|  |  |  |  |
| --- | --- | --- | --- |
| Brittany S. White | | | PSC 78 BOX 3884 - APO, AP 96326  (302)670-4492 - brittanyshaywhite@gmail.com |
|  | Profile:  Qualifications include an Associate in Information Systems Technology, 11 years of Information Technology (IT)/Cybersecurity experience working for the United States Air Force, DoD, and Internal Revenue Service. CompTIA Security + certification (satisfies IAT level II & IAM level I), and Top Secret security clearance with a Single Scope Background Investigation (SSBI) periodic reinvestigation (PR) closed Feb 2018. Currently preparing to follow my family from Yokota AB, Japan back to the United States and searching for a new opportunity to continue my Cybersecurity career. | | | |
|  | **Experience:**  DoD Contractor (GS-2210-13 Equivalent) – *Current location*: Yokota AB, Japan  **Functional Mission Analyst** (From Aug 2020 to Current) working 40 hours a week  Serves as a PACAF contractor Functional Mission Analyst working with the Yokota Mission Defense Team (MDT) to map out PACAF priorities for weapon system cyber analysis.   * Develops Functional Mission Analysis (FMA) Cyber reports and snapshots to capture current vulnerability information on Yokota’s weapon systems and top priorities as directed by MAJCOM Cyber Director. * Leads detailed assessments of weapon systems at the base to assist in determining mission priority for MDT. * Identifies cyber weaknesses in weapon systems and provided recommendations and way forwards. * Coordinates with PACAF to obtain a higher level of EMASS read access needed to properly conduct duties that had a positive impact on not only MDTs but Wing Cybersecurity Offices as well. * Used EMASS to manage systems/applications artifacts to include System Security Plans (SSPs), ISCPs, hardware/software lists, and POA&Ms. * Provides FMA support to identify critical information technology architecture and supporting infrastructure that supports the warfighting mission. * Familiar with Mission Assurance Database Support System (MADSS)   IRS Federal Employee (GS-2210-12) – *Previous location*: Memphis, TN  **Internal Revenue Service (IRS) Information Technology Specialist (Security)** (From Aug 2019 to May 2020) working 40 hours a week  Served as an IT Specialist (Security) in the Cybersecurity section ensuring the vital integration of IT programs and services; developing solution to integration/interoperability issues; designing, developing, and managing IT security systems that meet current and future business requirements. As an Information System Contingency Plan (ISCP) Testing Facilitator I led ISCP testing for up to 140 applications/systems ensuring disaster recover procedures are tested with disaster recovery testing, and functional testing. I coordinated with eOPs, application owners, Information System Security Officers (ISSOs), data collectors, and application development to ensure FISMA registered systems are updated each FISMA year and tested as required.   * Developed Information System Contingency Plans (ISCPs) to verify the integrity, security, and availability of the system during disaster recovery operations. * Led compliance checks verifying that the security of the programs to minimize system vulnerabilities. * Identified weaknesses in system recover plans and tests and documents them on Plan of Action and Milestones (POA&Ms). * Reviewed and implemented NIST security requirements paying close attention to details guaranteeing accuracy. * Used TFIMS to manage systems/applications artifacts to include System Security Plans (SSPs), ISCPs, hardware/software lists, and POA&Ms, * Completed 8 annual hours of FISMA required training keeping up with federal requirements * Documented correspondence between application, security, and testing POCs for projects involving testing contingency planning controls   TN Air National Guard (ANG) Drill Status Guardsman (DSG) - USAF—Current Location: Memphis ANGB, TN  Wing Cybersecurity Officer (3D073) – TSgt/E-6, (From June 2016 to Present) Drill Weekends and AT days  Currently serves as a Wing Cybersecurity Officer for Memphis ANGB, TN. Strives to provide all members expert level COMSEC, COMPUSEC, TEMPEST, and policy/procedures training in order to motivate all members to become mission ready and qualified. Subject Matter Expert (SME) in COMSEC, COMPUSEC, and TEMPEST providing the Memphis ANGB with superb expertise in all areas cybersecurity. Led a 4 member team of airmen and NCOs through training and providing cybersecurity support to nearly 2K base personnel.  DoD Contractor – *Previous Location*: Yokota AB, Japan  **University of Maryland University College (UMUC) Asia Headquarters Technical Support Specialist** (From Sept 2018 to June 2019) working 40+ hours a week  Served as a technical support specialist for 33 UMUC locations across Asia. Provided basic and advanced troubleshooting, logistical support, inventory management, and technical support to National Test Centers, Field Office’s, Classrooms, and labs.   * Submitted WOMS/CIPS requests to FSS IT in order to have POTS and VOIP DSN lines/ports activated for users. * Used System Center Configuration Manager (SCCM) to image new and old systems to Windows 10 and conducts after install tasks to conform to IT policies as required. * Deployed new Windows 10 machines replacing all student PCs, staff PCs, and NTC computers. * Responsible for installation, testing, troubleshooting, and maintenance of hardware, software, and database systems. * Assisted in configuring network servers, routers, switches, and network monitoring tools to include troubleshooting connectivity issues. * Installed and configured software and hardware for network and stand-alone machines. * Used an IT ticketing system called ITworks (similar to Remedy and Kisam) to submit, respond, troubleshoot, and resolve IT related problems from users across Asia. * Responsible for all IT assets in Asia requiring annual inventories of sensitive and non-sensitive IT assets. * Issued asset tracking forms to members receiving any sensitive IT assets. * Installed cables and connects wired and wireless network connections to UMUC systems. * System administrator that made changes in active directory, software, updates, GPOs, and etc as required. * Contributed to the IT strategic management in terms of formulating and executing policy, developing long-rang objectives. * Led team of technicians through planning, developing, acquisition, security requirements, and implementation of a major software and hardware upgrade project across Asia.   DoD Contractor (GS-2210-12 equivalent) — Previous Location: Columbus AFB, MS  **Base Information System Security Manager (ISSM) / Alt Base Communications Security (COMSEC) Manager / Alt Base TEMPEST Manager** (From May 2016 to May 2018) working 40 + hours a week  Served as a Base ISSM for Columbus AFB, MS managing over 80 unit Information Security Officers (ISOs) across the base ensuring they educate their users and implement DoD Information Assurance (IA) policies across the base of approximately 3,000 network users. Secured circuit registration, network accreditation, and security of Columbus AFB’s multi-million-dollar enterprise network.  - Utilized DoD mandated systems such as DoD Information Assurance Certification and Accreditation Process (DIACAP) and Risk Management Framework (RMF) to accomplish unclassified and classified network assessment and accreditation process to obtain Authorization to Operate (ATO) and ensure continued use of networks and their security.  - Employed IT service management tools to approve Government-Off-The-Shelf (GOTS)/Commercial-Off-The-Shelf (COTS) hardware and software for use on the Air Force (AF) network to include reviewing vulnerabilities and mitigation for that software  - Ensured that all devices were properly configured to meet Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) standards.  - Reviewed Assured Compliance Assessment Solution (ACAS) vulnerability scans to ensure vulnerabilities were properly identified and mitigated in a timely manner.  - Developed policies/procedures for disaster recovery plans, IT contingency of operations plans, and conducted audit/review exercises on those plans for the entire base.  - Reviewed/signed Data Loss Prevention waivers across the base then submitted them to HBSS for resolution.  - Processed Universal Serial Bus (USB) violation report from Host Based Security System (HBSS) multiple times a week to include contacting unit Commander, Cybersecurity Liaison, and disabling accounts.  - Provided technical level support to all customers ensuring proper use of all equipment and programs related to communications.  - Frequent use of Remedy 2.0 for IT trouble ticket management and change management.  - Inspected units to verify that they maintained all of the proper paperwork prior to allowing users on the AF network (DD Form 2875, Privileged user agreements, AF user agreements, AF form 4433, and other various forms.  - Voting member of Configuration Control Board (CCB) reviewing all changes to the network and their potential vulnerabilities.  - Submitted base Ports, Protocols, and Services (PPS) worksheet and registration requests to AF PPS office in order to ensure enclave remains registered in DoD registry.  - Registered, requested, and maintained circuit enclave Authorization to Connect (ATCs) in Systems/Network Approval Process (SNAP) and Global Information Grid Interconnection Approval Process (GIAP).  - Managed the COMSEC program for the base to include daily form 16 inventories, hand receipts, destruction reports, Information Assurance Vulnerability Alert (IAVA) updates on the Key Management Infrastructure (KMI) system, semi-annual inventories, Inventory Reconciliation Status Transaction (IRST), and etc.  - Responsible for issuing, accounting, updating, and troubleshooting secure voice devices to include OMNIs, SECTERAs, Secure Terminal Equipment (STEs), Vipers, and Iridium Phones.  - Inspected local COMSEC accounts semi-annually as required per AF/DoD polices and regulations and served as Subject Matter Expert (SME) inspecting COMSEC and Computer Security (COMPUSEC) accounts on behalf of the Wing Inspector General (IG).  - Plans, leads, coordinates, communicates, integrates, evaluates, and ensures the success of IT systems and their security.  - Overseas the integration of IT systems; develops information systems testing strategies, plans, or scenarios; and identifies standards/requirements for configuration.  - Provided training to Cybersecurity Liaisons across the base on an initial and annual basis to ensure they were familiar with AF and DoD level requirements in regard to COMPUSEC, TEMPEST, and all other related information assurance issues.  Active Duty USAF —Previous Locations: Dover AFB, DE and Misawa AB, Japan  Alternate Base COMSEC Manager/ Base Information System Security Officer (ISSO)/ Inspector General SME (From Feb 2011 to June 2016) Working 40 + hours a week  Served as a Base ISSO for Dover AFB, DE securing their bi-annual Cyberspace Defense Analysis Operations Notice and Consent Certification. Worked side by side the base Information System Security Manager (ISSM) securing the AF network and identified DoD Information Assurance policies to be implemented. Served as an Inspector General SME for the COMSEC program. Inspected over 50 accounts during a 3-year time frame. Implemented/enforced National Security Agency (NSA), DoD, and AF policies, and managed daily operations of a $43M enterprise network and $24.7B aircraft fleet at Dover Air Force Base, Delaware.  Served as an Alt Base COMSEC Manager overseeing and managing the COMSEC and Secure Voice program for 27 organizations and 19 partner units. Accounted for Top Secret NSA crypto, implemented/enforced NSA, DoD, and AF policies, and managed daily operations of a $65M enterprise network and its $1.5B intelligence center at Misawa Air Base, Japan. EKMS experience with over 4K line items. | | | | |
|  | Education & Credentials:  University of Maryland University College — UMUC Asia  Bachelor’s Degree in Computer Networks and Cybersecurity Candidate — ***Degree Expected: December 2021***  Community College of the Air Force — Maxwell, AL  Associates Degree in Information Systems Technology — ***Degree Awarded: November 2015***  COMPTIA Security + Certification – ***Obtained in 2011 certified until 2023***  Top Secret/SCI Security Clearance – ***Last SSBI PR in Feb 2018*** | | | | |
|  | | Training Highlights:  Formal AF training in: Cyber Surety (2010), Communication Security Account Manager (2015), Electronic Key Management Systems (2013), Emissions Security Manager (2016), Airman Leadership School (2015), Key Management Infrastructure (2016), IT PM I: Initiating and Planning Successful Projects (2020), and Functional Mission Analysis – Cyber Course (2021)  Awards:  Information Assurance Dominance Award (2012, 2014, & 2015)  Communications Squadron NCO of the Quarter (2016)  Mission Support Group NCO of the Quarter (2018)  UMUC Asia HQ, Above and Beyond Award (2019) | | | | |