Safeguarding Child Support Data in the Information Age

Building Strong Families Through Innovation

WICSEC

Spokane, Washington | October 6th - 10th

Three Critical Data Security Goals

1. **CONFIDENTIALITY** – prevent unauthorized disclosure of information
2. **INTEGRITY** – ensure that data cannot be modified in an unauthorized manner
3. **AVAILABILITY** – make information readily available for authorized users

WICSEC

Personally Identifiable Information (PII)

- PII can be used to distinguish or trace a person's identity or can be linked to a specific individual.
- PII includes but is not limited to:
  - Social Security number
  - Name, email, home address, phone number
  - Driver's license or state ID number
  - Passport number
  - Alien registration number
  - Financial account number
  - Biometric identifiers (such as fingerprints, iris/retina scans, or facial patterns)

WICSEC

How to Secure Federal and State Data

In Electronic Format:

- Access sensitive data only on approved devices, such as encrypted laptops (federal employees) or properly secured state computers with updated security patches.
- Encrypt all email containing sensitive data using Personal Identity Verification (PIV) credentials for federal employees or encryption software tools for state employees.

WICSEC

Child Support Portal

- Used by states and other partners to provide access to web-based tools and functions that support the OCSE mission
- Includes tools, data collection functions, query functions, and data exchange functions to resolve some of the problems caused by interstate movement of custodial parties and noncustodial parents.
- Increases establishment or modification of paternity and support obligations and enforcement of support orders by identifying information about persons involved in interstate child support enforcement cases

WICSEC

Protecting Child Support Data

WICSEC

Protecting FPLS Data

- Safeguard and protect information in both electronic and paper format.
- Grant access on a need-to-know basis
  - Provide necessary permission to achieve assigned tasks
  - Prevent potential harmful disclosure of data by separating duties and identifying privileges
- Prevent data breaches — they can harm the integrity and reputation of your agency

WICSEC

Security of Child Support Data

- Log-in Security
- Password Security
- Emailing
- Faxing
- Storing
- Mailing
- Destroying
- Incident Reporting and Responsibilities
- Incident Examples

WICSEC

Log-in Security

- **Use federal or state furnished equipment** whenever possible
  - More secure
- If remote, **always use a secure wireless network**
  - Not public Wi-Fi such as that offered at coffee shops, airports, or hotels
  - Hackers can "Wi-Fi sniff" to steal sensitive data from your device
- **Use a Virtual Private Network (VPN).**
  - Encrypts your connection to a server
  - Allows you to access a private network yet share data remotely through the public network
  - Protects sensitive data on your device

WICSEC

Password Security

- Use a strong, complex password
- Change your passwords frequently. If system admin is set — you are automatically prompted
- Do not use the same password twice or for multiple accounts

Note: States handle their own registration, and there is a secure connection between states and OCSE

- Role-based access control
- Proxy server connectivity

WICSEC

Emailing

- Always use encryption when emailing FPLS information to another party even if the recipient is within your network
- Use FIPS 140-2 compliant encryption software
- Include the information in an encrypted attachment, never in the main body of the email
- Send the passcode to decrypt the attachment via phone call, text message, or voicemail

WICSEC

Faxing

- Notify the recipient of the incoming fax before sending
- Include a disclaimer notice on the fax cover sheet
- Remain at fax machine until documents are transmitted
- Advise recipient to wait at the fax machine to receive documents
- Tell recipient to notify you if there is a transmission delay

WICSEC

Storing

- Never store FPLS information on your personal computer
- Never store FPLS information on portable media unless it is encrypted with FIPS140-2 compliant encryption
- Never store FPLS information on your shared network drives

WICSEC

Mailing

- Seal content in an interior envelope that's marked. “Confidential, To Be Opened by Designated Official Only”
- Put interior enveloped into exterior envelope and double seal it
- Send FPLS information via UPS, FedEx, or courier with package tracking software
- Monitor package while in transit
- Notify recipient of incoming documents
- Have recipient notify you if the package does not arrive in a timely manner

WICSEC

Destroying

- Place documents in secured shred containers
- Shred documents using a cross cut shredder
- Destroy electronic media using a media destruction machine
- Erase electronic records so no FPLS information remains

Destroy physical and electronic records when you are done with them!

Spokane, Washington
October 6 - 10th

WICSEC

Incident Reporting and Responsibilities

- Report known or suspected incidents within one hour
- Know your role and responsibilities in the reporting process
- Know the types of security incidents to report

The integrity and reputation of your agency depend on how quickly you report, manage, and resolve incidents

WICSEC

Incident Examples

- Office break-ins
- Laptop or case files theft (especially from cars)
- Malware
- Ransomware

WICSEC

Security Requirements

Security Compliance

- IRS Publication 1075
- FIPS140-2
- NIST SP 800-53
- 45 CFR 303.21- Safeguarding and Disclosure of Confidential Information
- Automated Systems for Child Support Enforcement: A Guide for States - OCSE
- Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration

WICSEC

Questions

Contact Info

Derek Cullum

Cyber Security Engineer

(202) 690-0029

Linda Boyer

Director, Division of Federal System

(202) 401-5410

WICSEC