**Fay Peterson, MSc, PMP, ITILv3, TOGAF**

(240) 463-1304 Mobile/Direct

**Email**: [fpeterson@eamsecured.com](mailto:fpeterson@eamsecured.com)

**SUMMARY**

* Fay Peterson has 20+ years of employing Architect and project management techniques to provide hands –on project management experience.
* Ms. Peterson’s current focus is Information Assurance (IA) and Cyber-Solution Architecture for the enterprise, Governance Risk & Compliance (GRC)Audits and Assessment Accreditation management, as well as full system development life-cycle (SDLC) security controls auditing using the NIST SP 800 - 53 security controls guidance, the NIST 800 -37 & 39, Risk Management Framework (RMF), Identity, Credential, and Access Management (ICAM), and NIST 800 -171v.6, Cybersecurity Maturity Model Certification (CMMC) audits for non-federal organizations.
* Strong communication skills evident in her ability to develop, draft and finalize Federal Government enterprise governance policies, and Standard Operating Procedures (SOPs), Incident Responses strategies to promote effective contingency planning (CP) and continuity of operations (COOP) capabilities.
* Ms. Peterson has a solid reputation of providing hands-on expert-level support to “C-Suite” managers, as well as technical staff to solve major security issues including the Risk Assessments (RA), security requirements analysis, Continuous Monitoring Assessments, Assured Compliance Assessment Solution (ACAS) implementation, vulnerability management planning, development, deployment. She successfully completed the security authorization processes for the Federal Energy Regulatory Commission (FERC) Google Federal Cloud – IaaS and PaaS capability under the Federal Risk Authorization Program (FedRAMP). All the system management by Ms. Peterson were successfully granted a three (3) year Authorization-to-Operate (ATO).
* Ms. Peterson has established security configuration management (CM) planning, change control, policies, and standardized procedures to verify and validate correct IT security implementations. She developed a comprehensive Vulnerability Management Program for the Defense Information System Agency (DISA) classified (SIPRINET) and unclassified (NIPRNET) laboratories to improve network scanning times and IT system vulnerability mitigation.
* She also established multiple security data analytics pilot programs for testing and evaluation for critical software deployments. Her penetration tools and security analytic experience includes Tripwire, Core Impact, Assured Compliance Assessment Solution (ACAS), Tenable Nessus, and HP Web Inspect. She is well versed in Federal Information Security Management Act (FISMA), the Department of Defense Information Assurance Technology Certification and Accreditation Process (DIACAP), and the National Information Assurance Certification and Accreditation Process (NIACAP).
* Currently these two processes are the main approaches used as methods to define the Intelligence Community & Defense (ICD) 503 IT Assessment and Accreditation (A &A) process, scope, roles, responsibilities, and guidance not only for Department of Defense, but also for all federal departments, agencies, and bureaus of the executive branch of the U.S. Federal Government.
* Ms. Peterson has worked as an independent third-party certifier and traveled to many locations in the US to performed audits for classified, and unclassified IT systems to validate security compliance with an established set of security requirements identified by system owners or by the NIST Special Publications (i.e., 800-53a, Rev3 & 4).
* As the Information Assurance Manager (IAM) for Joint Guardian Installation Protection Program, Ms. Peterson collaborated with GS-14 and 15 stakeholders to establish, maintain, and communicate a technical enterprise security roadmap to successfully certified and accredited the DISA Joint Interoperability Test Command (JITC) NIRPNET and SIPRNET laboratories at FT Meade, MD, with a full (3 year) Authority-to Operate (ATO).
* Ms. Peterson has subject matter expertise in analyzing and defining IT cyber security requirements and developed and finalized many policies for a variety of computer and telecommunications systems to

ensure compliance with Department of Army (DOA), the US Air Force, the Department of the Navy (DON).

* Ms. Peterson is an experienced IT Full System Life-Cycle Development (SDLC) Engineer. She assessed evaluates requirements for IT system usage and developed continuity of operations (COOP), and configuration management plans for the necessary acquisition to support future automation (hardware and software) requirements.

**CERTIFICATIONS**

# IT Management:

* PMP - Program Management Institute (PMI) **PMP** Certification ID **# 2804325**
* Information Technology Infrastructure Library (ITILv**3**) - Foundations: Cert. **# 882761**

# Enterprise Architect

* The Open Group Architecture Framework (TOGAFv**9.1**) version 9.1
  + Certified TOGAFv9.1 Level I Foundations cert **# 97248**
  + Certified TOGAF v9.1Level II-Master Certification **# 97561**
* Zachman EA Center of Excellence, Certified **Enterprise Assurance (EA) Solutions Architect**,
* Department of Defense Architecture Framework (**DODAFv2**),
* Federal Enterprise Architecture Framework **(FEAF**),
* NIST FedRAMP- Risk Management Framework (**RMF**), **NIST SP -800 series 37, 39,53 and 171**
* NIST Certified Federal Information Technology Security Program – Manager (**FITSP-M**)

# DoD8570 Level III

* + Certified Information Security Manager (**CISM**) Cert. **# 1116600**
  + Certified in Risk and Information Systems Controls (CRISC) Cert. **# 1106328**
* CompTIA Security+
  + Security Plus 201 (**Security+)** Cert. **# COMP001020160731**

### Cloud

* AMAZON **AWS Cloud Practitioner**, **# AWS03849135**
* AMAZON **AWS Cloud Security Compliance**, 2019
* AMAZON **AWS Security Services Fundamentals** 2019

**PROFESSIONAL EXPERIENCE**

**ENTERPRISE ASSURANCE MANAGEMENT CORP., (EAMC)**

|  |  |
| --- | --- |
| **Senior Cyber Project Consultant& Manager** | **07/2022– Present** |
| * Project Management | * Business Development |
| * Cyber Security and GRC Consulting | * Risk Assessments, and IT Audits |
| * Business Accounting * Project delivery and oversight experience with daily/regular customer interactions (Federal Managers and Technical staff, as needed) * Excellent verbal and written communication skills, and demonstrated leadership attributes. * Ability to implement, understand and communicate information security requirements for IT systems through the Risk Management Framework (RMF) * Ability to effectively communicate IT Security risks to senior executives and technical staff. * Certification(s) in information technology security (i.e., CISM, CISRC, Sec+, etc.)   Experience working with Governance, Risk and Compliance (GRC) tools (i.e., Kaseya Dashboard - RMM)   * Implement Continuous Monitoring, including annual   assessments and inputs of automated security tools | * Business Capability Briefings * Technical PM, or Senior Information System Security Officer (ISSO) / Information System Security Manager (ISSM) role for a large federal organization(s) or multiple Systems * Ability to manage customers and mentor staff on concurrent projects and tasks. * Possess deep functional knowledge in all areas of federal cybersecurity compliance and guidance documents, including OMB Memorandums, FISMA, FIPS and NIST Special Publications, including NIST 800-37,39, 800-   53 Rev 4 & 5, and 800-171 |

|  |  |
| --- | --- |
| (such as Kaseya vulnerability scanning tools) that will add to  the understanding of an Agency’s security Risk Posture |  |
| **CVS Aetna Health, Governance, Risk & Compliance (GRC) Lead Project Manager(PM)** | **05/2022 – 07/2022** |

* As a GRC consultant responsible for “Gap” analysis in cyber security policy, processes, and security controls. Draft, and finalized a deliverable with a comprehensive action plan (CAP).

## OBVERSE INC. 06/2021 – 10/31/2021

**Chief IT Cyber Security Compliance Project Consultant**

* Information System Security Manager (ISSM), Governance, Risk & Compliance (GRC) Lead for the District of Columbia (DC) Health Care Finance (DCHF) DC Access System (DCAS).
* Responsible for the development and maturing of the Information Technology Risk Management GRCprogram by developing and enhancing Information Security Policies and Standards, KPI’s, and KRI’s.
* Lead security projects to ensure security controls are applied appropriately in the Datacenter and Cloud environments.
* Perform Product and Vendor Security assessments for IT and SaaS solutions across the DCAS toconfirm, enhance, and monitor Information Security adherence.
* Provide independent oversight and challenge of all enterprise risk management activities, ensuring thatrisks are sufficiently mitigated.
* Manage a team of professionals who oversee all aspects of IT Risk across the DCAS.
* Performed cyber-security analysis and compliance with AWS and NIST, HIPPA, Sarbanes Oxley, Internal Revenue Pub 1075 compliance.
* Lead the DCAS CLOUD Working Group & Steering Committee for Federal Regulatory Compliance
* FISMA, FISCAM, audits and developed system Security plans (SSPs) for Office of the Technology Officer (OCTO) IT system for NIST SP 800- 37, 64, and 53 regulatory compliances
* Developed GRC policies, and standard operating procedures using Amazon WS
* Experience in different vendor (Ericsson) virtualized IoT core network, running on Linux platform, familiar.
* Cloud With IAM Security commands
* Collecting and analyzing network specific and IoT device logs from Linux systems
* Hands on experience in IoT devices (i.e., Quectel device, Sequan device) and Azure
* Developed and managed security awareness using Kaseya’s Security Suite, and Remote Monitoring Management (RMM) Dashboard tools.
* Developed and maintained cyber-security compliance documentation via DHCF/DCAS SharePoint Website
* Identify the scope of work and prepared thorough accurate and detailed schedule estimates for multiple IAM security projects and audits.

## ENQUIZIT INC., 09/2019 – 03/2020

* **Lead Cyber Security Project Manager**
* Department of Health and Human Services (HHS) Center for Medicare and Medicaid Serv ices (CMS), Lead Information System Security Officer (ISSO) responsible for the Agile/Lean methodology for
  + DevSecOps ATO accreditation for the CMS “Lift & Shift” Enterprise Identity Management (EIDM) On-premises data center to the Amazon AWS CLOUD project.
* Act as the lead for the translation of business objectives and requirements into functional AWS IAM security services specifications and azure cloud
* Lead brainstorming sessions and identify areas for process improvements.
* Drive technical deep-dive sessions with internal and external clients
* Prepare client recommendations, proposals, and quotes leveraging sound and creative technical solutions
* To validate network stability, used IoT devices with AT commands that connects with the core network
* Support occasional on-call duties for N e t w o r k O p e r a t i o n C e n t e r ( NOC) escalation.
* Develop and plan conceptual solution presentations and demonstrations.
* Demonstrate leadership and technical guidance in meetings and when responding to RFPs
* Clearly and effectively communicate IAM solution value to business and technical audiences
* Identify and provide recommendations for the acceptance or mitigation of any issues and risks associated with requirements, proposed systems or solutions, architectural designs, implementation plans and timelines

## TDI/ATD 04/2019 – 06/2019

Cyber- Security Compliance Project Manager

* Responsibilities Cyber- Security Compliance Project Manager for U.S. Department of Agriculture (USDA) Food and Nutrition Services (FNS) Microsoft Azure and AWS Cloud migration to the FNS Cloud General Support System (GSS). Managed a team of three highly technical security compliance staff - TDI contractors. Ensured ATO related documentation for MS Azure for IoT applications were reviewed for accuracy and updated in the CSAM for system assessment and certification.
* Lead the government client efforts to build a cybersecurity engineering framework designed to complement and enhance the Security Assessment and Authorization (SAA) process.
* Provide subject matter and industry expertise and assist our client with standards identification.
* Advise on and assist the government with Microsoft Azure Services best practices implementation.
* Assist with the management of vendor relationships to ensure our client security posture g oals are met.
* Analyze computer networks, identify possible issues, and assist the government to design solutions.
* Provided a strong working knowledge of our client security architecture and policy to design IoT systems that meet or exceed requirements.
* Communicate technical requirements to technical and non-technical personnel, partner with IT developers and project managers to represent IAM security requirements, and leverage threat intelligence to assist the government in modifying designs and plans to co unter such threats.
* Recommend security enhancements to managers, installed and used firewalls and data encryption programs, review systems designs for flaws or risks, build and deploy security infrastructure and automate enterprise IAM security operations, assist the government with internal build projects, develop technical content such as automation tools; reference architectures; and white papers, architect and develop customer applications for cloud optimization, provide software development subject mat ter expertise with respect cloud architecture, design IoT patterns, and programming.
* NOTE: United States (USDA) Lead Compliance Officer, responsible for managing a staff of three (3) Information System Security Officers (ISSOs). Responsible for the region al Microsoft Azure Cloud migration of the Food and Drug Administration (FDA). TDI/ATD lost re-compete.

## PERSPECTA INC. 09/2017 – 02/2019

### Information System Project Manager

* Department of Homeland Security (DHS) Senior Information System Security Officer (ISSO) and Technology Risk Assessment Consultant for DHS Data Center -2 (DC2) Cloud Infrastructure-as-a- Service (IaaS); scope of work includes but not limited to the development of NIST 800 53 security controls implementation, Plan of Action & Milestones (POAMs) mitigation and management, risk management framework (RMF), system classification, and system security life -cycle management documentation to obtain full authorization to operate (ATO)
* Department of Education (DoEd) systems security assessments. Overseeing FedRamp transformation, developing, and improving the overall security posture of the Security Operation of DoED Federal Student Aid (FSA) IT systems. Project deliverables included system security classificatio ns using NIST 800 60 vol, and vol2, System Security Plans (SSPs), Risk Assessments (RAs), Contingency Plans (CPs), Contingency Plan testing, and other associated documentation. Revision of IoT controls of the

system, and AWS security standard operating procedures (SOPs) based on NIST SP 800 series regulatory policy and industry best practices. CSAM configurations IoT management.

* Lead Subject matter Expert (SME) consultant to system owners for the IAM security of the system and system documentation, which included security incident reports, equipment/software inventories, operating instructions, technical vulnerability reports, and contingency plans. CSAM configurations IAM management.
* Attended IoT training and sessions as required.
* Performed interpretations of monthly vulnerability scan results of assigned systems.

## GLOBAL SOLUTIONS GROUP INC. 08/2017 – 10/2017

### Technical P r o j e c t Lead

* As Technical Lead/Security Engineer /ISSO consultant responsible for performing security assessments for the United States Department of Agriculture (USDA) and their 17 subordinated agencies within the

U.S. in accordance with Federal Department regulations as well as best practices and guidelines established within NIST SP 800 series, DISA STIGS, and the Open Web Application Security Project (OWASP) Top Ten. Conduct analysis of each USDA sub-agency information security architecture develop a threat profile for the IT components, or the layers and sub -layers of their IoT defenses in depth efforts.

* Manage security assessment team of 12 IT security professionals, and penetration testing activities in accordance with the Agriculture Security Operations Center (ASOC) Security assessment Methodology and the USDA Rules of Engagement for the Operational Security Assessment Penetration Testing.
* Develop, execute, and mange work breakdown structure (WBS), project management plan (PMP), integrated master plan (IMP), integrated master schedule (IMS), risk management plan (RMP), quality management plan (QMP), communication management plan (QMP), and the program management schedule (PMS) for the overall program to include the individual agency assessments, penetration tests, and web security assessments. Key management subtasks included but n ot limited to the following:
  + Creating weekly activity and monthly status reports to document project accomplishments, risks, expenses, burn rate, hours worked, and progress.
  + Coordinating and plan meetings.
  + Communicating with key USDA stakeholders
  + Providing Weekly Activity Reports (WARs), Monthly Status Reports (MSRs), and a monthly financial report that summarized the activities completed in a given week and month, planned activities for the following week and month, and outstanding is sues.
  + Providing timely notification to the contractor officer representative (COR)
* Update the Agriculture Security Operations Center (ASOC) Security Assessment Methodology, including Penetration Testing and AWS Web Security Assessment, and the USDA Rules of Engagement for the Operational Security Assessment Penetrations Testing to address inclusion of Web Security Assessments
* Identify threats and vulnerabilities based on the information technology associated with a USDA agency’s business.
* Examine and evaluate the USDA’s agency operational security policies, procedures, and systems through the performance of technology reviews.
* Identify strengths, vulnerabilities, and overall security posture of the agency, whether the agency’s IT architecture is adequately secure and in compliance with current security directives.
* Identify and evaluate attacker tools and methods.
* Individually develop and map identified threats to each asset within an agency.

## NIKSOFT INC., / C2ESSENTIALS INC. 10/2016 – 12/2016

### Chief Project Manager

(Contract ended due to the loss of Department of Defense (DOD) Funding. From 2014 to present currently working additional industry certifications)

* As the Chief Cyber-Security Compliance Officer (ISSO) for the Defense Health Agency (DHA) provided cyber- security solutions, and compliance audits for the Armed Forces Billing and Collections Utilization

Solution (ABACUS) program. Worked closely with their Cloud Service Provider (CSP) to ensure FedRAMP+ compliance, assessed the cyber security posture, and regulatory compliance of the Software-as a- Service (SaaS), and the Infrastructure/Platform-as-a-Services (IaaS/PaaS). My

assessments ensured the secure handling and transmission of protected health an d personal identifiable information (PHI/PII) of the military services and their families. Daily focused activities included;

* Providing guidance to the CSP for their strategic approach to Risk Management Framework (RMF). Assessed and evaluated all technology integration, software, and AWS application upgrades for the ABACUS program.
* Conducted risk assessments (RA) and technical status briefings and presented findings to the Program Management Officers (PMO), and project stakeholders.
* Evaluating and documenting the security framework for Defense Health Management System (DHMS) applications,
* Evaluating the security design for DHMS applications,
* Documenting the existing threat modeling for DHMS applications,
* Executing security code review for DHMS applications, and
* Examining and documenting the vulnerabilities, the threat attacks, and the counter measures that exist within the applications' security framework.

**NOTE**: From 2014 to the present Ms. Peterson continues to work closely with Small Business Admi nistration (SBA), U.S. Women’s Chamber of Commerce (USWCoC) to develop her company’s business plans and marketing strategy. Also, during 2015 she completed the Cisco Certified Network Associate (CCNA) and Amazon Solution Architecture training programs

## IBM GLOBAL BUSINESS SERVICES 08/2014 – 11/2014

### Chief Computer Cyber Security Project Manager

* (Contract ended due to the loss of Department of Defense (DOD) Funding)
* As the Information Assurance Lead/Chief Computer Security Scientist performed duties included acting as the principal technical advisor on issues pertaining to full life -cycle cyber security architecture development, information assurance (IA), continuity of operations (COOP), and logistical sustainment to the Project Manager (PM) for the DOD tactical Battle Command System Sustainment Support (BCS3) program located at C4 I Center of Excellence, Aberdeen Proving Ground (APG), MD. Responsibilities included providing advice on National, DoD Joint Services policies that affect the information assurance and cyber security of computer systems to include effective implementation of Chairman of the Joint Chief of Staff (CJCS0 Directive 6510.01B, Cyber Incident Handling Program.
* Documenting the software development process and of the properties of software components. Planning computer architectures, Department of Defense Architecture Framework (DODAF) version 2.0, Data, and Information Viewpoint (DIV) guidance for supply chain analysis. Also used DODAF architecture content as a function of service and operating system concepts for application widgets. Selecting and applying relevant security requirements to systems in development and in their fielded environment.
* Auditing and organizing protective mechanisms into realizable components of a secure system architecture. Developing and executing plans for functional and penetration testing. Knowledge of Supply Chain Management processes and best practices, specifically practices associated with the Battle Command Software Sustainment Support (BCS3) system, and DOD and Army Supply Chain Logistics Expertise. Representing the customer at meetings and conferences addressing computer security issues related to the data center optimization planning.

## ALION SCIENCE & TECHNOLOGY INC. 02/2013 – 03/2014

(This company filed for bankruptcy 2014, https://blogs.wsj.com/moneybeat/2013/11/19/alion -reaches- preliminary-deal-with-creditors-group/ in 2014)

* As the (“Team Agility”) onsite project manager, I was responsible for meeting all progress reporting and contract requirements. I reported directly to the Joint Interoperability Test Command (JITC) Government Action Officers (GAO) to make sure planned activities are progressing as expected, resources are being utilized appropriately, and to identify risks and oversee mitigation plans. Timely delivery of quality products and services by actively monitoring adherence to procedures outlined in Alion’s Quality Assurance Plan and soliciting feedback on deliverable quality from the GAO. Ms. Peterson continually assesses and provides recommendations to GAO on task support adjustments so that performance meets/exceeds expectations. Using this methodology, I provided a Monthly Status Report (MSR) compliant with all DoD Form 1 requirements. This task supports multiple reimbursable DISA customers. Therefore, in order to enable accurate project tracking and accounting, Ms. Peterson created a Subcontract Line-Item Number (SLIN) for Monthly Status Reporting (MSR), which includes a summary of the total amount invoiced to each SLIN for that month. Ms. Peterson also employed the following proven processes and automated, web-based tools to effectively and efficiently manage and control cost, schedule, quality, staff, and all task-related operations, enabling task lead management, Program Management/Deputy Program (PM/DPM) oversight, rapid invoicing, and employee support at any location.
* In addition to her management duties, Ms. Peterson is responsible for creating technology and IT security efficiencies, enhance mission assurance, and improve test agility through offering centralized services and the sharing of assets, resources, and capabilities across the JITC Enterpris e, and Joint Information Environment (JIE) classified and unclassified Security Operations Centers (SOCs). Within the first months Ms. Peterson, was able to facilitate a three-year Authority –to-Operate for the JTIC NIPRNET AND SIPRNET Enterprise Operations Center (EOCs) laboratories at DISA FT Meade, Maryland. Ms. Peterson focused multi-faceted business process improvements focused on six core areas of operations designed to enhance network and security operations necessary to ensure situational awareness in the following key business benefits included hands-on design and development of:
  + Improved Programmatic Visibility of the Continuity of Operations Planning (COOP); wrote JITC/JT3D COOP working Group Charter, Project plan, COOP policy, and Network Operati ons Consolidation plans.
  + Improved Risk Management Capability; wrote the Network Vulnerability Management Standard Operating Procedures (SOPs) and the JITC Laboratory Physical Access Management Controls Policy and SOP
  + Developed guidance and process improvement planning, directed and managed JTIC Computer Incident Response Team (CIRT) for NIPRNET and SPIRNET Laboratories.
  + Managed IT Security Knowledge transfer through the development of IA SharePoint portal for all three JTIC sites (Indian Head, FT Meade MD, FT Huachuca)
  + Program Risk Assessments and IT Security Controls Verifications; Drafted and finalized the Assured Compliance Assessment Solution (ACAS-NESSUS Tenable) transition and implementation strategy for JTIC to align with the DISA Security Center im plementation,
  + Vulnerability Management duties included scheduling and performing system vulnerability scans, system updates and patch management
  + Program System Security Plans (SSPs), Policies, and Guidance for multiple JITC projects and initiatives to include Tripwire Enterprise for Security Configuration Management (SCM), Incident Response Management

## XLA INC. 10/2012 – 02/2013

### Sr. Technology Cyber Security Consultant/ Project Manager

* As a Sr. Technology Security Consultant/ Information System Security Officer (ISSO) for the United States National Archives and Records Administration (NARA), Ms. Peterson provided direct “6 months Bridge Contract” support to the Chief Information Security Officer (CISO) Leo Scanlon (301) 837 -0752, Deputy Information Security Officer, Sandra Paul-Blanc (301) 837-3048, and their entire team, which consisted of five (5) senior IT staff members. Collaborate with stakeholders to establish, maintain, and communicate a technical enterprise security roadmap. Duties included providing expert-level cyber security consulting support for the security operations center (SOC), configuring and normalization of

enterprise continuous monitoring for the NARA Security Operations Center (SOC). Security tools used included Tenable NESSUS, NetForensics, Splunk for Windows and Linux, McAfee ePolicy Orchestrator, and Black Straus Log Storm. Ms. Peterson personally responsible for the development of the following NARA Contract deliverables:

* + NARA IT System Continuous Monitoring Service Catalog
  + NARA IT System and System Owner (SO)/ Information System Security Officer (ISSO) Directory
  + NARA IT System Authorization & Continuous Monitoring Dashboard
  + NARA Minor Application & Subsystem Inventory Management Inventory Registration Form
  + Ms. Peterson acted as the subject matter expert (SME) IT security liaison for NARA and Google Inc., for the NARA eMail Cloud Initiative Program. Other duties included provide expert consultations to NARA senior staff such as the NARA Business Support Services Focus Group, Description and Authority Services (DAS) Cloud Computing Integration Meeting. She reviewed Google Service Level Agreements (SLA) for cyber security and NIST SP 800 -53 Revision 3, compliance. Developed Computer Incident Response Plan and Standard Operating Procedures (SOPs).

## GENERAL DYNAMICS INFORMATION TECHNOLOGY (GDIT) 05/2011 – 08/2012

### Sr. Principal IT Security Project Manager

* As a Sr. Principal IT Security Analyst/Security Solutions Architect for the U.S. Department of Energy (DOE); Federal Energy Regulatory Commission (FERC), Ms. Peterson provided expert -level support in all security issues, including research, studies, requirements, analysis, assessments, planning, development, deployment, and maintenance. Assist in prioritizing network troubleshooting and maintenance and ensure that the FERC technical infrastructure meet’s FERC’s Service Level Agreements (SLAs). Ms. Peterson completed the NIST Security Authorization Process, whi ch granted the Authority-to-Operate (ATO) for the FERC Google POSTINI Services Cloud capability under the new Federal Risk and Authorization Management Program (FedRAMP). She analyzes and defines IT security requirements, and policies for a variety of computer and telecommunications issues.
* Responsible for design, development, and implementation policies for technical solutions per requirement, gathers and organizes technical information regarding the individual FERC component business mission goals, and needs, existing security products, and ongoing programs.
* Performing risk analyses and assessments using NIST SP 800 -37- Risk Management Framework (RMF), developing, analyzing and implementing security architectures for IT security service catalog management.
* Conducts required security audits, and system certification & accreditations (C&A). Interfaces with the user community to understand security needs for service-oriented architecture (SOA) for mobile iCloud computing and wireless and implements procedures and support accordingly.
* Review Intrusion Detection and Prevention logs for trend analysis.
* Ensured user community understands and adheres to necessary security compliance, policy and procedures.
* Served as the project lead / point of contact (POC) for the FERC Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) Technical Architecture working group

**EDUCATION**

* Carnegie Mellon Chief Information Officer (CIO) Institute
  + Certified Federal CIO Program (Pursuing)
* Walden University
  + Doctoral Candidate (PhD), Public Policy Administration (PPA)-Specialization International Government, School of Management Sciences (Degree Pursuing/Pending)
* Central Michigan University
  + Master of Science in Business Administration (MSc), Software Engineering and Technology Management concentration - 1999
* George Washington University
  + Attended Executive Master of Science, Information Technology, School of Engineering, and Applied Sciences (SEAS) transferred credits and completed Master at CMU
* University of Baltimore
  + Master of Business Administration (M.B.A- transferred and completed Master at CMU)
* Rutgers University
  + Bachelor of Science (B.S.), Economics and Political Science-1981