Trevor Jex, CISSP

ICAM Engineer

Phone: (801) 866-3202 Email: tjex07@hotmail.com
Address: Hooper, UT 84315
Citizenship: United States
Clearance: Secret

PROFESSIONAL SUMMARY

- Security Controls Assessor (SCA) NIST 800-53 Risk Management Framework (RMF) Auditing experience implementing and evaluating Control Family artifacts, Security Technical Implementation Guide (STIG), and Security Requirement Guide' (SRG)
- Familiarity with NIST SP 800-53, NIST SP 800-63, ISO 27000-1, SOC-2, FedRAMP, CMMC
  Exposure and experience implementing Zero Trust Identity Access Management (IAM) Identity, Credential, and Access Management (ICAM), familiar with tools Radiant Logic, Beyond Trust Password Safe Privilege Access Management (PAM), Okta.
- Active Directory (AD) management creating and deploying group policy, leveraging LDAP connections and management of unique Microsoft System Center Configuration Manager (SCCM, MECM) administration application packaging and deployment, package creation, task sequence generation, operating system deployment (OSD), application package creation and patch management. Endpoint Deployment using msi/exe switches, CMD batch files, PowerShell to endpoint devices. Endpoints include virtual machines (VMware) and physical laptops, desktops, tablets, printers. SCCM log scraping.
- Troubleshoots software suites to include Adobe, MS Office, Skype, Lync, AutoCAD, Zoom, Teams.

QUALIFICATION HIGHLIGHTS

- Zero Trust
- Tenable.io
- Cisco IOS
- Brocade IOS
- Technical Analysis
- Project Planning
- Best Security Practices
- Technical Writing
- Network Engineering
- SCCM/MECM management
- Printer Support
- Vulnerability Patching
- Vulnerability Scanning
- Customer Service
- Patch Management

CERTIFICATIONS AND TECHNICAL EXPERTISE

- **Certifications**: CISSP, CompTIA Security+, CompTIA Network+, CompTIA A+, Beyond Trust Password Safe Admin v7, MTA Network Fundamentals, MTA Security Fundamentals, CompTIA Strata, CCNA (expired 8/31/19), AMCA (expired 8/31/20)
- **Operating Environments\Systems**: Windows XP/Vista/7/8/10, Windows Server 2008/2012
- **Software**: Cisco IOS, Brocade IOS, Dameware, Remedy, Netsight, Aruba, Excel, Visio 2013, Putty, Tera, McAfee, Acrobat Pro, eMASS, CDRS, Artifactory, BeyondTrust, Okta, Radiant Logic, SCCM
- **Hardware**: PCs/Laptops/Servers, Video Conferencing, Routers, USB hard drive, Peripherals, Mobile devices
- **Coding Languages**: JavaScript, Java, Node.JS, HTML 5, CSS, SQL, PowerShell, Express, Sequelize.
  - **GitHub**: https://github.com/Tjex07
- **Other**: Technical writing, Project Management, Acquisition Documentation, Git, GitHub

PROFESSIONAL EXPERIENCE

IDAM Engineer — May 2022 – Present

Credence Management Solutions LLC — *Remote*

- Ensures PKI systems are properly routing requests to ensure users are granted the appropriate access
- Assists with implementation of mobile device authentication leveraging derived credentials to enable two factor mobile implementation in a secure environment
- Reviews and evaluates ICAM configuration to ensure Zero Trust is properly implemented utilizing federated identities resolving from a single source of truth.
- Meets with DoD Information System Owners and Stakeholders to establish system requirements to obtain required authority to operate status.
- Author's cybersecurity deliverables, including RMF packages and associated artifacts.
- Assesses DoD Information Systems against the RMF security controls IAW DoDI 8500, DoDI 8510 and NIST SP 800-53, and NIST SP 800-63,
- Develops and reviews for compliance documentation and artifacts such as Configuration Management Plans, Network Infrastructure Plans, Business Continuity and Disaster Recovery Plans, Plan of Action and Milestones (POA&Ms), topology diagrams and all supporting policies in support of RMF A&A activities
- Performs interviews of technical Subject Matter Experts (SMEs) as well as non-technical management personnel to ascertain the security posture of an IT system
- Identifies mitigating controls for identified risks and proposes additional mitigation strategies for identified vulnerabilities
- Evaluates a wide array of IT devices for Security Technical Implementation Guide (STIG) compliance using ACAS/ Nessus, Tenable, SCAP Compliance Checker, and manual checklist reviews. This includes Windows, Solaris, and Red Hat Linux servers and desktops, routers, switches, firewalls, IDS, etc.
- Coordinates with multiple projects to ensure Cybersecurity posture is complaint with NIST 800-53 and NIST 800-63.

ICAM Senior Engineer/ Security Analyst V — November 2020 – May 2022

NCI Information Systems, Inc. — *Left due to Contract Expiring*

Remote

- Configured and implemented a Zero Trust solution comprising of Radiant Logic, Okta, and Beyond Trust.
- Configured and implemented a Privilege Access Management (PAM) solution utilizing Beyond Trust.
- Ensures that identities are you unique to enforce non-repudiation.
- Configured a Federated Identity Management (FIM) utilizing Radiant Logic as the Federated Identity Manager.
- Administered Role Based Access (RBAC) utilizing Saviynt to distribute entitlements.
- Using Radiant Logic as the FIM implemented Zero Trust Architecture.
- Assists in the implementation and design of Zero Trust Identity and Access Management (ICAM) solutions.
- Works with and coordinates with vendors to ensure Zero Trust solutions are configured properly

- Meets with Verizon and the US Army Information System Owners to provide ICAM solutions and to improve security posture
- Creates high-level and low-level documentation of ICAM infrastructure
- Performs administrative duties pertaining to the ICAM solution
- Coordinates with Cyber personnel to ensure Security Posture meets the requirements set by NIST SP 800-53 and NIST SP 800-63.
- Assists Cyber Security team in performing and analyzing scan data of cloud infrastructure.
- Configures LDAP to enable LDAP communication between software solutions.
- Meets with US Army Information System Owners and Stakeholders to establish system requirements to obtain required authority to operate status.
- Author's cybersecurity deliverables, including RMF packages and associated artifacts.
- Assesses DoD Information Systems against the RMF security controls IAW DoDI 8500, DoDI 8510 and NIST SP 800-53, and NIST SP 800-63,
- Develops and reviews for compliance documentation and artifacts such as Configuration Management Plans, Network Infrastructure Plans, Business Continuity and Disaster Recovery Plans, Plan of Action and Milestones (POA&Ms), topology diagrams and all supporting policies in support of RMF A&A activities
- Performs interviews of technical Subject Matter Experts (SMEs) as well as non-technical management personnel to ascertain the security posture of an IT system
- Identifies mitigating controls for identified risks and proposes additional mitigation strategies for identified vulnerabilities
- Evaluates a wide array of IT devices for Security Technical Implementation Guide (STIG) compliance using ACAS/ Nessus, Tenable, SCAP Compliance Checker, and manual checklist reviews. This includes Windows, Solaris, and Red Hat Linux servers and desktops, routers, switches, firewalls, IDS, etc.
- Utilizes GIT LAB when working with stakeholders
- Applies STIGs to a variety of devices to ensure compliance
- Author's government deliverables such as the SAR, RMF recommendation memorandum, etc.

Senior Systems Administrator — September 2020 – November 2020

Left due to Contract Expiring

Kihomac — *Hill AFB, UT*

- Meets with US Air Force Information System Owners and Stakeholders to establish system requirements to obtain required authority to operate status.
- Performs interviews of technical Subject Matter Experts (SMEs) as well as non-technical management personnel to ascertain the security posture of an IT system
- Identifies mitigating controls for identified risks and proposes additional mitigation strategies for identified vulnerabilities
- Evaluates a wide array of IT devices for Security Technical Implementation Guide (STIG) compliance using ACAS/ Nessus, Tenable, SCAP Compliance Checker, and manual checklist reviews. This includes Windows, Solaris, and Red Hat Linux servers and desktops, routers, switches, firewalls, IDS, etc.
- Applies STIGs to a variety of devices to ensure compliance
- Establishes System Image security and software baselines for Windows and Red Hat Linux operating systems that are distributed to the customer

- Responsible for continuous monitoring of devices residing with the Network Boundary and ensuring a strong security posture.

Security Analyst V — November 2019 – August 2020

Left due to Contract Expiring

NCI Information Systems, Inc. — *Remote (Contracted by Ft. Huachuca)*

- Meets with US Army Information System Owners and Stakeholders to establish system requirements to obtain required authority to operate status.
- Author's cybersecurity deliverables, including RMF packages and associated artifacts.
- Assesses DoD Information Systems against the RMF security controls IAW DoDI 8500, DoDI 8510 and NIST SP 800-53
- Develops and reviews for compliance documentation and artifacts such as Configuration Management Plans, Network Infrastructure Plans, Business Continuity and Disaster Recovery Plans, Plan of Action and Milestones (POA&Ms), topology diagrams and all supporting policies in support of RMF A&A activities
- Performs interviews of technical Subject Matter Experts (SMEs) as well as non-technical management personnel to ascertain the security posture of an IT system
- Identifies mitigating controls for identified risks and proposes additional mitigation strategies for identified vulnerabilities
- Evaluates a wide array of IT devices for Security Technical Implementation Guide (STIG) compliance using ACAS/ Nessus, SCAP Compliance Checker, and manual checklist reviews. This includes Windows, Solaris, and Red Hat Linux servers and desktops, routers, switches, firewalls, IDS, etc.
- Applies STIGs to a variety of devices to ensure compliance
- Author's government deliverables such as the SAR, RMF recommendation memorandum, etc.

Cyber Security IT Specialist SME — May 2018 – November 2019

Hx5 (Hill Air Force Base) — *Hill AFB, UT*

- Serves as a Subject Matter Expert IT Specialist for the Air Force Munitions division. Responsible for providing security and technical insight, coordinating with Security Controls Assessors (SCA), coordinating and providing direction to Cyber Analysts to ensure systems remain complaint following a continuous monitoring model. Responsible for Life cycle management, configuration management, implementation of policies and procedures for implementation of ITIL Service Management Programs providing service and support, and continuous monitoring of existing information systems and thereby ensuring systems retain system accreditation. Assists in the creation of System Security Plans (SSP), continuity of operations plans (COOP), and creates and implements POAMS. Conducts internal audits of IT Systems.
- Provides Technical and Cyber SME input to assist with the new cloud-based initiative munitions system known as the Theatre Integrated Combat Munitions System. Works with contracted software developers to oversee implementation of required system functionality. Briefs bi-weekly to senior staff to report program status.
- Coordinates with Air Force and Army and maintains interrelationships. Assists in the creation of Service Level Agreements (SLA). Documents requirements and oversees implementation to ensure joint interfaces send and receive data to and from TICMS.
- Acts as the single focal point program lead for the Munitions Integrated Tablets (MITS).

- Evaluates MITS to determine usability in the field.
- Ensures MITS are Hazards of Electromagnetic Radiation to Ordnance (HERO) certified.
- Ensures MITS configuration is current and poses minimal risk by constantly evaluating and updating system software.
- Created and managed MITS Active Directory (AD) Forest
- Deployed Group Policies to MITS AD Forest
- Responsible for patching and vulnerability of MITS endpoint devices using SCCM.
- Reviews acquisition MIT contract proposals to ensure requirements are met to support the field users.
- Performs system acquisition duties to include creation of acquisition documentation, Department of Defense Architecture documentation, system design, and creation of various other artifacts required to meet the statutes of the Clinger Cohen Act (CCA), Joint Interoperability Test Command (JITC), Interoperability Certification (IOP), Net Ready Key Performance Parameters (NR-KPP) and the Information Support Plan (ISP).
- Conducts weekly review boards recording progress towards system milestones. Workflows assigned are broken down into manageable tasks. Works with team to gather requirements and to record accomplishments. Ensures security best practices upon implementation.
- Enforces RMF to meet compliance standards defined in NIST Special Publication 800-53
- Participated in Change Request Boards (CRBs) and Technical Review Boards (TRBs) to evaluate proposed changes to system configuration to minimize risk and promote confidentiality, integrity, and availability.
- Tools include: eMASS, JIRA, ITIPS, CDRS, ETIMS.

Network Administrator/SCCM Administrator October 2015 – May 2018

Glacier Technical Solutions/Woodbury Technologies Inc *Dugway, UT*

- Ensures all new network equipment installations, operated and maintained across Army managed network systems, are coordinated with the Information Assurance Manager (IAM) prior to installation.
- Maintained network inventory including network software and network hardware such as switches, routers, firewalls, IDS, HIDS, NIPS.
- Provides technical and security assistance for Cicso and Brocade network devices on the unclassified NIPRnet and classified SIPRnet.
- Responsible for monitoring security posture of the network to prevent anomalies, incidents, and classified data spills.
- Conducted research to identify system vulnerabilities and potential security risks, then patched and tested accordingly.
- Assists information assurance department with RMF by providing required documentation and artifacts.
- Ensures 99% uptime for army information systems and army managed systems, responds to network outages and promptly restores service.
- Ensures device security is up to standard with Army Information Assurance Program by Assessing and reviewing security posture of networked devices using Army STIG guides and ensures all devices meet compliance.
- Maintains network device software by updating firmware and securing the devices using best practice security configurations.
- Provides technical assistance for trouble calls, installs, configurations, upgrades, and troubleshooting for intermittent connection issues.
- Maintained DHCP scopes and relevant DHCP architecture documentation
- Updates and maintain hardware lists, software lists, and network topologies.
- Develops SOP troubleshooting procedures to enable the network team to resolve like incidents more efficiently
- Maintains a Network continuity book and makes modifications to keep it up-to-date.
- Advised Glacier Technology Solutions purchasing specifications to ensure all the equipment needed would suit the needs of the contract and ensure the needed support would be provided.
- Planned for network interruptions to keep impact minimal to allow for upgrades and network modifications that avoided stoppage and work flow loss.
- Demonstrate customer service skills by explaining problems and solutions to customers in an easy-to-understand manner.
- Manage and maintain network database and file shares and allocates space on the share.

- Managed local Enterprise SCCM 2007 & 2012 server as needed performed other duties as assigned.
- Submit documentation to DISA SNAP database when Circuits are added or certified.
- Operated SCCM 2007 & 2012 and automated update packages on a regular basis to ensure end user machines were secure and compliant. End user machines were kept up to date a met IAVA requirements. Corrective action was taken on machines that failed to meet DISA IAVA standards.
- Using SCCM 2007 & 2012 configured and deployed the Operating System Deployment system. Managed and updated the U.S. Army provided image regularly.
- Ran and ACAS vulnerability scans to identify machines that contained system vulnerabilities due to a software being out of date or a patch that failed to apply. Machines that failed to patch were manually patched via PSEXEC, C$, and remote desktop when necessary.

- Planned and ran three test phases for each package to be deployed to ensure customer work flow would not be interrupted. Worked with change management for proper implementation and to ensure smooth patch management. Implemented test phases that included evaluating problems any patches may have caused for the corresponding software. Isolated the causes of any malfunction and ensured the system software would function as intended before the patch would be pushed to the network.
- Performed analysis on vulnerable software that refused to patch by traditional means and created custom scripts ensure these vulnerabilities were mitigated.
- Surveyed the SCCM 2007 & 2012 server to ensure resources were not being over utilized.
- Educated and provided guidance to end users on about the importance to keep software updated to ensure a secure network.
- Maintained a passing grade security posture by keeping machines updated with the latest software and security patches.
- Participated in monthly board of technician's meetings to discuss security issues and patch implementation. Advised others on my findings and fixes.
- Developed TPM script to activate Dell TPM chips to comply with the OPBORD to enable Bit locker. This script was re-distributed throughout the region.

Help Desk Technician — February 2015 – October 2015

Woodbury Technologies (Dugway Proving Ground/US Army) — *Dugway, UT*

- Provided Tier 1 and Tier II desktop support
- Responded to service request trouble tickets or work order CRM's using Remedy ITSM Service Desk software.
- Identified network problems impacting users and worked with appropriate Tier II or III administrators to quickly restore optimum service.
- Supports McAfee antivirus and ensures client EPO packages are in sync.
- Troubleshot WIFI and GFE provided broadband devices and VPN connectivity.
- Resolved desktop problems via Remote Control;
- Added/deleted accounts and reset passwords as needed;
- Assisted with Information Assurance Vulnerability Alert (IAVA) remediation.
- Applied diagnostic techniques to identify problems, investigate causes, and recommend solutions to include but not limited to more complex network, hardware, software, account, and e-mail issues.
- Provided end-user assistance at the workstation or docking stations, and performed troubleshooting and repair services for all hardware and software issues
- Moved and reinstalled IT assets during personnel moves, conducted changes and deletions to deployed IT assets, printers, scanners, and other peripherals.
- Performed maintenance on computers, printers and other Automatic Data Processing (ADP) equipment not under warranty including, but not limited to assessment of the problem, and replacement of hard drives and other available components.

- Assisted in providing end-user knowledge (both oral and written) of safeguarding classified, unclassified, and/or sensitive information and material in accordance with prescribed security regulations.
- Provided on-site technical assistance to end-users at their building/work station Provide technical support for printers, scanners, and other peripherals.
- Communicated network security and enterprise system concepts to technical and non-technical personnel
- Developed technical documents and produce system design documentation.
- Managed customer computers for the reimage process
- Utilized network monitoring tools such as Solarwinds to monitor and proactively respond or alert appropriate support personnel.
- Submitted daily systems reports and contact next level of support to escalate unresolved problems.
- Performed Baseline and Above Baseline services based on C4IM. Ensure solutions are accurate and compliant with regulations, policies, and standards.

Client Support Administrator (CSA), Hill AFB, UT Oct 2014 – Jan 2015

- Maintained Security Clearance: Secret
- Provides Technical Desktop Support services for over 1,600 eTools (Windows 7) devices and software; as well as associated peripheral devices
- Develops and documents processes for desktop configuration management and associated implementation of upgrades and maintenance
- Tools include: Active Directory, ESN, Remedy and Dameware
- Manages standard images using remote distribution tools
- Maintains client support for LAN access and remote access via the VPN and wireless services
- Maintains Virus protection and manages anti-spyware software
- Provides technical assistance for trouble calls, installs, configurations, upgrades, and troubleshooting on communication problems, application problems, internet operations and access questions

Computer Tech Expert, PC Laptops, Riverdale UT Dec 2013 – Oct 2014

- Troubleshot and diagnosed PC's ranging from Windows XP to Windows 8.1
- Generated over $70,000 gross profit
- Maintained the store network and created home networks for customers
- Removed viruses and malicious software to optimize end user PC's
- Performed system maintenance to include tuneups to ensure customer machines were operating at peak performance
- Sold and upgraded PC's to customers based on customer needs

EDUCATION

Davis Applied Technology College, Kaysville UT February 2013 - October 2014

Technical Degree, Network Security 3.48 GPA