for 2004, a diagram of the county network and its connection to the Michigan Child Support Enforcement System (MiCSES) network. Also, FOC/PA staff must include a description of the security features maintained to secure the state network and the MiCSES application against unauthorized access. These are necessary because of potential security issues surrounding the access to MiCSES and the need to follow the standard for systems that contain IRS data. OCS has evaluated compliance with the

¹ <http://www.irs.gov/pub/irs-pdf/p1075.pdf>

standard for MiCSES operations located in Lansing. However, because the MiCSES network and application are connected to county networks, the FOC/PA must also evaluate these local networks and connections against the standard. County staff may contact their computer systems departments for their evaluation. The Annual Safeguard Activity report must contain any conclusions and shortcomings in the evaluation. This will be an initial burden but for the future should only require updates.

FOC/PA staff offices must also review section 6.2 (Employee Awareness) of IRS Publication 1075, which describes the required annual certifications and training, related to confidential tax return information. Each FOC/PA must meet these requirements. The FOC/PA must report activities in the Annual Safeguard Activity Report (and the Safeguard Procedures Report every sixth year). OCS staff will summarize the information provided by FOC/PA and include it in OCS' report to the IRS. The FOC/PA must use the Michigan Department of Treasury Vendor, Contractor, or Subcontractor Confidentiality Agreement (see attachments 1, 2 and 3 for forms and instructions) to meet the above listed requirements. Each employee and any county contractor that accesses federal or state tax information must sign this form. The form is a Michigan Department of Treasury form that was not specifically designed for the relationship between OCS and FOC/PA, however, it covers tax information confidentiality requirements and penalties that apply both to the State of Michigan and the federal tax information. Each employee or county contractor must certify that (s)he understands the policies and procedures and penalties related to safeguarding tax information before (s)he is granted access to the system. In addition to the information contained on the above-mentioned form, the FOC/PA must provide additional information related to the use or storage of hard copies of any tax return information to employees and contractors.

II. OCS Employees and Contractors

All OCS employees and OCS contractors will be required to sign the appropriate Michigan Department of Treasury agreement before OCS will grant them access to the system.

APPLICATION AND SCOPE:

This AT applies to all staff (either employee or contract) that access/use/store any tax return information provided to the Michigan Title IV-D program.

LEGAL REFERENCES:

Federal

IRC sections 6103, 7213, and 7431.

State

MCL section 205.28 (1)(f) and (2).

POLICY REFERENCE:

AT 2003-007, *Security Guidelines for Federal, State and Local Agencies Receiving Tax Information*

AT MAINTENANCE: Retain Action Transmittal.

EFFECTIVE DATE: Upon receipt.

REVIEW PARTICIPANTS: Jeff Albaugh, Friend of the Court Association
Dave Clagett, Prosecuting Attorney Association of Michigan
Steve Capps, State Court Administrative Office, Friend of the Court Bureau
Darrell Dontje, Enterprise Security

CONTACT PERSON: Duane Noworyta
Financial Manager
Noworytad@michigan.gov
(517) 241-7728

CC: Darrell Dontje, Enterprise Security

ATTACHMENTS: Template for Annual Safeguard Activity Report
Instructions for Vendor, Contractor or Subcontractor Confidentiality Agreement.
Vendor, Contractor or Subcontractor Confidentiality Agreement

MFS/DN

AT 2005-032 Attachment 1

Template for Annual Safeguard Activity Report

Directions:

Annual Safeguard Activity Reports must be submitted on agency's letterhead, and must be dated and signed by the friend of the court (FOC) or the prosecuting Attorney (PA), and must follow the outline listed below. If a report covers more than one county or covers both the FOC and PA functions in a county please indicate that fact on the report.

Report only changes to any of the following:

I. RESPONSIBLE OFFICERS (added or deleted)

Provide:

Name

Title

Address (street and email, if available); and

Telephone number

II. LOCATION OF DATA

Describe the functions that use the tax information.

III. FLOW OF DATA

Provide a chart and/or detailed narrative of:

(A) The flow of information through the Agency;

(B) How the information is used and stored;

(C) How the information is protected

IV. SYSTEM OF RECORDS

Describe the permanent records, which are used to document:

(A) Requests;

(B) Receipt;

(C) Distribution;

(D) Disposition of Taxpayer Information

V. SECURE STORAGE OF DATA

Describe the security measures for data when not in use (identify at least two levels of security, i.e., a locked building / office and a locked file cabinet within the office.)

VI. LIMITED ACCESS TO DATA

Describe the procedures or safeguards (including physical barriers) used to ensure only authorized individuals access the information.

VII. DISPOSAL

Describe the method(s) used for tax information disposal/destruction.

VIII. COMPUTER SECURITY

For any tax information that is stored on computers outside of the Michigan Child Support Enforcement System (MiCSES) application provide for:

(A) MICROPROCESSORS AND MAINFRAME SYSTEMS

Provide a detailed description of the systemic controls employed to ensure compliance with C2 level of access control.

(B) Local Area Network (LAN), Wide Area Network (WAN)

Provide a detailed description of the security precautions, if the computer system is connected to a LAN or WAN.

(C) Provide your security process for employees who need or use a laptop that has access to MiCSES.

(D) PERSONAL COMPUTERS

Provide a detailed description of the procedures used to ensure all data is protected from unauthorized access or disclosure, including those that:

- ensure storage of disks and all electronic data;
- limit access to the disks or computer screens;
- destroy data.

Report the following information (this is not limited to just changes):

IX. AGENCY DISCLOSURE AWARENESS

Describe the how all persons who had access to the tax information were made aware in the current period of the confidentiality requirements, the FOC/PA security requirements, and any penalties for unauthorized inspection and or disclosure. Also include how often these people review the awareness requirements.

X. DISPOSAL

Report on the disposal of tax information in the current period.

XI. COMPUTER SECURITY, ADDITIONAL INFORMATION

(A) Provide a diagram of how the MiCSES network is connected to the county network. Label the equipment, on the diagram, with the manufacture's make and model. Basically the diagram should show how the county connects into the State's network (both physical and logical) as well as how the county is

connected to any other Internet Service (ISP) provider (if the county is connected to an ISP). All routers, firewall, ISP and network equipment should be shown. (For example a simple diagram would be two boxes with a line between them. The box on the left would be labeled State of Michigan router and the box on the right would be labeled FOC Hub with manufacture and series number.)

(B) Describe the hardware/software that is in place to ensure there is no unauthorized access to tax information maintained on the MiCSES system through the county connection.

(C) Provide the type of anti-virus software used as well as the process for updating the devices using this software.

(D) Provide your patch management process for your devices.

(E) What, if any session time-time outs (such as screen savers that require a password) are used.

XII. PLANNED ACTIONS AFFECTING SAFEGUARDS

Report any planned actions that create a major change to current procedures or computer security.

AT 2005-32 Attachment 2

Instructions for Vendor, Contractor or Subcontractor Confidentiality Agreement

The **Vendor, Contractor or Subcontractor Confidentiality Agreement** form must be completed by friend of the court (FOC), prosecuting attorney (PA) and contract staff with access to the Michigan Child Support Enforcement System (MiCSES). FOC and PA offices must certify in the Annual Safeguard Activity Report that a **Vendor, Contractor or Subcontractor Confidentiality Agreement** is signed and on file in the local office for each MiCSES user. DO NOT send copies of the **Vendor, Contractor or Subcontractor Confidentiality Agreement** directly to the Office of Child Support or the Department of Treasury.

Completion by Contractor Staff

The **Vendor, Contractor or Subcontractor Confidentiality Agreement** form was designed specifically for contractor staff and therefore is self-explanatory.

Completion by FOC and PA staff

FOC and PA staff completing the **Vendor, Contractor or Subcontractor Confidentiality Agreement** must take note of the following sections:

1. Under Company Name and Address list County FOC/PA name.
2. The Name of the State of Michigan Agency is Family Independence Agency, Office of Child Support.
3. The Sub-Contractor section is "N/A" for FOC/PA county employees.
4. The box that requires a description of the product or service provided is "N/A" for FOC/PA county employees.

Vendor, Contractor or Subcontractor Confidentiality Agreement

The Revenue Act, Section 28(1)f, 1941 PA 122, MCL 205.28(1)(f), makes all information acquired in administering taxes confidential. The Act holds a vendor, contractor or subcontractor and their employees who sell a product or provide a service to the Michigan Department of Treasury, or who access Treasury data, to the strict confidentiality provisions of the Act. Confidential tax information includes, but is not limited to, information obtained in connection with the administration of a tax or information or parameters that would enable a person to ascertain the audit selection or processing criteria of the Michigan Department of Treasury for a tax administered by the department.

INSTRUCTIONS: Read this entire form before you sign it. If you do not complete this agreement, you will be denied access to Michigan Department of Treasury and federal tax information. After you sign and date this form, keep a copy for your records. Send the original to: Michigan Department of Treasury, Office of Policy Communications and Disclosure, Disclosure Officer, 430 W. Allegan, Lansing, MI 48922.

Company Name and Address (Street or RR#, City, State, Zip Code)	Official or Employee Name
	Employee Identification Number or Driver's License Number
Name of State of Michigan Agency	Sub-Contractor's Name if Product/Service Furnished to Contractor
Describe here or in a separate attachment the product or service being provided to the State of Michigan Agency.	

Confidentiality Provisions. It is illegal to reveal or browse, except as authorized:

- All tax return information obtained in connection with the administration of a tax. This includes information from a tax return or audit and any information about the selection of a return for audit, assessment or collection, or parameters or tolerances for processing returns.
- All Michigan Department of Treasury or federal tax returns or tax return information made available, including information marked "Official Use Only". Tax returns or tax return information shall not be divulged or made known in any manner to any person except as may be needed to perform official duties. Access to Treasury or federal tax information, in paper or electronic form, is allowed on a **need-to-know** basis only. Disclosure of return information to other employees of your department, agency, division or office, must meet **need-to-know** criteria and be required for them to perform their official duties.
- Confidential information shall not be disclosed by a department employee to confirm information made public by another party or source which is part of any public record. 1999 AC 205.1003(3).

Penalty. Violating confidentiality laws is a felony, with penalties as described:

Agency Discipline

Absence of criminal prosecution does not prevent your agency from pursuing internal sanctions for unauthorized accessing, browsing, or disclosing state or federal tax returns or tax return information.

Michigan Penalties

MCL 205.28(1)(f) provides that you may not willfully browse any Michigan tax return or information contained in a return. Browsing is defined as examining a return or return information acquired without authorization and without a **need to know** the information to perform official duties. Violators of §28(1)(f) are guilty of a **felony** and subject to **fines of \$5,000 or imprisonment for five years, or both** per the Michigan Revenue Act, 1941 PA 122, MCL 205.28(2). State employees will be discharged from state service upon conviction.

Any person who violates any other provision of the Revenue Act, 1941 PA 122, MCL 205.1, et seq., or any statute administered under the Revenue Act, will be guilty of a misdemeanor and **fined \$1,000 or imprisonment for one year, or both**, MCL 205.27(4).

Federal Penalties

If you willfully disclose federal tax returns or tax return information to a third party, you are guilty of a **felony with a fine of \$5,000 or imprisonment for five years, or both, plus prosecution costs** according to the Internal Revenue Code (IRC) §7213, 26 USC 7213.

In addition, inspecting, browsing or looking at a federal tax return or tax return information without authorization is a **felony violation** of IRC §7213A, 26 USC 7213A, subjecting the violator to a **\$1,000 fine or imprisonment for one year, or both, plus prosecution costs**. Taxpayers affected by violations of §7213A must be notified by the government and may bring a civil action against the federal government and the violator within two years of the violation. Civil damages are the **greater of \$1,000 or actual damages** incurred by the taxpayer, plus the costs associated with bringing the action, 26 USC 7431.

CERTIFICATION		
I acknowledge that I have read this Agreement, which is intended to help me understand applicable Michigan and Federal law related to the protection of confidential information. I understand that failure to comply with applicable law, including the laws referenced in this Agreement, may subject a violator to criminal and civil penalties.		
Print name of person signing this agreement	Signature of person named above	Date signed
WITNESS		
Print name of witness	Signature of witness	Date signed



JENNIFER M. GRANHOLM
GOVERNOR

STATE OF MICHIGAN
DEPARTMENT OF HUMAN SERVICES
LANSING

MARIANNE UDOW
DIRECTOR

MICHIGAN IV-D ACTION TRANSMITTAL 2005-008

TO: All Friends of the Court (FOCs)
All Prosecuting Attorneys (PAs)
All Office of Child Support (OCS) Staff
State Court Administrative Office (SCAO), FOC Bureau (FOCB)
Office of the Attorney General (AG)

FROM: Marilyn F. Stephen, Director
Office of Child Support

DATE: March 18, 2005

SUBJECT: Dissemination of Ad Hoc Reports

PURPOSE:

This Action Transmittal (AT) provides policy for the proper dissemination and handling of ad hoc reports to IV-D workers.

DEFINITIONS:

- **Ad hoc report** — A report generated by running a query on the *Functional Prototype Queries* (FPRO) screen in the Michigan Child Support Enforcement System (MiCSES). The query produces information on several cases in an Internet Explorer window and the user creates the report by saving the information in a text file and importing it to Microsoft Excel or Access. The report typically contains the following types of information: party's name; case number; court action referral (CAR) number; docket number; date of birth; arrearage and payment information; bench warrant information; scheduled events; etc.
- **IV-D worker** — Any staff employed or contracted by a IV-D agency, including, but not limited to staff of the following offices:
 1. FOCs;
 2. PAs;
 3. Michigan State Disbursement Unit (MiSDU);
 4. MiCSES;
 5. OCS;

6. SCAO;
 7. AG's child support unit; and
 8. Workers contracted to help in any of these offices.
- **Federal tax information** — Data obtained from the Internal Revenue Service (IRS). This information includes any taxpayer identifying information, or any taxpayer identifying information and the refund intercept amount.
 - **Domain name** — Everything to the right of the “@” symbol in an email address. For example, if the email address is doe@j@michigan.gov, then the domain name is michigan.gov.
 - **Creator** — The IV-D worker who developed the ad hoc report.
 - **Recipient** — The IV-D worker who received the ad hoc report.
 - **Public folder** — A folder on a hard drive that multiple IV-D workers have access to through the network.

BACKGROUND:

According to AT 2004-040, *Transmission of Restricted Information via Email*, any report that contains identifying information on any case participant is considered restricted and must be protected from unauthorized persons. Therefore, an ad hoc report is restricted and must only be shared with IV-D workers that need access to the information to perform IV-D duties. The IV-D worker must protect the report as (s)he would with any other confidential information.

REQUIREMENTS:

The creator of an ad hoc report will:

- Only distribute to appropriate staff that portion (or portions) of a report pertaining to cases assigned to that staff;
- Immediately retrieve the report after it is printed; and
- **Not** leave any hard copies unattended if the work area is accessible by non-IV-D employees or the public, unless in a locked container.

When sending the ad hoc report to a IV-D worker, the creator will:

- Send the report to an email address with the same domain name,¹ or deliver it in person or via fax; and

¹ For additional information on secure transmission of information refer to AT 2004-040 at: <http://mi-support.cses.state.mi.us/policy/stateat/pdf/2004-040.pdf>.

- **Not** leave any hard copies unattended if the work area is accessible by non-IV-D employees or the public, unless in a locked container.

The recipient of the report will:

- **Not** leave any hard copies unattended if the work area is accessible by non-IV-D employees or the public, unless in a locked container;
- Avoid storing confidential materials in a shared electronic public folder (“public drive”) on his/her computer;²
- Immediately retrieve the report after it is printed; and
- Shred the report when it is no longer needed and serves no purpose.³

Ad hoc reports that contain federal tax information must be protected with a higher level of security. Creators and recipients of ad hoc reports that contain federal tax information must not leave any hard copies unattended, unless in a locked container.

LEGAL REFERENCES:

Federal
26 USC §6103
42 USC §653
IRS Publication 1075

State
MCL 400.64

POLICY REFERENCE:

AT 2004-040, *Transmission of Restricted Information via Email*

AT MAINTENANCE:

Retain until further notice.

EFFECTIVE DATE:

Upon receipt.

REVIEW PARTICIPANTS:

Steve Capps, SCAO, FOCB
Dave Clagett, Prosecuting Attorneys Association of Michigan
David Huntley, Alpena FOC
Lynn Davidson, Macomb FOC
Establishment WIT

CONTACT PERSON:

Ian Broughton
Policy Analyst
broughtoni@michigan.gov
(517) 241-5034

² If the recipient must store it in a public folder, (s)he must delete it when it is no longer needed.

³ For additional information on the confidential information protection, refer to IRS Publication 1075 at: <http://www.irs.gov/pub/irs-pdf/p1075.pdf>.

ENCLOSURE:

None

CC:

None

MFS/IMB



JENNIFER M. GRANHOLM
GOVERNOR

STATE OF MICHIGAN
FAMILY INDEPENDENCE AGENCY
LANSING



MARIANNE UDOW
DIRECTOR

MICHIGAN IV-D ACTION TRANSMITTAL 2004-021

TO: All Friends of the Court
All Prosecuting Attorneys
All Office of Child Support staff

FROM: Marilyn F. Stephen, Director
Office of Child Support

DATE: October 26, 2004

SUBJECT: Emergency Remote Access to the Michigan Child Support Enforcement System (MiCSES)

PURPOSE:

This Action Transmittal (AT) contains the guidelines for obtaining emergency remote access to MiCSES. Remote access is defined as access outside of the official workplace. The Office of Child Support (OCS) will grant limited remote access to MiCSES in situations deemed necessary for the operation of the IV-D program¹. OCS will only approve requests for these accounts under exceptional circumstances.

Note: This AT only provides the process for requesting emergency remote access approval to MiCSES. Local FOC and PA staff must continue to follow the current process for obtaining hardware. This AT is in no way meant to comment on or change the current practice for requesting or obtaining computer equipment for local office staff.

REMOTE ACCESS:

OCS will grant remote access accounts on either a long-term or short-term basis. A long-term account is valid for one year and is for a recurring situation that requires the IV-D worker to have continuous access outside of the workplace. A short-term account is valid for three months and is for a situation that requires the IV-D worker to have temporary access outside of the workplace.

¹ The IV-D worker will still need to gain approval from their local information technology (IT) department for remote access to the county network.

Valid situations include:

- A worker assigned to a satellite office on an ongoing basis and standard access is not available.
- A worker on temporary medical leave is the only worker able to complete specific work for the office (e.g. interstate work).

Invalid situations may include:

- A worker has an adjusted schedule that includes working from home and needs MiCSES to fulfill their assignments.
- A worker wants access to MiCSES on a laptop for the convenience of access outside of the designated workplace.

CONDITIONS OF APPROVAL:

The IV-D worker must have access to MiCSES before submitting a request for remote access. The IV-D worker must sign the *MiCSES Request for Remote Access* (FIA-394, see attachment 1) defining the security measures that must be followed. The FIA-394 contains the following conditions — the permitted user must:

- **Not** print or download any information contained within MiCSES;
- **Not** permit anyone access to the computer that runs MiCSES;
- **Not** permit anyone to view the screen while MiCSES runs (laptop computers included);
- Store the computer running MiCSES in a locked and secure area; and
- Only run MiCSES on an agency-owned computer.

Note: Any violation of these security measures is cause for immediate termination of the remote access account.

Pursuant to Internal Revenue Service (IRS) Publication 1075, the IV-D worker must use an agency/county-owned computer to access MiCSES. The local IV-D agency is responsible for supplying the IV-D worker with the necessary hardware. In addition, the local IV-D agency must provide the necessary access and connection costs (e.g., virtual private network (VPN) with SecurID access and digital subscriber line (DSL) or cable modem).

The Department of Information Technology's Office of Enterprise Security will conduct periodic security audits of remote access sites. If the permitted user violates any of the above security measures, OCS will immediately terminate the remote access account. All remote access sites are also subject to IRS security audits.

APPLICATION FOR REMOTE ACCESS:

The IV-D office requesting remote access for an employee must submit the FIA-394 form. The form requests the following information:

- Name and job title of IV-D worker;
- Reason remote access is needed;
- Type of account requested (i.e., long- or short-term);
- Address, phone number, and description of remote access site; and
- FOC/PA IV-D Contact's² or authorized requester's name and signature.

The IV-D worker and the IV-D worker's FOC/PA IV-D Contact or authorized requester must read and sign the FIA-394.

Mail or fax the FIA-394 to:

Michigan Family Independence Agency
 Office of Child Support
 Attn: Program Development Division
 P.O. Box 30748
 Lansing, MI 48909-7978
 Fax: (517) 373-4980

OCS staff will respond to remote access requests within 30 days. If remote access is granted, OCS staff will contact the IV-D worker and log a Child Support Enforcement System (CSES) Hotline ticket under the requester's name within one business day. The requesting office will be contacted to arrange for installation of MiCSES at the remote site.

LEGAL REFERENCES:

Federal
 45 CFR 95.621(f)(ii)(D)
 20 CFR 603.5
 20 CFR 603.7
 IRS Publication 1075
 IRS Manual 11.3.33.2

State
 MCL 400.234
 MCL 421.11

AT MAINTENANCE: Retain until further notice.

EFFECTIVE DATE: Upon receipt

² The FOC/PA IV-D Contact was previously known as the Local Project Coordinator (LPC).

REVIEW PARTICIPANTS:

Virginia Hambric, MiCSES Project Staff
Carol Webber, MiCSES Project Staff
Jim Fricke, MiCSES Project Staff
Duane Noworyta, FIA-Office of Child Support
Darrell Dontje, Enterprise Security
Establishment Work Improvement Team
Dave Clagett, Prosecuting Attorney Association of
Michigan
Jeff Albaugh, Friend of the Court Association
Steve Capps, State Court Administrative Office,
Friend of the Court Bureau

CONTACT PERSON:

Ian Broughton
OCS Policy Analyst
(517) 241-5034
broughtoni@michigan.gov

ENCLOSURE:

MiCSES Request for Remote Access (FIA-394)

CC:

Darrell Dontje, Office of Enterprise Security

MFS/IB



Michigan Child Support Enforcement System (MiCSES) Request for Remote Access

Last Name:	First Name:	Employee's Work Email Address:
Address of Remote Access Site:		Phone Number of Remote Access Site:
Department:		Title:
IV-D Agency Name:		County:
Brief Description of Remote Access Site (e.g., locked doors, window access, wall materials, etc.)		
Reason Remote Access Is Needed:		
FOC/PA IV-D Contact:		FOC/PA IV-D Contact's Phone:
*FOC/PA IV-D Contact Signature:		Date Signed:

Access Requested: Long-term (1 year) Short-term (3 months)

As a user of MiCSES, I accepted and agreed to the following:

1. **To use MiCSES to perform only my IV-D child support job functions and not to perform any other functions not permitted under IV-D regulations.**
2. To comply with the State of Michigan Computer Crime Laws (1979 PA 53).
3. To safeguard and not divulge confidential information obtained from MiCSES (42USC 654A[d] & 45 CFR 307.13).
4. To keep confidential the MiCSES access codes issued to me.
5. To report to the child support system director any threat to or violation of system security.
6. To comply with State of Michigan Telecommunications Network Acceptable Use Policy (DMB Administrative Procedure 1460.00) and FIA-NET Acceptable Use Policies and Guidelines.

In addition to the above conditions, I also accept and agree to the following conditions pertaining to remote access:

1. To not print any information contained within MiCSES.
2. To not download any information contained within MiCSES.
3. To store the computer that runs MiCSES in a locked and secure area.
4. To not permit anyone access to the computer that runs MiCSES.
5. To not permit anyone to view the screen while MiCSES runs.
6. To only run MiCSES on an agency-owned computer.

I have read the above security agreement. I understand it, and I agree to comply with its contents. Further, I understand any violation of its contents may result in termination of access privileges and/or recommendation for prosecution.

*Employee Signature:	Office Location:	Office Phone:	Date:
----------------------	------------------	---------------	-------

FOR OCS USE ONLY

COMPUTER ACCESS WILL NOT BE GRANTED UNLESS:

- All required (*) signatures are on the form.
- The user has already obtained a MiCSES user account.
- OCS deems this remote access account necessary for the operation of the IV-D program.

Analyst Initials: _____ Today's Date: _____

APPENDIX E7 – IV/D (Child Support) SECURITY REFERENCES

Freedom of Information Act:

Michigan Compiled Law (MCL 15.232 (d)(v) [MCL 15.232\(d\)\(v\)](#), [MCL 15.235](#),
[MCL 15.241](#)

Office of Child Support Act:

[MCL 400.234](#) (Information or Records from Other Agencies)

[MCL 400.235](#) (Availability and Purposes of Information)

Social Welfare Act:

[MCL 400.64](#) (Records Maintenance and Disclosure of Information)

Michigan Employment Security Act:

[MCL 421.11](#) (Disclosure of Information)

[MCL 421.54](#) (Penalties)

Friend of the Court Act:

[MCL 552.509\(5\)](#) (Providing Statement of Account to Parties)

[MCL 552.517\(b\)\(4\)](#) (Availability of Documents)

[MCL 552.518\(6\)](#) (Information from Employer or Former Employer Relative to Parent)

Unemancipated Minors; Parental Rights [MCL 722.2](#)

Status of Minors and Child Support [MCL 722.3](#)

[Child Support Manual](#) (CSM) 500

[Combined Policy Manual](#) item 4DM 135

Federal Provisions:

Title 42 Public Health and Welfare

Federal Parent Locator Services (FPLS):42 United States Code 653(b) [42 USC 653\(b\)](#) (Disclosure of Information)

[42 USC 653\(l\)](#) (Restriction on Disclosure and Use)

State plan for child and spousal support

[42 USC 654A\(f\)](#) (Automated Data Processing, Information Comparisons and Other Disclosure of Information)

Use of Federal Parent Locator Service in connection with enforcement or determination of child custody in cases of parental kidnaping of child
[42 USC 663](#) (Use of FPLS in Connection with Enforcement or Determination of Child Custody in Cases of Parental Kidnapping of Child)

Collection and reporting of child support enforcement data

[42 USC 669a\(b\)](#) (Prohibition of Disclosure of Financial Record Obtained by State Child Support Enforcement Agency)

Title 20 Employees' Benefits: Income and Eligibility Verification System:

[20 CAR 603.5](#) (Disclosure of Information)

[20 CAR 603.7](#) (Protection of Confidentiality)

Title 45 Public Welfare

[45 CAR 205.50](#) (Safeguarding Information for the Financial Assistance Programs)

[45 CAR 302.34](#) (Cooperative Agreements)

[45 CAR 302.35](#) (State Parent Locator Service (FPLS))

[45 CAR 303.15](#) (Agreements to Use FPLS in Parental Kidnapping and Child Custody of Visitation Cases)

[45 CAR 303.70](#) (Requests by FPLS for Information from the FPLS)

[IRS Publication 1075](#) (Tax Information Security Guidelines for Federal, State, and Local Agencies)

TITLE 26 INTERNAL REVENUE CODE

[26 USC 6103](#) (Confidentiality and Disclosure of Returns and Return Information)