**David J. Olkowski, Jr.**

**1024 N. Utah St. #620**

**Arlington, VA 22201**

**(571) 213-9194**

**Dave.Olkowski@gmail.com**

**QUALIFICATIONS SUMMARY:**

* Twenty-one years experience as an information assurance analyst/engineer performing federal government agency information security program support, security controls assessment, and security reviews for information system Assessment and Authorization (A&A) formerly known as Certification and Accreditation (C&A).
* In-depth understanding of methodologies used to assess and test federal government information system security strengths and vulnerabilities as measured against National Institute for Standards and Technology (NIST) and Department of Defense (DoD) computer security guidance and standards.
* Six years experience as a network engineer building Pentagon systems as a DoD contractor and a United States Air Force computer communications officer.

**EDUCATION:**

**George Mason University MBA January 2000**

**University of Notre Dame BS, Computer Science with May 1994**

 **concentration in Business Administration**

**TECHNICAL CERTIFICATIONS:**

* International Information Systems Security Certification Consortium (ISC)2® Certified Information System Security Professional (CISSP),® Certificate 96917, September 2006.
* Cloud Security Alliance (CSA), Certificate of Cloud Security Knowledge (CCSK), 433387302031, September 2014.
* Certified Ethical Hacker (C|EH)™, ID ECC942324, August 2010.
* Project Management Institute (PMI)® Project Management Professional (PMP)® PMP No. 514185, February 2008.
* SANS Global Incident and Analysis Center (GIAC) Security Essentials Certification (GSEC), April 2007.
* National Security Agency – Information Assurance Methodology (NSA-IAM), November 2007.
* Cisco Certified Network Associate (CCNA), May 1999.

**PROFESSIONAL ORGANIZATION LEADERSHIP:**

* Information Systems Security Association (ISSA), Northern Virginia Chapter, Vice President for Education Programs for 2013-2014. Active chapter member since 2005.

**SECURITY CLEARANCES**

* DoD Top Secret SCI (SSBI), Special Access Program (SAP) including Counterintelligence Polygraph.

**PROFESSIONAL EXPERIENCE:**

**System High and SAIC, Inc. Security Control Assessor (DARPA Client) 2018-Present**

* Security controls assessor (SCA) for the Defense Advanced Research Projects Agency (DARPA) Strategic Technology Office (STO).
* Responsible for the assessment of 25 performer and partner Wide Area Networks (WANs), Local Area Networks (LANs), and stand alone systems at classified Special Access Program (SAP) against Joint Special Access Program (SAP) Implementation Guide (JSIG) for SAP systems and DoDI 8510.01, “Risk Management Framework for DoD Information Technology.”
* Provides risk recommendations of performer systems for Authorization to Operated (ATO) decisions for the DARPA Senior Authorization Official (SAO) and STO Program Security Officer (PSO). Evaluation of risk includes briefing the SAO and PSO with consideration of Department of Defense SAP, JSIG, and DARPA policies and mandates with consideration of mission success and risk appetite..
* Prior to internal promotion to STO SCA, served as lead DARPA SCA for classified enterprise information systems and networks.
* Responsibilities included oversight evaluation and continuous monitoring of secure configuration and compliance for the DARPA Authorization Official and Chief Information Security Officer (CISO) on the SAVANNAH SAP, ASCEND SAP, DARPA cyber range enterprise SAP network, DARPA Secret Network (DSN), and DARPA Secret Wide Area Network (DSWAN).
* Performed full and partial risk assessments of DARPA classified networks against JSIG for SAP systems and DoDI 8510.01, “Risk Management Framework for DoD Information Technology.” Assessments are prepared and briefed to the DARPA AO and CISO for decisions on Authorization to Operate.
* Managed database reporting for a DARPA inventory of approximately 150 performer SAP systems for reporting to the DARPA AO. Tracks security control issues on performer SAP systems for failed compliance and current ATO status.
* Provided Subject Matter Expert (SME) representation and ad hoc risk analyses for the AO and CISO through participation in DARPA Information Technology Directorate (ITD) operations and security status meetings.
* Reviewed configuration management changes and provides recommendations to approve or reject based on the risk level of hardware and software components under evaluation for integration into DARPA classified networks.

**SAIC, Inc. (formerly Engility) Security Engineer (U.S. Army G-2 Client) 2016-2018**

* Served as the security engineer on the Army Intelligence Campaign Initiatives Group (AICIG) project to build, operate, and maintain the Analytic Assessment Tool (A2T) application for the Department of the Army, Office of the Deputy Chief of Staff (ODCS) G-2 (Military Intelligence).
* Evaluated the security risk and compliance for the A2T application version currently in development through the Risk Management Framework (RMF) process. A2T is a multi-tier web application, business logic, data store, and report generation tool designed with RESTful architecture and a MongoDB database hosted on a Red Hat Enterprise Linux operating system.
* Functioned as the information security officer (ISO) and expert for assessing current application controls in compliance with DoDI 8500.01, "Cybersecurity," and DoDI 8510.01, "Risk Management Framework for DoD Information Technology."
* Categorized information sensitivity and selects, provides guidance for implementation, and assesses effective implementation for validation by the Army NETCOM Security Control Assessment Validator (SCA-V) and G2 Authorization recommendation.
* Served as liaison for AICIG to the Army INSCOM infrastructure hosting and G2 client organization through which he obtained support for inheritance and implementation of required security controls.
* Collaborated with the AICIG software development, quality assurance, and system administration teams in identifying vulnerabilities and directing mitigation actions to build and maintain the A2T system within security requirements.
* Managed A2T's integration in the Enterprise Mission Assurance Support Service (eMASS) Governance Risk Compliance (GRC) tool for entry, validation, management, and Plan of Action and Milestones (POA&M) of security controls, supporting artifacts, and vulnerabilities.

**Lunarline, Inc. Security Engineer 2015-2016**

* Security Engineer and Analyst for the BNY Mellon client in support of Ginnie Mae.
* Performed FISMA analysis on the Ginnie Mae General Support System (GSS), GinnieNet, Integrated Pool Management System (IPMS), and Unclaimed Funds System.
* Prepared analysis and briefs senior BNY Mellon management for tactical and strategic security program planning and budgeting to provide optimum risk management and continuous monitoring.
* Provided guidance and mentoring to Lunarline technical team at BNY Mellon to integrate their technical vulnerability scanning, audit analysis, and planning with Splunk and Nessus with client security program.
* Reviewed security controls on Ginnie Mae systems for compliance with NIST SP 800-53 R4 and FISCAM standards.
* Authored, drafted, edited, and reviewed required security documentation including the System Security Plan for the GSS.
* Prepared security control review and security documentation development for BNY Mellon’s Small Business Administration Fiscal Transfer Agent (FTA) system.

**Tantus Technologies Information Assurance Analyst 2011-2015**

* Information Assurance Analyst assigned to the U.S. Department of State (DoS) Bureau of Human Resources, Executive Office (HR/EX) System Development Division.
* Provided guidance and task management for the HR/EX Director and Government Program Managers for security of three internal and two external applications.
* Performed the annual security control assessments on all internal HR/EX systems including the Integrated Personnel Management System (IPMS), Human Resource Network (HRNet), Personnel Reporting and Statistics (PRAS) systems using the NIST SP 800-53A test cases against the system’s critical, vulnerable controls annually and a sampling of one third of all other controls.
* Communicated annual assessment results to the system owner, Information System Security Officer (ISSO), operations team lead, and system development lead formulating clear and measurable Plans of Action and Milestones (POA&Ms) for mitigation.
* Analyzed the security impact and required security control changes to support proposed introduction of changes to HR/EX production environment applications, software subsystems, and interconnections through the development of planned change comparative analysis reports.
* Coordinated the mitigation of vulnerabilities from A&A Security Assessment Reports (SAR) into and through POA&Ms and serves as the liaison between the independent assessment teams from the State Information Resource Management (IRM) Bureau, Information Assurance (IA) Assessment and Authorization division and the HR/EX system owner in order to manage the process to authorize, re-authorize, and report on the status of system owner designated continuous monitoring tasks.
* Prepared system administrators, database administrators and developers for security assessments through analysis of configuration settings at the operating system, database, and application levels.
* Created, edited, maintained, and updated the System Categorization Document (SCD), eAuthentication Risk Assessment, Privacy Impact Analysis (PIA), System Security Plan (SSP), Information System Contingency Plan (ISCP) for all internal HR/EX systems and reviews plans applications hosted externally by contractors.
* Coordinated the A&A of the new Entrance on Duty (EOD) web application with Peoplesoft back end. Worked with the HR/EX development and operational teams to prepare and mitigate vulnerabilities in the initial assessment. EOD is a high visibility new system with a front end accessible to DoS new employees from the public Internet. EOD enables advance loading of personal information and benefits elections prior to initial orientation date at DoS to greatly reduce cost and time involved in the hiring process.
* Managed certification and accreditation (C&A) task for the major upgrade on the Integrated Personnel Management System (IPMS), which is a collection of 50 web applications and PeopleSoft with an Oracle 11g and Microsoft SQL database back end. IPMS is the primary human resources management application for all domestic and overseas government civil service and Foreign Service employees at DoS.
* Prepared responses to data calls from the State Office of Inspector General (OIG) and Government Accountability Office (GAO) on HR/EX information system security program and individual information systems. Solicits direct and concise responses regarding specific control areas on both internal and external (contractor owned, contractor operated) for State.
* Managed the HR/EX POA&M mitigation process. Verifies that mitigation actions meet compliance to ensure HR/EX applications maintain the system owner’s acceptable level of risk in accordance with the DoS’ authorization official requirements.
* Represented the HR/EX at DoS Homeland Security Presidential Directive-12 (HSPD-12) working group. Works with Diplomatic Security (DS) and Information Resource Management (IRM) bureaus to ensure Human Resources requirements are met to enable the success of Department-wide deployment of Personal Identity Verification (PIV) cards for physical and logical access as mandated by HSPD-12.

**Knowledge Consulting Group Security Assessor/Primary Certifier 2009-2011**

* Performed security control assessments and compliance monitoring for the TSA Chief Information Security Officer (CISO) and Information Assurance and Cyber Security Division.
* Evaluated, analyzed, monitored, and reported on the status of TSA information systems in accordance with the Federal Information Security Management Act (FISMA), National Institute for Standards and Technology (NIST) SP 800-53, Department of Homeland Security (DHS) Management Directive (MD) 4300A, and TSA MD 1400.3.
* Held security assessor responsibilities on critical, high visibility systems including TSANet, which is the administration’s primary General Support System (GSS); the TSA Security Operations Center (TSA SOC); Crew Vetting Program (CVP); and the TSA Contact Center (TCC).
* Managed security engineer teams in performance of technical vulnerability scans during security control assessments of systems to prepare for initial or renewal of authorizations to operate.
* Conveyed findings of managerial, operational, and technical vulnerabilities through a combination of briefing and written reporting for the CISO to determine the system’s operational risk and to support the Authorization Official’s authorization decision making.
* Represented the TSA Information Assurance and Cyber Security Division assessor team for ongoing efforts including the IT Security Technical Standards Working Group, System Configuration Control Board (SCCB), and U.S. airport regional outreach support.
* Assisted information system owners and management in understanding risks to system operation “as is” and develops strategies for risk mitigation and resolution.
* Provided leadership and oversight for TSA Information System Security Officers (ISSOs) through assigned system’s engineering and security lifecycles.
* Assisted ISSOs with activities prior to and following system security assessments including preparation for Security Test and Evaluation (ST&E) and weakness mitigation under the TSA Plan of Action and Milestones (POA&M) process.
* Responsible for review and evaluation of ISSO certification documentation including System Security Plans (SSPs), Contingency Plans (CPs), Federal Information Processing Standard (FIPS) 199 System Categorization, and Privacy Threshold Analyses (PTAs).
* Evaluated and certified the completeness of mitigation actions with consideration of effective risk reduction provided by newly implemented and corrected security controls.

**Nortel Government Solutions Senior Information Assurance Analyst 2006-2009**

* Served as the Information Assurance (IA) Analyst Lead on DoD Information Assurance Certification Accreditation Process (DIACAP) and Air Force Certification and Accreditation Process (AFCAP) for design and implementation on Unified Capabilities Requirements (UCR) and Voice Over Internet Protocol (VoIP) systems.
* As the IA Analyst Lead, provided IA control requirements analysis and validation for VoIP upgrades and integration with existing Air Force telephony systems as a Type Accreditation of Nortel Assured Services (AS) 5300 and Multi Function Soft Switch (MFSS) communications platforms.
* Assisted multiple parties at the program level from the Air Force and Defense Information Systems Agency (DISA) and at the host installation level in developing artifacts to support IA controls.
* Coordinated review and application of DISA Joint Interoperability Test Center (JITC) IA test findings and Security Technical Implementation Guides (STIGs) for VoIP product designs in order to secure their deployments and obtain Interim Authorization to Test (IATT), Authorization to Connect (ATC), and Authorization to Operate (ATO).
* Applied the USAF IT Lean process as supported by the Security, Interoperability, Supportability, Sustainability, and Usability (SISSU) disciplines and the use of Enterprise Information Technology Data Repository (EITDR) for the AS 5300 and MFSS.
* Performed security control testing on the Nuclear Regulatory Commission (NRC) Digital Data Management System (DDMS) for the Atomic Safety and Licensing Board Panel (ASLBP) electronic courtroom facilities.
* Tested 25% of DDMS managerial, operational, technical, and functional security controls each quarter on security controls derived from NIST SP 800-53, SP 800-53A, and NRC requirements as part of the Continuous Monitoring of DDMS to maintain Authorization to Operate (ATO).
* Provided IT Verification and Validation (IV&V) Project Management Services to Education Department (ED) Office of Migrant Education (OME) Migrant Student Information Exchange (MSIX) system for the IT Contingency Plan, Self-Assessment, and Remediation Plan in accordance NIST and ED policies, methodologies, and templates.
* Responded to consultation requests from ED customer for MSIX on an ad hoc basis for security design and implementation issues such as data encryption solutions.
* Performed Risk Assessment (RA), SSP, and ST&E for the C&A of the OIG LAN GSS for the Pension Benefit Guaranty Corporation (PBGC) Office of Inspector General (OIG).
* Composed summary documents for NIST Special Publications, FIPS Publications, and the Committee on National Security Standards (CNSS) issuances to serve as training guides for Department of State (DOS) Information Assurance course teachers. Developed presentations for DOS IA Portal as instructional guides for system owners for RAs, Security Self-Assessments, Continuous Monitoring, and IT Contingency Planning at the Department of State (DOS).
* Assisted U.S. Patent and Trademark Office (USPTO) Electronic Business Center (EBC) in determining and planning to meet security requirements for contractor owned and operated information systems. Briefed EBC management on process for meeting compliance under the USPTO CIO IT Security Management Group C&A program including necessary actions to secure current and future EBC systems. Completed Preliminary RA and Privacy Impact Assessment for the EBC Survey application.
* Provided assessment of technical security controls to prepare information systems for certification testing for the National Aeronautics and Space Administration (NASA). Assessed controls on applications and general support systems against NIST SP 800-53 and NASA Procedures and Requirements (NPR) 2810.1A. Reviewed configurations of routers, switches, servers, and workstations to verify the implementation of configuration settings and auditing parameters on NASA information systems. Reviewed output findings from Foundstone and Microsoft Baseline Security Analyzer (MBSA) scans of Windows servers to provide mitigation actions in security assessment reports.
* Performed independent validation of DIACAP C&A of the Department of Defense (DoD) Civilian Personnel Management Service (CPMS) Defense Civilian Personnel Data System (DCPDS). Completed comprehensive analysis of role based access control user privileges across DCPDS. Assisted CPMS in a physical and environmental security RA of DCPDS. Control evaluation included a comprehensive assessment of role based access privileges, validating physical access to the facility, observing physical compartment restrictions within the facility, reviewing power supply infrastructure.
* Performed discovery and enumeration technical testing of the Farm Credit Administration (FCA) General GSS using software tools including Tenable Nessus, SolarWinds Toolset and LANsurveyor. Corroborated findings with client provided network information in a maximum knowledge test. Coordinated discovery and enumeration results with Nessus vulnerability scans of client hosts. Formulated test report based on findings to assist client in vulnerability prioritization and remediation.
* Conducted certification testing on the U.S. Department of Justice (DOJ) Unified Financial Management System (UFMS) application during the development and testing phase in order to provide the authorizing official with comprehensive and accurate information for making an accreditation decision. Performed ST&E in accordance with the FISMA; OMB A-130, Appendix III; FIPS 200; NIST SP 800-37; NIST SP 800-53; and DOJ Order 2640.2E. Verified compliance of UFMS’ documented and implemented security controls using the DOJ Information Technology Security Standards (ITSS) and the Cyber Security Assessment and Management (CSAM) ToolKit TrustedAgent application.

**SRA International, Inc. Senior Member of the Professional Staff 2000-2006**

 **Information Assurance Analyst**

* Provided information security support to the software development team for the Department of Justice (DOJ) U.S. Trustee Program (USTP). Duties included advice to program and technical management on the assessment of security posture and interpretation of federal, DOJ, and USTP requirements.
* Managed the efforts to prepare the USTP’s complex environment of web applications, Oracle databases, and IBM DB2/UDB databases for individual system certification and accreditation (C&A) through system security planning, contingency planning, patch management, configuration management, and remediation of findings from security assessments and audits.
* Performed C&A for 5 U.S. Food and Drug Administration (FDA) systems including development of SSPs, CPs, and RAs. Executed ST&Es through observations, management and staff interviews, and Technical Vulnerability Assessments of FDA servers.
* Member of the Information Assurance group assigned to the Department of Labor (DOL) National Office. Team contributions and tasks led to a high level of improvement of DOL information system security in review and ratings by the Office of Management and Budget (OMB) and Congressional oversight committees.
* Developed assessment process and executed evaluation effort for 52 critical systems in 13 DOL agencies for information assurance performance to comply with the Government Information Security Reform Act of 2000. Assessment followed guidance from the Federal Chief Information Officer Council and NIST SP 800-26, Security Self-Assessment Guide for IT Systems.
* Headed effort to facilitate completion of DOL agency information system contingency plans. Process included composition of a template for information system contingency planning for each DOL agency, training agency information resource managers on application of the template, and evaluating completed contingency plans.
* Guided the system security C&A of high visibility and high criticality systems for DOL including the GovBenefits.gov portal and a customized PeopleSoft consolidated human resource, time and attendance, and payroll system.

**SANS Institute Instructor/Mentor for the GIAC Security 2003**

 **Essentials Certification**

* Mentored 20 GIAC Security Essentials Certification (GSEC) candidates through presenting and leading discussions on practical applications of SANS GIAC’s comprehensive basic curriculum in areas of network design and security, defense in depth, security policy, organizational security best practices, risk management, intrusion detection, incident handling, malicious software, disaster recovery, and operating system specific security. Guided candidates on selecting and drafting written practical assignments.

**SRA International, Inc. Senior Member of the Professional Staff 1998-2000**

 **Systems and Network Engineer**

* Member of the engineering team tasked to develop engineering designs to migrate the National Military Command Center’s (NMCC) Command, Control, Communications, Computers, and Intelligence systems into a new facility as part of the Pentagon Renovation.
* Produced Engineering Design Package for NMCC Staff and Support Area including 18 DoD organizations and 24 data, voice, and video systems.
* Developed cable pathways study for Pentagon basement and mezzanine renovation areas.

**United States Air Force Communications and Computer Officer 1994-1998**

* Designed network engineering plan for organizational move of HQ U.S. Air Force components as part of the Pentagon renovation. Involved optimal planning of physical and logical network configuration changes to accommodate existing and new networks which will support 3,500 users.
* Managed integration of a new Windows NT server architecture for HQ U.S. Air Force through initial configuration and facility installation of $750,000 in servers.
* Coordinated projects and developed expertise in the computer network field to design, acquire, and implement an unclassified Internet-connected LAN/WAN and classified SIPRnet-connected LAN/WAN for Office of the Secretary of Defense, Office of the Director for Program Analysis and Evaluation (PA&E).

**TECHNICAL TOOLSET EXPERIENCE:**

* Red Hat Enterprise Linux (RHEL)
* DISA Security Technical Implementation Guides (STIGs)
* Pitbull Trusted Network Environment
* Xacta 360
* eMASS
* SCAP Compliance Checker (SCC)
* DISA Assured Compliance Assessment Solution (ACAS)
* vMWare vSphere
* McAfee Host Based Security Scanner (HBSS)
* Tenable Nessus
* eMASS
* Splunk
* Application Security AppDetectivePro
* IBM Rational AppScan
* HP WebInspect
* DISA Windows Gold Disk
* Microsoft Baseline Security Analyzer
* SolarWinds LANsurveyor
* McAfee Foundstone
* TrustedAgent FISMA

**TECHNICAL PAPERS:**

* “Information Security Issues in E-Commerce,” March 26, 2001,

http://www.sans.org/reading-room/whitepapers/ecommerce/information-security-issues-e-commerce-37