Perspecta

Title: Information Systems Security Officer (ISSO)

Location: Stennis Space Center in Hancock, MS

POC: Jennifer Jamison
Jennifer.Jamison@perspecta.com

Description:

- Comply with the ISSO Roles and Responsibilities as laid out in DHS 4300 A/B.
- Maintain the Security Authorization or Certification and Accreditation of their assigned system.
- Track the Security Authorization of their assigned system.
- Deliver all required documentation using the current DHS approved templates, forms, regulations, and methods.
- Continuously update all Security Authorization documentation as required by the ISSO SOP.
- Provide advisement to stakeholders to assign resources and establish timelines to ensure the successful Security Authorization of a system.
- Maintain all required documentation to maintain their assigned system's Authority to Operate or system go live dates.
- Document all relevant NIST 800-53 and 4300A Security Controls and/or applicable departmental policies for each IT system the ISSO is responsible for.
- Draft a Security Package and perform any modifications throughout the lifecycle of the IT system.
- Work closely with the System Owner to identify any additional controls that are applicable to the system to maintain a favorable security posture.
- Perform an annual physical assessment of all General Support Systems (GSS) and Major Applications and sub-system interfaces.
- Provide oversight and advisement on all proposed change requests on an IT System as it pertains to the potential change to the existing Controls Assessment.
- Work with auditors to identify Key Controls which must be assessed on a recurring annual basis.
- Evaluate and provide advisement on all privileged access requests to IT systems.
- Ensure software targeted for introduction to the production environment is evaluated and provide guidance regarding the potential for the software to introduce risk into the environment.
- Track the deployment of software to the environment that is not part of the base image. Ensure software installs are registered to individual users.
- Ensure software deployed in the environment is audited on a quarterly basis. ISSOs shall provide reports to System Owners, ISSM, and to O&M staff tailored with the level of detail or abstraction as appropriate.
- Perform oversight of Information System Vulnerability Management (ISVM) inquiries, and ensure that the inquiries are addressed and reported within the allotted timeframe and reported via the accepted methods and formats.
- Generate Plan of Actions & Milestones (POA&Ms) for each non-compliant control for each managed IT System. Proper documentation shall be filed and updated as required.

- Manage all applicable POA&Ms throughout the lifecycle of the IT system. This includes but is not limited to the drafting of well documented waivers and exceptions detailing the potential risk to the Authorizing Official.
- Support the Security Incident Response team in the remediation, documentation and reporting of all incidents for the ISSO assigned system.
- Perform a Weekly review of logs for each IT system.
- Participate in project discussions in support of the System Owner.
- Provide track and report security requirements throughout the project life cycle of all projects that are within the accreditation boundary of their assigned system.
- Work closely with Office of the Chief Information Security Officer (CISO) to provide guidance and oversight for all requested initiatives.
- Provide timely and detailed responses to all data calls.
- Provide support for all Office of the Inspector General (OIG) and other external audit activities.
- Provide oversight and guidance regarding requests to modify technical policies such as firewall rules, ports, protocols, etc. for each IT system.
- Coordinate with and brief Federal staff on all activities pertaining to each IT system as requested.
- Continuously maintain a thorough understanding of all configurations, architecture, installed software, accounts (both Operating System and Application), data flows, ports, protocols, and other relevant data for each IT System.
- Coordinate with the appropriate operational group to accurately update the System Design Document for each IT system to reflect the approved state of each IT system.
- Ensure the Configuration Management Database (CMDB) is continuously updated with the appropriate operational group if it is available.
- Experience with Authority to Operate (ATO) process, continuous monitoring, POA&Ms, Security Authorizations (SA), NIST 800-37, NIST 800-53 Rev3 / Rev4, working with System Owners (SO)

- 5-7 years applicable professional experience
- Experience with the C&A process
- Understanding of FISMA compliance
- Works well with team members
- CISSP, CISA or equivalent certifications (DoD 8570 IAM 2 equivalent)
- System Admin or other technical background
- Bachelor's degree or equivalent experience
- Experience with Ongoing Authorizations
- Experience with Xacta
- U.S. Citizenship required
- Must be able to pass a Federal background investigation
- Desired**:** Experience working at DHS and with DHS 4300