Cybersecurity Assessor Cybersecurity Assessor Cybersecurity Assessor Alexandria, VA I have 14 years of Security Analysis and Information Assurance (IA) skills and knowledge to include, but not limited to; Operating Systems (OS) installation, maintenance, troubleshooting, monitoring Intrusion Prevention Systems, Data Loss Prevention (DLP) solution and tools, security impact and assessments (SIA), and policies. I have conducted security assessments for Certification and Accreditation (C&A) and Assessment and Authorization (A&A) for commercial and Federal organizations. I have Privacy Analysis security knowledge on Personally Identifiable Information (PII) and Protected Health Information (PHI) security controls requirements and assessments within the IA field as well. I work successfully in environments where frequent and direct interaction with customers, stakeholders, and Government personnel is common. I pride myself on completing task and providing the best of my abilities at all times. Work Experience Cybersecurity Assessor Credence LLC - Vienna, VA November 2017 to October 2018 Provided Azure Security and Compliance System Security Plan (SSP) through Cyber Security Assessment and Management (CSAM) system for use in developing an SSP that documents both customer security control implementations and controls inherited from Azure for the Housing and Urban Development (HUD) system enterprise Identity Credential and Access Management (eICAM). Provided Azure Security and Compliance reviews and solutions for government systems to facilitate the secure and compliant use of Azure Cloud solutions for HUD and third-party vendors on behalf of government. Ensured Azure Government system was compliant to meet a FedRAMP Provisional Authority to Operate (P-ATO) and DoD Provisional Authorization (PA). Utilizes Customer Responsibility Matrix (CRM) to aid Azure Government customer by implementing and documenting system-specific security controls implemented within Azure which lists all National Institute of Standards and Technology (NIST) NIST SP 800-53 rev. 4 with Appendix J for privacy security control requirements for FedRAMP and Defense Information Systems Agency (DISA) baselines that include customer implementation requirement. Reviewed implementation statements in SSP for accuracy and compliance with Federal Information Security Modernization Act (FISMA), NIST, FedRAMP, and Security Requirements Guide (SRG). Interacted with Cloud Service Provider (CSP) to conduct

Incident Response (IR) and Contingency Plan (CP) exercises for Disaster Recovery Plan (DRP) and procedures. Performed Information Assurance (IA) consulting, assessment, documentation and IA compliance program development (DevOps) dealing with programs which must comply with or follow guidance of Federal Information Security Management Act (FISMA), OMB A-130, NIST SP 800 Series, NIST FIPS Publications, and/or DoD DITSCAP or DIACAP programs. Prepared and updated C&A package to obtain an Authority to Operate (ATO) approval. Prepared System Security Plan (SSP), System Security Authorization Agreement (SSAA), and the Application Security Plan (ASAP) as appropriate for C&A package submission. Performed risk assessment for Risk Management Framework (RMF) applicability on eICAM system presented through the Office of IT Portfolio Management Division (PMD). Provided GOVERNANCE, RISK, and COMPLIANCE (GRC) policies and procedures to key stakeholders departments for internal audits, compliance, risk, legal, finance, IT, HR as well as the lines of business, executive suite members. Attended weekly Sprint meetings with Developers, Program Managers, Key Stakeholders and Government personnel to achieve GRC compliance. RighIT Solutions Security Assessor Risk Management Framework RMF - Crystal City, VA July 2016 to November 2017 Conducted security assessments to ensure compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4 with privacy policies security controls. Supported the implementation of the Risk Management Framework (RMF) for NIST and Department of Defense (DoD) requirements to Department of Defense, Federal Civilian, and Intelligence Community customers per Federal Information Security Management Act (FISMA). Integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity following GRC policies and procedures. Executed and supported RMF system assessment and authorization tasks to obtain an Authority To Operate (ATO). Developed documentation (Security categorization worksheets, authorization boundary definition documents, security plans, contingency plans, incident response plan, risk assessments, Plan Of Action & Milestones (POA&Ms), to ensure that the current NIST SP 800-53 rev.4 security requirements are addressed during all phases of the System Development Life Cycle (SDLC). Recommended and drove solutions to eliminate, reduce,

or mitigate risk detected, and communicated solutions to both external parties and internal business stakeholders. Reviewed FISMA, DISA STIGs and SRGs, FDCC/USGCB, NVD/SCAP, Retina/ACAS scans, VMS data, and interprets IAVAs, POA&Ms and other continuous monitoring data. Recorded pertinent documentation and communications for all assessments in information technology (IT) governance, risk, and compliance platform. Assessed external party information security controls to ensure they met or exceeded information security risk management requirements for the services to be provided. Clearly and professionally communicated information security risks associated with internal and external services unit personnel and business leaders. Reported status of engagements to Information Security management, project managers, and other business stakeholders as appropriate. Privacy Analyst APEX Systems Security - Washington, DC February 2016 to July 2016 Provided overall System Security Plan (SSP) development for Department of Human Services (DHS) applications for District of Columbia Access System (DCAS) utilizing National Institute of Standards and Technology (NIST) 800-53 Rev 4, including Appendix J (Privacy Controls) for guidance and policies for a Moderate level system. Conducted security controls assessment of the application, and deployment characteristics based on security controls assessments and implementation. Provided compliance requirements in accordance with NIST 800-53 rev4 for Health Insurance Portability and Accountability Act (HIPAA), Internal Revenue Service (IRS) Publication 1075, Privacy Act of 1974, as amended, and Social Security Administration (SSA). Provided security guidance and policies for Federal Tax Information (FTI), Personally Identifiable Information (PII), and eProtected Health Information (ePHI). Conducted internal audits of security controls of DHS/DCAS application and documents in preparation for external audits to validate compliance with FISMA requirements. Reviewed all System Security Authorization and Assessment (SA&A) application documents for accuracy and validation for moderate level requirements per FISMA. Supported other tasks as assigned by appropriate Infosys personnel. Systems Cyber Security Analyst (C2 Labs Sub-contractor) APEX Systems Security November 2015 to January 2016 Tele-work Responsible for assisting with conducting security assessments to ensure compliance with National Institute of Standards and Technology

(NIST) Special Publication (SP) 800-53, Revision 4 security controls. Lead the development of a U.S. Government (USG) Certification and Accreditation (C&A) Package for Commercial Off the Shelf (COTS) applications. Wrote application System Security Plan (SSP) to achieve a FISMA Moderate level certification based on NIST 800-53 revision 4 controls and FISMA requirements. Provided oversight and guidance to COTS vendors' staff on modification of the application and deployment characteristics based on security controls assessments and implementation. Provided recommendations to COTS vendor as to the overall C&A process and changes required to the application. Reviewed all C&A application documents for accuracy and validation for moderate level requirements. Recommended best practices for security and privacy policies and procedures. Performed Privacy Impact Assessment (PIA) and Security Impact Assessment (SIA) for application. Demonstrated experience creating USG C&A packages with minimal oversight. Privacy Analyst Eliassen Group BOOZ ALLEN HAMILTON (BAH) - Herndon, VA March 2015 to October 2015 Recommended and provides proper security handling of sensitive information including the privacy of Personally Identifiable Information (PII), Protected Health Information (PHI), Controlled Unclassified Information (CUI), and Unclassified Controlled Technical Information (UCTI).

Supported the Enterprise Information Security (EIS) Compliance team in updating PII and PHI firm-wide guidance and policies per FISMA requirements. Supported the Firm's Information Protection Compliance (FIPC) program including the review and tracking of security and privacy controls (SIA's). Responsible for reviewing security and privacy controls for projects and working with the project teams to ensure that appropriate controls are in place and compliant. Expert knowledge of the National Institute of Standards and Technology (NIST) 800-53 Rev 4, including Appendix J (Privacy Controls) for guidance and policies. Created Rules of Behavior (ROB) guidance and policies for firm wide personnel. Categorized data based on the firm's Risk Matrix Framework (RMF) process for review of all projects handling PII and PHI. Assisted in the development and revision of security and privacy guidance and artifacts for PII, PHI, CUI, and UCTI guidance and related artifacts. Documented identified weaknesses resulting from analysis of the security control impact assessments (SIA's). Categorized data to its sensitivity and confidentiality

level that constitute PII, PHI, sensitive financial information and credit card information. Recommended Security Awareness and training policies and guidance per FISMA guidelines. Supported other tasks as assigned by appropriate Booz Allen personnel. UNITED STATES DEPARTMENT OF AGRICULTURE (USDA/FNS) Information Security Office (ISO) ATD, Inc - Washington, DC January 2015 to March 2015 Responsible for assisting with conducting security assessments to ensure compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4 security controls. Developed Incident Response Plan (IRP) and procedures for USDA FNS PII incidents document. Handled Incident Response (IR) for email PII breaches within Food Nutrition Services (FNS). Provided system(s) analysis and assessments of security controls for PII. Monitored web tools for security breaches pertaining to PII. Provided remediation for lost or stolen devices that contain PII. Reported and briefed stakeholders and Government personnel on PII breached incidents for USDA FNS. Utilized Agriculture Security Operations Center (ASOC) Remedy Ticket system for incident tracking and reporting. Sr. Privacy/ Security Analyst Consultant Officer Panum Group UNITED STATES DEPARTMENT OF AGRICULTURE (USDA/OCIO) Privacy Office - Washington, DC April 2014 to September 2014 Responsible for assisting with conducting security assessments to ensure compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4 security controls. Reviewed Privacy documentation which consisted of Privacy Threshold Analysis (PTA), and Privacy Impact Assessment (PIA). Performed Security Assessment and Authorization concurrency reviews. Reviewed USDA agencies guidelines, policies and procedures ensuring Personally Identifiable Information (PII) was safeguarded and protected in compliance with Privacy Act of 1974, as amended. Performed Privacy reviews with the USDA agencies point of contact for clarity to confirm PTA and PIA documents were compliant. Researched requirements for Computer Matching Agreements and Programs (CMA/CMP). Drafted and modified an outline/skeleton project plan, version 1.1, for the Computer Matching Agreement/Program in compliance with the Computer Matching and Privacy Protection Act of 1988 for USDA. Provided policy and procedure guidance on Data Loss Prevention (DLP) for PII within

USDA. Researched and provided DLP solutions and providers for USDA and entities within. Briefed Chief Information Officer (CIO) and stakeholders on DLP security plans, features, cost and benefits. Subject Matter Expert IT Security Diligent eSecurity USAID - Crystal City, VA May 2012 to March 2014 Responsible for assisting with conducting security assessments to ensure compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53a/Revision 4 security controls. Provided security guidance to customers and corporate IT staff to meet security compliance requirements. Evaluated various technologies and provided security architectural considerations and developed mitigation recommendations as part of the risk management process (SIA's). Utilized Cyber Security Assessment and Management tool (CSAM) to assess, document, manage, and report on the status of IT security risk assessments and implementation of Federal and DoD mandated IT security control standards and policies. Utilized CSAM for the management of Plan of Action and Milestone (POA&M's) to include creating, tracking, and closing, as well as automating system inventory and FISMA reporting capabilities. Assisted with customers in performing Federal Information Security Management Act (FISMA) audit reviews; developing and updating IT security policy and guidance consistent with Departmental and Federal requirements. Performed risk management assessments; developed and reviewed system security plans, plan of actions and milestones, security control implementation, configuration management plans, contingency planning, incident response plans and disaster recovery plans. Reviewed information security policy, Rules of Behavior, vulnerability scans and other task specific security documentation. Addressed areas such as: securing remote access with SSH, SSL and IPSec; using National Institute of Standards and Technology (NIST) and Defense Information System Agency (DISA) configuration guidance to harden servers, operating systems and appropriate applications. Created security policies and procedures for corporate and federal information systems, applications and networks to meet federal security guidelines and requirements. Provided security guidance in Information Assurance (IA), Certification and Accreditation (C&A), network security, security life cycle management, risk management, security awareness and security training. Developed and reviewed System Security Authorization and

Assessment (SSA&A) documents, Security Test and Evaluation plans (ST&E), Contingency Plans and residual risk management assessments to support system accreditation. Performed (SIA's) and security audit review on USAID Federal systems. Resulted in positive results that these efforts of documentation will be delivered on schedule, security controls are properly implemented and documented, and customers were able to obtain positive security auditing without additional costs. Key Tools: Splunk, Nessus, CSAM. Information Assurance Engineer Advanced Systems Development, ASD Pentagon November 2010 to May 2012 Responsible for assisting with conducting security assessments to ensure compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3 security controls. Assisted with planning, organizing, and managing security, disaster recovery, and similar functions related to information systems Ensured that data systems and databases are protected from unauthorized users Applied sound Information Assurance practices, Intrusion Detection, and maintaining information security administration for computer networks, LAN/WAN systems, internet and server systems Evaluated the effectiveness and efficiency of existing security control measures Performed (SIA's to identify vulnerabilities that may cause inappropriate or accidental access, destruction, or disclosure of information and establishes security controls to eliminate or minimize exposures Performed established auditing and monitoring analysis to verify compliance with established security policies and notifies appropriate individuals of violations Organized the security investigation and implementation of corrective actions Assisted with documentation all inquiries relating to any perceived or alleged security breaches Assisted with maintaining training and awareness programs to ensure owners and clients are aware of their responsibilities Assisted and advised user departments in appropriate security and disaster recovery procedures Provided written and oral presentations on security issues Key systems: Windows 2003, 2008, XP, Windows 7, Vulnerability Management System (VMS), Retina, worked with ITA on PENTCIRT's, HBSS ePO, Information Assurance Officer/Configuration Manager Digital Systems, DISYS - Crystal City, VA November 2009 to September 2010 Responsible for assisting with conducting security assessments to ensure compliance with National Institute of Standards and Technology (NIST)

Special Publication (SP) 800-53, Revision 3 security controls. Served as the Information Assurance Analyst for all DoD clients, senior staff, and executive-level personnel, for the Defense Prisoner of War/Missing Personnel Office (DPMO), Office of the Secretary of Defense (OSD) Conducted compliance testing using Retina network scanning software on existing networks and systems for compliance with DoD and DISA Security Technical Implementation Guidance (STIGS) and directives Managed virus threats, security violations, and malicious activities through completion; reported all findings to the DPMO, Chief Information officer (CIO) and OSD CIO Managed the Vulnerability Management System's (VMS) database for monitoring the corrective actions taken to mitigate or eliminate known vulnerabilities and for reporting compliance with prescribed security directives and guidance Developed and administered system security programs and training that implement policy and directives consistent with DPMO and OSD guidance Acted as the focal point for policy and guidance in system security matters within DPMO Prepared and presented reports to the CIO and the Designated Approving Authority concerning the security stance of all computer systems maintained by DPMO Chaired the Configuration Management Board monthly meetings In conjunction with the Information Technology professionals and customers, evaluated the effects of modifications to the security posture on three networks, UNCLASSIFIED, SECRET, and TS/SCI Coordinated, tracked, and reported on annual training for all DPMO staff Key Tools: Windows hardening security measure, Microsoft baseline security analyzer Senior Functional Security Analyst EDS, An HP Company - Arlington, VA August 2008 to November 2009 Served as Operations Coordinator for Joint Task Force Global Network Operations (JTF-GNO) Analyzed and mitigated emerging technology used against Department of Defense (DoD) networks Provided defensive solutions to over 5 million Information Systems (IS) in the Global Information Grid (GIG) Provided technical and analytical support for global deployment of Host-Based Security System (HBSS) to augment Computer Network Defense (CND) efforts Performed duties as member of the Technical Advisory Group (TAG) chartered to implement advanced in-depth capabilities to HBSS Performed initial requirements gathering and provided responses to Request For Information (RFI) and proposals, acquisitions, and deployment Provided

technical and process support for the user Communication Tasking Order (CTO) tracking module in the Vulnerability Management System (VMS) v6.2 Managed JTF-GNO requirements, responsibilities, and policy to ensure Computer Network Analysis (CNA) and compliance statistics are standardized throughout DoD Researched latest Cyber security risk and mitigation solutions Provided weekly reports and briefings to Commander JTF-GNO and CDR Strategic Command (STRATCOM) on deployment of HBSS Provided weekly status reports, i.e. 50% of devices scanned, 90% patched, 2%, has vulnerabilities Information Security Specialist - Sr EDS, An HP Company - Crystal City, VA November 2007 to August 2008 Responsible for assisting with conducting security assessments to ensure compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4 security controls. DoD FISMA lead for Department-wide development of Plan of Action and Milestone (POA&M) efforts for the annual FISMA requirements to OMB and Congress Managed the security POA&M process at the DoD level Provided responses to DoD Inspector General (IG) on various security issues Developing and coordinating the DoD requirements and guidelines in preparation of the FY06 DoD FISMA reporting requirements Responsible for coordinating and briefing the DoD FISMA Integrated Product Team (IPT) of 45 personnel that includes all the DoD Services and Agencies Developed the DoD security policy in coordination with senior DoD Officials Knowledgeable on DoD security policies and certification and accreditation (C&A) process Knowledgeable on NIST requirements Responsible to brief POA&M procedures and responsibilities to senior leadership and the FISMA IPT and Core Team DoD Exhibit 300's Business Cases Provided capabilities that integrated the governance, management and assurance of performance, risk, and compliance activities utilizing GRC policies and procedures. Supported and resolved security issues with regards to DoD business case submissions to OMB Developed and modified the DoD grading criteria for grading security section of the Exhibit 300s internally in DoD Scored the DoD Exhibit 300 business cases each year prior to submission to OMB Reporting to the DoD IG Provided responses to DoD Inspector General on various security issues Secondary administrator to MS Access database for FISMA and security policy issues and information Supported the development of the annual DoD

FISMA report to OMB, Congress and GAO	Supported development of the DoD FY FISMA Guidance each year

Name: Brandon Williams

Email: orodgers@example.net

Phone: 795.834.9812