

Department of Health and Human Services

# Security Self-Assessment Tool

Tribal IV-D Agencies Receiving FPLS Information

Administration for Children and Families, Office of Child Support Enforcement  
6/30/2016

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**Contents**

Overview..... 2  
Access Control (AC)..... 3  
Awareness and Training (AT) ..... 8  
Audit and Accountability (AU) ..... 10  
Security Assessment and Authorization (CA) ..... 13  
Configuration Management (CM) ..... 16  
Contingency Planning (CP) ..... 18  
Identification and Authentication (IA)..... 21  
Incident Response (IR) ..... 24  
Maintenance (MA)..... 27  
Media Protection (MP) ..... 29  
Physical and Environmental Protection (PE)..... 31  
Planning (PL) ..... 34  
Personnel Security (PS) ..... 36  
Risk Assessment (RA) ..... 39  
System and Service Acquisition (SA)..... 41  
System and Communications Protection (SC)..... 44  
System and Information Integrity (SI)..... 49

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

## Overview

The federal Office of Child Support Enforcement (OCSE), Division of Federal Systems, developed a tribal IV-D Self-Assessment Tool to assist tribal IV-D agencies assess and document compliance with OCSE's security requirements. The tool provides two important functions to tribal agencies:

1. It can be used by an independent assessor or assessment teams to conduct impartial assessments of the tribal agency's information systems.
2. It can strengthen the tribal agencies' security program by identifying weaknesses and vulnerabilities.

We based this tool on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, "[Security and Privacy Controls for Federal Information Systems and Organizations](#)," updated January 22, 2015, (NIST SP 800-53 Rev 4) and our security agreements with tribal IV-D agencies. We organized the tool to comply with the 17 "control families" found in NIST SP 800-53 Rev 4.

The tool includes assessment questions addressing the requirements in the OCSE security agreements with tribal IV-D agencies as well as most of the NIST SP 800-53 Rev 4 security controls from the moderate catalog.

Depending on the level of your computing systems and technology, not all tribal IV-D agencies will be able to provide responses to some of the controls within this document. If that is the case, provide a N/A (not applicable) in the response box next to the control.

While we do not require tribal IV-D agencies to use this tool or submit this assessment to us, we recommend using this as a guide to assess your security posture using an independent assessor or assessment team who are individuals or groups who conduct impartial assessments of organizational information systems. Impartially implies that assessors are free from any perceived or actual conflicts of interests with regard to development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness.

We will update and redistribute this tool when federal security requirements and guidelines change. If you have questions, please contact Linda Boyer, Data Access and Security Manager, at [linda.boyer@acf.hhs.gov](mailto:linda.boyer@acf.hhs.gov) or 202-401-5410.

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**Access Control (AC)**

<b>ACCESS CONTROL</b>	<b>ASSESSMENT RESULTS</b>
<p>Does your tribal IV-D agency have formal access control policies and procedures in place?            Do you review and update the procedures annually?</p> <p>NIST SP 800-53 Rev 4, AC-1</p>	
<p>Does your tribal IV-D agency have policies and practices to establish and monitor system accounts?            Do account managers approve, review, and monitor accounts?            Does the system disable accounts automatically after a prescribed period of inactivity?</p> <p>NIST SP 800-53 Rev 4, AC-2</p>	
<p>Are mandatory access control procedures in place limiting the permissible actions of authorized users?</p> <p>NIST SP 800-53 Rev 4, AC-3</p>	
<p>Does the tribal IV-D agency control the flow of information within the system and networks?</p> <p>NIST SP 800-53 Rev 4, AC-4</p>	
<p>Does the tribal IV-D agency separate the following duties: 1) data creation and control, 2) software development and maintenance, and 3) security functions to prevent the abuse of privilege and reduce the risk of collusion?</p> <p>NIST SP 800-53 Rev 4, AC-5</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>ACCESS CONTROL</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the tribal IV-D agency use the principles of least privilege to ensure only authorized users have access to the information needed to perform their work?  Do information system processes operate at a privilege level no higher than necessary?  Are activities by privileged users audited?</p> <p>NIST SP 800-53 Rev 4, AC-6</p>	
<p>Does the tribal IV-D agency enforce lockout after a predefined number of consecutive invalid logon attempts?  Are users locked out for a defined time period after unsuccessful attempts?</p> <p>NIST SP 800-53 Rev 4, AC-7</p>	
<p>Are privacy and security notices consistent with applicable laws, directives, policies, and regulations displayed before users are permitted to login?</p> <p>NIST SP 800-53 Rev 4, AC-8</p>	
<p>Is the information on the user display concealed when the session is locked?</p> <p>NIST SP 800-53 Rev 4, AC-11</p>	
<p>Does the system automatically terminate a user session after 30 minutes of inactivity?</p> <p>NIST SP 800-53 Rev 4, AC-12</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>ACCESS CONTROL</b>	<b>ASSESSMENT RESULTS</b>
<p>Has the tribal IV-D agency defined the actions that can be performed on the information system without identification or authentication?</p> <p>NIST SP 800-53 Rev 4, AC-14</p>	
<p>Does the tribal IV-D agency control remote access through managed network access points?  Does the agency employ a Network Access Control (NAC) solution to enforce security policies for remote users?</p> <p>NIST SP 800-53 Rev 4, AC-17(1)</p>	
<p>Are remote access sessions encrypted?</p> <p>NIST SP 800-53 Rev 4, AC-17(2)</p>	
<p>Does the tribal IV-D agency require authorization for wireless access before allowing such connections?  Is wireless access encrypted?</p> <p>NIST SP 800-53 Rev 4, AC-18</p>	
<p>Does the tribal IV-D agency require full-device encryption or container based encryption for mobile devices to protect the confidentiality and integrity of information?</p> <p>NIST SP 800-53 Rev 4, AC-19</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

ACCESS CONTROL	ASSESSMENT RESULTS
<p>Does the tribal IV-D agency require a written agreement before users may access the information system from an external system?</p> <p>Does the tribal IV-D agency require a written agreement before users may process, store, or transmit agency information on an external system?</p> <p>Does the tribal IV-D agency require written approval before users may access system resources from non-tribal agency furnished equipment (for example, personally owned and contractor furnished)?</p> <p>Does the tribal IV-D agency prohibit the use of digital media and computing and communications devices resident in commercial or public facilities (for example, hotels, convention centers, and airports) from accessing, transmitting, or storing NDNH information?</p> <p>NIST SP 800-53 Rev 4, AC-20</p>	
<p>Do authorized users receive training and guidance before sharing restricted information with partners?</p> <p>NIST SP 800-53 Rev 4, AC-21</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>ACCESS CONTROL</b>	<b>ASSESSMENT RESULTS</b>
<p>Are designated individuals trained on what information can be posted to a publicly accessible information system? Is public information reviewed before posting and every two weeks thereafter to be sure non-public information is not present?</p> <p>NIST SP 800-53 Rev 4, AC-22(1)</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**Awareness and Training (AT)**

<b>AWARENESS AND TRAINING</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the tribal IV-D agency have written security and privacy awareness and training policies and procedures?  Do you review and update the procedures annually?</p> <p>NIST SP 800-53 Rev 4, AT-1</p>	
<p>Are new employees trained on security and privacy awareness before accessing the tribal agency's systems and information or performing assigned duties?</p> <p>NIST SP 800-53 Rev 4, AT-2</p>	
<p>Is refresher security and privacy awareness training conducted at least annually?</p> <p>NIST SP 800-53 Rev 4, AT-2</p>	
<p>Does security and privacy awareness training include information on how to respond to suspected security incidents?</p> <p>NIST SP 800-53 Rev 4, AT-2</p>	
<p>Does security and privacy awareness training include information on recognizing and reporting indicators of insider threat?</p> <p>NIST SP 800-53 Rev 4, AT-2(2)</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>AWARENESS AND TRAINING</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the tribal IV-D agency provide role-based security and privacy awareness training to all users with significant security roles and responsibilities (for example, security officers, executive staff, and IT administrators) before granting access to the system?</p> <p>NIST SP 800-53 Rev 4, AT-3</p>	
<p>Does the tribal IV-D agency provide refresher role-based training to all users with significant security roles and responsibilities (for example, managers, executive staff, and IT administrators) annually?</p> <p>NIST SP 800-53 Rev 4, AT-4</p>	
<p>Does the tribal IV-D agency maintain security and privacy awareness refresher training and role-based security training records (for example, sign-in-sheets) as proof of attendance?</p> <p>NIST SP 800-53 Rev 4, AT-4</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**Audit and Accountability (AU)**

<b>AUDIT AND ACCOUNTABILITY</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the tribal IV-D agency have formal audit and accountability policies and procedures in place?</p> <p>NIST SP 800-53 Rev 4, AU-1</p>	
<p>Are the auditable events defined and periodically reviewed and updated?</p> <p>Are the following events tracked?</p> <ul style="list-style-type: none"> <li>• Server startup and shutdown</li> <li>• Loading and unloading of services</li> <li>• Installation and removal of software</li> <li>• System alerts and error messages</li> <li>• User logon and logoff</li> <li>• System administration activities</li> <li>• Accesses to sensitive information, files, and systems</li> <li>• Account creation, modification, or deletion</li> <li>• Modifications of privileges and access controls</li> </ul> <p>NIST SP 800-53 Rev 4, AU-2</p>	
<p>Does the system generate audit records that include the type of event, the date and time of event, where the event occurred, the source of the event, the outcome of the event, and the identity of individuals or subjects associated with the event?</p> <p>NIST SP 800-53 Rev 4, AU-3</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>AUDIT AND ACCOUNTABILITY</b>	<b>ASSESSMENT RESULTS</b>
<p>Is sufficient data storage allocated to reduce the probability that the audit storage allocation will be exceeded?</p> <p>NIST SP 800-53 Rev 4, AU-4</p>	
<p>Are personnel automatically alerted to audit processing failures?</p> <p>NIST SP 800-53 Rev 4, AU-5</p>	
<p>Do appropriate personnel review the audit records at least weekly for indications of inappropriate or unusual activity?  Are audit reports generated using automated tools?</p> <p>NIST SP 800-53 Rev 4, AU-6</p>	
<p>Can you manipulate your audit reports based on events of interest without altering the content of the logs?</p> <p>NIST SP 800-53 Rev 4, AU-7</p>	
<p>Are internal system clocks used to generate the time stamps for audit records?  Are they re-synched with an authoritative time source (for example, NTP server) regularly?</p> <p>NIST SP 800-53 Rev 4, AU-8</p>	
<p>Does the information system protect audit information and audit tools from unauthorized access, modification, and deletion?  Does the tribal IV-D agency restrict access to the audit logs to specific security personnel, the security officer, and designated administrators?</p> <p>NIST SP 800-53 Rev 4, AU-9</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
**TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL**

<b>AUDIT AND ACCOUNTABILITY</b>	<b>ASSESSMENT RESULTS</b>
Does the tribal IV-D agency document and adhere to audit record retention times including the retention of records involved in reported incidents?  NIST SP 800-53 Rev 4, AU-11	
Is the system capable of generating audit logs with the auditable events defined in AU-2 and the content defined in AU-3?  NIST SP 800-53 Rev 4, AU-12	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**Security Assessment and Authorization (CA)**

<b>SECURITY ASSESSMENT AND AUTHORIZATION</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the tribal IV-D agency have formal security assessment and authorization policies and procedures in place to manage the information and information system security posture?</p> <p>Does the tribal IV-D agency review and update the security assessment and authorization policies and procedures annually?</p> <p>NIST SP 800-53 Rev 4, CA-1</p>	
<p>Does the security assessment plan reveal whether the security controls in place are implemented properly and operating as expected?</p> <p>Does the tribal IV-D agency conduct or participate in biennial system security reviews of installations involved in the administration of the tribal child support program?</p> <p>NIST SP 800-53 Rev 4, CA-2</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>SECURITY ASSESSMENT AND AUTHORIZATION</b>	<b>ASSESSMENT RESULTS</b>
<p>Are security control assessments conducted by an independent assessor?</p> <p>Does an independent assessor conduct a security control assessment at least every five years?</p> <p>NIST SP 800-53 Rev 4, CA-2(1)</p>	
<p>Are interconnection security agreements executed when connecting internal information systems to other internal and external information systems?</p> <p>NIST SP 800-53 Rev 4, CA-3</p>	
<p>Does the interconnection policy include a “deny all, permit by exception” provision for external system connections?</p> <p>NIST SP 800-53 Rev 4, CA-3(5)</p>	
<p>Does the tribal IV-D agency maintain a plan of action and milestones (POA&amp;M) or other corrective action plan to identify, assess, prioritize, and monitor the progress of corrective actions taken to mitigate information and information system weakness?</p> <p>NIST SP 800-53 Rev 4, CA-5</p>	
<p>Is the POA&amp;M tracked, maintained, reviewed, and validated at least quarterly?</p> <p>NIST SP 800-53 Rev 4, CA-5</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>SECURITY ASSESSMENT AND AUTHORIZATION</b>	<b>ASSESSMENT RESULTS</b>
<p>Does a tribal IV-D agency official review the information system security controls periodically or when major changes occur and accept the residual risks?  NIST SP 800-53 Rev 4, CA-6</p>	
<p>Is a continuous monitoring strategy and program in place to safeguard the information and information system?  NIST SP 800-53 Rev 4, CA-7</p>	
<p>Does the appropriate tribal IV-D agency official receive reports periodically on the security posture of the information and system?  NIST SP 800-53 Rev 4, CA-7</p>	
<p>Are security controls for information and information systems monitored on a continual basis by an independent assessor?  NIST SP 800-53 Rev 4, CA-7(1)</p>	
<p>Does the tribal IV-D agency individually authorize internal connections of information system components (for example, intra-system connections: mobile devices, printers, and servers)?  NIST SP 800-53 Rev 4, CA-9</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**Configuration Management (CM)**

<b>CONFIGURATION MANAGEMENT</b>	<b>ASSESSMENT RESULTS</b>
Does the tribal IV-D agency have formal configuration management policies and procedures in place?  NIST SP 800-53 Rev 4, CM-1	
Are configuration management baselines in place and maintained?  NIST SP 800-53 Rev 4, CM-2	
Are system changes tested, validated, and documented under configuration control before implementation?  NIST SP 800-53 Rev 4, CM-3	
Is a security impact analysis conducted before changes?  NIST SP 800-53 Rev 4, CM-4	
Is access to the information system limited to prevent unauthorized changes to the system?  NIST SP 800-53 Rev 4, CM-5	
Are system configuration settings monitored and controlled according to policy?  NIST SP 800-53 Rev 4, CM-6	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>CONFIGURATION MANAGEMENT</b>	<b>ASSESSMENT RESULTS</b>
<p>Are unnecessary and nonsecure functions, ports, protocols, and services identified and disabled?</p> <p>NIST SP 800-53 Rev 4, CM-7</p>	
<p>Are automated tools used to update the system inventory?</p> <p>NIST SP 800-53 Rev 4, CM-8</p>	
<p>Is there a configuration management plan in place that addresses roles, responsibilities, and configuration management processes and procedures?</p> <p>NIST SP 800-53 Rev 4, CM-9</p>	
<p>Are software and associated documentation only used in accordance with contract agreements and copyright laws?</p> <p>NIST SP 800-53 Rev 4, CM-10</p>	
<p>Do tribal IV-D agency policies restrict users from installing software?</p> <p>NIST SP 800-53 Rev 4, CM-11</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**Contingency Planning (CP)**

<b>CONTINGENCY PLANNING</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the tribal IV-D agency have formal contingency planning policies and procedures in place?</p> <p>Are the policies and procedures updated annually?</p> <p>NIST SP 800-53 Rev 4, CP-1</p>	
<p>Is the system contingency plan coordinated with related plans, such as the disaster recovery plan, the business continuity plan, and the incident response plan?</p> <p>NIST SP 800-53 Rev 4, CP-2(1)(3)(8)</p>	
<p>Does the tribal IV-D agency provide contingency plan training as required?</p> <p>NIST SP 800-53 Rev 4, CP-3</p>	
<p>Does the tribal IV-D agency test the contingency plan annually and take remedial action based on test results?</p> <p>NIST SP 800-53 Rev 4, CP-4</p>	
<p>Has the tribal IV-D agency established an alternate storage site, separate from the primary site, with equivalent security controls? In the event of an area wide disturbance, is the alternate site accessible?</p> <p>NIST SP 800-53 Rev 4, CP-6(1)(3)</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>CONTINGENCY PLANNING</b>	<b>ASSESSMENT RESULTS</b>
<p>Has the tribal IV-D agency established an alternate processing site, separate from the primary site, with equivalent security controls?            In the event of an area wide disturbance, is the alternate site accessible?            Can the system be recovered within the agency-defined Recovery Time Objective (RTO)?</p> <p>NIST SP 800-53 Rev 4, CP-7(1)(2)(3)</p>	
<p>Has the tribal IV-D agency established alternate telecommunications services to eliminate a single point of failure and permit the resumption of operations within the agency-defined RTO?</p> <p>NIST SP 800-53 Rev 4, CP-8(1)(2)</p>	
<p>Is the tribal IV-D agency backup user, system, and security documentation consistent with the requirements of the tribal agency's Recovery Point Objective (RPO)?            Does the tribal IV-D agency ensure the security of the backup information?            Does the tribal IV-D agency test the validity of the backups at least annually?</p> <p>NIST SP 800-53 Rev 4, CP-9(1)</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>CONTINGENCY PLANNING</b>	<b>ASSESSMENT RESULTS</b>
Has the tribal IV-D agency developed formal reconstitution plans to restore the system to a known state, including transaction recovery?  NIST SP 800-53 Rev 4, CP-10(2)	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**Identification and Authentication (IA)**

<b>IDENTIFICATION AND AUTHENTICATION</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the tribal IV-D agency have identification and authentication policies and procedures in place?  Are they reviewed and updated annually?</p> <p>NIST SP 800-53 Rev 4, IA-1</p>	
<p>Are users identified and authenticated before access is allowed to information systems and resources?</p> <p>NIST SP 800-53 Rev 4, IA-2</p>	
<p>Is multifactor authentication used for network access to privileged accounts?</p> <p>NIST SP 800-53 Rev 4, IA-2(1)(2)</p>	
<p>Are replay-resistant authentication mechanisms (for example, nonce, one-time password, and time stamps) used for network access to privileged accounts?</p> <p>NIST SP 800-53 Rev 4, IA-2(8)</p>	
<p>Is multifactor authentication used for remote access to nonprivileged and privileged accounts?</p> <p>NIST SP 800-53 Rev 4, IA-2(11)</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>IDENTIFICATION AND AUTHENTICATION</b>	<b>ASSESSMENT RESULTS</b>
<p>Are devices identified and authenticated before establishing a connection?</p> <p>NIST SP 800-53 Rev 4, IA-3</p>	
<p>Does a tribal IV-D agency official (for example, supervisor) authorize assignment of user or device identifiers?</p> <p>NIST SP 800-53 Rev 4, IA-4</p>	
<p>Are identifiers selected that uniquely identify a user or device?</p> <p>NIST SP 800-53 Rev 4, IA-4</p>	
<p>Are user and device identifiers prevented from reuse based on a defined period (for example, three years)?</p> <p>NIST SP 800-53 Rev 4, IA-4</p>	
<p>Does the system disable user identifiers after a defined period of inactivity (for example, 30 days)?</p> <p>NIST SP 800-53 Rev 4, IA-4</p>	
<p>Do passwords require a minimum complexity (for example, one character from the four character categories [A-Z, a-z, 0-9, special characters])?</p> <p>NIST SP 800-53 Rev 4, IA-5(1)</p>	
<p>Do passwords require a minimum number of changed characters (for example, eight) when creating a new password?</p> <p>NIST SP 800-53 Rev 4, IA-5(1)</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>IDENTIFICATION AND AUTHENTICATION</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the information system prohibit the reuse of a password for 24 generations?</p> <p>NIST SP 800-53 Rev 4, IA-5(1)</p>	
<p>Does the information system require an immediate password change from the temporary password to a permanent password during initial system login?</p> <p>NIST SP 800-53 Rev 4, IA-5(1)</p>	
<p>Is the password obscured during the authentication process to protect the information from possible view and exploitation by unauthorized individuals?</p> <p>NIST SP 800-53 Rev 4, IA-6</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**Incident Response (IR)**

<b>INCIDENT RESPONSE</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the tribal IV-D agency have documented incident response policies and procedures?  Are the incident response policies and procedures reviewed and updated annually?</p> <p>NIST SP 800-53 Rev 4, IR-1</p>	
<p>Is incident response training provided to all users annually?  Is the training consistent with assigned roles and responsibilities?</p> <p>NIST SP 800-53 Rev 4, IR-2</p>	
<p>Are incident response exercises conducted when needed and at least annually?</p> <p>NIST SP 800-53 Rev 4, IR-3</p>	
<p>Are tests or exercises conducted with tribal agency groups responsible for associated plans (for example, contingency plans, disaster recovery plans, and business continuity plans)?</p> <p>NIST SP 800-53 Rev 4, IR-3(2)</p>	
<p>Is the incident handling capability implemented based on the tribal IV-D agency's business processes supporting systems and information?</p> <p>NIST SP 800-53 Rev 4, IR-4</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>INCIDENT RESPONSE</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the tribal IV-D agency use automated mechanisms (for example, online incident management systems) to support incident-handling processes?</p> <p>NIST SP 800-53 Rev 4, IR-4(1)</p>	
<p>Are incidents and suspected incidents monitored, documented, and tracked until resolved?</p> <p>NIST SP 800-53 Rev 4, IR-5</p>	
<p>Does the tribal IV-D agency have procedures in place to report incidents and suspected incidents of Federal Parent Locator Service (FPLS) information in either electronic or physical form to the FPLS Information Systems Security Officer within one hour of discovery?</p> <p>Does the tribal IV-D agency have procedures in place to report incidents and suspected incidents of child support confidential information in either electronic or physical form to the FPLS Information Systems Security Officer within one hour of discovery of suspected or confirmed incidents involving: 1) an unauthorized individual who obtains access, either physical or virtual, to the information systems of the tribal child support agency or 2) the unauthorized disclosure or use of personal information pertaining to multiple individuals?</p> <p>NIST SP 800-53 Rev 4, IR-6</p>	
<p>Are incidents and suspected incidents reported to the appropriate agencies per the tribal agency's requirements?</p> <p>NIST SP 800-53 Rev 4, IR-6</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>INCIDENT RESPONSE</b>	<b>ASSESSMENT RESULTS</b>
Are automated mechanisms used to support the reporting of incidents and suspected incidents?  NIST SP 800-53 Rev 4, IR-6(1)	
Do users receive help (for example, help desk) when handling and reporting incidents and suspected incidents?  NIST SP 800-53 Rev 4, IR-7	
Are automated mechanisms used to increase the availability of incident response information and support?  NIST SP 800-53 Rev 4, IR-7(1)	
Does the tribal IV-D agency have a documented incident response plan?  NIST SP 800-53 Rev 4, IR-8	
Is the incident response plan reviewed and updated annually?  NIST SP 800-53 Rev 4, IR-8	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**Maintenance (MA)**

<b>MAINTENANCE</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the tribal IV-D agency have formal policies and procedures that address the purpose, scope, roles, and responsibilities for system maintenance?</p> <p>NIST SP 800-53 Rev 4, MA-1</p>	
<p>Is all system maintenance scheduled and approved?</p> <p>NIST SP 800-53 Rev 4, MA-2(1)</p>	
<p>Are all maintenance activities monitored?  Is equipment sanitized to remove all information before being taken offsite for repair?</p> <p>NIST SP 800-53 Rev 4, MA-2(2)</p>	
<p>Are tools and diagnostic media inspected before being allowed in the facility?</p> <p>NIST SP 800-53 Rev 4, MA-3</p>	
<p>Are nonlocal maintenance and diagnostic activities documented, approved, and monitored?  Is strong authentication required?</p> <p>NIST SP 800-53 Rev 4, MA-4</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>MAINTENANCE</b>	<b>ASSESSMENT RESULTS</b>
<p>Are hardware and software maintenance personnel authorized in advance and escorted while on premises?</p> <p>Is the maintenance process documented?</p> <p>NIST SP 800-53 Rev 4, MA-5</p>	
<p>Does the tribal IV-D agency maintain spare components or have contracts in place to recover critical system security components within short timeframes to minimize the risk to the tribal agency?</p> <p>NIST SP 800-53 Rev 4, MA-6</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**Media Protection (MP)**

<b>MEDIA PROTECTION</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the tribal IV-D agency have documented media protection policies and procedures in place?  Are the media protection policies and procedures reviewed and updated annually?</p> <p>NIST SP 800-53 Rev 4, MP-1</p>	
<p>Is access to electronic (for example, external/removable hard drives, CDs, and USB drives) and hard copy (for example, printed documents) media restricted to authorized personnel?</p> <p>NIST SP 800-53 Rev 4, MP-2</p>	
<p>Is electronic (for example, external/removable hard drives, CDs, and USB drives) media with sensitive information labeled to denote the level of sensitivity of the information and limitations on distribution?</p> <p>NIST SP 800-53 Rev 4, MP-3</p>	
<p>Are hard copies of reports and documents with sensitive information labeled to denote the level of sensitivity of the information and limitations on distribution?</p> <p>NIST SP 800-53 Rev 4, MP-3</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>MEDIA PROTECTION</b>	<b>ASSESSMENT RESULTS</b>
<p>Are electronic and hard copy media with sensitive information stored in a secure location (for example, locked container) when not in use?</p> <p>NIST SP 800-53 Rev 4, MP-4</p>	
<p>Are electronic and hard copy media with sensitive information restricted from transport off premises unless approved by a tribal IV-D agency official?</p> <p>NIST SP 800-53 Rev 4, MP-5</p>	
<p>Is electronic media with sensitive information encrypted at the disk or device level before allowing transport off premises?</p> <p>NIST SP 800-53 Rev 4, MP-5(4)</p>	
<p>Are electronic and hard copy media with sensitive information destroyed or sanitized when no longer needed using an approved method (for example, purging, degaussing, shredding, or burning)?</p> <p>NIST SP 800-53 Rev 4, MP-6</p>	
<p>Does the tribal IV-D agency have automated or manual safeguards (or both) in place to restrict the use of digital and nondigital media to store sensitive information?  Are there restrictions against using digital media with no identifiable owner?</p> <p>NIST SP 800-53 Rev 4, MP-7</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**Physical and Environmental Protection (PE)**

<b>PHYSICAL AND ENVIRONMENTAL PROTECTION</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the tribal IV-D agency have documented policies and procedures that address the purpose, scope, roles, and responsibilities for physical and environmental protection?</p> <p>NIST SP 800-53 Rev 4, PE-1</p>	
<p>Does the tribal IV-D agency maintain a list of individuals with authorized access to the facility where the information system resides?</p> <p>NIST SP 800-53 Rev 4, PE-2(1)</p>	
<p>Does the tribal IV-D agency that maintains the authorized access list also issue the authorization credentials for facility access?</p> <p>NIST SP 800-53 Rev 4, PE-2</p>	
<p>Does the tribal IV-D agency control physical access to the facility by verifying the individual's authorization at access points?</p> <p>NIST SP 800-53 Rev 4, PE-3</p>	
<p>Are visitors to the controlled areas logged and escorted?</p> <p>NIST SP 800-53 Rev 4, PE-3</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>PHYSICAL AND ENVIRONMENTAL PROTECTION</b>	<b>ASSESSMENT RESULTS</b>
<p>Is access to information system distribution and transmission lines controlled?</p> <p>NIST SP 800-53 Rev 4, PE-4</p>	
<p>Is access to information system output devices controlled?</p> <p>NIST SP 800-53 Rev 4, PE-5</p>	
<p>Is physical access to the data center restricted and monitored?</p> <p>NIST SP 800-53 Rev 4, PE-6</p>	
<p>Does the tribal IV-D agency retain the facility access logs for a specified period?</p> <p>NIST SP 800-53 Rev 4, PE-8</p>	
<p>Are power equipment and cabling protected from damage and destruction?</p> <p>NIST SP 800-53 Rev 4, PE-9</p>	
<p>Are emergency power shutoff devices in use?  Is emergency power shutoff capability protected from unauthorized activation?</p> <p>NIST SP 800-53 Rev 4, PE-10</p>	
<p>Is the information system protected by short-term uninterruptible power supply?</p> <p>NIST SP 800-53 Rev 4, PE-11</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>PHYSICAL AND ENVIRONMENTAL PROTECTION</b>	<b>ASSESSMENT RESULTS</b>
<p>Does automatic emergency lighting for the information system activate in the event of a power outage?</p> <p>NIST SP 800-53 Rev 4, PE-12</p>	
<p>Are fire suppression and detection devices/systems for the information system in place and supported by an independent energy source? Does the fire suppression system activate automatically?</p> <p>NIST SP 800-53 Rev 4, PE-13</p>	
<p>Are the temperature and humidity levels monitored?</p> <p>NIST SP 800-53 Rev 4, PE-14</p>	
<p>Is the information system protected from water damage by master shutoff or isolation valves?</p> <p>NIST SP 800-53 Rev 4, PE-15</p>	
<p>Are all deliveries and removals from the facility approved and monitored?</p> <p>NIST SP 800-53 Rev 4, PE-16</p>	
<p>Are security controls at alternate work sites assessed for effectiveness?</p> <p>NIST SP 800-53 Rev 4, PE-17</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**Planning (PL)**

<b>PLANNING</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the tribal IV-D agency have documented security planning policies and procedures?            Are policies and procedures reviewed and updated annually?</p> <p>NIST SP 800-53 Rev 4, PL-1</p>	
<p>Is there a documented system security plan for information systems? Is the system security plan reviewed and updated annually?</p> <p>NIST SP 800-53 Rev 4, PL-2</p>	
<p>Are security-related activities planned and coordinated with tribal agency entities before conducting such activities (for example, security assessments, audits, or patch management) affecting the information system?</p> <p>NIST SP 800-53 Rev 4, PL-2(3)</p>	
<p>Do users sign the rules of behavior before accessing information and information systems?</p> <p>NIST SP 800-53 Rev 4, PL-4</p>	
<p>Do users re-sign rules of behavior if changes are made to the document?</p> <p>NIST SP 800-53 Rev 4, PL-4</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>PLANNING</b>	<b>ASSESSMENT RESULTS</b>
<p>Is the template for the rules of behavior reviewed and updated annually?</p> <p>NIST SP 800-53 Rev 4, PL-4</p>	
<p>Does the template for the rules of behavior prohibit posting sensitive information on public websites?</p> <p>NIST SP 800-53 Rev 4, PL-4(1)</p>	
<p>Is the information system security architecture documented?</p> <p>Is the security architecture reviewed and updated at least annually?</p> <p>NIST SP 800-53 Rev 4, PL-8</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**Personnel Security (PS)**

<b>PERSONNEL SECURITY</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the tribal IV-D agency have formal personnel security policies and procedures?            Are the personnel security policies and procedures reviewed and updated annually?</p> <p>NIST SP 800-53 Rev 4, PS-1</p>	
<p>Are risk designations assigned to all tribal agency positions with specific screening criteria for the individuals filling those positions?            Are the risk designations reviewed periodically?</p> <p>NIST SP 800-53 Rev 4, PS-2</p>	
<p>Are tribal IV-D agency employees screened before authorizing access to information and information systems?</p> <p>NIST SP 800-53 Rev 4, PS-3</p>	
<p>Are tribal IV-D agency employees rescreened according to agency-defined conditions?</p> <p>NIST SP 800-53 Rev 4, PS-3</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>PERSONNEL SECURITY</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the tribal IV-D agency disable employee access to systems and information immediately when an employee is terminated?</p> <p>NIST SP 800-53 Rev 4, PS-4</p>	
<p>Is the tribal IV-D agency's security-related property (for example, ID badges, or keys) collected when an employee is terminated?</p> <p>NIST SP 800-53 Rev 4, PS-4</p>	
<p>Does the tribal IV-D agency notify (within prescribed timeframes) appropriate managers, administrators, and physical security officials when an employee is terminated?</p> <p>NIST SP 800-53 Rev 4, PS-4</p>	
<p>Does the tribal IV-D agency modify the transferred or reassigned employee's access to information and systems within a specified timeframe (for example, 30 days from transfer)?</p> <p>NIST SP 800-53 Rev 4, PS-5</p>	
<p>Does the tribal IV-D agency collect security-related property (for example, ID badges and keys) from the transferred or reassigned tribal agency employee?</p> <p>NIST SP 800-53 Rev 4, PS-5</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>PERSONNEL SECURITY</b>	<b>ASSESSMENT RESULTS</b>
<p>Are tribal IV-D agency employees required to sign access agreements (for example, nondisclosure agreements and acceptable use agreements) before accessing information and information systems?</p> <p>NIST SP 800-53 Rev 4, PS-6</p>	
<p>Are tribal IV-D agency employees required to re-sign access agreements (for example, nondisclosure agreements and acceptable use agreements) annually or when agreements are updated?</p> <p>NIST SP 800-53 Rev 4, PS-6</p>	
<p>Do third-party providers (for example, contractors, external information technology services, or outsourced entities) working on behalf of the tribal IV-D agency comply with personnel security requirements?</p> <p>NIST SP 800-53 Rev 4, PS-7</p>	
<p>Are tribal IV-D agency employees advised of sanctions (during training or on nondisclosure agreements) for noncompliance with federal and/or tribal agency policies, procedures, standards, and guidance?  Are tribal IV-D agency employees sanctioned for noncompliance?</p> <p>NIST SP 800-53 Rev 4, PS-8</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**Risk Assessment (RA)**

<b>RISK ASSESSMENT</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the tribal IV-D agency document formal risk assessment policies and procedures?            Are the risk assessment policies and procedures reviewed and updated annually?</p> <p>NIST SP 800-53 Rev 4, RA-1</p>	
<p>Are information and information systems categorized based on the potential adverse impact of loss of confidentiality, integrity, or availability?</p> <p>NIST SP 800-53 Rev 4, RA-2</p>	
<p>Are risk assessments conducted on information and information systems?</p> <p>NIST SP 800-53 Rev 4, RA-3</p>	
<p>Are risk assessment results included in other tribal agency security documents (for example, security plan or risk assessment report)?</p> <p>NIST SP 800-53 Rev 4, RA-3</p>	
<p>Are risk assessment reports reviewed annually and disseminated to appropriate tribal agency officials?</p> <p>NIST SP 800-53 Rev 4, RA-3</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>RISK ASSESSMENT</b>	<b>ASSESSMENT RESULTS</b>
<p>Are risk assessments reports updated before implementing major changes to the system or every three years, whichever comes first?</p> <p>NIST SP 800-53 Rev 4, RA-3</p>	
<p>Does the tribal IV-D agency use appropriate vulnerability scanning tools and techniques to scan the system periodically (for example, monthly) and when changes occur?</p> <p>NIST SP 800-53 Rev 4, RA-5</p>	
<p>Does the tribal IV-D agency analyze and share vulnerability scanning results with appropriate tribal agency officials to remediate vulnerabilities in the information systems?</p> <p>NIST SP 800-53 Rev 4, RA-5</p>	
<p>Are vulnerability scanning tools readily updated as new vulnerabilities are discovered?</p> <p>NIST SP 800-53 Rev 4, RA-5(1)</p>	
<p>Are information systems scanned when vulnerability scanning tools are updated?</p> <p>NIST SP 800-53 Rev 4, RA-5(2)</p>	
<p>Is privileged access authorization required to conduct vulnerability scanning?</p> <p>NIST SP 800-53 Rev 4, RA-5(5)</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**System and Service Acquisition (SA)**

<b>SYSTEM AND SERVICE ACQUISITION</b>	<b>ASSESSMENT RESULTS</b>
<p>Are there formal access control policies and procedures for system acquisition and services?</p> <p>NIST SP 800-53 Rev 4, SA-1</p>	
<p>Are requirements defined and resources allocated as part of the capital planning and investment process (or tribal process equivalent)?</p> <p>NIST SP 800-53 Rev 4, SA-2</p>	
<p>Does the tribal IV-D agency use a defined development life-cycle methodology with defined security roles and responsibilities?</p> <p>NIST SP 800-53 Rev 4, SA-3</p>	
<p>Are information system developers required to implement and document security functional and assurance requirements?</p> <p>NIST SP 800-53 Rev 4, SA-4</p>	
<p>Are information system developers required to provide a description of the functional properties of the security controls?</p> <p>NIST SP 800-53 Rev 4, SA-4(1)</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>SYSTEM AND SERVICE ACQUISITION</b>	<b>ASSESSMENT RESULTS</b>
<p>Are information system developers required to provide design, develop, test, and evaluation plans for security controls in system documents?</p> <p>NIST SP 800-53 Rev 4, SA-4(2)</p>	
<p>Early in the system development life cycle, are information system developers required to identify the functions, ports, protocols, and services to be used?</p> <p>NIST SP 800-53 Rev 4, SA-4(9)</p>	
<p>Are information system developers required to provide documentation on the security controls administration and the user accessible security functions?</p> <p>NIST SP 800-53 Rev 4, SA-5</p>	
<p>Is the use of information system security engineering principles required in the specification, design, development, implementation, and modification of the information system?</p> <p>NIST SP 800-53 Rev 4, SA-8</p>	
<p>Are external information system services required to comply with the same information security requirements that apply to the agency?</p> <p>NIST SP 800-53 Rev 4, SA-9</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>SYSTEM AND SERVICE ACQUISITION</b>	<b>ASSESSMENT RESULTS</b>
<p>Are external information system services required to identify the functions, ports, protocols, and other services required for the use of their services?</p> <p>NIST SP 800-53 Rev 4, SA-9(2)</p>	
<p>Are system developers required to perform configuration management, including change control and weakness management during system design, development, and implementation?</p> <p>NIST SP 800-53 Rev 4, SA-10</p>	
<p>Are system developers required to perform security testing and evaluation with enough depth to determine the security controls are implemented properly, perform as designed, and meet the agency's security requirements?</p> <p>NIST SP 800-53 Rev 4, SA-11</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**System and Communications Protection (SC)**

<b>SYSTEM AND COMMUNICATIONS PROTECTION</b>	<b>ASSESSMENT RESULTS</b>
<p>Are formal systems and communication protection policies and procedures in place for system acquisition and services? Are they updated annually?</p> <p>NIST SP 800-53 Rev 4, SC-1</p>	
<p>Does the information system separate user functionality (including user interface services) from information system management functionality?</p> <p>NIST SP 800-53 Rev 4, SC-2</p>	
<p>Does the information system prevent unauthorized and unintended information transfer through shared system resources?</p> <p>NIST SP 800-53 Rev 4, SC-4</p>	
<p>Does the information system protect against denial of service attacks by configuring devices securely, using IDPS and other tools, monitoring for suspicious activity, and monitoring bandwidth?</p> <p>NIST SP 800-53 Rev 4, SC-5</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>SYSTEM AND COMMUNICATIONS PROTECTION</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the information system monitor and control communications at the external boundary and only allow connections through managed interfaces?</p> <p>NIST SP 800-53 Rev 4, SC-7</p>	
<p>Is the number of external connections limited and are the connections monitored?</p> <p>NIST SP 800-53 Rev 4, SC-7(3)</p>	
<p>Is there a managed traffic flow policy for each external interface?</p> <p>NIST SP 800-53 Rev 4, SC-7(4)</p>	
<p>Is managed traffic flow denied by default and allowed only by exception?</p> <p>NIST SP 800-53 Rev 4, SC-7(5)</p>	
<p>Does the information system, in conjunction with a remote device, prevent the remote device from simultaneously establishing nonremote connections with the system and communicating through some other connection to resources in external networks?</p> <p>NIST SP 800-53 Rev 4, SC-7(7)</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>SYSTEM AND COMMUNICATIONS PROTECTION</b>	<b>ASSESSMENT RESULTS</b>
<p>Does the information system protect the confidentiality and integrity of transmitted information?</p> <p>NIST SP 800-53 Rev 4, SC-8</p>	
<p>Are cryptographic mechanisms employed to protect against unauthorized disclosure?</p> <p>NIST SP 800-53 Rev 4, SC-8(1)</p>	
<p>Does the communications system terminate the network connection at the end of the session and after 30 minutes of inactivity?</p> <p>NIST SP 800-53 Rev 4, SC-10</p>	
<p>Are cryptographic keys established according to the tribal agency's policy?</p> <p>NIST SP 800-53 Rev 4, SC-12</p>	
<p>Is the type of cryptography used in accordance with Federal Information Processing Standards Publication 140-2, updated December 30, 2002 (FIPS PUB 140-2)?</p> <p>NIST SP 800-53 Rev 4, SC-13</p>	
<p>Does the system prevent remote activation of collaborative computing devices?</p> <p>NIST SP 800-53 Rev 4, SC-15</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>SYSTEM AND COMMUNICATIONS PROTECTION</b>	<b>ASSESSMENT RESULTS</b>
<p>Are public key certificates obtained under a tribal IV-D agency-defined certificate policy or from an approved service provider?</p> <p>NIST SP 800-53 Rev 4, SC-17</p>	
<p>Has the tribal IV-D agency defined acceptable and unacceptable mobile code?  Are usage restrictions in place for acceptable mobile code?  Is the use of mobile code monitored and controlled?</p> <p>NIST SP 800-53 Rev 4, SC-18</p>	
<p>Are usage restrictions in place for VOIP?  Is VOIP monitored and controlled?</p> <p>NIST SP 800-53 Rev 4, SC-19</p>	
<p>Does the information system provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data that the system returns in response to external name/address resolution queries?</p> <p>NIST SP 800-53 Rev 4, SC-20</p>	
<p>Does the information system request and perform data origin authentication and data integrity verification on the name/address responses received from authoritative sources?</p> <p>NIST SP 800-53 Rev 4, SC-21</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>SYSTEM AND COMMUNICATIONS PROTECTION</b>	<b>ASSESSMENT RESULTS</b>
<p>Is the tribal IV-D agency's name/address resolution system fault tolerant?</p> <p>NIST SP 800-53 Rev 4, SC-22</p>	
<p>Does the information system protect the authenticity of communications sessions?</p> <p>NIST SP 800-53 Rev 4, SC-23</p>	
<p>Does the information system protect data at rest through encryption?</p> <p>NIST SP 800-53 Rev 4, SC-28</p>	
<p>Does the information system maintain a separate execution domain for each executing process?</p> <p>NIST SP 800-53 Rev 4, SC-39</p>	

Department of Health and Human Services  
 Administration for Children and Families  
 Office of Child Support Enforcement  
 TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

**System and Information Integrity (SI)**

<b>SYSTEM AND INFORMATION INTEGRITY</b>	<b>ASSESSMENT RESULTS</b>
<p>Are there formal system and information integrity policies and procedures in place?            Are they reviewed and updated annually?</p> <p>NIST SP 800-53 Rev 4, SI-1</p>	
<p>Are there procedures in place to identify, report, and correct information system flaws, including testing software and firmware updates related to flaw remediation?            Are flaws mitigated within the tribal IV-D agency-defined timeframes (for examples, high within two business days, moderate within seven business days, low within 30 days)?            Is flaw remediation incorporated in configuration management?</p> <p>NIST SP 800-53 Rev 4, SI-2</p>	
<p>Are automated mechanisms in place to determine the state of information system components with regard to flaw remediation?            Does the system check at least weekly?</p> <p>NIST SP 800-53 Rev 4, SI-2(2)</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>SYSTEM AND INFORMATION INTEGRITY</b>	<b>ASSESSMENT RESULTS</b>
<p>Are malicious code protection mechanisms used at information system entry and exit points to detect and eradicate malicious code?  Are scans for malicious code run at least weekly?</p> <p>NIST SP 800-53 Rev 4, SI-3</p>	
<p>Are malicious code protection mechanisms centrally managed?</p> <p>NIST SP 800-53 Rev 4, SI-3(1)</p>	
<p>Are malicious code protection mechanisms automatically updated?</p> <p>NIST SP 800-53 Rev 4, SI-3(2)</p>	
<p>Is the system monitored to detect attacks and indications of potential attacks, unauthorized local, network, and remote connections and unauthorized use of the information system?</p> <p>NIST SP 800-53 Rev 4, SI-4</p>	
<p>Are automated tools employed to support near real-time analysis of events?</p> <p>NIST SP 800-53 Rev 4, SI-4(2)</p>	
<p>Is inbound and outbound communications traffic monitored for unusual or unauthorized events or activities?</p> <p>NIST SP 800-53 Rev 4, SI-4(4)</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>SYSTEM AND INFORMATION INTEGRITY</b>	<b>ASSESSMENT RESULTS</b>
<p>Are system alerts generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, and boundary protection devices, such as firewalls?</p> <p>NIST SP 800-53 Rev 4, SI-4(5)</p>	
<p>Are information system security alerts, advisories, and directives received from internal and external sources (for example, peer and supporting agencies or U.S. Computer Emergency Readiness Team) on an ongoing basis?</p> <p>NIST SP 800-53 Rev 4, SI-5</p>	
<p>Are integrity verification tools in use (for example, parity checks) to detect unauthorized changes to software, firmware, and information?</p> <p>NIST SP 800-53 Rev 4, SI-7</p>	
<p>Does the information system perform integrity checks of security relevant events at startup and shutdown?</p> <p>NIST SP 800-53 Rev 4, SI-7(1)</p>	
<p>Is the detection of unauthorized security-relevant changes to the information system integrated into the organizational incident response capability?  Are historical records of changes maintained?</p> <p>NIST SP 800-53 Rev 4, SI-7(7)</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>SYSTEM AND INFORMATION INTEGRITY</b>	<b>ASSESSMENT RESULTS</b>
<p>Are spam protection mechanisms employed at information system entry and exit points?</p> <p>NIST SP 800-53 Rev 4, SI-8</p>	
<p>Are spam protection mechanisms centrally managed?</p> <p>NIST SP 800-53 Rev 4, SI-8(1)</p>	
<p>Are spam protection mechanisms automatically updated?</p> <p>NIST SP 800-53 Rev 4, SI-8(2)</p>	
<p>Are information system inputs checked for valid syntax and semantics (for example, character set, length, numerical range, and acceptable values)?</p> <p>NIST SP 800-53 Rev 4, SI-10</p>	
<p>Do the system generated error messages provide information necessary for corrective actions without revealing information that could be exploited by adversaries?</p> <p>NIST SP 800-53 Rev 4, SI-11</p>	
<p>Is information from the information system handled and retained according to the appropriate laws, directives, policies, regulations, standards, and operational requirements?</p> <p>NIST SP 800-53 Rev 4, SI-12</p>	

Department of Health and Human Services  
Administration for Children and Families  
Office of Child Support Enforcement  
TRIBAL IV-D AGENCY SELF-ASSESSMENT TOOL

<b>SYSTEM AND INFORMATION INTEGRITY</b>	<b>ASSESSMENT RESULTS</b>
Are protections in place to prevent unauthorized code execution in memory?  NIST SP 800-53 Rev 4, SI-16	