

Information System Security Officer Information System Security Officer Information System Security Officer - Department of Transportation Frederick, MD United States Citizen Work Experience Information System Security Officer Department of Transportation - Washington, DC April 2014 to Present Federal Contractor

Conduct kick off meetings to collect systems information (information type, boundary, inventory, etc.) and categorize systems based on NIST SP 800-60.

Conduct IT controls risk assessments including reviewing organizational policies standards and procedures and providing advice on their adequacy, accuracy and compliance with industry standards.

Assist with the development of system Security Plan (SSP) to provide an overview of federal information system security requirements and described the controls in place to meet those requirements.

Conduct document reviews of NIST, OMB, FISMA and other policy documents and vendor publications related to enterprise technologies and recognize, modify and update procedures resulting from the new guidance.

Develop Security Assessment Reports (SAR) detailing the results of the assessment along with Plan of Action and Milestones (POA&M).

Provide Continuous Monitoring support through POA&M's, system and user audits, analyze and report scanning results, and update all corresponding security documents as needed.

Provide senior level security consulting to Federal customers in addition to guidance and support to Department ISSOs/System Owners on the FISMA and NIST Security Assessment and Authorization process.

Prepare Security Assessment and Authorization (SA&S) packages to ensure management, operational and technical security controls adhere to NIST SP 800-53 standards.

Assist System Owners and ISSO in preparing certification and Accreditation package for company's IT systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 R4.

Provide ISSO and CISO support by assisting in reviewing risk waivers and ISA, MOU review before authorization.

Create and update the following Security Assessment and Authorization (SA&A) artifacts: FIPS 199, System Security Plan (SSP), Risk Assessment (RA), Privacy Threshold Analysis (PTA), Privacy Impact Analysis (PIA), E-Authentication, System Security test and Evaluation (ST&E), Contingency Plan, Plan of Actions and Milestones (POA&M).

IT Security Analyst Security Assessment and Authorization -

Rockville, MD April 2007 to April 2014 MD    Developed security control test plans and conducted in-depth security assessments of information systems that evaluate compliance of administrative, physical, technical, organizational and policies safeguards to maintain NIST compliance.    Updated System Security Plan, Risk Assessment, Privacy Impact Analysis, ST&E and POA&M.    Conducted Information systems security risk assessments including reviewing organizational policies standards and procedures and providing advice on their adequacy, accuracy and compliance with industry standards.    Conducted comprehensive assessment of the management, operational, technical security control employed within or inherited by an Information System to determine the overall effectiveness of the control.    Created standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans and security authorization packages.    Reviewed security policy documents and make recommendations on documentation compliant.    Created and updated the following Security Assessment and Authorization (SA&A) artifacts: FIPS 199, SSP, RA, E-Authentication, ST&E, Contingency Plan, and (POA&M).    Assisted System Owner and ISSO in preparing certification and Accreditation package for major systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 R4.    Performed vulnerability assessment, making sure risks are assessed and proper actions taken to mitigate them.

Information Security Analyst System Security Plan (SSP) - Gaithersburg, MD January 2001 to April 2007 MD    Analyzed and updated System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E) and the Plan of Actions and Milestones (POA&M)    Conducted IT controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with FISMA Standard.

Assisted System Owner and ISSO in preparing certification and Accreditation package for agency's systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 R4.

On a quarterly basis, conducted reviews on Information Systems security documents for all hosted

systems to include: Plan of Action & Milestones (POA&Ms) and Security Control Testing & Evaluation (ST&E). Scheduled monthly POA&M meetings with stakeholders, collected documentation and evidence to determine adequacy and sufficient artifacts to close out POA&Ms. Performed vulnerability assessment making sure risks are assessed, evaluated and proper actions taken to limit impact on the information and information systems. Created standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans and security authorization packages. Education compliance NIST communication and interpersonal skills NIST Skills SECURITY (10+ years), SHARE POINT, REMEDY, PEOPLESOFT, NESSUS, Organizational Skills, Typing, Customer Service, Stocking, Word Additional Information Technical Skills Software/Hardware/Platform: UNIX, Windows, PeopleSoft, Remedy Service Desk, ServiceNow, Security Control Testing, MS Office Suite (Power Point, Visio, Word, Share Point, Excel, Access), Azure, HP ALM, Rational Requisite Pro, JIRA, Nessus Security Center, Bigfix, CSAM.

Name: Elizabeth Beck

Email: christopher72@example.com

Phone: 562.321.6764x7047