|  |  |  |  |
| --- | --- | --- | --- |
| Certifications  Certified Information Systems Security Professional (CISSP)  NSTISSI-4011 - INFOSEC Professional  NSTISSI-4014 - Information Systems Security Officers (ISSO)  Fully Qualified Navy Validator #I0841  Key Skills  Risk Management  Security Controls Assessment and Validation  Enterprise Policy, Procedure, and Compliance  POA&M Tracking, Management, and Remediation  Creation and Evaluation of C&A packages  Education  Master’s of Science (MS) in Computer Science, with a focus in Information Security from James Madison University |  | Information Security specialist with over 20 years of experience with civilian and military policy and procedure, implementation and evaluation of security controls, vulnerability management/analysis and protection of assets. Extensive experience with enterprise risk management, security controls testing/validation, enterprise compliance, vulnerability management, remediation, and tracking. Extremely familiar with compliance standards such as NIST 800-53, IRS 1075, HIPPA, FISMA, and MARS-E. Have authored enterprise policies and procedures, system security plans, security architectures, security metrics, staffing plans, and many other security and risk related documents. Have created and briefed presentations and whitepapers for many different audiences, including senior leadership. Have excellent experience with project management, including financial and personnel management. Have international work experience. Experienced in working with diverse personnel including subcontractors, vendors, government and military personnel. | |
| Experience |  |
| State of South Carolina, Columbia, SC | **2016 - Present** |
| Booz Allen Hamilton, Charleston, SC | **2000-2016** |
| Recent Projects | |
| * Senior Information Security Architect/Engineer – State of South Carolina - Assist with the implementation, integration and operationalizing advanced security technologies. Develop operational plans for integrating and implementing security technologies within existing division and agency infrastructure and operational processes. Develop full life cycle processes and procedures along with repeatable guides for standard implementation and assist agencies as needed to incorporate systems. Creating and writing policies and procedures and security controls implementation in order to comply with multiple standards such as CJIS, NIST 800-53, MARS-E, and IRS 1075. Work with staff to architect and deploy advanced information security systems in a highly complex distributed enterprise environment. Work with Security Operations Center to identify enhanced data collection and correlation capabilities in existing data and gaps in data collection/analysis architecture, systems and procedures. * IA Team Lead - Veteran’s Administration Chapter 33 - Led IA team supporting the C&A efforts for a large VA educational benefits program. Led efforts in ensuring C&A compliance and overall security of the system that processed billions of dollars of benefits. Efforts included policy and procedure review and edit, vulnerability management, creation and update of the C&A package, creation of Security SOPs and whitepapers, evaluate the security consequences of proposed system modifications, identify and analyze system malfunctions, ensure security tests were performed and results documented, ensured audit trails were maintained, reviewed, and archived regularly, and provide security guidance to end users, operational staff, and provided security training to staff. | |
| * Lead Security Controls Assessor - National Science Foundation Office of Polar Programs – Led security controls assessment and testing for multiple locations of the program. Develop and execute test plans on large enterprise level networks. Organized teams, set team assignments and supervised testing efforts. Efforts include policy and procedure review and edit, creation of SOPs, evaluation of security consequences for proposed system modifications, ensure security tests were performed and results documented, and review of mitigations of the system. | |
| * Accreditation Lead - Veteran’s Administration Agile Integrated Development Environment - Led C&A documentation efforts for the VA AIDE program. Ensured all documents related to the successful maintenance of the Authority to Operate were created, updated, and maintained. Ensured that all documents follow proper Federal and VA guidance and policies such as NIST 800.53, VA 6500 series, and others. Also performed vulnerability management tasks such as scanning systems with Retina, analyzing mitigations reports, and evaluating mitigations. | |
| * Information Assurance Officer - JFCOM J2/JIOC – Assigned as the Information Assurance Officer (IAO). Performed IAO duties such as policy and procedure review and edit, IAVA and vulnerability management, Certification and Accreditation activities such as creation and update of SSAAs and DIACAP packages. Worked with the Office of the Designated Accreditation Authority (ODAA) to produce C&A documentation for successful issuance of Authority to Operate (ATO). Created other IA related documents such as Security SOPs and whitepapers. Familiar with policy documents such as DCID 6/3, DoD 8500 controls, ICD 1253, and other IA related policies and controls. Analyzed vulnerability reports and recommend mitigation strategies. Evaluated the security consequences of proposed modifications, identified and analyzed system malfunctions, ensured security tests were performed and results documented, ensured audit trails were maintained, reviewed, and archived regularly, and provided security guidance to end users, operational staff, and the IO JMO Program Office. | |
| * Information Assurance Officer - JFCOM J2/JIOC - JFCOM Information Operations Joint Management Office (IO JMO) – (Nov 2007 – Oct 2009) Assigned as the Information Assurance Officer (IAO). Performed IAO duties such as policy and procedure review and edit, IAVA and vulnerability management, Certification and Accreditation activities such as creation and update of SSAAs. Created other IA related documents such as Security CONOPS and whitepapers. Familiar with policy documents such as DCID 6/3, DoD 8500 controls, ICD 1253, and other IA related policies and controls. Ensured all personnel were briefed on IA matters within their scope of responsibility. Maintained a current inventory of security related hardware and software, evaluated the security consequences of proposed modifications, identified and analyzed system malfunctions, ensured security tests were performed and results documented, ensured audit trails were maintained, reviewed, and archived regularly, and provided security guidance to end users, operational staff, and the IO JMO Program Office. | |
| * Lead Security Advisor - Australian Government Department of Human Services Project - Was the Lead Security Advisor for Booz Allen on the $1.1B(AU) Access Card project. Worked with a small set of AU government employees to design technical solutions, security procedures and policies for the security of the program, not only for IT/Communications systems, but smart cards as well. I was the primary person for creating the security architecture for the program, as well as helping design the overall technical conceptual architecture. I gave input to the Request For Tender documents, and was an SME on the evaluation team for evaluating vendor responses. | |
| **Certifications**   * **CISSP - Certified Information Systems Security Professional** * **NSTISSI CNSS-401 - INFOSEC Professional** * **NSTISSI CNSS-4012 - Senior System Managers** * **NSTISSI CNSS-4014 - Information Systems Security Officers (ISSO)** * **NSTISSI CNSS-4015 - System Certifiers** * **FQNV - Fully Qualified Navy Validator (Cert#I0841)** | |