Cyber Security Analyst

We are seeking a Cyber Security Analyst who is innovative, dedicated, and highly motivated to solve challenging problems for our client, the Division of Federal Systems (DFS) for the Office of Child Support Enforcement (OCSE).

Our team provides program support to DFS OCSE to manage and monitor the development, implementation, operation, maintenance, technical support, and enhancement of the division's systems and services. Federal Parent Locator Service (FPLS) information is, by statute, made available to child support agencies and a limited number of federal and state agencies. These secure systems and services help child support agencies, employers, insurers, and financial institutions exchange information about child support cases; locate parents; establish paternity, custody and visitation; collect support; and identify fraud.

Responsibilities:

- Responsible for conducting and coordinating security reviews and audits of federal and non-federal data exchange partners that access or host OCSE data. Duties include reviewing partner security documentation, performing up to five site audits annually (e.g., TANF, SWA, MFH, Child Welfare, SNAP), ensuring compliance with HHS/ACF and OCSE security requirements, maintaining audit templates, and supporting Federal Agency Redisclosure Site Security Reviews as needed.
- Provide support to the Security Team in responding to external audits. The candidate will support OCSE during federal audits and site reviews conducted by agencies such as FISMA, IRS, and other oversight entities. Responsibilities include coordinating audit activities, facilitating evidence collection, preparing responses to auditor inquiries, supporting corrective action planning, and tracking remediation activities to closure.
- Provide security compliance expertise and guidance to federal staff, partner organizations, and development teams to ensure compliance with Federal mandates, OMB and NIST guidelines, and HHS/ACF/FPLS security requirements. Advise on security design and implementation issues, assist in developing Security Authorization documentation, and serve as a Subject Matter Expert (SME) on security controls and risk management practices.
- Participate in the continuous monitoring of FPLS systems and applications in support of the security authorization process through system development lifecycle reviews, risk assessments, vulnerability testing, inventory and configuration audits, technical assessments, control validations, and development of security documentation.
- Provide security expertise and support the development, implementation, and maintenance of security policies, procedures, standards, and governance documentation to ensure compliance with Federal mandates, OMB and NIST guidelines, and HHS/ACF/FPLS requirements.
- Provide security support for incident response activities involving FPLS systems, federal partners, state agencies, tribal organizations, and external stakeholders by analyzing and correlating security events, assessing technical and operational impact, coordinating containment and remediation activities, supporting reporting and notification requirements, and ensuring compliance with federal incident handling procedures.
- Coordinate response efforts for security incidents involving sensitive data, including unauthorized disclosures, potential compromises, safeguarding violations, and cybersecurity events affecting OCSE

systems or partner environments. Facilitate communications among security personnel, system owners, business stakeholders, and external organizations throughout the incident lifecycle.

- Develop and maintain incident response procedures, playbooks, reporting processes, and lessons-learned activities to strengthen organizational readiness and improve response effectiveness.
- Support security governance activities associated with data-sharing partnerships, safeguarding agreements, security provisions, and recurring compliance reviews to ensure external organizations maintain required security controls and protections for sensitive OCSE data.
- Support security efforts by integrating information security policies and controls into network and system design, collaborating with technical and business stakeholders to ensure consistent application of information assurance principles, and promoting adherence to established security policies and procedures.
- Promote organizational security awareness by integrating security principles into strategic goals, researching emerging threats and vulnerabilities, supporting the publication of security alerts, advisories, and bulletins, and assisting with the development and delivery of Security Awareness Training.
- Develop policies and procedures to ensure information systems reliability and accessibility and to prevent and defend against unauthorized access to systems, networks, and data.

Skill Set (required):

- Exceptional written and verbal communication skills, including the ability to develop audit reports, assessment findings, corrective action recommendations, executive briefings, and formal security documentation. A writing sample may be requested.
- At least 2 years of professional work experience in a cybersecurity role.
- Experience handling multiple tasks simultaneously, and the ability to work independently in a high stress environment with an orientation towards customer service.
- Ability to coordinate effectively with technical teams, leadership, external partners, auditors, and oversight organizations during active security incidents and investigative activities.
- Expertise in multi-stakeholder collaboration, partnering with federal, state, and industry entities on providing advisory assistance for data protection and cloud modernization initiatives.
- Experience reviewing and analyzing security policies, procedures, system security plans, interconnection agreements, data-sharing agreements, or other security-related documentation
- Experience developing, maintaining, or standardizing security assessment methodologies, audit procedures, compliance processes, or governance frameworks.
- Knowledge of information assurance principles including application security, network security, operational security, personnel security, physical security, and data protection requirements
- Demonstrated expertise in conducting risk and vulnerability assessments, supporting security audits and compliance reviews, and performing partner/contractor site security assessments to ensure adherence to federal standards and data protection requirements.
- Demonstrated commitment to continuous improvement, process optimization, and strengthening organizational security posture through proactive planning and stakeholder engagement

Desirable Qualifications:

- Demonstrated experience conducting security assessments, compliance reviews, audits, site visits, or control validations against federal security frameworks such as NIST SP 800-53, NIST SP 800-171, FISMA, IRS Publication 1075, or comparable regulatory requirements.
- Strong understanding of governance, risk, and compliance (GRC) principles, including risk assessments, corrective action management, continuous monitoring, security documentation, and audit readiness activities.
- Demonstrated experience supporting or coordinating cybersecurity incident response activities, including event triage, impact analysis, containment, remediation, recovery, and post-incident reporting.
- Experience investigating security incidents involving sensitive or regulated data and coordinating response efforts across multiple stakeholders and organizational boundaries.
- Experience developing incident reports, executive briefings, corrective action plans, after-action reviews, and other incident management documentation
- Security or IT certifications (e.g. CISSP, CISA, etc.)
- Knowledge of the Child Support Enforcement program and system operations.
- Experience handling sensitive data sources and distribution of data containing personally identifiable information.