Senior Information Assurance (IA)/ IT Security GRC Analyst Senior Information Assurance (IA)/IT Security GRC Analyst Senior Information Assurance (IA)/ IT Security GRC Analyst Gaithersburg, MD Work Experience Senior Information Assurance (IA)/ IT Security GRC Analyst Guidehouse, Tysons, VA April 2018 to February 2019 As a subcontractor to Guidehouse (formerly PwC Public Sector), lead Information Security and GRC projects and tasks, including: the production of the company's Compliance Framework; production of Guidehouse's Information Security Policy, and supporting policies, plans, processes, and procedures; review of change requests and requests for exceptions to policy, including but not limited to Identity and Access Management (IAM) changes; and leading implementation of RSA Archer and the design and production of Guidehouse's GRC Program Plan. Senior Information Assurance (IA)/ IT Security GRC Analyst DXC Technology - Herndon, VA September 2017 to February 2018 Managed the production of repeatable security processes, procedures, and concepts of operations (CONOPS), and System Security Plans (SSPs) for the Food and Drug Administration (FDA): Worked with the Chief Information Security Officer (CISO) to produce the FDA Cybersecurity Program CONOPS. Lead projects to determine gaps and metrics for reengineering and introducing new authoritative interdisciplinary standards of operation. Worked with assessment team to assist the ISSO in preparing a large General Support System (GSS) for annual assessment according to Risk Management Framework (RMF) requirements. Computer Systems Security Specialist - Level III Data Networks Corporation - Reston, VA October 2016 to June 2017 As a member of a small IT security team supporting the Centers for Medicare and Medicaid Services (CMS), assisted in the preparation of a build-in security model that can be used by CMS to guide the phases of system lifecycles from initial business interest through assessment and decommissioning: Participated in meetings with the Federal client and others, e.g. MITRE analysts. Ensured that deliverables, including the security model and automated processes and tools that support it and CMS's phasing in of DevOps methodology, are defined to meet client requirements within the scope of the statement of work. Senior IA GRC Analyst JHC Technology - Waldorf, MD October 2015 to July 2016 Subject Matter Expert (SME) supporting KPMG's Amazon Web Services (AWS) GovCloud system engineering and development, including

determination and documentation of system's support of organizational and Federal security requirements, standards, and NIST SP800-171 and SP800-53 controls in support of FISMA requirements: As SME and liaison between project staff (Federal client and JHC) and CISO staff supported the transition of United States Patent and Trade Office (USPTO) and NOAA shared services to AWS. Participated in JIRA and Trello-managed scrum sprints that included the development of SSP and other system security documentation required for the successful security assessment of the systems. Assisted JHC Technology's sales and internal project management. IT Security GRC Specialist (Lead Technical Consultant) Aquilent - Laurel, MD May 2015 to September 2015 Supported the ISSO for systems that provide the functionality for the "Learning" pages of the Center for Medicare and Medicaid Services' (CMS) Healthcare.gov site. Systems are built and hosted on Amazon Web Services (AWS) Infrastructure as a Service (IaaS) cloud offerings, including Linux Virtual Machines (VMs) on Virtual Private Clouds (VPCs) behind Elastic Load Balancers (ELBs), and are provided to consumers via Akamai services. Tasks included preparation for, participating in, and remediation after assessment of NIST SP800-53 security controls in support of FISMA requirements of numerous FISMA-reportable systems, including the following: Privacy Impact Analysis. Preparation of Memoranda of Understanding (MOU). System accreditation boundary determination. Audit Record Management procedure boilerplate and system specific document preparation. Security Impact Analysis. Risk Assessment and Vulnerability Assessment. Incident Response Planning. Senior Information Security Engineer (ISSO) ActioNet - Germantown, MD November 2013 to April 2015 Acted as Department of Energy (DOE) Office of the CIO (OCIO) ISSO Team Lead before temporary, but lengthy, disablement due to an accident. Returned as a senior member of the team. As a Senior ISSO, main responsibilities included acting team lead tasks in the absence of new team lead, maintaining Authorization to Operate (ATO) certifications and supporting Risk Acceptance and Annual Review efforts by verifying FISMA/NIST RMF, DOE, and OCIO compliance of new client systems as well as reauthorization of current systems; maintained/updated artifacts for those systems, in particular SSPs, and represented the ISSO team in meetings concerned with GRC, including weekly configuration management board

and continuous monitoring and other projects. Represented system owners in IATO, initial ATO, and reauthorization efforts. Addressed vulnerabilities found by Tenable/Nessus scanning. POA&M remediation and risk acceptance guidance and documentation. PIA, SSP, BIA, and Exemption/Waiver/Tailoring documents. Acceptance or rejection of change requests due to security posture. Reviewed, and provided guidance for, work by other DOE OCIO ISSOs. Assigned and scheduled work, and assisted in the suggesting additional services for the customer. Information Security Engineer/ISSO CACI - Frederick, MD October 2012 to September 2013 Maintained JMLFDC system ATO certifications and supported Risk Acceptance and Annual Review efforts, by verifying DIACAP RMF compliance on assigned client systems that required annual baseline and validation scans with automated scan tools (Retina, WebInspect, AppDetective and PGD, DBSRRs) and DISA STIG compliance: Produced and maintained updated DIACAP artifacts for systems Developed MSRs (Mitigation Strategy Reports) and POA&Ms, issued server certificates, maintained system records in VMS and TAD, and addressed manual checklists. Implemented, documented, and helped develop formal security programs, policies, and plans throughout the organization, and monitored compliance with those policies and programs. Responsible for providing technical guidance focused on information security architecture. Performed security research, analysis, and design for assigned client computing systems and the network infrastructure. Responsible for the prevention, detection, investigation and response with respect to security threats and attacks. Responsible for security alert incident response. Helped plan configuration changes for major security infrastructure platforms. Contributed general consulting (risk analysis) and project support in the area of information security to IT infrastructure and division computing projects as needed to support new business requirements. Participated in internal security audits and investigations. Monitored trends in information technology and security that could have an impact on the security of the organization's products, processes, infrastructure, or customers. Provided advice and guidance to less experienced staff. Participated in Agile development process. Information Security Analyst / Subject Matter Expert (SME) Valiant Solutions - Wake Forest, NC January 2012 to May 2012 Lead incident management process and procedures

development Technology Specialists, Inc. (TSI), Bowie, MD - McLean, VA October 2010 to December 2011 Under contract with LMI, Mclean, VA, assisted in the establishment of the Pension Benefits Guarantee Corporation's (PBGC) first overarching Information Security (InfoSec) Policy: Assessed all PBGC InfoSec Standards, Processes, and Procedures that support PBGC's InfoSec Policy for compliance with NIST and other Federal InfoSec standards, guidance, and requirements.

Developed matrix of moderate common/inherited and system-specific NIST controls with PBGC-assigned parameters. Lead incident management process and procedures development. Technology Specialists, Inc. (TSI), Bowie, MD October, 2010 - December, 2011 IA/Information Security Analyst / SME Supported the Administrative and Customer Services Division (ACSD) of the Bureau of the Census: Tracked, documented, provided guidance on, and managed the closure of 56 POA&Ms ahead of schedule, enabling ACSD to get a three-year Authority to Operate (ATO) for its largest system and continued in the closure of more than 200 POA&Ms in first year of contract in compliance with NIST and other Federal regulations and requirements. Ensured that system security baseline configurations were according to authoritative guidelines such as STIGS. Developed the Standard Operating Procedure (SOP) template used to document SOPs (facilitated by Team TSI guidance and management) as required to close many of the ACSD's POA&Ms that remain open. Managed the creation of ACSD's Configuration Control Board and developed their Configuration Management Plan. Managed technical writer tasks. Tracked and provided guidance on, and development of, the organization's initial Contingency Plan according to NIST SP800-34, including Business Impact Assessment (BIA) and SOPs. Senior Technical Writer (IA Analyst role and responsibility) Washington Technology Group - Silver Spring, MD August 2009 to June 2010 Reacquired Secret Clearance and utilized IA/technical experience and relationship-building/collaborative skills through interactions with DoD customers to achieve project goals by providing critical research, analysis, document management, inventory, and expert technical writing/editing services. Provided editorial assistance for proposals and collateral PR materials. Increased operational capabilities for the Biometrics Identity Management Agency (BIMA, formerly the Biometrics Task Force [BTF]) through development/implementation of

compliance initiatives in support of DoD IA requirements (DIACAP), Continuity of Operations Plan (COOP), Disaster Recovery, Security, and Continuity Plans, and general Information Assurance (IA) requirements. various companies 1984 to 2009 Contract work for various companies alternating between technical writing, and technical support, e.g. mil-spec documentation, and hands on hardware and software support. Managed all aspects of the IT of small companies as a contractor, including moving one company's IT to its new location fully functional in the course of one weekend. Education Certified Information System Security Professional University of Maryland Skills SECURITY, WEB SERVICES, DISASTER RECOVERY, HIPAA, NIST

Name: Zachary Perez

Email: lopezmaria@example.org

Phone: (904)971-4263x161