IT Security Specialist IT Security Specialist IT Security Specialist - DHS HQ Stafford, VA Cybersecurity Analyst with a Public Trust Security Clearance and over eight (8) years of experience in security program support, system authorization (SA), risk management (RA), systems development life cycle (SDLC), security assessments, and vulnerability management. Expert in reviewing, analyzing, and developing security policies, processes, and procedures. Solutions-focused, team oriented, customer-focused professional with in-depth knowledge of security cyber risks inherent in software, applications, complex networks, operating systems, and cloud platforms Work Experience IT Security Specialist DHS HQ - Arlington, VA February 2019 to Present February 2019 to Present Provide weekly status reporting to customer and Office of Biometric Identity Management (OBIM) Assess from a holistic point of view the MAS vulnerability mitigation strategy in relation to ongoing and upcoming patching deployments Review of vulnerability scan results and facilitate information on the various scan-related requests as well as coordinate mitigation strategies and schedule Address the compliance ISVM needs in the environment Coordinate and support MAS staff to complete the appropriate yearly trainings and upload proof to OBIM SharePoint Lead the access control and follow ups with issues related to privileged accounts, Xceedium, and RARs, Remedy, DHS OBIM Lan email accounts, and VPN access Updated Remedy and GLPI security-related tickets Coordinate with Data Center POCs and Service Delivery Managers to mitigate identified vulnerabilities across platforms (Windows, AIX, SuSe) As GFE custodian, lead the GFE configuration and port issues mitigation efforts Assist with the AV activity for various GFEs and provide paperwork to OBIM on GFEs Lead the various security related tasks such as vulnerability review, scanning requests, antivirus requests and many other duties on the OBIM Operations and Maintenance (O&M) team Coordinate the inventory and audit of GFE laptops, servers, and monitors within the environment for compliance purpose. Information System Security Officer FDIC - Arlington, VA September 2018 to January 2019 Develop, review and update security impact analysis (SIA) Responsible for maintaining FDIC's Office of the Chief Information Security Officer (OCISO) security posture through the development of security functions including contingency plan (CP), configuration management, system authorization (SA),

system development lifecycle (SDLC), e-Authentication, fire wall exceptions, and data loss prevention (DLP) Develop business impact assessment (BIA), acceptance of risk (AOR) and risk assessment (RA). Develop vulnerability/patch management procedure and templates for FDIC OCISO and information system managers (ISM) Review security functions, policies, procedures, evaluate effectiveness, identify risk areas and make recommendations to improve agency's security postures Perform Risk Management Framework (RMF) Assessment and Authorization (A&A) activities for agency's systems and applications Review system authorization packages of Cloud, On Premises, and Outsourced systems Review, analyze, and update Interconnection Security Agreements (ISA) and Memorandum of Understandings (MOUs) Ensure audit records are archived for future reference and audit artifacts are generated as needed Develop and manage plan of actions and milestones (POA&M), waiver requests, security guidelines and checklists for FDIC systems, applications, and devices IT Security & Compliance Analyst Department of Commerce - Washington, DC September 2017 to September 2018 Perform Risk Management Framework (RMF) Assessment and Authorization (A&A) activities for agency's systems and applications Analyze, validate, update, and develop security policies, processes, and procedures such as rules of behavior, access control, risk assessment, and incident response Review security functions, policies, procedures, evaluate effectiveness, identify risk areas and make recommendations to improve agency's security postures Review security documentation such as system security categorization (FIPS 199), e-authentication, Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), Risk Assessment Report (RAR), Contingency Plan (CP), and Contingency Plan Test (CPT) Attend weekly Governance Risk and Compliance (GRC) meetings for updates on projects and systems Review NIST 800-53 Rev 4, including Appendix J (Privacy Controls) for guidance and policies Assist ISSOs and System Owners to address security controls and implementation methods Analyze, mitigate, and manage risk within a federal information system that store, process, display or transmit Personally Identifiable Information (PII) and other sensitive information Ensures security baselines are maintained and validated at least annually. A report of the validation is provided to the ISSM for annual FISMA reporting. Ensure audit records

are archived for future reference and audit artifacts are generated as needed in CSAM IT Security Assessor Millennium Challenge Corporation - Washington, DC August 2014 to September 2017 Performed RMF A&A activities for Major Applications and General Support Systems (GSS) Updated IT security policies, procedures, standards, and guidelines according to privacy and federal requirements Reviewed Security Assessment Reports (SARs); created and completed Plan of Action and Milestones to track the remediation of findings and vulnerabilities Developed, reviewed, and updated information security policies, System Security Plans (SSPs), and security baselines in accordance with NIST, FISMA, Appendix III to OMB Circular No. A-130, and industry best security practices Conducted security assessments and audits to ensure compliance with established security standards, policies and procedures (NIST, FISMA, OMB) Coordinated with appropriate personnel to execute vulnerability assessments and patch management on a regular basis and ensure timely remediation of risks Performed IT risk assessment and documented the system security keys controls Reviewed and revised SSP, System Security Test and Evaluation (ST&E), Risk Assessment Report, Privacy Impact Assessment (PIA), and POA&M Designed and conducted walkthroughs, formulated test plans, produced results and develop remediation plans Developed and created training materials to provide continuous awareness of security issues and threats including Cyber Security and Awareness Training (CSAT) and Privacy Awareness Training (PAT) on an ongoing basis Conducted IT controls risk assessments (NIST 800-53A) including reviewing organizational policies, standards and procedures and providing advice on their adequacy, accuracy, and compliance with NIST standards and agency's requirements Reviewed and analyzed Configuration Management Plan (CMP), Incident Response (IR), and SSP IT Audit Security Analyst Admiral Security Services - Washington, DC July 2011 to August 2014 Liaised with System Owners and provided guidance and oversight during OIG audits Coordinated data collection, analysis and reporting for IT Security Data Calls, FOIA Requests, Incident reports and other types of data calls that may be necessary As requested by the Office of inspector General (OIG), assisted on investigative matters related to information security Provided necessary leadership, execution and support of compliance activities related to Federal Information Technology

security mandates including but not limited to: Federal Information Security Modernization Act (FISMA), Federal Information System Control Audit Manual (FISCAM), Federal Risk and Authorization Management Program (FedRAMP) Evaluated policies and procedures affecting organizational project objectives Scheduled and planned projects using Microsoft Project Directed the priorities of projects and measured progress toward reaching objectives effectively and economically Created, reviewed, and updated Certification and Accreditation (C&A) packages and Authority to Operate (ATO) documentation for systems hosted and owned by BLS Review, analyze, and update Interconnection Security Agreements (ISA) and Memorandum of Understandings (MOUs) Technical Support DataPrise - Charlotte, NC January 2011 to July 2011 Resolved customer complaints and concerns leveraging strong verbal and negotiation skills Resolved Remedy tickets daily Coordinated with other IT groups for remediation of complex issues Improved system performance by identifying problems and recommending changes Researched, diagnosed, troubleshoot, and identified solutions to resolve system issues Coordinated with merchants to scan their network to ensure compliance and network availability Assisted merchants with PCI DSS assessment Provided support to our merchant customers via inbound and outbound calls, emails, and/or, web-chat communication methods Educated customers of the importance of achieving and maintaining PCI-DSS compliance and provided the appropriate level of assistance for each step of the process. Provided excellent customer support and strive to achieve first call resolution by thoroughly and efficiently gathering the necessary information to fulfill the call Created formal awareness and training programs; designed and implemented site-specific safety strategies Planned, organized, and managed multiple projects; developed and wrote policies, proposals, and memos for clients, managements and workers. Education Master of Science in Strategic Marketing in Strategic Marketing University of Hertfordshire September 2007 to May 2009 Skills Cyber Security, Cybersecurity, Information Assurance, Information Security, It Security, Nist, Siem Certifications/Licenses Security+ CE Present

Name: Mr. Brent Henry

Email: brownthomas@example.com

Phone: 3185940281