

Deputy Program Manager, Cybersecurity Framework Subject Matter Expert Deputy Program Manager, Cybersecurity Framework Subject Matter Expert Deputy Program Manager, Cybersecurity Framework Subject Matter Expert - Emagine IT Inc Work Experience Deputy Program Manager, Cybersecurity Framework Subject Matter Expert Emagine IT Inc August 2018 to Present * Directing and managing a team of seventeen cybersecurity support staff for the Air Force Chief Information Security Officer (AF CISO Support) contract * Providing support to implement risk management framework (RMF) and cybersecurity framework (CSF) by changing the current culture to address enterprise risk management (ERM) * Assessing current status of CISO cybersecurity strategy program to identify gaps in current state, developing end-state objectives, analyzing opportunities for quick wins and prioritization of remaining shortfalls Cybersecurity Management Consultant SharePoint Inc February 2018 to November 2018 * Consulted with large commercial customer to develop authority to operate documentation for contractor developed system in accordance with Federal Acquisition requirements * Developed strategy and program-specific deliverables to the Continuous Diagnostics and Monitoring (CDM) Program's Lead Business Authority * Supported the development of cybersecurity and risk management decision support tools such as CONOPS, business processes, policies and SOPs * Provided subject matter expertise on federal enterprise security operations centers and agency SOC's including organizational constructs and operating processes Technical Cybersecurity Manager, General Dynamics Mission Systems General Dynamics Mission Systems June 2017 to February 2018 * Conducted certification tests and risk assessments to validate that the features and assurances required for each protection mechanism were implemented according to requirements * Established procedures to ensure that Configuration and Change Management data teams were able to maintain synchronized databases due to changes to the system to achieve security compliance * Ensured that data ownership and responsibilities were established for each system, including accountability, access rights, and special handling requirements * Ensured that system security requirements were addressed during all phases of the system life cycle * Assessed needs identified in request for proposal to architect a security solution for inclusion to a software project integration for large DHS customer * Performed

Initiation and Planning activities including drafting high-level requirements, identification of stakeholders, developing list of deliverables, and drafting a work breakdown structure * Researched cloud offerings for secure platform for hosting government data, drafting service level agreements and Memorandums of understanding IT Security Specialist, Administrative Office of U.S. Courts Axxum Technologies, LLC - Washington, DC March 2017 to June 2017 * Performed security assessments for enterprise information systems, general support systems, major applications, and sub-applications using NIST SP 800-53 Rev 3/4 * Prepared systems to convert from NIST SP 800-53 Rev. 3 to Rev 4 and ensured that all controls were assessed Consultant Dogwood Management Partners, LLC October 2016 to February 2017 Resilience Team Lead, FEMA IT Resilience, Mt. Weather, VA * Performed security assessments for non-classified enterprise information systems, general support systems, major applications, and sub-application systems and financial applications using NIST SP 800-53 Rev 4 and DHS 4300 A/B security controls * Provided Information System Security Management activities for 112 information systems. Developed and tracked all assessment activity for management and monthly FISMA reporting Program Manager, Senior IT Security Specialist Global Network Systems - Falls Church, VA February 2016 to October 2016 * Managed team of assessors and performed security assessments for classified and non-classified enterprise information systems, general support systems, major applications, and sub-application systems Developed and updated testing procedures, and Rules of Engagement (RoE) * Collaborated with stakeholders during the assessment to remove false updates, developed and tracked POA&Ms, and developed the security assessment report (SAR) and risk assessment documentation Senior Information Assurance Analyst Lockheed Martin - Fort Belvoir, VA June 2015 to February 2016 * Participated in working groups to identify Information Assurance requirements in the Program Management Process to identify and document assessment and authorization decisions * Analyzed Risk assessment designation through documentation of control ownership identified through business case analysis (BCA), business impact analysis (BIA), for FedRAMP information systems, local infrastructures, and information systems Information Assurance Manager, U.S. Army eVigilant Security January 2015 to June 2015 Tank and Automotive Research

Development and Engineering Center (TARDEC) * Provided IA support for the TARDEC Scientific Computing Network Pilot enclave by ensuring site compliance of DoD Directives and instructions, and Army Regulations (AR), specifically AR 25-2 and Assessment and Authorization and Best Business Practices * Participated in the implementation of the design for the computing environment to include servers, workstations, applications, operating systems, and network connectivity Deputy Program Manager, Federal Emergency Management Agency (FEMA) Network System Security Plus, Inc May 2014 to January 2015 * Managed team of 70+ personnel on enterprise assessment of FEMA physical assets to reduce 600 systems to 112 information systems based on system criticality, boundary, and business requirements * Provided on-site support to field offices by identifying systems, creating security documentation, and assessment services for rapid authority to operate decision * Reviewed technical vulnerability findings with the Information System (IS) administrators, system owners, and information system security officers to identify risk and proposed mitigations identified in various audits * Managed project timelines, identified discrepancies in work products, and reports the progress of A&A project milestones tasks to assigned Team Leads Senior Functional Analyst, Deputy, Security Compliance SAIC November 2013 to May 2014 U.S. Customs and Immigration Service (USCIS) * Prepared security control assessment plans, security control assessment results, security requirements traceability matrices, and developed draft plans of action and milestones for the system stakeholders * Provided guidance and proposed solutions for identified vulnerabilities and provided risk mitigation recommendations for Office of Inspector General and internal audit findings * Developed processes and procedures in support of security compliance and risk management and drafted required policies and procedures in support of the USCIS Cyber Program Management Office directives Associate, ST&E Lead/Project Manager, House of Representatives Blue Canopy - Washington, DC July 2013 to November 2013 Washington, D.C. (Short Term Assessment Engagement) July 2013-November 2013 Associate, ST&E Lead/Project Manager, House of Representatives * Provided consulting services in support of risk management framework that included categorization of network and financial information systems using NIST SP 800-60 * Selected relevant NIST SP

800-53 controls based on risk assessment, conducted review of security controls, and provided updates to system security plans ISSO, Subcontractor to HP February 2013 to July 2013 * Managed and directed team of ISSOs for internal general support system compliance audit activities * Performed configuration and audit of hardware, software, firewalls, and telecommunication equipment hosted internally and in disaster recovery site for continuous monitoring effort * Provided analysis and documentation for proposed system changes, including security impact analysis and cost benefit analysis to various stakeholders Information Assurance Lead Compusearch Software Systems July 2012 to February 2013 * Monitored and performed security day-to-day operations for proprietary applications hosted offsite * Developed continuous monitoring plan to support ongoing authorization of secure hosting facility * Provided security guidance to application developers and tracked proposed changes to development environment and application Senior Consultant, SME, Department of Defense Deloitte and Touche, LLP January 2012 to July 2012 * Collaborated with various vendors on integration programs for access and connection points for endpoint security in various information systems * Provided security impact analysis (SIA) to determine if proposed technologies provide adequate security controls and system interoperability with existing information system components * Managed monthly updates to the Program Management Review TekSystems August 2011 to January 2012 ISSO, Federal Emergency Management Agency (FEMA) * Developed security documentation and tracking of acquisition decisions to build a federated identity management solution * Collaborated with FEMA Enterprise Architecture group to ensure that web services could be leveraged to request and report common operating picture (COP) for both certificate and attribute level mobile verification for Federal, State, Local, and Tribal stakeholders Lead Consultant, Security Engineer Verizon Federal Network Systems January 2011 to August 2011 DoD) * Performed vulnerability and compliance scans, and developed patch and configuration management plans * Created and updated accreditation packages and associated policy and procedure documents * Supported establishment and maintenance of configuration baselines for Windows Server, Windows clients, and SQL database Associate, Senior Security Analyst/Certification Agent Veris Group, LLC June 2010 to January 2011 U.S. Department of State

* Performed vulnerability and compliance scans to support ISSO staff for yearly assessments *

Created security assessment plans and reports, and generated the risk report memo for the authority to operate decision Information Security Analyst, Various Federal Customers SRA International, Inc - Fairfax, VA October 2005 to June 2010 Responsible for the creation and maintenance of information security documentation deliverables including: system categorization (SC), system security plans (SSPs), risk assessments (RA), system test and evaluation plans (ST&E), security assessment reports (SAR), plans of action and milestone plans (POA&M), system architecture diagrams, and policy and procedure documents Education Certified Information Systems Auditor Teneble Security Center August 2017 to October 2017 B.S. in Environmental Science Wheeling Jesuit University 1999 Certifications/Licenses Certified Information Systems Security Professional (CISSP) Project Management Professional (PMP) ITIL v3 Certified Cloud Certification Knowledge (CCSK)- Cloud Security Alliance (CSA) Certified Authorization Professional (CAP)- ISC2 CRISC January 2019

Name: Alexandria Jones

Email: heatherclayton@example.org

Phone: (998)236-7351x9663