Cyber Security and Compliance Consultant (Iron Mountain.inc) Cyber Security and Compliance Consultant (Iron Mountain.inc) Senior Security Engineer Contractor - Iron Mountain.inc (Government Solutions) Fredericksburg, VA Director, Information Security Architecture & Vulnerability Management, Director of Cyber Security, Cyber Security Subject Matter Expert, Information/Mission Assurance, Senior Director, Project Manager, Project Lead   Ability Summary DOD Top Secret (SSBI) SCI Eligible   An Information Assurance and Information System Development Cybersecurity specialist (Architecture, Design, Process, Risk, ORM, Assessment, SLA, OLA) with over 30 years of experience in operation security, physical/personnel security, documentation preparation, Enterprise and Organization Risk Management, risk and threat analysis, policy development, systems security/administration, programming, customer support, and backup procedures. Perform as senior level position contractor for: FISMA NIST Certification and Accreditation program subject matter expert (SME), ST&E testing support and Risk Framework implementation for Commercial, Federal and Department of Defense customers. Navy certified as an Information Systems Security Officer (ISSO), Information Security Officer (ISO, CSO), Information System Network Certifier (NISTISSI 4015) and ISC2 CISSP. Demonstrated experience with DoD and NIST C&A tools Scan results, DISA STIGS, SRRs and similar standard tools to generate C&A artifacts and assessments. Demonstrated disciplines with Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act, Sarbanes-Oxley (SOX-OX), threat, risk, and mitigation analysis for implementation with various Certification and Accreditation (C&A) Risk Management processes. Authorized to work in the US for any employer Work Experience Cyber Security and Compliance Consultant (Iron Mountain.inc) JVT Advisors.inc, - Andover, MA August 2018 to Present

Iron Mountain Corporate and Government Sector Consultant. Provide Iron Mountain Risk Management, Cyber Security Architecture, Cyber Security Engineering and Information Security design, capabilities and product solutions.   Provided FedRAMP Cloud solutions, design and compliance evaluation, assessment in the product/service development life cycle.   Provided Government Cyber solutions for Architecture, evaluation and recommended actions for Government compliance frameworks.   Provided Information Security System Officer Tasks and operation to meet contract and government requirements. Provided IRM Global Policy Group with review, and updates for IRM Corporate Cyber Security Policy and Procedures. Provided IRM Cyber Solutions Architecture and Design review and updates for IRM Government Sector. Provided Government Sector Products and Services Architecture and Design reviews for meeting Government requirements, within multiple contracts and projects. Cyber Security Consultant (Contracts, ITAR, DFAR Business Proecess Reengineering) Oxford International (Jacobs Technology.inc) (HQ)) - Tennesse May 2018 to August 2018 Jacobs, a global provider of technical, professional, and scientific services, including engineering, architecture, construction, operations and maintenance. Provided experienced with procurement trade regulation standards in order to ensure our client s compliance. These standards are the International Traffic in Arms Regulations (ITAR), the Federal Acquisition Regulation (FAR), and the Defense Federal Acquisition Regulation (DFAR) and NASA RMF implementation. Provided Jacobs with NASA ATS contract, NASA certification and accreditation solution for NASA AO to issue a NASA to Contractor Authority to Operate and hold, process NASA sensitive data for the company network. (New NASA initiative). Provided DFARS, SOX-Oxley and MDA certification / accreditation services. Created cyber security program, defined, captured and implemented cyber security to DFAR and MDA requirements. Created, developed and amended corporate policy and work instructions. Developed compliant system s engineering processes, configuration management, auditing, multi factor identity management solution, and continuous monitoring solutions to meet NIST and DOD RMF and government requirements. Project Manager for indemnification and corrective actions for bringing company in line with regulatory and government expectations. Identity Management technologies worked with: Oracle Identity Governance Suite, RSA Token, Gemalto multi-factor authentication, SailPoint, and CA Technologies. Senior Security Solutions Design Engineer Contractor AT&T Government Solutions - Tysons Corner, VA May 2017 to May 2018 Responsible and accountable for solution quality, presenting solutions to client executive level; and representing AT&T solution direction to executive leadership, as well as alternative Managed Services. Responsibilities: assessing requirements, developing work breakdown, assigning engineering to cross functional teams, ensuring that cyber solutions integrate and interoperability, developing work statements to partner vendors, analyzing solution alternatives, assessing partner proposals, developing basis of estimates, developing proposal responses and developing solution cost model. Lead RFP, RFQ, RFI Teams using client strategy insights to capture proposals. Lead client executive leadership discussion on vision and challenges to include both solutions and design. Assess and develop new products, services and revenue streams for Cybersecurity Managed Services. Assess and recommend partner capabilities and teaming efforts within teaming. Work hand in hand with Business Development, Client Executives and Capture Managers for Cybersecurity technical and business requirements and overall positioning AT&T for opportunity capture. Total revenue work TCV approximately 2 Billion. Information System Security Officer Company Shift August 2016 to May 2017 Amyx.inc (8/2016) Cyber Security Subject Matter Expert (SME), ISSO Enhanced Veterans LLC - Reston, VA February 2015 to August 2016 SCA-R Role) for IT security and mission assurance for Defense Logistics Agency (DLA). DLA J64 provides assessor testing to discover vulnerabilities, cyber security risk evaluation, mitigation recommendations and SDLC Cybersecurity recommendations for all DLA, DLA Energy and DLA PMOs. Serve as advisor and Information System Security Officer / SCA-R, Assessor for multiple IT systems to include the DLA CONUS Enterprise WAN, the DLA OCONUS Enterprise WAN (Europe and Africa). Provide SME consultation for DLA DIACAP to RMF DOD transition (DOD Risk Management Framework (RMF)). Advise Program Managers and ISSM on FIPS 200/199 system documentation input and A&A (C&A) methodology strategy. Provide SME recommendations for DLA Enterprise IT Portfolios for Business Applications, Enterprise Capability, including Mil Cloud, DISA and DLA hosting. Cyber Security Subject Matter Expert Accreditation Representative Excentium, Inc - Reston, VA April 2014 to February 2015 Certification Authority Representative (CAR/SCA-R, SME) for Army G6/CIO Senior Information Assurance Officer (SIAO) and Army G6 CIO Policy SME, policy writing, field interpretation and Army G6 Representative. CAR Provided independent residual risk assessment for SES and General Officer level signature and review. As an Army CAR directly interface with Army IAPM's, System Owners, DAAs and Army Senior Leadership. Provide technical and mission residual risk and recommendation. Speak for the SIAO (CISO) in all communications regarding system Cyber Security measures. Perform as a team lead, team member and individual in a fast paced high performance environment. Provide Army cybersecurity Policy and regulation interpretation to internal and external of Army (DOD, Federal Agency, Contractors). Drafter Army Cybersecurity AR-25 which included Army RMF Policy and standard procedures and transition. Army Certification Authority / CIO Office (SCA) reviews and recommends approval for all IT used in the U.S. Army inventory, under development, and demonstration tests of new technologies. Maintain subject matter expertise in all legacy, current and developmental IT. Subject Matter Expert detail IT implementation weaknesses from Cloud to SCADA IT implementation. Define the weaknesses, mitigations, remediation, compliance to all regulatory requirements and mission. Support Army CIO mission. Assurance Manager (IAM) a CETA contractor to DLA J6 / DOD COMPCONTROLLER (20 Million+ DOD Budget Capability Development) Information Assurance Manager SAWDEY SOLUTION SERVICES, Inc July 2012 to June 2013 DLA PMO Bearvercreek, OH Provide Information Assurance Program support as Information Assurance Manager (IAM) a CETA contractor at Defense Logistics Agency (DLA) Project Management Office named Next Generation Resource Management System (NGRMS). Responsible for the secure and compliant acquisition, procurement, source selection and secure system development of DoD Budget this is a major application. NGRMS has Financial, Budget, multi-level security as well as multiple stakeholders from DoD Component to United States President. NGRMS is the automated system which delivers and provides justification for the entire DoD Budget to Congress and United States taxpayer. NGRMS will utilize emerging technology, processes, trends, capabilities and techniques to incorporate state-of-the-art information technology enabling the ability to process, administer and report resource management data and to automate business processes within a more robust analytical environment within the Office of the Under Secretary of Defense (Comptroller) OUSD . NGRMS will replace redundant inefficient legacy systems to provide for the effective formulation and justification of the Defense Budget. Responsibilities: Ensure compliance with Federal, DOD and DLA information technology and security requirements, policies, procedures and standards as applicable per DoD Business Capability Lifecycle (BCL) acquisition and development DTM. BCL is a DoD Business System Development Life Cycle (SDLC) process which replaces and augments the DoD System Development Life Cycle (SDLC) JCIDS/5000 process specifically for business system acquisition and application development. PMO Risk Manager working with PMO, Functional and Staff establish and execute the NGRMS Risk Program for the Program Manager. Develop and establish PMO Risk Management Program. Establish and execute PMO IAM PMO IA program. Establish PMO IA programmatic processes and programs, Working Integrated Product Teams, and Working Groups. Review all requirements, interfaces, design documents and test plans to ensure compliance with security requirements and Privacy Act compliance. Support the program office with the accreditation process by developing, supporting and maintaining DIACAP packages; develop IA related artifacts as required per BCL guidance; monitor software development for security issues, perform assessments of software releases and update documentation as necessary; perform informal security assessments; monitor and coordinate security actions for new interfaces; provide support to initiate and monitor corrective actions. Create IA related System Development Lifecycle documentation for PMO required for Milestone Decision Authority, Milestone A, B, C. Speak for Title 10 PMO on all IA related issues as Government Responsible to DLA CIO and DAA for IA Program and all IA related issues. Coordinate with DLA Certification Authority (CA), OSD CIO CA/DAA for hosting security requirements and building body of evidence to support application hosting. Source Selection Board Member for NGRMS contracts award. Coordinate with Contracting Officer, Contracting Officer Representative, Program Manager for all NGRMS specific IA language, constraints and IA requirements. Develop and defend NGRMS Acquisition Information Assurance Strategy (AIAS) Security Auditor (Project Management) Senior Information Assurance - Arlington, VA May 2012 to July 2012 Provide Information Assurance consultant services for NASA Mission Systems Chief Information Assurance Officer (CISO) and Chief Information Officer (CIO). Provide NIST and FISMA based IV&V Certification and Accreditation for NASA Mission Systems. NASA mission systems are primary NASA services which provide many external entities, US Government, Foreign Governments, Corporations capability for launching and control of space vehicles and ground control stations. Type of systems: Mission (Satellite Control), Mission Control (Rocket Launch Control), Business, LAN, WAN, Enclaves, Data Centers, Network Operations Center (NOC), Security Operations Center (SOC), Industrial Controls Systems (ICS), SCADA, SAP, Enterprise resource planning (ERP), Science, Research and Development (SR&D), Research, Test and Development, Industrial Control Systems (ICS). Responsibilities: Provide NIST and FISMA based Certification and Accreditation for NASA Mission Systems. Determine risk to organization, data and customers. Provide NIST based certification packages, Security Assessment Risk and Residual Risk statement and out brief with Authorizing Officer (AO). Manage customer expectations and insight services for proposal submission including content and structuring. Capture the work break down schedule to meet or exceed customer expectations. Negotiates acceptable risk and Plan of Actions and Milestone entries for NASA internal organizations. Conduct security assessments, ST&E and IV&V as the Independent Auditor. Interpret and apply the following policy and guidance to NASA IT Systems evaluations: ? NIST SP800-18 Guide for Developing Security Plans for Federal Information Systems. ? NIST SP800-30 Risk Management Guide for Information Technology Systems. ? NIST SP800-53 rev3 Recommended Security Controls for Federal Information Systems. ? NIST SP 800-53A rev1 Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans. ? SP 800-82 Guide to Industrial Control Systems (ICS) Security. ? NASA and NASA Goddard procedures and best practices. Responsible as a corporate entity to the NASA Goddard CIO and Authorizing Officer (AO/DAA) for accurate assessments of CIO IT Systems. Responsible for business development and contact development Responsible as a Team Lead for product and deliverable Responsible to certify the assessment products Advisor to Board, Business Development; Information INTEKRAS. inc - Sterling, VA January 2012 to February 2012 Business Development - Principle He provides consultant services for corporate business development efforts. Provides fresh perspective to drive INTEKRAS business forward in the areas of: Business Growth & Planning, Strategic Marketing & Planning, and Cost Reductions & Restructuring. He enables growing business relationships within the Information Assurance (IA) business community. Provides expertise in INTEKRAS ' IA business line and future of the IA and Cyber Security business line to the Partner's for business growth. Analyzes, recommends and provides long and short-term business strategy to capitalize on IA and Cyber Security community opportunities. Advises CEO and Corporate Partners on Federal, DoD and Corporate IA needs, targets specific business marketing strategies and opportunities that meet and grow the business vision. Using IA and Business expertise executes service as Red/Gold Team IA SME. Provides customer expectations and insight services for proposal submission for content and structuring the work break down to meet or exceed customer expectations within the proposal. Provides customer expectations and insight services for proposal submission for content and structuring the work break down to meet or exceed customer expectations within the proposal. Subject Matter Expert Information Assurance / Cyber Security NGB A6 CIO NCI. inc - Reston, VA March 2009 to December 2011 Support National Guard Bureau Directorate of Air Communications (NGB/A6) Chief Information Officer (CIO) as an embedded contractor to extend the Government's workforce with specialized expertise. Core responsibilities include Information, Compliance and Mission Assurance Subject Matter Expertise (IA SME) to the ANG/CIO and ANG/CISO. Responsible include IT capability investment, requirements and procurement compliance with OMB CPIC/ITIM. Provide key decision presentations of Air Force, NIST, OMB and Congressional mandates and instructions on matters of C&A, IA, mission assurance, IT Security, IT Investment, enterprise resiliency responsible execution of Enterprise Program Office responsibilities, technical security implementation, and Information Assurance and Security Program analysis. He provides SME services for FISMA implementation, ANG and ANG Program Mangers for Business Process Analysis and IA Compliance and Oversight using AF EITDR and EMASS. Directly advises the Chief Information Security Officer. During provides IT Portfolio Management with return on investment, requirements for capabilities to functionality review. Is one of two people designated in writing to represent NGB/A6 to the Air Force DIACAP TAG advisory body to the AF-CIO, represents ANG interest on multiple working groups on behalf of NGB/A6. Present Air National Guard IA Strategy and Concept of Operations to Senior Air Force Leadership (AF-DAA, Senior IA Officer and the AF CIO) offices. Briefs and provides Air National Guard unique implementation strategy for Senior Leader Buy-in, assist in scoping AF change in business process of IA, investment and Security strategy. Represent ANG interest and convey impacts to Senior Leaders at AF Working Groups, High Performance Teams for IT, IT Security, IT Governance and C&A. Working with other AF top level SME and Government Leaders deliver future strategy, impacts and vet decisions prior to Agency and organization implementation. Member of core AF SME working group develop Air Force C&A Transition from DIACAP to NIST security standards. Air National Guard Portfolio Manager (PfM) - ANG IT Investment Management (OMB ITIM) established, maintain, govern and monitor compliance with OMB Circular A-11 Section 300.7 through Capital Planning and Investment Control (CPIC) processes. CPIC structure ensures that all IT investments align with the Enterprise Architecture (EA), capability and functionality are appropriately applied to a mission and investments support business needs while minimizing risks and maximizing returns throughout the investment's lifecycle. ANG CPIC relies on a systematic approach to IT investment management in three distinct phases: select, control, and on-going evaluation, to ensure each investment's objectives support the business and mission needs throughout the lifecycle. As PfM managed and responsible for all Air National Guard's IT Portfolio Management program acting as decision authority and advisor for ANG EITDR Program Manager's System Development Life Cycle (SDLC) through Enterprise IT Investment Repository (EITDR) and ANG AF instance of EMASS. Developing policies, procedures, and methodologies for assessing the operational effectiveness, return on investment, capability overlap, and strategic/policy alignment of IT systems, applications, networks, and other infrastructure assets to comply with OMB CPIC and ITIM. Skilled with optimizing IT portfolios, identifying duplication systems/assets/technologies/ capabilities /functionality within the organization, and conducting alternatives analysis (AoA) to determine the optimal approach for eliminating unnecessarily redundant assets, and maximum return on Agency investment. Advise and assist System Owners and their Program Management Offices with preparation of Exhibit 53 and Exhibit 300s. Exhibit 53 is the budget report on Information Technology expenditures. The report contains basic information that links internal planning, budgeting, acquisition, and management of IT resources. Exhibit 300 is the budget justification and reporting document that is required by OMB for major IT investments. Exhibit 300s provide continued Business Case to Senior Agency Leaders normally applied to investments of three million dollars or more, or those investments, capability or functionality that have high executive visibility. In capacity of SME provides White Papers and similar analytical deliverables, developed the ANG 2010 FISMA Implementation Plan that resulted in 89% ANG Wide compliance an average of 45% increase over the last three years. He provided the plan that established ANG SBU Enterprise; this collapsed 200+ Unit enclaves under one governance and program co Business Development, Information Assurance Consultant MedTrends. inc - Reston, VA December 2008 to March 2009 Business Development - Principle He provides consultant services for corporate business development efforts advising for contract proposal submissions that have an Information Assurance focus to ensure feasibility and quality content. Provide Red Team IA SME services advising on customer expectations and insight for proposal submission for content and structuring the work break down expectations. Subject Matter Expert Information Assurance Knowledge Consulting Group, Inc - Reston, VA December 2008 to February 2009 Support Immigration and Customs Enforcement (ICE) a component of Department of Homeland Security (DHS). Provide Information Assurance Subject Matter Expert (SME) Information Assurance services in accordance with NIST, OMB, DHS mandates and Congressional Federal requirements. Capacity of only project SME provided FISMA Performance Plan for IAD Component implementation, Component wide Business Process Analysis for IA Compliance and Oversight and Information Assurance Governance branches. FISMA compliance analysis, Office of Management and Budget (OMB) mandate compliance, support services include: Business Review and Analysis and follow on analysis and assessment report development. In capacity of SME provided White Papers and similar analytical deliverables. He provided CISO type analysis for IA Program improvement for Oversight, Compliance and Information Assurance Governance. Identity Management - During SME support by IdM Program Office Manager for DHS/ICE HSPD-12 Identity Management Office requested consult on Program Risk. He evaluated DHS/ICE implementation and execution of the Identity Management Program for Program Risk and resolution. Recommendations that resolved Program and Project risk factors were satisfactory delivered to the customer. Evaluation resulted in a deliverable and executable strategy for customer implementation. Alternatives and inter-agency-component actions were included that would lead to successfully implement HSPD-12 DHS/ICE CaC Card and PIV 201 compliant credential program. Plan of Actions and Milestones for the Project and Program level execution included: evaluation of Program objectives and timelines, evaluation and assessment of Active Directory execution and Active Directory technical implementation to meet PIV 201 technical requirements. Senior IT Security Analyst - Principle Data Systems Analysts, Inc - Fairfax, VA July 2006 to December 2008 Supported clients by providing Security C&A Subject Matter Expert (SME) services in accordance with NIST: 800-53 (Security Controls), 800-26 (Self Assessment) / FISMA Self Assessment, 800-37 (C&A of Federal Systems), 800-34 (Contingency Planning), 800-32/35 (PKI), 800-30 (Risk Management), 800-27/64 (SDLC IA), 800-18/61 (Security Planning), 800-42/85A (Security Testing/PIV Testing). Also testing and compliance with Federal Information Processing Standards (FIPS): 191 (Analysis Network Security), FIPS 199 (Security Categorization), FIPS 200 (Security Requirements), FIPS 201 (PIV) and all federal mandates such as FISMA, Homeland Security Presidential Directive - 12 (HSPD-12), HIPPA, Department of Defense Intelligence Information Systems (DoDIIS) and Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) requirements. Support services include: System Security Authorization Agreements (SSAA) Review and Analysis, System Security Plan Review and Analysis, Security Control Assessments Planning and Implementation, and Security Certification Documentation. Also, perform follow on analysis and assessment report development. In capacity of SME provided SCAP standards and technologies integration and deployment analysis. In capacity of SME provides executive level briefs, and customer interface for issue analysis and solution implementation. C&A Team Lead FISMA - Veterans Affairs O&IT FISMA and VA6500 Certification for 604 systems in a 10 month time frame at Hospitals, Finance Centers, Central Pharmacies. As Team Lead coordinated team C&A efforts, established senior technical representative on site and managed customer expectations for Information Security Officers, Chief Information Officer, Facility Director, and System Owners.

Operate, review and recommend improvement into IA2 software suite development (SCAP compliant tool). E-Commerce / E-Authentication Security Consultant - State of Delaware Internal Revenue Service GRT Program. Provided SME services E-Commerce Security Technical, Programmatic, source code development, High Level and Low level design analysis to the GRT E-Commerce Enabled Program within the Delaware State complex network. GRT Program provides a secure web-enabled interface for 80% of the United States incorporated companies for corporate tax E-Filing. GRT system resides inside the State of Delaware's secure enterprise infrastructure in a Mid-Tier environment. C&A Project and Technical Lead FISMA - Veterans Affairs PIV (HSPD-12) Identity Management Program - Lead for DSA.inc C&A team resulting in the certification of the Veterans Affairs Personal Identity Verification (credential) Program. Provided VA PIV project C&A for the body of evidence to include VA policy, government regulations and compliance for OMB regulations (A-123, A-127, A-130), FISMA law, NIST and FIPS requirements. He represented DSA and sub-contractors to the Government Customer as Project and Technical Lead. C&A Project and Technical Lead Identity Management (HSPD-12) Commercial - Capacity of the FiXs Security Working Group Lead Certification Authority evaluated all FiXs systems and solution for risk acceptance. Certification Authority responsibilities executes independent Security Control Assessments, provides for Implementation Technical Guidance of established security requirements and concepts and manages all authorized system POA&Ms to provide a complete FiXs Risk Assessment. Evaluates all applying companies and organization systems documents SDLC, Business, Security Risk Assessment and assigns recommended Plan of Actions and Milestones (POA&M) to reduce the FiXs Organization's Risk. Final delivery to FiXs.org Board provides a recommendation to the FiXs Chairperson/DAA (Authorizing Authority) and the FiXs Board. The Federation for Identity and Cross-Credentialing Systems (FiXs) - Executed DMDC (DEERS) C&A using NIACAP process, DoDi 8500.2 and NIST 800-53 security control standards. Resulted in successful establishment of DoD Cross-Bridge of FiXs and DEERS CaC systems. FiXs CA provides the Federation for Identity and Cross-Credentialing Systems (FiXs) C&A and authorizing through the FiXs Authorizing Official (AO, DAA). Provides support as the only authorized Certification Authority

(CA) for FiXs. CA is responsible for advising the FiXs AO and applying companies for Certification disposition, evaluation and certification body of evidence of petitioning systems to NIST, FIPS and FiXs Policy, Guidelines and Business Practices. FiXs is a not-for-profit HSPD-12 compliant dispersed organization for IdM solutions that meet FiXs and use FiXs certified credentials. For FiXs provided key technical expert evaluation. Submarine Force Information Security Officer U.S. Navy COMSUBFOR - Norfolk, VA February 1984 to October 2006 Established and maintained Information Assurance Program, Certification and Accreditation Program and Operational Requirements for Component Level programs. Executed Program Manager of IA Team for six sailors and 3 contractors to successfully implement IA and C&A tasks to meet DIACAP and DITSCAP requirements. Provided Submarine Fleet with DAA and Developmental DAA interface for all Ashore facilities, Afloat units and developmental systems of the Undersea Enterprise. Position requiredresource scheduling, budgeting, technical proposal review, technical guidance and training the IA Team. Established Team working environment for complex technical problems involving all aspects of Information Assurance and IT Operational Programs. Analyze Program needs and current security regulations and guidelines to determine and address Information Assurance Program solution and Request for Proposal requirements. Provided direct oversight and managements of data collection and DoD reporting for all activities. Performed reviews, analysis, tests and evaluations, and produced reports, presenting findings and recommendations, to DAA and other Executive groups. Performed Certification and Accreditation and FISMA Compliance Reviews within the Undersea Enterprise to meet DoD requirements. Update component Guides and Templates, in accordance with published DoD and NIST standards. Managed and approved weekly and monthly Status reports, scorecards and other management tools to achieve 100 % compliance with DoD requirements. Conduct quality assurance on all tasks and contractor deliverables prior to submission to Executive Groups. Evaluated personal performance of IA Team Members for career advancement, and provided evaluation of contract performance to COTRs. Submarine Force Information Systems (Certification and Accreditation Compliance and Implementation, All Information Systems Requirements) - Manager, Mentor, SME Submarine Force IT Operational, Developmental Requirements and Security - Manager, SME ? Includes: Identify IA, security and operational system issues, research and recommend preventative/mitigation controls, develop recovery strategies, conduct business impact and privacy impact analysis, C&A compliance, system security control assessment, development of continuous monitoring program, configuration management and control, Interconnection Agreement development and compliance. Submarine Force IAVM (Information Assurance Vulnerability Management Program) - Manager, SME Submarine Force PKI implementation, planning, policy - Manager, SME Submarine Force Command and Control - Manager, SME Submarine Force Certification and Accreditation to DITSCAP, DIACAP and DoDIIS requirements - Manager, SME Submarine Force Wide Network Inspections Shore and Afloat - Manager, SME Submarine Force IS Policy, Documentation, Training, Planning, Metrics - Manager, SME Member DoD IAWG (Information Assurance Working Group) Developing DoD 8500-1M - impacts Member Navy IAWG (Provide validated requirements and provide priority to Navy IA implementation) Member COSG (Development Working Groups interacting with Contractors/Program Offices to provide Leading Edge IT solutions that meet requirements and recommend acceptance) - IA SME (DoD IIS, DITSCAP, DIACAP, HME, Verification and Validation (IV&V). SWFTS (federated architecture incorporating a multi-level (SCI, Secret, Confidential) periods processing environment, DoDIIS, DIACAP standard) IA, C&A, process and development review- Customer acceptance. Education Bachelor of Business Administration in Management Information Systems Strayer University - Fredericksburg, VA January 2013 to January 2017 Master's Certificate in Secure System Development Lifecycle Naval Post Graduate School NPS - Monterey, CA February 2005 to April 2005 CERTIFICATE Naval Post Graduate School March 2004 University of Phoenix Skills training, budget, Word, Strategic Planning Military Service Branch: United States Navy Rank: COMSUBFOR IT ISSM Certifications/Licenses Certified Information Systems Security Professional (CISSP) October 2005 to September 2018 CISSP Security Guard

Name: Jeremiah Davis

Email: wwoodward@example.org

Phone: 2013600135