IA SMR IA SMR Information Assurance Compliance Officer- NexSolv / MHBE Clinton, MD To secure a position in which my skills and experience as an Cyber Security Compliance Officer will be effectively utilized in a challenging environment that promotes development and employee growth. Work Experience IA SMR NexSolv / MHBE March 2019 to Present Mar 2019 - Present Analyze and define security requirements for Multilevel Security (MLS) issues. Design, develop, engineer, and implement solutions to MLS requirements. Gather and organize technical information about an organization's mission goals and needs, existing security products, and ongoing programs in the MLS arena. Perform risk analyses, which also include risk assessment. Work independently and lead MHE security staff through an assessment of information security controls related to MARS-e version 2.0. Complete Security Control Technical Testing, Network and Component Scanning, Configuration Assessment, Documentation review, Personnel Interviews and Observations for a moderate system. Create an independent Security and Privacy Assessment Report. Adhere to all security, change control and client processes, tools and methodologies. NexSolv / MHBE September 2017 to December 2018 Ensure that the AIS are operated, used, maintained, and disposed of in accordance with internal security policies and practices. Ensure that the AIS are accredited based upon NIST guidance and accredited the AIS utilizing the templates provided by DHS in 4300B, if it processes classified information Enforce security policies and safeguards on all personnel having access to the AIS for which the ISSO has responsibility Ensure users and system support personnel have the required security clearances, authorization and need-to-know; have been indoctrinated; and are familiar with internal security practices before access to the AIS is granted Ensure audit trails are reviewed periodically in accordance with departmental policy and the C&A documentation (e.g., weekly or daily) Ensure that audit records are archived for future reference and audit artifacts are generated as needed Initiate protective or corrective measures if a security problem is discovered Report security incidents in accordance with DHS Management Directive 4300 to the Authorizing Official and System Owner when an AIS is compromised or a suspected compromise has occurred Report AIS security status as required by DHS Management Directive 4300 and the AO. Determine when time-sensitive system patches identified by the DHS

Security Operations Center must be quickly implemented to protect systems Evaluate known vulnerabilities to ascertain if additional safeguards are needed Maintain a plan for site security improvements and progress towards meeting the accreditation Performing all ISSO duties as directed by DHS Management Directive 4 NOAA, Department of Commerce IT Security Program Policy, OMB, and NOAA Chief Information Officer NexSolv / MHBE September 2016 to September 2017 Sept 2016 - Sept 2017 Provide cyber security subject matter expertise to corporate and federal executives as it pertains to proposal development and security program development. Develop and maintain strategic and tactical infrastructure security plans Develop the NOAA, Department of Commerce IT Security Program Policy, OMB, and NOAA Chief Information Officer Develop and maintain plans, policies, and guidelines for the security architecture Perform a wide range of IT security support activities including: ? Security architecture, audit, and assessment ? Policy review and development ? Implementation, oversight, and enforcement of all security documentation, Plan of Action and Milestones (POA&Ms) and their timely closure, and artifacts in Cyber Security Assessment and Management (CSAM) ? IT security awareness and training, monitor and enforce compliance. Information Security Compliance Officer Collabralink/DOJ December 2015 to August 2016 Provided Program and Project Management of the DOJ Information Assurance initiatives which defined processes geared at satisfying NIST, FISMA, DHS, and FedRAMP requirements; Collaborated with federal program managers to ensure compliance with departmental security policies, and provide mitigation strategy and support for designated Corrective Action Plans. Program tasks completed: ? Provided management of Cyber Security reporting of data calls to DOJ CIO ? Managed and performed Policy analysis, development, and planning ? Performed compliance review of Risk Assessment, Security Assessment Reports, Pen Test ? Managed and performed update, review and audit of departmental Core Security documentation ? Provide Risk Management Framework compliance reviews for all DOJ OCIO managed systems ? Provided Management of DOJ OCIO Compliance Reviews for all bureau level systems Core Security documentation Security Authorization Documentation ? Provided Management review of Security Authorization and Assessment for all DOJ OCIO managed systems seeking ATO sign off ?

Managed development, dissemination, and implementation of DOJ OCIO security policies and procedures ? Developed and facilitated the Security training of DOJ employees when called upon Cyber Security Compliance Officer NOAA SMOMS October 2014 to December 2015 Managed internal organizational Assessment and Accreditation (A&A)in accordance with NOAA and DOC requirements ? Managed the organization's execution and reporting of the quarterly FISMA continuous monitoring reporting ? Managed the remediation of POA&Ms as part of the Assessment and Accreditation for each mission system ? Managed compliance reviews of system security plans and core security documentation based on the NIST, DOC CITR and NOAA Risk Management Framework ? Audited Reviewed, Updated and provided guidance of security program that includes Governance (A&A, Continuous Monitoring, FISMA, NIST, DOC, NOAA, and NESDIS policies and procedures). ? Applied Risk Management Framework techniques in accordance with DOC CITR 19 NOAA, and NIST SP800-37 Revision 1 ? Provided management of vulnerability scans/ review and vulnerability analysis reports for compliance with DOC and NOAA requirements. ? Managed A&A artifact acquisition in accordance with NIST SP-800-53A, DOC CITR 019 and NOAA Risk Management Framework Process ? Reviewed Tripwire Reports to detect anomalies and changes that deviate from "Known Good" baselines and provided feedback to determine corrective action for insecure or weak system configurations Cyber Security Compliance Officer NOAA OCIO October 2011 to October 2014 Provided comprehensive Cyber Security and Information Assurance Management support to the NOAA OCIO IT Security Risk Management Framework and compliance initiatives regarding adherence to FISMA, OMB A-130, FIPS 200 and NIST SP 800-53 mandates Specific examples include: ? Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of systems maintained on behalf of NOAA ? Ensuring compliance with the security requirements of Doc and NOAA policies, procedures, standards, and guidelines. ? Ensuring that information security management processes are integrated with NOAA strategic and operational planning processes. ? Provide optimal service in support of NOAA IT Security Continuous Monitoring effort by contributing significantly to the implementation of safeguards and processes designed to protect the confidentiality, integrity, and availability of NOAA's IT environment. Supported the NOAA OCIO Risk ? Reviewed and Assessed the implementation of Arcsight SIEM tool to ensure the configuration satisfied NOAA and federal security control requirements ? Manager by providing processes and procedures aimed at preparing NOAA to achieve more secure information systems and ensured compliance with federal information security standards by: ? Enabling more consistent, comparable, and repeatable assessments of security controls; ? Promoting a better understanding of NOAA-related mission risks resulting from the operation of information systems; ? Creating more complete, reliable, and trustworthy information for the NOAA OCIO - to facilitate more informed security authorization decisions and the issuance of ATO. Initiated development of an NOAA Information Assurance Program which defined processes geared at satisfying NIST requirements; work in concert with the existing compliant DoC/ NOAA security policies, and provide mitigation strategy and support for designated Corrective Action Plans and POA&M tasks. Program tasks completed: ? Provided Management of NOAA OCIO Compliance Reviews for all NOAA systems Core Security documentation Security Authorization Documentation ? Provided Management of NOAA OCIO Security Authorization and Assessment for all NOAA systems seeking ATO sign off ? Managed development, dissemination, and implementation of NOAA OCIO security policies and procedures ? Developed and facilitated the Security training of NOAA employees when called upon ? Provided management of Cyber Security reporting of data calls to Department ? Managed and performed Policy analysis, development, and planning ? Managed and performed compliance review of Risk Assessment, Security Assessment Reports, Pen Test and SCAs ? Managed and performed update, review and revision of System Security Plan, Contingency Plans and Core Security documentation ? Provide Risk Management Framework compliance reviews for all NOAA systems Senior Information Security Consultant Science and Technology Corporation May 2008 to October 2011 Provided comprehensive Cyber Security and Information Security support to the ESPC IT security compliance initiatives regarding adherence to FISMA, OMB A-130, FIPS 200 and NIST SP 800-53 mandates. Specific examples include: ? Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of systems maintained on behalf of ESPC ? Ensuring compliance with the security requirements of DoC, NOAA and NESDIS policies, procedures, standards, and guidelines. ? Ensuring that information security management processes are integrated with ESPC strategic and operational planning processes. Provided optimal service in support of ESPC IT Security Continuous Monitoring effort by contributing significantly to the implementation of safeguards and processes designed to protect the confidentiality, integrity, and availability of ESPC's IT environment. Supported the OSDPD ISSO by providing processes and procedures aimed at preparing ESPC to achieve more secure information systems and ensured compliance with federal information security standards by: ? Enabling more consistent, comparable, and repeatable assessments of security controls; ? Promoting a better understanding of ESPC -related mission risks resulting from the operation of information systems; and ? Creating more complete, reliable, and trustworthy information for DAAs - to facilitate more informed security accreditation decisions and the issuance of ATO. Initiated development of an ESPC Information Security Program which defined processes geared at satisfying NIST requirements; work in concert with the existing compliant DoC/ NOAA security policies, and provide mitigation strategy and support for designated Corrective Action Plans and POA&M tasks. Program tasks completed: ? Provided C&A Documentation review and remediation ? Developed, disseminating and implementing security policies and procedures ? Developed and facilitated the Security training of ESA employees ? Provided security reporting of data calls ? Policy analysis, development, and planning ? Review of Risk Assessment ? Review and planned revision of System Security Plan ? Review, update and revision of Contingency Plans Senior Information Security Consultant Radius Technology February 2006 to May 2008 Supported Agency Information Security Officer in the role of Compliance Officer providing FISMA, NIST, OMB A130, and FIPS 200 policy/procedural resource information and compliance road map data. ? Spearheaded agency 800-53 Implementation Plan in support of departments FISMA compliance mandate ? Perform research and analysis of federal regulations, compliance activities and industry best practices in development of agency Cyber Security processes ? Perform policies development, Analysis Reporting, and system assessments in support of Information Security Program development. ? Performed review of system audits to determine mitigation and resolution of negative findings ? Instrumental in development of strategic and tactical remediation response to security issues, incidents and vulnerabilities. ? Reviewed and updated Risk Assessments, Security Policies, ATO and Security Controls to bring client into compliance with OMB, NIST, FISMA, PDD 67 FPC-65, etc. ? Developed and Facilitated Tabletop Exercises, ST&E, After Action Reports and Plans in support of Disaster recovery program and Contingency Plan development. Senior Information Security Consultant Litmus Logic - Reston, VA January 2005 to February 2006 Perform research and analysis of federal regulations, compliance activities and industry best practices for Business Continuity and Disaster Recovery processes. ? Perform policies development, Analysis Reporting, and system assessments in support of Information Security Program development. ? Performed and documented Gap Analysis and closure reports. ? Developed Disaster Recovery and Contingency plans in accordance with NIST SP 800-34 as mandated by OMB A-130 section III and FISMA. ? Performed system assessments, technical analysis, and operational analysis in support of business impact analysis development. ? Researched IT organizational shortfalls and develop Plans of Actions and Milestones to assist in the mitigation and corrections of discrepancies. ? Facilitated Tabletop Exercises in support of disaster recovery program and COOP development. ? Developed Requirement matrix and checklist for Emergency Relocation Facility design and selection. ? Instrumental in developing road maps for implementing strategic and tactical system availability solutions. IT Security Specialist/Business Continuity Coordinator ANCON January 2003 to January 2006 Develop and manage Contingency Planning and Disaster Recovery Programs. ? Perform business impact analysis to determine system criticality in development stages of Business Continuity Planning. ? Development and testing of alternate relocation facilities. ? Develop presentations and road maps to address the remediation of critical vulnerabilities and mitigation of risk. ? Brief Management, staff and other clientele of the importance of security in the System Development Life Cycle Development process. ? Provide security education and awareness training to Management, staff and contractors. ? Performed system audits to acquire operational specifications to assist in design of alternate relocation facilities. ? Reviewed and updated Risk Assessments, Security Policies and Security Controls to bring client into compliance with OMB, NIST, FISMA, PDD 67 FPC-65, etc. Network Administrator/ Security Analyst Dewitt Army Community Hospital/C.E.S - Fort Belvoir, VA April 1997 to January 2003 * Evaluated corporate clients' needs, current systems and equipment and made recommendations and proposals for future enhancements to ensure security is incorporated in the SDLC. * Assisted in upgrading existing network configurations; supported implementation of new infrastructure to serve all applications. * Managed 14 subnets for IP Distribution to over 1300 workstations and associated network devices providing secure communications in the DOA MEDCOM. * Provided technical support and supervision for five System Administrators and their assigned applications to ensure compliance with Security Policy. * Installed, configured and managed backup solution and disaster recovery options. * Managed 23 servers (WINS, DHCP, DNS, FILE, PRINT, BDC, DBSS and SHARE) including 4 remote locations. * Researched and implemented vulnerability remediation for entire LAN. * Analyzed LAN and operating systems to identify and resolve security issues, ensuring excellent customer satisfaction and solid client retention. * Access Control Management: Administered WinNT/2000 domains, groups, rights, permissions and shared resources for 1500+ users throughout the LAN. * Provided configuration management support for WinNT/2000 Network including building, configuring, upgrading and troubleshooting all software and hardware. * Assisted in upgrade and company-wide implementation of WinNT and testing all units and network for complete functionality. * Responsible for workstation configuration, LAN repair and system maintenance. * Performed all levels of troubleshooting such as desktop support, hardware repair, software installation, software testing and Server repair. * Assisted the Lead Engineer with installation and configuration of hardware (Hubs, Switches and Routers) that enhance the overall performance of the network. * Provided network printer installation and configuration; provided implementation and assignment of TCP/ IP configurations and network interface. * Maintained 100% uptime for over 100 workstations in a fast paced, medical office environment contributing to the optimum performance status of the ADA. * Analyzed Server, PC and application issues, resolving quickly and completely ensuring maximum productivity and peak performance. US Navy, Various Locations Tactical System Specialist * Provided micro miniature electronic repair for airborne speech security systems and onboard computer systems. * Provided intermediate and organizational level testing and calibration for avionics and communication/ navigation systems. * Managed Maintenance Instructional Publications as assigned by Quality Assurance and Compliance office in setting threshold for IMD RFI Standards. * Provided I/O technical support to Navy fighter and photographic squadrons. * Supervised Tactical Air Reconnaissance Pod I-level team. * Provided tactical and mission capable system resolution for TACAN, Doppler, APQ-76, Radar Altimeter, IFF and Airborne Fire Control Systems. Education Certificate ISC2 Institute Security Management - Manassas, VA June 2007 Certificate COMPUTER LEARNING CENTER - Alexandria, VA March 2001 Information Systems & Networking Technology WINSTON-SALEM STATE UNIVERSITY - Salem, NC 1997 Military Service Branch: United States Navy Rank: E5 Certifications/Licenses Driver's License

Name: Deborah Cox

Email: levydawn@example.net

Phone: 874.592.4459