Mr. Jude Dominique Joseph

Howard University

Adjunct Instructor

Information Systems and Supply Chain Management

jude.joseph@howard.edu

Teaching Experience

INFO 010, Business Problem Solving, 1 course

INFO 396, Project Mgmt., 4 courses

MIS 204, Management Information Systems, 4 courses

OIST 509, Project Mgmt., 3 courses

PROFESSIONAL EXPERIENCE

Associate/Information System Security Manager – Fort. Meade, MD **February 2023 – Present**
Booz Allen Hamilton 40+ hours (F/T)

Responsible for establishing, documenting, and monitoring our DISA's cybersecurity program. Coordinate work with internal and external stakeholders to identify combinations of tools and techniques to translate customer's I.T. needs and future goals into a plan that will enable secure and effective solutions. Tasked to investigate new techniques, break free from the legacy model, and go where the industry is going. Leading a team through critical approaches to network design, providing alternatives and customizing solutions, to maintain a balance of security and mission needs.

Adjunct Professor – Washington, DC **August 2021 – Present**
Howard University, School of Business,
Department of Information Systems and Supply Chain Management 6+ hours (P/T)

Perform adjunct faculty duties to teach undergraduate and MBA students in specialized area of management information systems, cybersecurity, and project management. Assist and support full-time faculty teachers and professors. Develop lesson plans, special assignments, and field projects for students. Assess and evaluate student assignments and their academic performances.

Senior Consultant – Washington, DC **Jan 2022 – Jan 2023**
Knight Federal Solutions 40+ hours (F/T)

Appointed Information System Security Officer to support the Defense Intelligence Agency (DIA) cyber and enterprise operations. Advised and guided projects and programs through the accreditation and maintenance milestones, including aligning and implementing appropriate Risk Management Framework (RMF) with agency policies and procedures.

Major Duties include, but are not limited to:

- Reviewed and commented on technical documentation to ensure compliance with security standards and regulations using CNSSI 1253 and NIST SP 800-53 guidance.
- Recommended security monitoring solutions as required to meet IA requirements.
- Guided projects and programs through successful assessment and authorization of systems components for Authority to Operate (ATO).
- Reviewed the compliance and security features of software components in each of category of Security Technical Implementation Guides (STIGs). Worked with other ISSOs to identify the organization's specific security and compliance needs and policies with Security Technical Implementation Guides STIGs.
- Focused on threats, vulnerabilities, and the security of programs and systems.
- Provided special consideration to intrusion detection, finding and fixing unprotected vulnerabilities, and ensuring that remote access points are secure.
- Coordinated closely with internal and external stakeholders to support, monitor (using Splunk), test, and troubleshooted software and hardware IA problems related to security.
- Identified, developed, and implemented security standards, procedures, and solutions appropriate to the RMF environment.
- Coordinated with DIA stakeholders to assure compliance with security reporting requirements.
- Worked with Subject Matter Experts (SMEs) to help identify user audit records to be captured and reported using designated processes.
- Established, maintained, and audited program IT enterprises infrastructure baseline configuration.
- Provided IA and RMF services such as System Security Plans (SSP), risk assessment, audit policy, scanning policy, POA&AMs, HBSS implementation, Data interface CONOPS, COOP/DR, IA Certification Checks, and MOU/MOAs.

Cyber Security III – Washington, DC **Feb 2016 –Jan 2022**
CACI 40+ hours (F/T)

Appointed Information Systems Security Manager by the Department of The Navy to develop and maintain a formal Information System (IS) security program and policies under the BTR Project; Oversaw and developed operational information systems security implementation policy and guidelines; Ensured periodic testing is conducted to evaluate the security posture of IS by employing various monitoring tools; Maintained a repository of all system level cybersecurity-related documentation (including ATOs) for IS under their purview; Managed, maintained, and executed recurring information assurance activities to support continuous monitoring; Served as a voting member of the Configuration Control (CCB); Assessed changes to the systems, their environment, and operational needs that could affect the security authorization; Ensured all (Information System Security Officers) ISSOs receive the necessary technical and security training to carry out their duties. Conducted incident response training to BTR team members. Performed incident response data spill exercises. Scheduled and executed annual and quarterly review of RMF documents in accordance with the Joint Special Access Program (SAP) Implementation Guide (JSIG), NIST standards, financial management overlay requirements, and DoD RMF. Presented monthly briefings of Plan of Action and Milestones (POA&Ms) to government leadership. Reviewed the compliance and security features of financial management software components, databases, and operating system in each of category of Security Technical Implementation Guides (STIGs). Worked with other ISSOs to identify the organization's specific security and compliance needs and policies with Security Technical Implementation Guides STIGs.

Supported the United States Department of Homeland Security's Customs and Border Protection/OIT/PSPD Project; Performed information assurance duties related to Certification & Accreditation (C&A), vulnerability assessment and management, and oversees all IS users to ensure they follow established IS policies and procedures; Reviewed and interpreted Federal and DoD guidelines and policies, and industry standard best practices.

Senior Information Assurance Specialist – Arlington, VA **Jul 2014 –Jan 2016**
Lowest Cost Complete Computer (LCCCS), Inc. 40+ hours (F/T)

Supported the United States Department of Justice (DOJ)/Drug Enforcement Administration (DEA) - Security Programs Project; Performed information assurance duties related to Certification & Accreditation (C&A), vulnerability assessment and management, and oversaw all IS users to ensure they followed established IS policies and procedures; Reviewed and interpreted Federal and DoD guidelines and policies, and industry standard best practices; Collaborated with software development and testing teams to assist in defining necessary requirements to achieve full accreditation; and Determined cause-n-effect of security breaches and researches, recommends, and implements changes to procedures to protect data from future violations.

Major Duties include, but are not limited to:

- Conducted security compliance reviews to measure the security posture of the Drug Enforcement Administration (DEA) Headquarters and subordinate offices and ensured conformance with federal regulations, DOJ and DEA standards.
- Ensured compliance from internal and external perspectives; assessed of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy.
- Provided policy and guidance for the development, deployment, operations, use and replacement of DEA's IT systems.
- Assisted developers with interpreting National Security Agency (NSA), Office of Management and Budget (OMB), and DOJ policy for the inclusion of appropriate technical security controls.
- Certified that DEA IT production systems have a current C&A.
- Participated in classified and DEA Sensitive But Unclassified (SBU) programs through the certification of contract security specifications (DD254).
- Managed clients' IT infrastructure under various competencies such as Incident, Change, Reporting and Service Level Management using Information Technology Infrastructure Library (ITIL) concepts.
- Prepared, maintained and implemented System Security Plans that accurately depict the customer's contractual requirements.
- Initiated and completed Plan of Action and Milestones (POAMs) to closure.

Key Achievements:

- Maintained security posture of the **6** systems assigned to perform continuous monitoring.
- Integrated Cyber Security Assessment & Management (CSAM) III, National Institute of Standards and Technology Special Publication (NIST SP) 800-53 Rev.4, SP 800-30, SP 800-18, SP-800-34, Federal Information Processing Standards (FIPS) Pub 199 and 200, and Committee on National Security Systems Instructions (CNSSI) No. 1253 to support C&A activities.

Information Technology Security Analyst – Rockville, MD **Oct 2013 – Jul 2014**
Turning Point Global Solutions 40+ hours (F/T)

Provided information security expertise for the Hawaii Health Connector (HHC) Independent Verification & Validation (IV&V) Project; Specialized in IT audits, IT Risk assessments, unauthorized access, viruses, and a wide range of vulnerabilities and threats; Analyzed critical systems, developed reports to document system vulnerabilities, and recommended appropriate solutions; Developed audit reviews, developed and updated IT security policy, procedures, and standards; and Reviewed system security plans, incident response plans, information security policy, and other specific security documentation.

Major Duties include, but are not limited to:

- Contributed to the development of IV&V Management Plan, IV&V Checklist, IV&V Review Activities, test cases and execution of tests on selected IV&V projects.
- Implemented and enforced SOPs, suggesting process improvements and analyzing process areas and technical architecture.
- Substantiated HHC's contractor's compliance with the standards and industry best practices; ensuring requirements of all applicable federal and state laws, regulations, policies and guidance, including any amendments or updates during the life cycle of the project were met and deliverables were in accordance with the overall scope.
- Collaborated with various IT vendors to receive input, conduct analysis of issues and develop recommendations.
- Planned, implemented, monitored, or upgraded security measures to protect computer information and networks.

Key Achievements:

- Identified, reported and assisted in resolving nearly 100 security findings from documentation reviews and consultation with HHC's implementation and security teams.
- Leveraged and optimized existing Data and IT Security systems; obtaining accurate, real-time data to inhibit timely and strategic decision-making.
- Identified strategic issues, advised on risks and opportunities during the State of Hawaii's Affordable Care Act implementation from a security perspective.
- Maximized sustainability and increased the efficiency of HHC's security posture.
- Improved operational efficiency and added to transparency by reporting risk level findings.

Senior Managing Consultant – Herndon, VA **May 2010 – Jul 2013**
IBM Global Business Services, Data Security & Privacy Projects,
U.S. Department of Agriculture, MIDAS Project, & U.S. Department of Homeland
Security/Customs & Border Protection (CBP) Project 40+ hours (F/T)

Supported IBM Data Security and Privacy group in various private and government sector projects ensuring these projects met IBM security standards; Led consulting engagements, including Data Security Assessments, developing strategic plans and discovery projects; Subject Matter Expert (SME) in the design and management of cost-effective information systems and technology solutions; Convey security offering capabilities during pursuits; and Assisted data security and privacy and to ensure that the Wal-Mart Point of Sale (POS) Support & Development Program, Post Holdings Program, Department of Homeland Security's Customs and Border Protection (CBP) SAP Program, U.S. Transportation Command's (Air Force) Distribution Portfolio Management Program, and U.S. Postal Service Projects are in line with IBM's Data Security and Privacy policies.

Major Duties include, but are not limited to:

- Provided programmatic consultation, oversight, and guidance in support of information systems and networks; provided demonstration of IBM credentials in the Data Security domain.

- Provided oversight, consultation, and guidance to manage a set of guidance materials for IT governance and compliance.
- Ensured clients understood key security and privacy issues, risks, exposures and vulnerabilities using workshops to meet client's business needs; Developed and maintained client relationships.
- Implemented security controls with project managers and supporting team members to comply with data security and privacy framework, contributing content and advice to the development process.
- Set schedules for monthly, quarterly, and annual reviews of security documentation and processes to ensure client security requirements, government regulations, Federal Information Security Management Act (FISMA), NIST, and industry standards that apply are met.
- Provided security expertise and input for the development of new and existing business proposals for IBM.

Key Achievements:

- Oversaw a team consisting of **5** project managers ensuring their multi-million-dollar projects met IBM's Data Security and Privacy standards.
- Created and updated Systems Security Plans, User ID and Access Management, and On/Off Boarding process documents.
- As an ISSO, ensured the **3** assigned CBP's systems complied with federal and industry security standards.

Additional Work Experience Available Upon Request

EDUCATIONAL BACKGROUND

Doctoral/PhD Candidate (Expected Spring 2026)
Cyber Leadership
Capitol Technology University – Laurel, MD

Graduate Certificate (2005)
Information Assurance
University of Maryland Global Campus — Adelphi, MD

Master of Science (2004)
Information Technology
University of Maryland Global Campus — Adelphi, MD

Graduate Certificate (2002)
Telecommunication Management
University of Maryland Global Campus — Adelphi, MD

Bachelor of Business Administration (1997)
Computer-Based Information System
Howard University — Washington, D.C.

SPECIALIZED SKILLS / CERTIFICATIONS

PMI Authorized Training Partner - 2024
Project Management Professional (PMP) - 2021
Certified Information Systems Auditor (CISA) - 2021
Certified Information Security Manager (CISM) - 2015
IBM Data Security and Privacy Security Expert Certification - 2013
ITIL v3 Foundations - 2011