Information Security Officer Information Security Officer Information Security Officer - ASRC Federal Laurel, MD A seasoned Information System Security Officer (ISSO) and Security Risk Management professional holding a SECRET Level security clearance with more than 20 years related experience in the fields of Information Security and Information Security Auditing. Proficient in conducting Risk Management Assessments and IT Security Audits in compliance with regulatory initiatives and industry guidelines such as Risk Management Framework (RMF) for FISMA Compliance, HIPAA, Sarbanes Oxley, PCI, and NIST. Certifications include Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Authorization Professional (CAP) and SAINT Vulnerability Product Certified. Work Experience Information Security Officer ASRC Federal - Beltsville, MD September 2018 to Present Responsibilities include performing duties of the Information System Security Officer (ISSO) for NASA Goddard Space Flight Center. Responsible for the design and implementation of security solutions to protect the confidentiality, integrity, and availability of sensitive information. Provides support for proposing, coordinating, implementing, and enforcing information systems security policies, standards, and methodologies. Plan and develop Risk Management Framework (RMF) procedures for the six steps (Categorize System, Select Controls, Implement Controls, Assess Controls, Authorize System and Monitor Controls) of the RMF process to ensure compliance for the government system. Maintain operational security posture for the program to ensure information systems security policies, standards and procedures are established and followed. Interface with multi-disciplined teams and work with stakeholders in analyzing, evaluating, and mitigating system security threats, vulnerabilities and risks throughout the program lifecycle. Evaluate security solutions to ensure they meet security requirement for processing classified information. Perform vulnerability and risk assessment analysis to support certification and accreditation. Assist with the management of security aspects of the information system and perform daily security operations. Support development, implementation, verification and validation of system security solutions in hardware, software, firmware, data and procedures. Complete Plan of Action and Milestones (POA&M) and continuous monitoring activities as required. Prepare and review documentation to

include System Security Plans (SSPs), Risk Assessment Reports, Assessment and Authorization (A&A) packages and System Requirements Traceability Matrices (SRTMs). Management of the implementation of the global security policy, standards, guidelines and procedures to ensure maintenance and security regulations. Implementation of government regulated and recommended Assessment and Authorization (A&A) objectives (security control testing, security documentation development which includes System Security Plans, Risk Assessments, Plan of Action and Milestones (POA&M), Security Test and Evaluation (ST&E) Plan and Report). Client: NASA Goddard Space Flight Center, Cybersecurity Services Division contract, (Greenbelt, MD) Senior Risk Management Engineer Leidos - McLean, VA September 2015 to September 2018 Responsibilities include performing duties for the performance of system security implementation tasks for information assurance security pertaining to data integrity and PII regarding passport and visa services for the U.S. Department of State Bureau of Consular Affairs. Conduct the Assessment and Authorization (A&A) Risk Assessment for computer systems for the United States Department of State Bureau of Consular Affairs. Interface with multi-disciplined teams and work with stakeholders in analyzing, evaluating, and mitigating system security threats, vulnerabilities and risks throughout the program lifecycle. Conduct Annual Control Assessment testing of the Assessment and Authorization process. Provide Subject Matter Expert (SME) support for the Assessment and Authorization process. Support development, implementation, verification and validation of system security solutions in hardware, software, firmware, data and procedures. Conduct control testing of Oracle Databases and SQL Databases. Complete Plan of Action and Milestones (POA&M) and continuous monitoring activities as required. Create and perform documentation development, testing procedure for the Assessment & Authorization process. Advise the system owner regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (i.e. life cycle management). Assist in the determination of an appropriate level of security commensurate with the impact level. Assist in the development and maintenance of system security plans and contingency plans for all systems under their responsibility. Participate in risk assessments to

periodically re-evaluate sensitivity of the system, risks, and mitigation strategies. Participate in self-assessment of system safeguards and program elements and in certification and accreditation of the system. Notify the responsible IT Security Officer (ITSO) of any suspected incidents in a timely manner, and assist in the investigation of incidents, as necessary. Management of the implementation of the global security policy, standards, guidelines and procedures to ensure ongoing maintenance of regulated security. Information protection responsibilities included network security architecture, network access and monitoring policies, employee education and awareness. Implementation of government regulated and recommended Assessment and Authorization (A&A) objectives (security control testing, security documentation development which includes System Security Plans, Risk Assessments, Plan of Action and Milestones (POA&M), Security Test and Evaluation (ST&E) Plan and Report). Senior IT Security Consultant US State Department OBXtek contract - Vienna, VA February 2015 to July 2015 Responsibilities include performing duties for Payment Card Industry (PCI) and HIPAA Compliance. Conducted PCI related assessments. Conducted Gap Analysis for client PCI Compliant environments. Performed duties of Senior in a two man PCI assessment team. Developed ROC for PCI Compliance. Assisted Client with PCI self-assessment questionnaire. Assisted Clients with PCI readiness. Conducted Gap and Remediation of HIPAA engagements. Participated in any compliance related contract engagements (at any phase) for HIPAA, PCI, and Government Assessments where needed. Clients: Total Wine, LogicWorks, Jackson River, Sweetgreen, B&H Photo Reason for Leaving: New Job Opportunity Senior Security Analyst GeBBS Healthcare Solutions - Towson, MD June 2014 to December 2014 Responsibilities include performing duties for a Healthcare Security and Compliance contract. Conducted risk assessment, trading partner self-assessment evaluations. Created and improved processes and procedures for the trading partner evaluation program. Conducted contract BAA and SLA review for trading partner program.

Conducted and developed remediation process for the HIPAA audits with Plan of Action and Milestone process. Participated in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies. Participated in self-assessment of system safeguards and

program elements in IT audit programs to meet HIPAA, NIST, GLB, and ISO regulations and or controls. Developed common control catalogs and cross reference of controls in HIPAA, NIST, GLB and ISO 17799/ 27001. Conducted PCI documentation review and remediation. Conducted PCI Rock and artifact review status as presented from the PCI assessor. Contract Ended Carefirst Bluecross Blueshield (Owings Mill, MD) - Reston, VA April 2013 to May 2014 Information System Security Officer Responsibilities include performing duties of the Information System Security Officer (ISSO) for federal government agency contracts. Created and developed an Information Security Program for a government agency. Developed the roles and responsibilities for personnel and positions. Developed IT audit programs to meet government regulations. Developed the Certification and Accreditation Program with personnel. Developed an ISSO program with training and implementation across the agency. Developed and created security Standard of Operations (SOP) and programs for validation of IT SOPs. Created and performed documentation development, testing procedure for the Assessment & Authorization process. Advised the system owner regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (i.e. life cycle management). Assisted in the determination of an appropriate level of security commensurate with the impact level.

Assisted in the development and maintenance of system security plans and contingency plans for all systems under their responsibility. Participated in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies. Participated in self-assessment of system safeguards and program elements and in certification and accreditation of the system. Notified the responsible IT Security Officer (ITSO) of any suspected incidents in a timely manner, and assist in the investigation of incidents, as necessary. Management of the implementation of the global security policy, standards, guidelines and procedures to ensure ongoing maintenance of regulated security. Information protection responsibilities included network security architecture, network access and monitoring policies, employee education and awareness. Implementation of government regulated and recommended Assessment & Authorization (A&A) objectives (security control testing, security documentation development which includes System Security Plans, Risk

Assessments, Plan of Action and Milestones POA&M , Security Test and Evaluation ST&E Plan and Report). Client: Department of Homeland Security, Federal Protective Services (Washington, DC) Reason for Leaving: New Job Opportunity Information System Security Officer The Goal, Inc - Fairfax, VA September 2012 to April 2013 Responsibilities include performing duties of the Information System Security Officer (ISSO) for a government agency contract. Created and developed an Information Security Program for a government agency, developing the roles and responsibilities for personnel and positions. Developed IT audit programs to meet government regulations. Developed the Certification and Accreditation Program with personnel. Developed an ISSO program with training and implementation across the agency. Developed and created security Standard of Operations (SOP) and programs for validation of IT SOP's. Created and performed documentation development, testing procedure for the A&A process. Advised the system owner regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (i.e. life cycle management). Assisted in the determination of an appropriate level of security commensurate with the impact level. Assisted in the development and maintenance of system security plans and contingency plans for all systems under their responsibility. Participated in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies. Participated in self-assessment of system safeguards and program elements and in certification and accreditation of the system. Notified the responsible IT Security Officer (ITSO) of any suspected incidents in a timely manner, and assist in the investigation of incidents, as necessary. Management of the implementation of the global security policy, standards, guidelines and procedures to ensure ongoing maintenance of regulated security. Information protection responsibilities included network security architecture, network access and monitoring policies, employee education and awareness. Implementation of government regulated and recommended Certification and Accreditation A&A objectives (security control testing, security documentation development which includes System Security Plans, Risk Assessments, Plan of Action and Milestones POA&M , Security Test and Evaluation ST&E Plan and Report). Client: Department of Homeland Security,

Federal Protective Services (Washington, DC) Reason for Leaving: Contract Ended Senior Information Security Analyst GNS, Inc - Rockville, MD February 2012 to August 2012 Responsibilities include performing Certification and Accreditation duties for a government agency contract. Created and performed documentation development, testing procedure for the A&A process in the formation of an Enclave system. Reviewed and improved the A&A process, auditing and updating previous A&A packages. Created the baseline and development of client Information Security Program Framework, resource allocation planning and facilitation of training courses for business unit owners. Identification of data protection goals, objectives and metrics in alignment with corporate strategic plan. Management of the implementation of the global security policy, standards, guidelines and procedures to ensure ongoing maintenance of regulated security. Information protection responsibilities included network security architecture, network access and monitoring policies, employee education and awareness. Implementation of government regulated and recommended Certification and Accreditation A&A objectives (security control testing, security documentation development which includes System Security Plans, Risk Assessments, Plan of Action and Milestones POA&M , Security Test and Evaluation ST&E Plan and Report). Utilization of the government security standards (NIST SP 800-53) around IT security assessment for management, operations and technical controls. Utilization of OMB circular A-123 for Internal controls. Developed baseline security control requirements and ensuring implementation of acceptable security controls and baseline configuration settings in accordance with NIST and agency security policy. Categorized the information systems' data in accordance with Federal Information Processing Standard (FIPS) Publication (PUB) 199 and implemented security controls based on FIPS 199 categorization guided by FIPS 200. Performed analysis and verification of certification results. Conducted vulnerability and risk assessments in accordance with NIST 800-30 and agency information system policy Prepared executive and technical reports detailing vulnerabilities and risks. Developed Contingency Plans, based on NIST SP 800-34 and Configuration Management Plans, based on NIST SP 800-64. Client: Department of Energy (Washington, DC) Reason for Leaving: Contract Ended Senior Information Security Analyst Carson

& Associates, Inc - Bethesda, MD July 2008 to January 2012 Responsibilities include performing Information System Security Officer (ISSO) duties for government and private sector client contracts. Created the baseline and development of client Information Security Program Framework, resource allocation planning and facilitation of training courses for business unit owners. Identification of data protection goals, objectives and metrics in alignment with corporate strategic plan. Management of the implementation of the global security policy, standards, guidelines and procedures to ensure ongoing maintenance of regulated security. Information protection responsibilities included network security architecture, network access and monitoring policies, employee education and awareness. Assisted with the development of the PCI business providing guidance and layout for assessment procedures. Implementation of government regulated and recommended Assessment & Authorization (A&A) objectives (security control testing, security documentation development which includes System Security Plans, Risk Assessments, Plan of Action and Milestones POA&M , Security Test and Evaluation ST&E Plan and Report). Utilization of the government security standards (NIST SP 800-53) around IT security assessment for management, operations and technical controls. Utilization of OMB circular A-123 for Internal controls. Developed baseline security control requirements and ensuring implementation of acceptable security controls and baseline configuration settings in accordance with NIST and agency security policy. Categorized the information systems' data in accordance with Federal Information Processing Standard (FIPS) Publication (PUB) 199 and implemented security controls based on FIPS 199 categorization guided by FIPS 200. Performed analysis and verification of certification results. Conducted vulnerability and risk assessments in accordance with NIST 800-30 and agency policy. Prepared executive and technical reports detailing vulnerabilities and risks. Developed Contingency Plans, based on NIST SP 800-34 and Configuration Management Plans based on NIST SP 800-64. Executing FISMA audits and security reviews. Clients: National Institute of Health (NIH) Office of Information Technology(Rockville, MD), NIH National Institute of Environmental Health Science (Raleigh, NC), Corporation for National and Community Service (Washington, DC), NIH National Institute on Alcohol Abuse and Alcoholism (Rockville, MD) Reason

for Leaving: Contract Ended Information Security Manager HMSHOST - Bethesda, MD October 2006 to June 2008 Responsibilities include serving as the Information System Security Officer for the organization. Identified protection goals, objectives and metrics consistent with corporate strategic plan. Managed the development and implementation of global security policy, standards, guidelines and procedures to ensure ongoing maintenance of security. Physical protection responsibilities included asset protection, workplace violence prevention, access control systems, and video surveillance. Information protection responsibilities included network security architecture, network access and monitoring policies, employee education and awareness. Established and sustained professional relationships with local, state and federal law enforcement and other related government agencies. Oversaw incident response planning as well as the investigation of security breaches, and assists with disciplinary and legal matters associated with such breaches as necessary. Worked with outside consultants and vendors as appropriate for independent security audits. Developed and enforced an Information Security Program with security architecture of Policy, Training and Awareness, Data Protection (Classification & Identification), Intrusion Detection and Disaster Recovery. Educated and promoted an organizational culture to accept industry standards and best practices in providing the Confidentiality, Integrity, and Availability of data. Provided guidance in meeting compliance towards regulatory initiatives and industry guidelines such as Sarbanes Oxley, PCI, HIPAA, Italian Law 262, NIST, and ISO17799. Project manager for information security projects, which included the coordination of contractors, evaluation of tasks and timeline, and performance risk assessments across Business Units. Evaluated security approaches, systems, hardware, software, and made appropriate recommendations for implementation to management with vendor and product selection. Advised and promoted all new developments and projects in establishing information security measures addressing access control, change management, physical security, backup and recovery. Reason for Leaving: New Job Opportunity Technology Risk Management Professional Jefferson Wells - McLean, VA November 2004 to October 2006 Mclean, VA 11/2004 - 10/2006 Technology Risk Management Professional Responsibilities included planning, directing, and

completing information systems audits and business process control review engagements. Worked closely with directors and staff on client management, practice development, and business development. Planned, executed, directed, and completed information systems audits, business process control reviews. Understood and managed project risk on audits and proposals. Identified security engagement issues and risk management issues. Worked closely with clients and staff to develop client and project risk assessments, implement opportunities, and recommendations regarding business and IT process optimization, profit improvement, internal control, and compliance. Led engagements, performing general computer and application controls reviews. Reviewed operational, financial, and technology processes to provide management with an individual assessment of business risk, internal control, and the overall effectiveness and efficiency of the process. Led the development and implementation of Business Continuity and Disaster Recovery Plans at various clients. Provided recommendations for security issues in accordance with state and federal regulations, in conjunction with providing industry knowledge to client security teams. Clients: American National Red Cross (Washington, DC), TNS (Herndon, VA), Bon Secours (Baltimore, MD), E*Trade (Arlington, VA), Orkin (Toronto, CA), Rollins (Parsippany, NJ), SEC (Washington, DC), NASD (Rockville, MD) Reason for Leaving: New Job Opportunity IT Security Administrator Washington Suburban Sanitary Commission - Laurel, MD September 2002 to October 2004 Development of the Information Security Program Framework. Developed and implemented Information Security Policies and Procedures. Expanded and enforced an Information Security Program including Security Awareness, Policies and Procedures, Incident Response, and Disaster Recovery. Supervised Administrators for eTrust, ACF2, and Security Policies throughout network. Evaluated and assessed security approaches, systems, hardware, software, resulting in appropriate recommendations for secure system implementation. Evaluated RFP, hardware, software, and application proposals to measure security requirements. Conducted Security and General Control audits of Networks and Mainframe Systems to evaluate the goals of data confidentially, integrity, and availability to align with industry standards, following best practices. Reason for Leaving: New Job Opportunity IT Audit Manager Old Dominion University - Norfolk, VA

1998 to 2002 EDP Audit Manager Norfolk State University - Norfolk, VA 1996 to 1998 Site Administrator The Sherwin Williams Company - Baltimore, MD 1994 to 1996 Computer/Data Processing Instructor MTC, WTCC - Baltimore, MD 1991 to 1994 Customer Engineer IBM - Beltsville, MD 1987 to 1991 Education Master of Science in Management Information Systems Bowie State University - Bowie, MD December 1993 Certificate Bowie State University - Bowie, MD December 1992 Bachelor of Science in Electronics Technology Norfolk State University - Norfolk, VA December 1983 Skills Customer Service, Security, Word, Organizational Skills Certifications/Licenses Certified Information Systems Security Professional (CISSP) February 2002 Continous renewal to present Certified Information Systems Auditor (CISA) February 2002 Continous renewal to present

Name: Samantha Barber

Email: gabrielharrington@example.com

Phone: +1-224-807-6577x3132