James Jeffries

Fredericksburg, VA 22405
WoodU26@Gmail.com
+1 857 350 0611

Work Experience

Encryption Architect

Experian-Fredericksburg, VA
January 2022 to Present

• Chief resource responsible for evaluating, planning, deploying, and preparing operations for the tools and systems used by the Data Protection (DP) Team.

• Develop roadmaps and set technical direction for the DP team. You will focus on evaluating new technologies/products and supporting systems that are not supported or managed by other teams within the Global Security Organization.

• Provide SME expertise on security tool capabilities and configuration adjustments when needed to contain and implement controls such as encryption, key management, and database monitoring as applicable

• Collaborate with the Manager to identify capability gaps and operational inconsistencies within the Data Protection controls environment, and develop a plan to address them through product enhancement, reconfiguration, upgrades, or process automation

• Ensure build documentation for all security controls is available on the Enterprise cybersecurity WiKi, including configuration standards and repeatable processes to support the tools

• Build, manage, and maintain the automated reporting dashboards systems

• Build, manage, and maintain the intake process for requests on ServiceNow or a suitable tool

• Define plan and roadmap for dashboard automation and ServiceNow intake process and report weekly progress against plan

• Ensure Technical and Process documentation is 100% current all the time (all changes thoroughly documented)

• Ensure new builds/integrations/agent implementation follow operational readiness processes, are documented, health/performance KPI's are defined and in place, and monitoring and alerting is in place before promoting

• SME with operations and maintenance of data protection at an enterprise scale

• Architecting and implementing encryption strategies on AWS, Azure, or Google Cloud, including working on CMKs/BYOK and integrating with a third-party HSM Provider

• SME with Gemalto/SafeNet/Thales HSM and Key management, or Vormetric Key management, is required

• Certificate Lifecycle Management of all enterprise certificate usage, including automation

• Work with BYOK processes and client-side encryption on cloud platforms such as AWS, Azure, or Google Cloud

• Manage and implement application-level encryption, database-level encryption, and file-level encryption

• Collaborate and work closely with global teams across different time zones.

CAKMI Team Lead

Phacil-McLean, VA
February 2019 to January 2022

22102

• Hands-on, working experience using Key Management Infrastructure (KMI).

• Performing COMSEC logistics function regarding the ordering and distribution of COMSEC material.

• Entering data into the COMSEC accounting system.

• Responding to routine requests for cryptographic material, properly packaging and transporting material to the Diplomatic Courier pouch room.

• Responding to urgent requests for cryptographic material.

• Plan and coordinate deployments in collaboration with technology groups and business partners

• Manage, maintain and troubleshoot Vormetric infrastructure

• Create key management policies and write security rules based on rule definitions and specific requirements

• Design, test and evaluate results and communicate findings, audit results

• Implementing and supporting cybersecurity cryptographic infrastructure based on defined strategy

• Assessing cryptographic approaches, requirements and capabilities

• Coordinate with and/or Operate Local Registration Authorities (LRAs)

• Distribution of and accounting for keying material

• Compromise recovery (Vormetric)

• Key recovery (Vormetric)

• Establish appropriate identifiers for all personnel involved in the operation and use of CAKMI

• Contingency planning (Vormetric)

• Protection of secret and private keys and related materials

• Setting up Guard Points and Host Groups

• Working with AD to establish Host Groups

• Setting up Sys log Servers and Splunk agents to capture logs

• Configuring DSM Primary and Failovers through Linux to create clusters in established Enclaves

• Setting up Domain and Security Administrator accounts

• System Administrator of the DSMs in Production for the Dept of State CA

• Contingency Planning

• Responsible for maintaining CAKMI related documents and applicable websites (ELM/CLM/Confluence/ CAKMI Sharepoint)

• Draft Deployment Plans, Firewall rule requests and system impact analysis

• Responsible for all admin related issues Windows and Linux for the DSM

Windows Administrator

Robotech Science Inc-Quantico, VA

March 2018 to February 2019

22134

• Deploy desktop computers using System Center Configuration Manager and Windows Deployment Services.

• Manage user accounts using Active Directory, e.g. create accounts, reset passwords, update contact information. IT asset management of hardware, software, and licenses.

• Coordinate with vendors for warranty repair or replacement.

• Decommission and sanitize computers and equipment for disposal.

• Perform Tenable suite component installation and testing. Analyze vulnerability scan results and troubleshoot issues.

• Manage the Local Area Network along with any network related outages and or upgrades.

• Analyze data to plan out short and long term objectives.

• Manage folder permissions or any IT related issues/VPN/VMware/Software installation and OS upgrades/ patching/imaging for the client.

• Respond to and resolve incidents related to the network and applications using a ticketing system.

• Fulfill request for services, e.g. install software, change passwords, image computers.

• Escalate unresolved incidents or problems to the System Administrator and assist with troubleshooting.

• Update knowledge system to document solutions for resolved incidents and workarounds for known problems.

Facilities/IT/Security Manager

National Capitol Contracting-McLean, VA

June 2017 to March 2018

22102

• Manage GSuite Domain Maintain Key fob phone and laptop access.

• Order all office supplies along with maintaining all equipment Servers/Printers/Wireless/VoIP.

• Go through Company Credit Cards to approve or dispute charges.

• Maintain Auto Insurance for the Vehicles used in the field along with driver list.

• Manage all of Company Leases with Vendors and Property Management.

• Control access to IDS Keri Doors Key Fobs and security Cameras.

• Help with new employee Onboarding and employee Offboarding.

• Assist FSO to be DSS compliant and having an accurate account for the Cage Code.

• Maintained badges for all employees on contract.

Telecommunications Analyst/Communications Security Specialist/ GVS-C

Bylight Professional IT Services-Falls Church, VA

June 2015 to June 2017

22041

• DISA/SE35 COMSEC CONAUTH for ISDN VTC users on GVS.

• Draft and release AMHS messages requesting COMSEC key, changes and cancellations to CSLA/NSA.

• Maintain and update DISA Key Users Manual that provides COMSEC Policy and Doctrine for GVS keying material to Australian, Canadian, New Zealand, UK and U.S. sites.

• Perform end of month COMSEC rollover at GVS hub. Write COMSEC SOP/EAP and CONOPS as required.

• Maintain/account for over 1000 short titles and users. Review DIACAP/RMF packages along with ATOs for approval.

VTC Technician

Serco Inc / USMC MSTP-Quantico, VA

April 2014 to June 2015

22134

• Day to Day operation and maintenance of Planar Video Wall / Projectors / LCD Monitors

/ AMX system set up to 5 different locations.

• Operates and maintains visualization equipment, and RGBS cabling infrastructure.

• Operates and maintains Video Tele-Conferencing (VTC) systems to include IP and ISDN. H.320 and H.323 capabilities operate and manage TANDBERG CODECS MCUs CISCO EX90 EX60 SX20 C20.

• Manage COMSEC equipment for the USMC MSTP (KIV7 and Taclane).

• Support VIP level and MSTP personnel with VTC, VoIP, and CISCO Call Manager.

Network Administrator

General Dynamics IT / Federal Bureau of Investigation-Washington, DC

January 2014 to April 2014

20535

• Installation and maintenance of Secure Terminal Equipment (STE) secure fax, and General Dynamics Sectera Talk Secure vIPER Voice over the Internet Protocol (VoIP) phones.

• Manage inventory assets, replacements, upgrades, disposal and destruction of Secure Communications equipment.

• Conducts operational testing and documentation of results.

• Investigate, resolve technical and hardware issues.

• Provide support for classified equipment and/or systems including Secure Terminal Equipment (STE), Secure Facsimiles (ILEX and RICOH), DTE load devices, KSV-21 ECCs, Sectera vIPER and VoIP emerging technologies.

• Provide account registration, support over the air rekeying and General Keying material inventory and storage.

• Provide management and preparation of Keying Material/ COMSEC for all devices to include STE and Sectera vIPER telephone devices.

• Provide implementation, operations, maintenance and administration for all COMSEC equipment (KYK-30, CYZ-10,SKL).

• Diagnose problems with Secure Phones and Secure Facsimiles, including problems with cards, audio connectivity, and power supply issues.

• Repair Secure Phones and Secure Facsimiles, including upgrading vIPER, STE, ILEX software and testing communication ports.

DHS COR EKMS Administrator

FEMA

December 2012 to July 2013

Mt. Weather, Va 20135

• Work as a System Administrator on customer EKMS.Function as a COMSEC Custodian to support federal government COMSEC accounts and be responsible for accounting, distribution, destruction, and management of electronic key.

• Manage multiple accounts that require electronic key for voice and data communications at various levels of Government providing guidance, maintenance, and usage of electronic keying material.

• Maintain COMSEC records of accountability for cryptographic keys and equipment transferred to customer accounts.

• Assist in maintaining COMSEC Controlling Authority responsibilities for a variety of COMSEC short titles.

• Use the COR EKMS suite consisting of the Local Management Device and Key Processor for downloading electronic keying material from the Central Facility.

• Use STE phones for electronic key downloads and transfers.

• Configure and provide technical support on COMSEC cryptographic devices such as AN CYZ 10, AN PYQ 10C, KIK 20, KG 75, KG 175, KIV 7, a variety of secure cellular phones, OMNI, OMEGA, Iridium, and SME PED.

• Have operational experience with KSV-21 cards and STE phones.

• Maintain accountability for electronic keying material and supportive COMSEC equipment in EKMS and DIAS COMSEC accounting systems.

Alternate Base COMSEC Manager

Hanscom AFB-Lexington, MA

September 2012 to December 2012

providing cryptographic keying material and equipment to all organizations assigned to Hanscom AFB, identified Geographically Separated Units (GSUs), contractor accounts, and Guard and Reserve units throughout the Northeast region.

• Assist the COMSEC manager in managing COMSEC resources to provide a secure, efficient COMSEC posture.

• Establish access controls to COMSEC material, conduct training for all COMSEC Responsible Officers (CROs) and their alternates, thoroughly familiar with applicable directives concerning COMSEC material and operations (AFI, ASSISI, AFH, KAFKA, CNSSI, DOD, NSA, etc.).

• Maintain records of all COMSEC issued to users, conduct semiannual inventories, assist supported controlling authorities when conducting crypto-systems management revalidations and surveys, destruction of COMSEC.

• Review of operations and emergency plans containing COMSEC appendices, maintain minimum mission essential on-hand requirements, request increases/decreases/disposition instructions for surplus or unneeded material.

• Prepare Emergency Actions Plans, initiate COMSEC deviation/incident reports, perform semiannual assessments/audits of the COMSEC account and user accounts.

• Maintain COMSEC account files and prepare and submit accounting report to the COR as required, ensure new or additional COMSEC material is properly requisitioned or generated, assist controlling authorities on how to manage their cryptonets and provide extracts of applicable status publications.

EKMS Manager

SAIC-Washington, DC

August 2011 to June 2012

20593

• Maintain accurate records and accountability of over 2500 short titles via Cryptographic

Accounting, Reporting and Distribution System (CARDS).

• Manager the receipt, transfer, inventory, accounting and destruction of keymat utilizing the Electronic Key Management System (EKMS) LMD/KP cryptographic system.

• Responsible for training the State Department personnel and outside agencies on various areas of COMSEC and cryptographic equipment to include Black Key Distribution (BKD) and EEKD.

• Program, configure and provide technical support on COMSEC Cyptographic devices (ANCYZ/10, KIK 20, and KIK 30) in support of Embassies and Consulates Worldwide.

• Assist other Government Agencies (FBI, DIA, DEA, USSOUTHCOM, and USCENTCOM) with administrative and logistical support of communication circuits through EKMS.

• Provide support for VIP level personnel. Supported secure data transmissions using secure voice media.

• Conduct required maintenance on LMD/KP cryptographic system.

• Compile records/data in weekly reports for analysis.

EKMS Manager

United States Coast Guard-Boston, MA

June 2009 to April 2011

• Manage a 225 line item account to include Controlled Cryptographic Items, and COMSEC Keymat on a daily basis.

• Duties included Destruction, and daily use of AN/CYZ-10, KOI-18, AN/PYQC-10.

• Have maintained 100% accountability while handling COMSEC, meeting accurate required fixed cycle inventories/audits.

• Issue, load and maintain Keymat with all hand receipts for KYV-5, KY-58, KG-175D, KG-84s KIR-1C and ROB.

• Conduct local spot checks on Local Elements IAW (EKMS 1B) and set up training schedule for Local Elements.

• Collateral duties include STE manager, and Alternate Top Secret Control Officer.

EKMS Primary Alternate, STE Manager

United States Coast Guard-Washington, DC

June 2005 to June 2009

• Managed the Help Desk and tickets through Remedy. Management of 852 line item account, created a database/library to track the distribution with the accountability of 350 KOV-14s and STEs.

• Expert experience in daily troubleshooting on STEs, KIV-7M, KG-175, KG-235, KG-75, KIV-19 and helped in the installation of multiple Secure VTCs.

• Was a Vital role in the transition of the STE off of analog to VOIP with countless hours of testing closely with 3Com and L3 Communications.

• Performed OTAT and OTAR on various missions using the AN/CYZ-10 and AN/PYQ-10 via STE. Assisted in the inspection/audits and training of 12 local elements along with the issuing and destruction IAW controlling authorities.

• Work with VIP level troubleshooting and keeping systems operational.
• Was apart of 2 EKMS inspections from Coast Guard ISIC and 2 CMS A&A team visits which met and exceeded all requirements IAW EKMS 3B.
• Collateral duties include Top Secret Control Officer, NATO Control Officer, STE Manager.

SAR Controller

Radio Watch, COMSEC User, United States Coast Guard-Woods Hole, MA
August 2002 to June 2005

• COMSEC local account holder. Expert in the COMSEC equipment and their uses.
• Certified Search and Rescue Controller.

Telecommunications Technician

Telstar Communications-Chantilly, VA
June 1999 to August 2002

• BICSI certified pulled and terminated CAT5/CAT3/Fiber.
• Took part in multiple Cut overs to make sure of continuity of operations.

Education

High school or equivalent

Skills

• Operating systems and networks: (Windows and MACs)
• Software and applications: (MS Office suite (Word, Excel, Access, PowerPoint)
• VOiP
• VTC (IP and ISDN)
• Secure Communications (Network Encryptors, Handhelds, GSM, STE, Viper, Sectera)
• Inventory
• Management
• Microsoft Office
• problem solving
• training
• Vormetric Management
• COMSEC
• System Administration
• VMWare
• VPN
• Information Security
• Active Directory
• LAN
• Cybersecurity
• SCCM

- Help Desk
- Network Administration
- Cabling
- DNS
- Microsoft Exchange
- Cloud Computing
- Encryption

Military Service

Branch: United States Coast Guard
Rank: E6

Certifications and Licenses

Top Secret Clearance

Secret Clearance

CompTIA Advanced Security Practitioner (CASP+)
November 2022 to November 2025

Microsoft Certified Azure fundamentals
Present

Certified Information Security Manager (CISM)
November 2022 to November 2025