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) Line of Business (LoB) Division, established in 2011, and designated as a Department of Homeland Security (DHS) Federal Shared Service Provider (FSSP) for Information System Security Services. HHS ESS was given a letter of Recognition in Performance for cost savings to the Government of nearly $8M in FY22.
- The purpose of this service is to support **Federal Agencies** to 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 LoB provides a wide variety of services related to the following:
  - Information Privacy and Security Officer (IPSO) Services *(Formerly ISSO)*
  - Security Control Assessment (SCA) Services
  - Security Consulting Services (SCS)

Information Privacy and Security Officer (IPSO) Services

(Formerly ISSO)

ESS Information System Privacy and Security Officer (IPSO) Service Offerings

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

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

ESS Information System Privacy and Security Officer (IPSO) Service Offerings

- IPSO 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.)

  - **IPSO Services are available to federal agencies only.**

Security Control Assessment (SCA) Services

ESS Security Control Assessment (SCA) Service Offerings

- Interview, Examine, and Test system implementations in accordance with NIST 800-53 Revision 5 to determine the information system's 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 5 and NIST SP 800-53A guidance
- Interview, Examine, and Test control implementations in accordance with NIST ST 800-79-2 to provide a high degree of assurance that federal PIV cards are being managed correctly throughout the federal space.
- PIV Control Assessment validation through Interview and Examination (I&E) based on complying with HSPD-12, NIST SP 800-79-2 and FIPS 201-3 Federal regulations.
- **Security Control Assessment Services are available to federal agencies only.**

ESS Security Control Assessment (SCA) Services

- SCA services include:
  - **Vulnerability Assessments and Tools**
    - Web Application Testing - WebInspect and Burp Suite
    - General Application Control Testing - Manual Testing
    - Network/Host-based Scans - Nessus and Nipper Studio
  - **Security Controls Assessments**
    - Evaluation of security and privacy controls
    - Control Assessment of Low/Moderate/High baseline systems
    - Results provided in a Security and Privacy Assessment Report (SPAR)
  - **PIV Card Issuance Facility (PCIF) Assessments**
    - Evaluation of security controls around identifying and authenticating federal employees and contractors to provide access to federal buildings and systems.
    - Results provided in a PIV Assessment Report

ESS LoB Services

Security Consulting Services

(SCS)

Security Consulting Services (SCS) Offerings

- Develop, update, and review system security documentation necessary to obtain or renew a system's SA&A Authorization to Operate (ATO) and for continuous monitoring purposes in compliance with federal regulations and agency and departmental policies
- Support the entire SA&A process or the development of individual security documents
- Perform quality assurance of system security documentation
- Serve as security subject matter expert (SME)
- Assist with POA&M development and remediation

Security Consulting Services (SCS)

- Security Consulting Services include:
  - **Assisting the IPSO and System Owner** in determining a system's security categorization in accordance with FIPS 199
  - **Developing/Updating system security documentation** necessary to obtain or renew the system's authorization to operate
  - Developing/Updating documentation for continuous monitoring purposes
  - **Conducting quality assurance** of system security documentation to meet federal regulations and agency and departmental policies
  - **Assist IPSO in ensuring compliance with federal regulations** and agency and departmental policy regarding security
  - Serving as subject matter expert (**SME**)
  - **Assisting with Plan of Action and Milestones (POA&M)** development and remediation to include tracking and verifying system weaknesses

  - **Security Consulting Services are available to federal agencies only.**

Customer Service Agreement (CSA) Process

Customer Service Agreement (CSA)

- Upon contacting HHS ESS LoB for services, ESS will meet with potential Federal customers to identify requirements and provide a summary of desired services
- Potential Federal customers will complete a system questionnaire regarding the system to facilitate identification of requirements
- HHS ESS LoB will develop/provide a cost estimate based on services requested in the questionnaire
- Upon cost estimate approval the HHS ESS LoB will create a Customer Service Agreement (CSA) or Interagency Agreement (IAA) and will submit to the customer for funding and signatures
- 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
- Work can only be established between federal agencies.

ESS ISS LoB Points of Contact

- **HHS ESS LoB Director:** Markeshia Gould (202) 836-2045
- **IPSO Services Manager**: Chelsea Ward (202) 868-9773
- **SCA Services Manager (Acting)**: Kimberley Eccles (202) 868-9112. SCA inquiries should be sent to the SCA Mailbox scateam@hhs.gov
- **Security Consulting Services (SCS) Manager**: Trish Hunter (202) 853-4055
- **Business Operations Support –** Roxana Robbins (202) 815-1948

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