Cybersecurity Governance Consultant Cybersecurity Governance Consultant Cybersecurity Governance Consultant | IT Executive | Valued Leader & Mentor Dahlgren, VA Experienced Cybersecurity professional with 15+ years of experience designing security monitoring and cyber response solutions for large enterprises. Displays hands-on experience in planning, coordination, and maintenance of an organization s information security. Specializes in security assessments and authorizations for businesses and corporations. Visionary leader and highly capable change-agent that consistently refines and revitalizes strategies and procedures, introduces innovation, designs change, and facilitates solutions-driven team collaboration. Authorized to work in the US for any employer Work Experience Cybersecurity Governance Consultant N-FOSEC Consulting - Remote January 2014 to Present Serve as the principal advisor to program managers and information system owners on all Cybersecurity matters (technical and otherwise). Assist managers developing and implementing agency-wide security programs that require in-depth planning, installation and management. As a Cybersecurity Expert, understanding the nuances of security for each environment is imperative for strategic planning, management, testing, training and implementation. Improve Cybersecurity defenses, analyze and define security requirements for Multilevel Security (MLS) issues, and design, develop, engineer, and implement solutions to MLS requirements. Assist Administrators and Engineers with patching vulnerabilities, which is a critical function in maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems. Streamline installation, testing, and maintenance systems through development of an effective configuration management plan and establish baselines for tracking, controlling, and managing the assets comprised in the system. Utilize processes and technologies to detect compliance and risks associated with organization s environment, through assessing people, processes, and systems working together to support efficient and effective operations. Provide recommendations and assist with implementation of controls to address risks identified within these components. SME on host of other cyber-related topics. Sr Information Systems Security Engineer Tatitlek Corporation October 2015 to August 2016 Supported Program Managers, Project and Application leads across NAVSEA/NSWCCD and ensuring the required C&A

documentation is prepared, reviewed, and maintained in accordance with DoD/Navy/FISMA guidance Conducted Monthly, Quarterly and Annual Security Assessments to monitor the security posture and identify risks of various networks by reviewing security controls, ACAS/NESSUS scans, STIGs/SRRs, and POA&Ms. Actively participated in A&A and other Technology and Security related meetings. Developed and Integrated Master Schedule (IMS) to assist in the planning and scheduling of A&A work efforts. Served as Primary RMF contributor and SME for Prime re-compete proposal development. Developed IRP Checklist for record of events and proper tracking. Subject Matter Expert (SME) Syneren Technologies Corporation October 2013 to August 2014 Provided technical guidance for the NOAA Weather Service Program to include security analysis and mitigation findings for significant activities involving advanced persistent threats, system level compromise, and incidents deemed of high interest. Maintained responsibility for planning and monitoring of Cybersecurity and privacy policies, programs, compliance artifacts, and standards in support of government and industry security compliance, systems accreditation and management. Reviewed accreditation documentation, performing security analyses and risk/vulnerability assessments, conducting security tests and evaluations, and the coordination of SA&A activity for project teams. Applied knowledge of risk management framework, analysis, IA policy and procedures, and workforce structure to develop, implement, and to maintain or enhance the security posture of the system. Information Assurance Manager Seneca Resources March 2013 to August 2013 Provided Information Assurance (IA) leadership to twelve Information Assurance Officers (IAOs) for the F-35 Lightning II Program supporting 2000 users in locations throughout the US and eight international partnering countries Developed Vulnerability Management Tracking and VMS Reporting Schedule to address Patch deployment and Vulnerability tracking challenges. Led the HBSS enterprise upgrade effort for classified and unclassified networks to ensure DISA compliance. Created vulnerability management plan for the F-35 Lightning II Program to proactively prevent the exploitation of IT vulnerabilities that exist within the organization, and to reduce the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities. Provided oversight and approvals of enterprise IA certification documentation for various JSF classified and unclassified networks and applications, prior to DAA review by identifying, implementing, and managing IA capabilities and services to ensure that security risks are not posed to the network.   Led and coordinated in preparation for United States Cyber Command s (USCYBERCOM) Command Cyber Readiness Inspection (CCRI) and Staff Assistance Visit (SAV) of the F-35 Lightning II Program. Senior Information Assurance Analyst PSI Pax - Lexington Park, MD May 2012 to March 2013 Supported Program Managers, Project and Application leads across NAVAIR/NAWCAD in ensuring the required C&A documentation is prepared, reviewed, and maintained in accordance with DoD/Navy/FISMA   guidance   Validated the implementation of DIACAP IA security controls and reviewed package documents including System Identification Profile (SIP), DIACAP Implementation Plan (DIP), Validation Plan/Report, Scorecard, Plan of Action and Milestones (POA&M).   Reviewed Gold Disk, Retina, and Security Blanket scans to ensure systems are configured per DISA Security Technical Implementation Guides (STIGs) and are IAVM Compliant.   Reviewed system artifacts and provide feedback to the customer for consistency and accuracy as it pertains to the DoD 8500.2, including but not limited to Contingency plans (CP), Incident Response Plans (IRP), Standard Operating Procedures (SOP), Configuration Management Plans (CMP), etc. in effort to validate the systems/ networks security posture.   Utilized traceability matrix to depict a correlation of the Inherited, Non-compliant, and Not Applicable security controls between the DIP, Validation Plan/Report, and POA&M to ensure consistency between the documents. IT Security Engineer/Tester ManTech - Indian Head, MD June 2010 to May 2012 Contract with the Defense Information Systems Agency (DISA/JITC)   Coordinated the requirements, planning, training execution, and assessment phases of JITC IA exercise assessments for purposes of evaluating the COCOMs, Services, and Agencies ability to protect and defend the Department of Defense networks and respond to potential attacks against the Global Information Grid (GIG)   Developed and reviewed Director of Operational Test and Evaluation (DOT&E) reports for DoD information assurance risk assessment exercises. Collected and tracked data related to all POA&M activities in TAF.   Examined DoD Information Assurance Certification and Accreditation Process (DIACAP) scorecards for completion to gauge what additional information is required from the site, including the number of IA controls required, number of compliant/noncompliant areas, and assessed risk status of each non-compliant area to identify deficient IA controls and to ensure a successful exercise assessment. Conducted SharePoint Server Administration on classified network, which houses DoD technical and nontechnical assessment data collected during training exercises for further evaluation and analysis as it relates to the Incident Handling Program (CJCSM 6510) and DoD's IA Implementation guide (8500.2), including system backups and reviewing event logs, to ensure integrity and availability of system data. Developed, reviewed, and modified DoD IA Data Collection and Demographic forms in effort to satisfy requirements set by DOT&E Core Metrics Manual to produce accurate and valuable reports to maximize DoD network's compliance and security posture against vulnerability risks. Performed user account audits in Active Directory on SharePoint server as an access control measure to enhance system and network security (Contract with the Department of Homeland Security). Conducted vulnerability and compliance scan services for network devices, websites, and system applications in effort to enhance confidence and protection of valuable data and assets utilizing Nessus, Nipper, AppDetective, and Cenzic Hailstorm. Performed manual assessments identify false positive results and to verify that initial vulnerabilities have been mitigated or rectified. Reviewed system artifacts stored in the Trusted Agent FISMA (TAF) system to validate a system's compliance against DHS Security Requirements Traceability Matrix (SRTM), which list the NIST 800-53 and DHS 4300A security controls. Developed Security Assessment Reports (SARs) of vulnerability findings and recommendations of scanned systems and devices to the Chief Information Security Officer for approval, prior to implementation on the production environment. Updated Nessus compliance check scripts to correlate to DHS configuration guidance Navy Systems Consultant (Contract with the Naval Air Systems Command - NAVAIR/JTDI). Navy Systems Consultant Intergraph Corporation - Lexington Park, MD October 2008 to May 2010 Contract with the Naval Air Systems Command - NAVAIR/JTDI Implemented and monitored security measures for DOD networks devices using eEye Retina Security Scanner, DISA Gold Disk, and DISA Security Technical Implementation Guides (STIGs). Established and satisfied information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands. Built and managed VMware ESX servers 3.5 for JTDI and Electronic Maintenance Support System (EMSS) and Joint Knowledge Caching Servers (JKCS) Regional Servers and applications DoD programs. Developed security and procedural documentation, including sustainment plans, installation and configuration guides, vulnerability testing procedures, and baseline procedures. Implemented monthly DVD based technical manual update process for DoD disconnected military sites and ships. Education Master of Information Technology in Internet Security American InterContinental University - Hoffman Estates, IL Bachelor of Science in Business in Information Systems Bowie State University - Bowie, MD Skills Security (10+ years), Network Security (10+ years), Risk Management (10+ years), Risk Assessment (8 years), Networking (10+ years), Configuration Management (10+ years), Asset Management (10+ years), Computer Hardware (10+ years), Management (10+ years), Cloud Security Assessments & Authorizations (1 year) Links http://www.n-fosec.com https://www.linkedin.com/in/lisammonk/ Certifications/Licenses Certified Information Systems Security Professional (CISSP) Present MDOT Certified: Minority Business Enterprise (MBE) | Disadvantage Business Enterprise (DBE) | Small Business Enterprise (SBE) Present 541512 - MBE/DBE/SBE - COMPUTER SYSTEMS DESIGN SERVICES 541519 - MBE/DBE/SBE - OTHER COMPUTER RELATED SERVICES (SPECIFICALLY: COMPUTER DISASTER RECOVERY SERVICES; SOFTWARE INSTALLATION SERVICES, COMPUTER) 541690 - MBE/DBE/SBE - OTHER SCIENTIFIC AND TECHNICAL CONSULTING SERVICES (SPECIFICALLY: SECURITY CONSULTING SERVICES) Additional Information KEY SKILLS Risk Management Framework Incident Response Planning Security Governance and Policy Disaster Recovery Network Security Physical Environment Access Control Cloud Security Information Classification Systems Development Life Cycle (SDLC) Patch and Vulnerability Management Public Key Infrastructure (PKI) Physical Security Classified Environments Continuity Planning

Name: Danielle Santiago

Email: matthewhernandez@example.org

Phone: 333-788-9632