LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

Enterprise Security Services (ESS) Line of Business (LoB) Service Offerings

Value of ESS LoB Services

- Ensures Federal information systems provide mission-critical services in a secure manner

Overview

- The Department of Health and Human Services (HHS) Office of Information Security (OIS) Enterprise Security Services (ESS) Division, established in 2011, and designated as a Department of Homeland Security (DHS) Shared Service Center (SSC) for Information System Security Services. HHS ESS was given a letter of Recognition in Performance for cost savings to the Government of nearly $3m in 2017.
- The purpose of this service is to support and facilitate the implementation of all mandates and guidance under the federal Risk Management Framework (RMF) solutions as identified by NIST 800-37 to:
  - provide subject matter expertise in security accreditation and authorization
  - reduce the cost of completing accreditation and authorization on systems across the Federal Government
  - provide evaluation and validation of information system security risks to ensure compliance with NIST Special Publication (SP) regulations, policies and procedures
  - comply with agency-defined frequencies for technical analysis of information system vulnerabilities
- HHS ESS Line of Business (LoB) provides a wide variety of services related to the following:
  - Information System Security Officer (ISSO) Services
  - Security Control Assessment (SCA) Services
  - Security Consulting (SC) Services
  - Information System Security Manager (ISSM) Services

ESS LoB Services

Information System Security Officer (ISSO) Services

ESS Information System Security Officer (ISSO) Service Offerings

- ESS ISSOs support the System Owner across the system development life-cycle (SDLC) to:
  - ensure a system's appropriate operational security posture is maintained
  - ensures system-level security controls are implemented and security documentation is maintained
  - serve as the focal point for IT security/privacy incident reporting and resolution

- ISSO Services can include the following:
  - support a current ISSO, or
  - serve in the ISSO role

ESS Information System Security Officer (ISSO) Services

- ISSO Services include:
  - **Security Assessment and Authorization (SA&A) ATO Support:** develop/review/update/maintain required system security-related documentation; Ensure SA&A ATO package is complete and submitted
  - **Plan of Actions & Milestones (POA&M) Management:** assist with development, monitoring and remediation of POA&Ms into the agency system of record
  - **System Management:** ensure a secure posture is in place (i.e., assign security controls; participate in change control/configuration management; ensure deployment of security patches; review system-level reports, etc.)
  - **Account Management:** verify and manage account access/controls
  - **Risk Management:** identify risks; participate in security risk assessments and risk waiver process
  - **Incident Management:** develop/update incident response plans and procedures
  - **Security Guidance and Analysis:** serve as security advisor/security subject matter expert
  - **Information Security Continuous Monitoring (ISCM):** provide continuous monitoring process support to ensure a secure system posture (i.e., ensure system backups are performed, audit log reviews, update of security documentation and inventories, assessment of security controls. etc.)

ESS LoB Services

Security Control Assessment (SCA) Services

ESS Security Control Assessment (SCA) Service Offerings

- Independent Verification and Validation (IV&V) of information system risks, vulnerabilities, and control compliance for information systems hosted internally and externally to the agency to include Cloud Service Providers (CSPs)
- Performance of technical vulnerability analysis to include web application scanning and network/host based scanning to validate system readiness for Authorization to Operate (ATO), Interim Authority to Test (IATT) and ad-hoc scanning
- Control Assessment validation through Interview and Examination (I&E) based on NIST SP 800-53 Revision 4 and NIST SP 800-53A guidance

ESS Security Control Assessment (SCA) Services

- SCA services include:
  - Independent verification and validation assessments
  - Vulnerability Assessments and Tools
    - Web Application Testing - Web Inspect and Burp Suite
    - General Application Control Testing - Manual Testing
    - Network/Host-based Scans - Nessus and Nipper
  - Security Controls Assessments
    - Evaluation of Management, Operational and Technical security controls
    - Control Assessment of Low/Moderate/High baseline systems

ESS LoB Services

Security Consulting (SC) Services

ESS Security Consulting (SC) Service Offerings

- Develop, update, and review system security documentation necessary to obtain or renew a system's SA&A Authorization to Operate (ATO) in compliance with federal regulations and agency and departmental policies
- Ensure SA&A ATO Package is complete when submitted for approval
- Support the entire SA&A process or the development of individual security documents
- Provide consulting services, evaluate security programs, and serve as security subject matter expert
- Assist with POA&M development and remediation

ESS Security Consulting (SC) Services

- Security Consulting Services include:
  - Determining system's security categorization in accordance with FIPS 199
  - Developing security documentation necessary to obtain or renew the system's authorization to operate and developing annual security documentation
  - Conducting Business Impact Analyses (BIA)
  - Conducting Independent Verification and Validation of security documentation to meet federal regulations and agency and departmental policies
  - Supporting the entire system security authorization process
  - Ensuring compliance with federal regulations and agency and departmental policy
  - Ensuring security controls and processes are implemented to maintain the system's security posture
  - Providing consulting cervices in establishing Risk Management Framework Practices
  - Providing continuous monitoring support to include tracking and verifying system weaknesses (POA&Ms)
  - Serving as security subject matter expert

ESS LoB Services

Information System Security Manager (ISSM) Services

ESS Information System Security Manager (ISSM) Service Offerings

- Ensures the Agency/Division Information Security Program is fully implemented and maintained throughout the organization
- Serves as the Point of Contact for all Agency/Division information security matters; provides subject matter guidance to Agency executives, Business and System Owners as well as departmental security contacts and officials
- Serves as key advisory for the assessment and mitigation of risks and vulnerabilities for all systems utilizing policy, procedures, and best practices to ensure security controls are maintained over the life of systems

ESS Information System Security Manager (ISSM) Services

- Ensures compliance from planning, through the HHS Enterprise Performance Life Cycle (EPLC)/System Development Lifecycle (SDLC) process and procedures
- Provides oversight and coordination with the System Owners and ISSOs to ensure current system specific plans are in place for all information technology (IT) systems
- Serves as Audit Liaison as it pertains to internal and external audits of all organizational IT systems to ensure compliance with federal and departmental policy and procedures
- Monitors information assurance practices to ensure that security controls are maintained over the life cycle of all systems
- Manages the system security authorization process to ensure all systems are authorized and accredited prior to operation and are reaccredited within the system life cycle or whenever a significant change occurs
- Develops, manages and reports on remediation of Plans of Action and Milestones (POA&Ms) resulting from SCA testing; Audits and annual assessments as part of vulnerability/weakness management efforts

Customer Service Agreement (CSA)

- HHS ESS LoB will meet with potential customers to identify requirements and provide a summary of desired services
- Potential customers will complete a questionnaire regarding the system to facilitate identification of requirements
- HHS ESS LoB will provide a cost estimate based on services requested in the questionnaire
- HHS ESS LoB will create a Customer Service Agreement (CSA) or Interagency Agreement (IAA) proposal and will submit to the customer for review and approval
- The CSA/IAA, a standard form for reimbursable agreements between HHS ESS LoB and the customer, includes:
  - general provisions
  - financial and funding information
  - contact information and approvals
- Work is not initiated until the CSA/IAA is signed

ESS ISS LoB Points of Contact

- **ESS LoB Director:** John Richardson (202) 603-1702
- **ISSO Services Manager**: Marla Redwine (301) 945-5488
- **SCA Services Manager**: Markeshia Gould (202) 836-2045. SCA inquiries should be sent to the SCA Mailbox scateam@hhs.gov
- **Security Consulting Services Manager**: Trish Hunter (301) 945-5548
- **ISSM Services Manager**: Marla Redwine (301) 945-5488

Do you want to learn more? Contact esslob@hhs.gov or isslob@hhs.gov to explore how the ESS LoB Team can help you