Independent Consultant & Senior Security Advisor Independent Consultant & Senior Security Advisor Independent Consultant & Senior Security Advisor - TMR Concepts Rockville, MD Work Experience Independent Consultant & Senior Security Advisor TMR Concepts October 2016 to Present * Assessment Lead and Assurance Manager: Oversaw and performed Security Assessment and Authorization work with a team of 20 junior to mid-level assessors. Fulfilled the Compliance and Assurance Manager role by ensuring all work was properly completed and the independence was maintained during assessment work. Served as the project manager and audit liaison for the Office of the Chief Information (OCIO) to facilitate compliance with OIG FISMA audit activities. * IT Security Control Assessment and Reporting: Providing IT controls assessment support to OCC, USAID, and MCC, including planning and conducting a broad array of IT security control tests for each Agency's general support systems (GSS) and major applications. Conducted and supported IT control reviews related to network infrastructure components, MS Windows infrastructure platforms, Linux operating system platforms, major database management system (DBMS) platforms, Agency financial system, web applications, Citrix remote access implementations, and enterprise content management applications (SharePoint and OpenText). Conducted reviews of Agency controls implemented for external information system service providers, as well as key system interconnections and interfaces. Assessment results documented in GRC tools including RSA Archer and CSAM. * IT Audit, Controls, and Independent Assessment: Supported OCC in the development of corrective action plans for IT control weaknesses identified through annual OCC assessments and OIG audits. Provided technical consulting support related to control design, efficiency, and effectiveness, and performed independent assessments related to the adequacy and effectiveness of remediation activities. Led a team of technical specialists in conducting an independent assessment of current IT contingency and disaster recovery plans and capabilities at a critical DHS component organization. Conducted an independent assessment of the procurement planning processes and draft solicitation materials for a major State of Maryland human resources management system implementation. Provided feedback on process definition documents and process diagrams for 12 core process areas (benefits administration, timekeeping, etc.), as well as

functional, non-functional, and process-specific implementation requirements. Developed and provided summary briefings and detailed findings and recommendations to the Deputy CIO and business office executives. * IV&V Management: Working with OCC personnel and stakeholders to remediate identified vulnerabilities. Provide guidance and expert analysis regarding methods of closure and completeness to assist in the complete mitigation of identified vulnerabilities and ongoing threats. Senior Information System Security Specialist Oasis Systems, LLC January 2012 to October 2016 * Training and Agency Support: Provided in-house instructor led training courses to Nuclear Regulatory Commission (NRC) employees and stakeholders. Created and taught the information system security officer (ISSO) and the systems administrator training courses with a concentration in security concepts and assurance subject matter. * Enterprise Assessor: Performed in-depth security risk assessments (SRA) with a highly-focused review on security scanning and vulnerability results and their impact the security posture of the agency. Performed security risk assessments on new and emerging technologies as an integral part of the acquisition and implementation phases at the NRC under the Office of the Chief Information Officer (OCIO). * Internal Control Assessment and Reporting: Supported NRC's Information Security Directorate (ISD) in the completion of the organization's annual management assessment of internal controls, in accordance with OMB Circular A-123 (Appendix A) requirements and associated implementation guidance and methodologies. Led and assisted with the development test plans and provided technical guidance to staff on the completion of tests. Assessed test results and advised Federal Agency personnel on the remediation of identified control deficiencies. * IT Audit and Controls: Assessed Agency policies, procedures, and guidelines against Federal laws, regulations, and standards, and assisted with the development and implementation of updates to address deficiencies. Assisted DHS with the development of a control crosswalk between OMB Circular A-123 and NIST Special Publication (SP) 800-53 and led the development of a new compliance framework for NRC-Designated Systems designed to integrate OMB Circular A-123 requirements with FISMA and NIST requirements and guidelines. As a consultant to the NRC Chief Information Officer (CIO), established detailed Security Test and Evaluation (ST&E) procedures to address OMB

Circular A 123, FISMA, and NIST requirements for annual security assessments of financial systems. Provided financial audit preparation, execution, response, and remediation support to the NRC CISO to increase IT system security compliance and reduce repeat audit findings at both the component and Department levels. * IT Governance: Assisted NRC in the establishment and refinement of IT governance structures, processes, and procedures, to include establishing a more robust enterprise configuration management board, updating systems development lifecycle (SDLC) templates and tools, and implementing mechanisms to more effectively leverage existing IT capabilities and pending investments, including SharePoint. * Procurement Support: Provided independent acquisition support services to clients related to significant system implementation initiatives. Developed functional and non-functional requirements based on optimized business processes, and supported the development of procurement documentation, including independent cost estimates, statements of work, instructions to offerors, evaluation criteria, and applicable terms and conditions. Supported the evaluation of technical proposal submissions, to include developing responses to vendor technical questions. * Information Systems Security Officer (ISSO): Provided assurance, documentation and security requirements support to NRC offices and information systems by building the supplemental security program for the different offices to prepare their information systems for security assessments and mandated audits. Security Specialist, ISSO Health and Human Services Department - Food and Drug Administration (FDA) October 2014 to June 2016 * Contractor Selection and Procurement Oversight: As a Federal employee, served on technical evaluation panels, and assessed vendor/contractor technical and management approaches against evaluation criteria. Reviewed FDA procurements, grants, and cooperative agreements for conformance to Federal Acquisition Regulations (FAR) and FDA policies and requirements. Oversaw the selected contractor internal independent assessment and audits of FDA information systems control assessments, security authorization packages, and integrating controls for FedRAMP cloud environments as well as on-premises data center security. * Program and Project Management: Provided program management oversight to assigned projects and project managers. Developed and oversaw the implementation of industry standard project management

methodologies and tools. * Process Optimization: Supported an office-level initiative to assess current organizational functions and processes and identify opportunities for improvement. Additionally, coordinated and assisted in the evaluation and deployment of cloud-based solutions. * Vulnerability Mitigation Program: Identified and assessed plan of action and milestone (POA&M) items as part of the FDA's security implementation program. Closed over 500 POA&Ms in conjunction with agency-wide efforts to strengthen the FDA's security posture. Information Assurance Analyst Richard S. Carson & Associated, Inc January 2010 to January 2012 * IT Audit and Controls: Planned and managed IT security audits and assessments related to user administration, change and configuration management, certification and accreditation (C&A), security planning, risk assessment, POA&Ms, and IT contingency planning. Facilitated the identification and assessment of automated testing tools for use in audits and supervised and performed security tests. Evaluated the results of technical testing and the adequacy of internal control mechanisms and developed recommendations to address identified weaknesses. Briefed senior agency officials on the objectives, scope, and methodology of the audits, as well as the audit findings and recommendations. Prepared and directed the preparation of over 12 audit reports to the NIH office of the Chief Information Officer (OCIO). * Process Optimization: Supported a division-level initiative to assess current organizational processes related to technical security testing, including testing preparation and the validation of test results. Identified and supported the implementation of opportunities for improvement. * Privacy Program Implementation and Disaster Recovery: Performed and reviewed Privacy Impact Assessments (PIAs) and security categorization documentation in accordance with FIPS requirements to assess level of data sensitivity for NIH information systems. Worked alongside NIH technical staff and stakeholder to conduct Contingency Plan testing using hypothetical scenarios and Lessons Learned documentation. IT Associate KPMG, LLP February 2009 to January 2010 * IT Audit and Controls: As a contractor to the OIG of many federal agencies, planned and managed an IT security audit related to remote and on-site access security at these agency's components. Facilitated the identification and assessment of the automated testing tools for use in the audit and supervised and performed security tests. Evaluated

the results of technical testing and the adequacy of internal control mechanisms and developed recommendations to address identified weaknesses. Briefed senior agency officials on the objectives, scope, and methodology of the audit, as well as the audit findings and recommendations. Prepared and directed the preparation of an audit report to agency officials and the OIG. * IT System Implementation Evaluation: Evaluated the implementation of federal information system's certification and accreditation tools and authority to operate (ATO) packages. Analyzed the description of functional system requirements, the translation of functional requirements into technical requirements, and the degree to which the development effort achieved technical system requirements. Reviewed the results of IV&V tests to determine system functionality and the adequacy of IV&V testing. Education Bachelor of Science in Management Information System Robert H. Smith School of Business, University of Maryland, College Park - College Park, MD 2008 Skills access (6 years), Active Directory, testing, HTML, security Certifications/Licenses Certified Information Systems Security Professional (CISSP) March 2016 to Present Additional Information * Leadership: Senior Security Assessment and Authorization (SA&A) and vulnerability analysis and management team lead heading multiple teams performing different security functions under one umbrella. Extensive knowledge surrounding different service and delivery platforms for customer requirements. Performance and review analysis of teams consisting of 5-20 security professionals. * IT Security, Audit, and Controls: Extensive security authorization, certification and accreditation as well as audit knowledge and experience assessing hundreds of government information systems for FISMA and FedRAMP compliance. * Information System Security Officer (ISSO): Provided information and assurance support to federal agencies as a system's representative performing front-end security functions to ensure the security and safe operation of federal support systems. Additionally, achieved the authority to operate (ATO) for the aggregate of systems at the FDA. * Vulnerability Analysis and Threat Management: Expert level experience and familiarity with vulnerability scanning and analysis tools including Qualys, Tenable Security Center, Core Impact, ThreatGuard, DISA SCAP content. * Risk Assessments: Experienced risk assessment and vulnerability analysis and mitigation specialist. Used discovered and known weaknesses to brief

senior leadership on the security posture of their agencies against vulnerability results and operating environment deficiencies.

Name: Angela Sherman

Email: antoniolynch@example.org

Phone: (755)495-2479x49234