Cyber Security Engineer Cyber Security Engineer Cyber Consultant - Identity Management

Washington, DC Authorized to work in the US for any employer Work Experience Cyber Security

Engineer Booz Allen Hamilton - McLean, VA December 2018 to Present   Experience with COTS

IAM tools, including Cyberark, Sailpoint, and CA PAM   Experience in supporting access

management solutions, including user privileges management, user credential management, and

user security related behavior monitoring   Experience with implementing identity and access

management solutions   Experience with requirements, design, implementation, integration, testing,

and change management   Knowledge of: Active Directory or LDAP design and configuration, PKI

X509, SSO across multiple domains, RSA SecurID, 2FA via PIV or CAC   Experience with Splunk

Experience with authoring Cybersecurity guidance, including policies, strategies, and whitepapers

Experience with supporting IAM in a Cloud environment, including Azure or AWS   Experience with

implementing PKI and PIV standards   -Experience with HSPD-12, FIPS 201-2, FICAM, OMB

11-11, FedRAMP, PCI, FISMA, or NIST 800-53, 800-63, 800-79-2, or 800-157 policies and

standards a plus Systems Engineer III CACI International Inc - National Harbor, MD November 2017

to October 2018   Resolve issues that require specialized training and experience in system

operations and the use of the system administration and monitoring tools.   Work collaboratively

with DC2 technical teams, support teams, ISB (Identity Services Branch) vendors, and Development

and Engineering technical teams in support of the ISB mission   Execute a suite of regression tests

on nights and weekends where a production deployment or data center patch has been applied to

validate the production functionality is behaving as expected.   Experience with Smart Cards and

other multi-factor methods of authentication   Perform trend analysis of reported incidents

Develops security procedures for design reviews, and for operational monitoring, recording, and

responding to security events Systems Administrator CACI International Inc - Bagram September

2017 to November 2017 Professional and responsible system administration of Microsoft Windows

servers)   Troubleshooting and administering Microsoft windows 10 desktop systems   Active

directory account creation and administration experience   Experience with Smart Cards and other

multi-factor methods of authentication   Automation using Microsoft PowerShell, VBScript, or batch

files   Experience with enterprise backup solutions System Engineer III CACI International Inc - Washington, DC March 2017 to September 2017 Responsibilities   Deep understanding of Public Key Infrastructure (PKI) Services   Solid understanding of requirements for NIST SP 800-63 Levels of Assurance 1 through 4 (LOA1, LOA2, LOA3, LOA4)   Experience with Active Directory Federation Services (ADFS)   Experience Administering Windows 7 client environments   Understanding of NIST 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials   Experience with Smart Cards and other multi-factor methods of authentication   Experience with Entrust, and related Card and Identity Management Systems   Experience with Active Directory / Microsoft Windows Server 2003 through 2012 R2.   Experience in applying PKI technology to business systems   Provide hands-on engineering, analysis and systems integration to implement federated authentication and authorization, application onboarding, and PKI-related projects and programs   Work with clients to securely onboard new applications   Conduct information gathering meetings with clients to identify their operational and security requirements   Develop solutions and recommendations including timelines, benefits, and risks for each solution   Develop solution architectures, models, and designs to meet the client s operational and security needs   Implement practical, cost-effective solutions applying state-of-the-art PKI technologies   Establish strong relationships with client representatives and project managers   Align tasks with desired outcomes and expectations   Assist the Project Manager in identifying, tracking, and reporting status on issues, challenges, and risks   Provide support to eMentum corporate efforts, which includes bids and proposals, strategic objectives System Engineer III eMentum - Washington, DC March 2016 to March 2017 Responsibilities Deep understanding of Public Key Infrastructure (PKI) Services   Solid understanding of requirements for NIST SP 800-63 Levels of Assurance 1 through 4 (LOA1, LOA2, LOA3, LOA4)   Experience with Active Directory Federation Services (ADFS)   Experience Administering Windows 7 client environments   Understanding of NIST 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials   Experience with Smart Cards and other multi-factor methods of authentication   Experience with Entrust, and related Card and Identity Management Systems   Experience with Active Directory / Microsoft Windows Server 2003 through

2012 R2.   Experience in applying PKI technology to business systems   Provide hands-on engineering, analysis and systems integration to implement federated authentication and authorization, application onboarding, and PKI-related projects and programs   Work with clients to securely onboard new applications   Conduct information gathering meetings with clients to identify their operational and security requirements   Develop solutions and recommendations including timelines, benefits, and risks for each solution   Develop solution architectures, models, and designs to meet the client s operational and security needs   Implement practical, cost-effective solutions applying state-of-the-art PKI technologies   Establish strong relationships with client representatives and project managers   Align tasks with desired outcomes and expectations   Assist the Project Manager in identifying, tracking, and reporting status on issues, challenges, and risks   Provide support to eMentum corporate efforts, which includes bids and proposals, strategic objectives Information Security Analyst (Senior) NCI Information Systems, Inc. - Fort Belvoir, VA May 2015 to March 2016 Responsibilities ? Supports the Army Cyber-Security Directorate Identity Management Directorate in the areas of Army Communications Security to include Cryptographic Modernization, Key Management Infrastructure (KMI), Common Access Card (CAC) and Public Key Infrastructure (PKI)   ? Provide specialized expertise as a Registration Authority Specialist to assist the Local Registration Authority personnel in creation of SIPR (Classified) and NIPR (Unclassified) PKI tokens   ? Understanding of Active Directory Certificate Services, including installation and implementation on Windows Server 2008/12   ? Execute training sessions with new PKI specialist utilizing DoD practices, policies, procedures and standards   ? Issue, revoke, renew and recover certificates for the Common Access Card CAC/PKI office in compliance with DoDI 8520.2   ? Create PKI Mobile-Code Signing Certificates and PKI GO (General Officer) tokens   ?Create NPE Soft-Certificates and Soft- Cert Pilots which are used for iPad and other   mobile devices   ? Operate, maintain, and ensure successful implementation of the PKI program   ? Ensures the NIST 800.53 v4 security controls are in place and validated on PKI systems   ? Registers and/or terminates of Local Registration Authorities (LRAs) to perform their duties   ? Establishes and maintains certificate distribution, alternate CAC tokens, and CAC pin reset for locations globally   ? Resolves

customer issues related to smart cards and supports the CAC/PKI service desk coordinator   ?

Manages smart card process for SIPR (Classified) and NIPR (Unclassified) environments   ?

Generates DoD PKI Alternative Smart Card logon (ASCL) tokens   ? Performs third party key

recovery and approving issuance of certificates to network Non Person Entities (NPEs)   ? Create

ASCL token lifecycle tracking records and DoD PKI ASCL pins and unlock codes International

Affairs Assistant (Intern) U.S. Department of Energy - Washington, DC May 2012 to September

2012 Responsibilities   - Help to develop long-term SC strategy for international activities   -

Assisted with the coordination of US Labs and foreign organizations   - Maintained legal integrity

and remained aware of national security concerns when appropriating with foreign nationals   -

Created a database for lab agreements   - Completed analysis of multiple lab agreements   - Help

maintain bilateral programs focused on nuclear energy research and development with Russia,

China, Japan, France, Canada, Argentina and Brazil Aviation Logistics Info Systems Specialist

United States Marine Corps - Cherry Point, NC May 2007 to May 2009 Troubleshooting Windows

2000/XP - Performed troubleshooting LAN/VLAN networks - Provided support in areas of e-mail,

directories, and standard Windows XP/Win 7 desktop applications - Windows Server 2003/Windows

Server 2008 - Account unlocks, password resets through an active directory program- Directory and

Resource Administrator (DRA) - Served as the initial point of contact for troubleshooting hardware,

software, printer, and profile issues Education Bachelor of Arts in Political Science University of the

District of Columbia - Washington, DC 2012 to 2016 Skills Certified Ethical Hacker (CEH) course ,

CISSP course - Train Ace - Greenbelt MD (Sept 2014, STATA (2 years), SAS, French Reading (1

year), French Writing (1 year), FISMA policy (3 years), NIST 800-157 (3 years), System

Administrator, Active Directory, Vmware, CA PAM - Xceedium (2 years), AWS, Information Security,

Nist, Cyber Security, Comptia, Cybersecurity, It Security Military Service Branch: USMC Service

Country: United States Rank: Lance Corporal May 2007 to May 2009 Certifications/Licenses

CompTia Security+ September 2014 to September 2020 Manager and Process Owner ISO

9001:2015 April 2017 to Present AWS Technical Professional March 2017 to Present AWS

Business Professional March 2017 to Present Local Registration Authority August 2015 to Present

DISA PKI Training Key Recovery Agent August 2015 to Present DISA PKI training Registration Authority August 2015 to Present DISA PKI training Additional Information CompTIA Security+ Certification CA PAM (Xceedium) DISA Registration Authority (RA) Certification CISSP Training DoD & CNSS DISA Training   DOD & CNSS Public Key Infrastructure RA, LRA, and Key Recovery Agent Training   RadiantLogic VDS Powershell Remedy/ HEAT Ticketing System   Windows Remote Desktop Microsoft Office 2010 Altiris Imaging   Windows Migration 90x meter PKI Support Boot Camp 3.0 Microsoft SCCM SCOM

Name: Kristie Harris

Email: carrnicole@example.org

Phone: 492-211-5697