Senior Information Security Audit & Compliance Analyst Senior Information Security Audit & Compliance Analyst Senior Information Security Audit & Compliance Analyst - Lockheed Martin Corporation Westminster, MD Work Experience Senior Information Security Audit & Compliance Analyst Lockheed Martin Corporation - Woodlawn, MD April 2013 to Present April 2013 to present Description of duties and responsibilities: Serving as Lead Senior Information Security and Risk Management - IT Audit Support liaison to the Centers for Medicare and Medicaid Services (CMS). Responsible for ensuring CMS' Baltimore Data Center (BDC) Information Technology infrastructure is operated and maintained in a manner that protects hardware/software assets along with mission information, and promotes the confidentiality, integrity, availability, and authentication, and privacy as defined in CMS's security policies and standards. Provide support in conducting Certification and Accreditations for Federal FISMA Systems; associated with HIPAA Security Rule, HITRUST, IRS Safeguard Reviews, PCI, CFO, FISMA, A-123, and Security Control Assessments of CMS's General Support System (GSS) and Major Applications (MA) compliance with Core CMS Security requirements. Assist in preparing corrective action plans. Responsible for the development of agency Information Assurance/ Security policy such as Acceptable Risk and Safeguards, Authorization to Operate Package, Information Security Risk Acceptance, and Information System Security and Privacy Policy. Support CMS during 3rd party security audits and act as liaison between technical teams and auditors (KPMG, Deloitte, Grant Thornton, and Ernst & Young) to deliver operational status information to support the audits while employing expertise in IT compliance, FISMA and NIST regulations, and utilizing technical knowledge gained from prior audit experience to resolve outstanding security issues discovered during vulnerability assessments. Utilize the Trusted Agent - CMS FISMA Controls Tracking System (CFACTS) and Remedy Trouble Ticket Tracking System extensively daily in support of planning, supporting, and conducting Statutory Compliance Audit requirements (i.e., FISMA, FISCAM, HIPAA, PCI, NIST and OMB). Prepare and manage Corrective Action Plans (CAP) and Plans of Actions and Milestones (POAM). Develop and maintain technical documentation. Report status to all executive management levels. Facilitated as directed the successful implementation of all tasks/projects related to the following:

Provided audit security documentation to auditors in support of CFO, FISMA, A-123, and SCA audit activities. Provided management response to CMS points-of-contact in support of audit findings. Collectively worked with internal Functional Area points-of-contact to develop strategic methods for avoiding audit findings. Assisted with the Office of Management and Budget (OMB) initiative to perform Risk and Vulnerability Assessments (RVA) against High Value Assets (HVA) within the data center. Also performed vulnerability assessment using Center for Medicaid and Medicare services enterprise vulnerability scanning tool (IP360), create reports using pre-defined filters. Generate executive and technical summaries for upper management review. Monitor and analyze Sourcefire IDS alerts and other reported threats and determine threats impact on CMS network. Participate in various proofs of concepts workshops for the enterprise security tools such as McAfee DLP and E-Discovery forensic solutions. Attends configuration review board (CRB) meetings to discuss outstanding changes on CMS network. Performed system security evaluations and incident response reporting; as a well as performed computer security incident response activities and coordinated with other agencies to record and report incidents. Served as the team's primary curator of documentation for security engineering and incident response procedures. Lead Systems Security, Internal Controls and Compliance Task Areas; ensured that the security posture of the division's mission-critical, highly visible financial management information system was maintained at 'high' confidentially, integrity and availability impact levels. Facilitated as directed the successful implementation of all tasks/projects related to the following: Provided Quality Assurance, Independent Verification and Validation, and Technical Writing support services including but not limited to, performing quality assurance activities; vigorous testing to validate development of business requirements; development of requirement traceability matrixes along with test plans to support the validation that the identified requirement is satisfied. Senior IT Security Analyst Constellation West April 2017 to May 2018 Description of duties and responsibilities: Served as Senior IT Security Impact and Accreditation Analyst in support of the Office of Cyber Security (OCS) MWRS program. Developed the agencies Security Impact Analysis (SIA) specializing in assessment activities with VA stake-holders. Performed internal audits with stakeholders to achieve compliance

of all computer systems and major applications to ensure secure operations and compliance; while providing executive level recommendations for preventative and counter measures. Additionally, provided support with the agency's Governance Risk and Compliance (GRC) tool Risk Vision to support all facets of SIA, System Assessment and Authorizations in compliance FISMA, FedRAMP, HIPPA/HITECH standards and the implementation of security common controls. Provided guidance to customers and internal technology teams on cyber security and privacy controls. Provided key compliance deliverables to management as a result of internal assessments and Authority to Operate (ATO) processes with key stakeholders; as well as engaged with development teams and promote secure design/development early in the SDLC. Coordinated all aspects of security documentation development and artifact gathering in support of Risk Assessments and Audit engagements. Senior Compliance and Information Security Project Lead Information Security Enterprise Consulting, LLC - Washington, DC March 2012 to April 2013 Washington, D.C. Senior Compliance and Information Security Project Lead March 2012 to April 2013 Description of duties and responsibilities: Serve as a member on the Internal Audit Team developing and implementing NRCS Security Programs to ensure compliance with Federal Security mandates. Responsibilities include assessing and documenting security controls, guiding and critiquing security certification and accreditation documents for NRCS systems, developing/updating/writing other security plans (e.g., physical and environmental security plan, personnel security plan, laptop plan, etc.), and developing NITC security directives. As an integral part of the Office of the Chief Information Officer (OCIO), provided insight and knowledge to support the International Technology Services (ITS). Responsible for providing comprehensive information technology assistance for daily operations, security, and technical support services adhering to OMB Circular A-123 (Management's Responsibility for Internal Control). Following the guidance on OMB Circular A-123, ISEC provided a testing methodology framework that included an Initiation Phase, Planning Phase, a Document and Testing Phase, Evaluation, Remediation and Validation Phase, and a Reporting and Sustainability Phase. In addition, helped facilitate Audit Remediation and POA&M Coordination. Day to day tasks involves conducting interviews, performing examinations and tests to gather evidence and make

performance and compliance assessment of controls with established guidelines and standards; documenting the assessment results within USDA's CSAM tool and the internal assessment team database, report results to OCIO and OCFO as required, in addition to briefing the Chief Information Security Officer (CISO) and NRCS Executive Management on a biweekly and monthly basis, respectively; identifying and documenting the root cause of any identified deficiencies and recommend courses of remedial action; and work with the Risk Management Team to cooperatively translate root cause and any improvement recommendations into appropriate Plans of Action and Milestones (POA&M). Directly responsible for managing and conducting penetration tests utilizing agency commercial off the shelf (COTS) tool Core Impact and customized tools, vulnerability and risk management assessments using variuous application tools and technical solutions; while generating corresponding reports for executive management review. Developed and implemented appropriate, cost-effective internal security access controls to mitigate risks to the federal agency. Established as well as assessed current internal controls in Federal programs and operations. Separately assessed and documented internal controls over financial reporting. Provided subject matter expertise with understanding the clients and corresponding stakeholder's business objectives; while identifying needed improvements and providing corrective actions with IT Audit solutions to assist the agency in achieving compliance. Developed automation process by which to report on internal controls through management assurance statements. Collectively worked with "Big 4" entity KPMG to coordinate all aspects of audit coordination, audit remediation and POAM coordination efforts; to ensure task completion and deliverable management within the desired time.

Deployed enterprise level management of end-point, network and content security solutions to include antivirus updates; centralized management of policy to include client workstations and agency servers. Engineered continuous monitoring solutions that centrally monitored and analyzed intrusion detection and prevention alerts and other various security threats in correlation to the impact on agency networks. Researched and provided product/vendor analysis and cost analysis for enterprise security tools such as Arc Sight, Source Fire's Next Gen, McAfee DLP and E-Discovery forensic solutions; while providing recommendations to agency security executives. Managed help

desk and incident request tickets utilizing Remedy ticketing system. Utilized network inspection tools such as Wire Shark, Splunk, Nessus, and Retina to analyze agency data. Developed Splunk infrastructure and related solutions as per automation toolsets. Installed, tested and deployed monitoring solutions with Splunk services. Provided technical services to projects, user requests and data queries. Analyzed and monitored incident management and incident resolution problems. Resolved configuration based issues in coordination with infrastructure support teams. Maintained and managed assigned systems, Splunk related issues and administrators. Responsible for designing and implementing security awareness and training programs for the Information Security Program Office. Additionally, responsible for managing Plan of Action and Milestone (POAM) items within the Cyber Security Assessment Manager (CSAM). Applied standards, regulations and best practices such as NIST, FIPS, OMB memorandums to assist the IT Security division in achieving regulatory compliance. Reviewed artifacts from agency stakeholders and identified key areas for improvement; in addition to articulating weaknesses within the agency and detailing a written and verbal corrective measure plan. Provided excellent writing and communication skills toward creating business processes for IT Governance and various sub-agencies within USDA. Worked effectively to create strategic test plans to perform assessments for testing security controls. Senior Information Security Consultant and Risk Management Specialist Information Security Enterprise Consulting, LLC - Woodlawn, MD February 2009 to March 2012 Woodlawn, Maryland Senior Information Security Consultant and Risk Management Specialist February 2009 to March 2012 Brief Description of duties and responsibilities: Accountable for security auditing, risk, threat and vulnerability mitigation for 17 critical systems and any new systems introduced into the enterprise network requiring security management; ensuring system security management conducted maintained by continuously monitoring of: Ensuring strong password policy is in effect and changed every 90 days Regularly scheduled audits and log reviews are conducted Documented and updated security plans System configuration management and critical software security updates are applied Developing system contingency plans, patch management and anti-virus updates. Develop security incident reports and documentations Plan of Action and Milestones

(POA&M). Serve as a resource to customers and end users for all questions concerning complex classified systems Manage changes to the classified system baseline components, environment, and location Provide reaccreditation recommendation to the DAO As a principal member of the configuration control boards (CCB) providing and supporting critical information on assessment of needs for security updates, end user vulnerabilities and software anomalies for all information systems under my purview. Responsible for direct management and lead oversight with the Office of Information Security (OIS) information security policy and business process development. Provided Subject Matter Expertise for security policy development, agency program planning, technical operations support and intra-agency business process advisement. Key participant in the OIS Information Technology Security Advisory Group (IT) meetings, to discuss various information security tasks and provide solutions to agency stakeholders and components. Directly responsible for managing and leading weekly OIS policy meetings to brief the Director of the Division of Security Policy and PII (DSPP) on information security tasks relevant to the team. Key Accomplishments and milestones Key accomplishments and milestones included developing the agency's Information Security Program Plan (ISPP), which provided agency compliance in support of an Office of the Inspector General (OIG) audit. As a result of a Government Accountability Office (GAO) audit, developed, a required International Travel policy to be implemented agency wide to provide guidance and policy to key personnel on safeguarding data during foreign travel. Directly responsible for leading and managing the development and implementation of business and workflow processes in support of Interconnection Security Agreements (ISA) between agency business owners and external business entities; regarding the exchange and transmission of agency data. Supported the design, strategy and implementation of new emerging technologies to further protect agency and business associates' Personally Identifiable Information (PII). Directly responsible for providing support in resolving all security, hardware and software related issues pertaining to incident handling. Designed, implemented and developed monitoring solutions for the agency's infrastructure. Performed internal audits of all computer systems and major applications to ensure secure operations and compliance; while providing executive level recommendations for

preventative and counter measures. Provided level three troubleshooting for all security related problems and events which included Firewall/IDS issues, incident response and network related issues. Additional cross-functional responsibilities included leading investigations of breaches being reported to US CERT and provided recommendations for strengthening the agencies network. Provided key recommendations to the client for increasing productivity across various agency divisions and offices. Instrumental in conducting security tests and evaluations, as well as security risk assessments, audits and reviews to ensure compliance with agency best practices and standards. Coordinated with external vendors in the analysis and procurement of new technologies and infrastructure. Performed internal security analysis, vulnerability analysis and application security testing. Responsible for all manner of certification and accreditation support such as the development of security and contingency plans with risk and vulnerability assessments. Assessed clients' security and control readiness and provided appropriate security assistance. Analyzed policies and procedures against Federal laws and regulations and provided recommendations for closing gaps. Conducted security program audits and developed solutions to mitigate the identified risks. Developed strategies to comply with privacy, risk management and e-authentication requirements. Provided Information Assurance support for the development and implementation of security architectures to meet new and evolving security requirements. Participated on the agencies product review board to determine security requirements for planned and existing information technology projects. Designed and implemented various network security safeguards such as Web Proxy Servers, Syslog Servers, Spam Filtering solutions and Data Loss Prevention. Senior Project Manager & Cyber and Information Security Consultant (Engineer) RTGX - Greenbelt, MD February 2006 to February 2009 February 2006 to February 2009 Provided technical leadership to the State Department enterprise, both nationally and internationally, for the information security program. Mentored and trained colleagues within the Diplomatic & Cyber Security division in information and network security, as well as train other technical groups. Installed and maintained security infrastructure including IPS, IDS, log management and security assessment systems. Assessed threats, risks and vulnerabilities from emerging security issues; in conjunction with USCERT.

Published security updates newsletter for technical groups. Drafted enterprise security standards and guidelines for system configuration. Managed processes and lead all efforts for computer security incident response team. Performed and created procedures for system security audits, penetration-tests and vulnerability assessments. Developed scripts to maintain and backup key security systems. Provided malware analysis on intrusions and alerts that were threats to the agency's network. Responsible for providing daily analysis reports to the customer Operations Manager, subsequently making them available for situational awareness within the Security/Enterprise Operations Center. Lead all aspects of direct implementation of Tier 1, 2 and 3 security help desk analysis and mitigation of Diplomatic Security issues for Department of States posts, networks and host based intrusion detection systems. Designed, implement and developed network monitoring solutions for the Network Monitoring Center's computer infrastructure. Directly responsible for providing unmatched customer/client service in resolving all security, hardware and software related issues pertaining to incident handling. Provided in depth analysis and resolution to customer for pre-emptive solutions. Developed, maintained, ensured and monitored Department of State IT security policies in the areas of Administrative, Physical and Technical Safeguard Policies. Took a holistic approach to securing business needs relative to data and network security. Implemented controls and capabilities to monitor data traveling through the network. Additional cross functional responsibilities included coordinating with vendors in the analysis and procurement of new technologies and infrastructure. Managed all coordination and execution for executive staff briefings and support, while providing advisement to key engineers with timely completion of service requests to ensure IT service delivery. Performed internal ethical hacking techniques, vulnerability analysis and penetration testing. Responsible for all manner of certification and accreditation support such as the development of security and contingency plans and the conduct of risk and vulnerability assessments. Assessed clients' security and control readiness and provided appropriate security assistance. Analyzed policies and procedures against Federal laws and regulations and provided recommendations for closing gaps. Conducted security program audits and developed solutions to mitigate the identified risks. Developed strategies to comply with privacy,

risk management and e-authentication requirements. Responsible for training and leading junior-level security analysts with implementing standards, regulations, best practices and security architecture techniques Provided IA support for the development and implementation of security architectures to meet new and evolving security requirements. Provided comprehensive auditing of networks, operating systems and applications respective of data that comprised of Computer Security Briefs (CSB). Network Security Administrative duties included vulnerability assessment of networks, operating systems and applications. Supervised ticket queue and distributed workload among a team of technicians according to severity level. Provided in depth analysis of OpenNet and Classified environments while developing Standard Operating Procedures (SOP) with security incident response. Developed and implemented Penetration Testing/Intrusion Detection test lab environments to enhance pre-emptive security countermeasures and assisted the engineering team with firewalls, proxies, virus prevention and remediation. RTGX Surface Deployment and Distribution Command (SDDC) Alexandria, Virginia Senior Project Manager & Cyber and Information Security Consultant (Engineer) February 2006 to February 2009 Responsible for Data and Network Security Center Management of the Surface Deployment and Distribution Command (SDDC) which manages the Department of Defense's (DoD) $1.8 billion Personal Property Program. Performed internal and client side vulnerability assessments to enforce confidentiality, integrity and availability as well as established security baselines and policy development. Conducted penetration testing against the security baselines, risk mitigation assessments and business impact analyst. Key Lead for White and Blue Team hacking and analysis of corporate security posture. Verified findings for compliance with NIST Special Publications, NISPOM, ISO 15408, DITSCAP and DCID 6/3 for certification and accreditation processes. Performed comprehensive security assessment of all designs within customer networks and advised on mitigation strategies for network vulnerabilities. Performed penetration testing of all applications and network elements for adherence to customer and federal regulations. Lead network analysis, network enumeration, wireless penetration, application security, system auditing, computer forensics and incident response projects. Senior Project Manager & Information Security Lead AT&T Government Solutions -

Vienna, VA February 2005 to February 2006 Vienna, VA Center for Medicare and Medicaid Services (CMS) Woodlawn, Maryland Senior Project Manager & Information Security Lead February 2005 to February 2006 Managed and led team operations involving over 20 Tier 1 and 2 Operating Center Analysts monitoring all critical systems and networks; including over 20,000 employees, 9000+ servers and 1300 Networks. Correlated trouble tickets with causes and involved higher level technical support personnel for timely resolution of IT network and systems outages. Day to day technical duties included installing and configuring CMS worldwide enterprise network solutions - to include IPS/IDS solutions, netowrk vulnerability scanners, Data Loss Prevention solutions, Windows Enterprise Server 2003 domain controllers, DHCP servers, DNS servers, WINS servers, application servers, print servers, file servers and SAV anti-virus servers. Implemented Standard Operating Procedures and updated procedures when necessary with prior approval of customer. Collectively worked with "Big 4" entity PWC to coordinate all aspects of audit coordination and remediation; to ensure task completion and deliverable management within the desired time. Also maintained security of voice and data networks and equipment. Monitored and maintained physical and logical security and access to systems. Responsible for support of existing security policies and procedures, as well as creation and implementation of new security procedures. Risk Assessment of Partners. Presented options to management for the enhancement of DNS, firewall, modernization of firewalls, and inbound e-mail security and robustness. Assisted with the upkeep of network infrastructure including switches and load balancers. Assisted in migration of VPN concentrators to new projects. Achievements include completing TruSecure enterprise certification and development of incident handling procedures. Restructured and implemented high level security operations program in the following disciplines: Secure enterprise remote access services with redundancy-including policy and procedures for remote access, Host and Network based Intrusion Detection / Prevention-including policy and procedures for Incident Response and Identity Management-including policy and procedures for two factor authentication pertaining to classified governmental information. Collected and analyzed data obtained by the customer's Security tools. Tools included, IDS/IPS, Firewall, SIM, scanning software etc. Centralized Audit Logging Solution

Administration and Maintenance Support; while supporting customer's efforts to maintain existing centralized audit logging solution (Log Logic) capability that logs significant events for operating systems and databases. Senior Project Manager and Information Systems Security Engineer Computer Systems Center Incorporated - Springfield, VA January 2002 to February 2005 January 2002 to February 2005 Directly responsible for management, development and implementation of Information Security Operations policy requirements for companywide production and research and development networks. Participated in cumulative efforts in performing various network administration, monitoring and intrusion prevention tasks. Implemented defense in depth approach by utilizing firewalls, packet sniffers, vulnerability scanners and penetration testing techniques. Initiated development, documentation, and certification and accreditation processes of the Trusted Information Infrastructure (TII)-TM within a Protection Level 3 (PL3) and Protection Level 4 (PL4) environment. Formulated the scope and objectives of security analyses of applications, networks and systems. Developed, conducted and implemented risk analysis; security audit methodologies; procedures for secure computer center and client-server operations; contingency planning, telecommunications security, information and computer security and prepared accreditation and certification documentation. Conducted high-level risk analyses for the Development environment. Conducted risk assessments (RA), systems security plans (SSP), security test and evaluation (ST&E) and Business Continuity Plans (BCP). Managed Research and Development of new technologies within the Trusted Information Infrastructure. Provided key leadership and vision for a combination of one hundred network infrastructure teams. Utilized such technologies such as Unicenter TNG for Enterprise Management. Responsible for the network architecture of overall environment utilizing Cisco switches and routers. Implemented computer, system and network security to overall infrastructure, including remote access and identity management - an integral part of evaluating and testing new technologies. Created matrix solutions for the selections of these potential products. Additional responsibilities were: Monitored the status of Intrusion Detection Systems to perform in-depth analysis of IDS security related events. Required to intimately understand the Customer's IT and Network infrastructure and analyze events in the context of the

Customer's environment for the purpose of identification, assessment and remediation of security events and to provide leadership on filtering/removing false positive events. Also responsible for daily administration of Checkpoint firewalls that served as shunning devices at the customer site. Validated attacks against customer's systems and assessed the impact. Responsible for making appropriate recommendation and if countermeasures were required - worked with the customer in implementing the recommendation. Responsible for assisting in firewall management, Intrusion Detection and Intrusion Prevention implementation. Utilized such tools as eTrust's Policy compliance to monitor overall network health security. Responsible for Information Systems Integration. Lead Engineer responsible for major Active Directory migrations from Microsoft Windows 2000 to Microsoft Windows 2003 for over 1000 users. Responsible for managing and maintaining ninety remote sites using Enterprise Management and VPN capabilities. Project Lead and Senior Network & Systems Security Engineer Integrated Management Services Incorporated - Arlington, VA January 2001 to January 2002 Arlington, VA Federal Communications Commission (FCC), Washington, D.C. Project Lead and Senior Network & Systems Security Engineer January 2001 to January 2002 Assessed requirements and supervised security assessments. Participated in security assessments, using a combination of proprietary, public domain and commercial assessment tools; developed recommendations to correct identified vulnerabilities; evaluated and developed security policy and procedures. Responsible for analyzing client's needs and current security regulations and guidelines to determine and address INFOSEC requirements. Required to possess strong customer service skills and ability to work directly with assigned customers to assist them as necessary with a bit of time spent keeping up with current vulnerabilities, attacks and countermeasures. Performed monitoring of IDS for suspicious traffic, and upon received security events and validated events. Coordinated with analysts, engineers, Computer Emergency Response Team, customer Security personnel, and law enforcement officials as directed by the customer ISSO or representative and management. Performed detailed traffic analysis and statistical correlation of events. Coordinated with customer to determine when appropriate security remediation based on analysis should be introduced. i.e., filtering, signature creation, policy

updates. Coordinated with vendors to determine product capabilities, enhancements and areas for improvement. Coordinated and provided leadership to customer on creating IDS Security policy. Researched events and incidents based on monitoring activities. Maintained systems and applications required to efficiently and effectively provide continuity of operations of the IDS. Ensured entire system is operational including database and application servers, IDS, event collectors, sensors, and periphery equipment. Performed system backup, restore, recover, purge, and update activities. Created and applied modifications to attack signature policies as well as updated and maintenance of IDS attack signatures Performed reviews, analyses, tests and evaluations and produced reports presenting findings and recommendations. Performed risk assessments, security tests and evaluations, and certification and accreditation's reviews to meet federal regulation guidelines. Assisted Network Development Team in designing and developing a recovery network in an offsite location. Supported the CIO, IT Director, and CSO in the creating and developing of a computer security database to track audits related to the computer security program. Prepared, reviewed and tested disaster, contingency, business resumption and incident handling plans. Evaluated and monitored compliance with existing security standards. Assisted in the development and conduct of security awareness and training courses, to include computer and web-based products, and maintaining the training database. Network and Security Engineering Project Lead Group EDS 2000 to 2001 Systems Security Operations Specialist Howard University 1999 to 2000 Network and Security Operations Lead Florida Board of Regents 1998 to 1999 Network and Security Administrator First District Court of Appeals 1996 to 1998 Systems and Security Administrator Crestmont Federal Saving 1991 to 1995 Education Computer Science Florida Agricultural & Mechanical University Skills Linux, Windows 2000, Novell Additional Information Operating Systems - Novell 3x-6x, Windows 2000/2003/2007/2010, various versions of Linux including RedHat 7.2, 8.0, and 9.1, Mandrake 9.1, SUSE, and Knoppix.

Name: Eric Williams

Email: david58@example.com

Phone: 600-605-8156