***AMY M. MIGYANKA***

Phone: 814-254-2431 [amm2531@atlanticbb.net](mailto:amm2531@atlanticbb.net)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Security Compliance/Cybersecurity Engineer**

**CLEARANCES**

Active TS SCI

**EDUCATION**

University of Maryland University College, Adelphi, MD, Master of Science, Information Technology, August 2004

Cambria County Area Community College, Johnstown, PA, Associate of Science, Computer Information and Communications Technology/Network Administration, December 1999.

Clarion University, Clarion, PA, Bachelor of Science, Business Administration, Management, May 1996

**CERTIFICATIONS**

Cloud Security Alliance (CSA) Certificate of Cloud Security Knowledge (CCSK) on May 17, 2013

CompTIA Security+ CE on November 29, 2011

CompTIA Security+ Certification on March 27, 2009

**SKILLS**

|  |  |
| --- | --- |
| Social Media Tools – Scraawl, OpenIO | Project Management |
| Organizational skills | Biometrics, PKI and CAC/PIV authentication |
| Technical Writing | HEAT Helpdesk software |
| FedRAMP (SaaS, IaaS) | ISO27001 |
| Security Compliance | DCID 6/3, ICD503, DIACAP |
| Security Cloud Services | Cyber Security Assessment Management System |
| SQL databases | XACTA IA Manager, eMASS |
| NIST SP800-53, NIST SP800-171, CMMC | Siebel, eRequestor |
| Assessment and Authorization | Risk Management Framework (RMF) |
| OPNET Modeling software | Insider Threat Assessments |
| Cybersecurity | Cloud Systems Security Assessments |
| Splunk | JIRA, Confluence |

**PROFESSIONAL EXPERIENCE**

**1/2017 – 1/2022**

**Cybersecurity Engineer**

**Stephenson Technologies Corporation (STC) – Baton Rouge, LA**

* Developed security compliance documentation for various projects relevant to Assessments and Authorizations (A&A), the Risk Management Framework (RMF), and FedRAMP requirements.
* Developed Cybersecurity Maturity Model Certification (CMMC) required documents, working towards Level 2 CMMC v2.0 certification.
* Developed security control policies for the Level 2 CMMC v2.0 certification and worked on self-assessment for the company. Maintained access to the SPRS system to upload and update the self-assessment score.
* Researched multiple vendors for GCC High and developed pricing matrices for executive management
* Responsible for developing security architecture frameworks for clients, researching Security Technical Implementation Guides (STIGs) and security tools needed for specific environments, developing policies, and conducting technical research.
* Performed continuous monitoring for government accredited system.
* Worked with agile management systems for tracking project activities, i.e., JIRA, Confluence.
* Developed real-time and scheduled alerts in Splunk to monitor and respond to specific events.
* Researched Threat Intelligence Platform (TIP) products and evaluated the key and critical criteria for project deliverable.
* Served as the Insider Threat Program Security Officer (ITPSO) for STC, working with the FSO to develop the insider threat plan and relevant security documentation for the company
* Served as the Assistant Facility Security Officer for STC:
  + Responsibilities included:
    - Submitting visit requests for cleared personnel
    - Submitting fingerprints to the Secure Web Fingerprint Transmission (SWFT) system for employees seeking a clearance
    - Working in formerly Joint Personnel Adjudication System (JPAS), now Defense Information System for Security (DISS), to create subjects, update subject information, submit customer service requests, and monitor status of cleared personnel

**2/2015 – 1/2017**

**Sr. Security Consultant/IT Security Specialist**

**The Newberry Group – St. Peters, MO**

* Performed security compliance with the Cloud Services team, reviewing security assessment and authorization (SA&A) documentation for Cloud systems obtaining an Agency Authority to Operate (ATO) with FedRAMP.
* Analyzed Security Control Implementation Statements developed by Cloud Service Providers (CSP), who offer low or moderate impact cloud services and must meet FedRAMP requirements.
* Reviewed and provided feedback for Concurrency Review Checklists provided by the Agency OCIO office.
* Reviewed annual assessment documentation and worked with the cloud services team and customer on the continuous monitoring phase of the Risk Management Framework (RMF).
* Worked with the Cyber Security Assessment Management (CSAM) system to maintain cloud services systems A&A documentation for the Agency.
* Met with the CSPs and Agency ISSO to discuss project status updates on a weekly and monthly basis.

**4/2008 – 2/2015**

**Senior Information Security Engineer**

**Concurrent Technologies Corporation - Johnstown, Pennsylvania**

**Certification and Accreditation Experience:**

* Security Assessment and Authorization (SA&A) Project lead on the Federal Risk and Authorization Management Program (FedRAMP) System Security Plan (SSP), which took approximately one year and a half to achieve the Provisional Authority to Operate (P-ATO).
* Developed the FedRAMP SSP and other IA documentation needed to achieve a FedRAMP provisional ATO.
* Developed authorization SA&A packages for various projects in the Intelligence Community, achieving Authority to Operate (ATO) status.
* SA&A Project Lead with developing and reviewing the security documentation for DoD Information Assurance Certification and Accreditation Process (DIACAP), Intelligence Community Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation
* Experience with DIACAP Application Manual DoD 8510.1M, and the DoD 8500 series IA documentation, System Security Plan (SSP), NIST SP800-53 security controls, NIST SP800-60 rev. 1, and NIST Risk Management Framework (RMF) (SP 800-37) and other documentation required in a security assessment.
* Performed validation testing and risk assessments with support team.
* Developed security policies and procedures needed for the baseline security controls.

**Information Systems Security Manager/Engineer Experience:**

* Remote Customer Service Agent and PKI Trusted Agent for multi-level networks in SCIF.
* Provided maintenance, administration and ongoing IT support to our corporate and offsite SCIF facilities.
* Information Assurance Manager (IAM) of TS/SCI facility (SCIF) at corporate office, overseeing the systems and the cleared staff members in the facility.
* Technical lead for Insider Threat Assessment internal Pilot Program.

**4/2006 - 3/2008**

**Information Security Engineer**

**Concurrent Technologies Corporation - Johnstown, Pennsylvania**

* Developed Certification &Accreditation (C&A) packages for various projects in the Intelligence Community.
* Developed and reviewed the security assessment documentation for accreditation process.
* Served as a technical lead on a project with a total funding of $500K.
* Provided JWICS support and develop Memorandum of Understanding (MOUs) for programs co-utilizing the network.
* Managed program deliverables on time and schedule and meeting quality standards for performing C&A work.

**4/2003 – 3/2006**

**Network Analyst**

**Concurrent Technologies Corporation - Johnstown, Pennsylvania**

* Served as Project Manager, technical (PMt) on program task from August through December 2005.
* Performed research to produce a Comprehensive Capabilities List (CCL) that can be used to describe Security Policy Management (SPM) tools based on usability, as well as, technical and operational attributes.
* Responsible for upgrades, maintenance, and monitoring logs on the antivirus servers and investigate new vulnerabilities.
* Responsible for sustaining quality service and technical support, which involved server maintenance and configurations, system optimization, network troubleshooting and network security.

**3/2001-3/2003**

**Network Administrator**

**Concurrent Technologies Corporation - Johnstown, Pennsylvania**

* Procurement of all personal computer related hardware/software.
* Configuration, installation, and maintenance of all system servers at the Johnstown locations.
* Provide daily and 24x7 technical support for the Help Desk.
* Train users within Windows environment.
* Provide Technical Support to users throughout the company, including remote CTC locations.