Larry Chaffin

223 Maplebrook Dr, Madison, AL 35756
(C) (256) 337-5343
larry.chaffin@yahoo.com lchaffin.adira@gmail.com

Senior Cyber Security Professional Certified Information Systems Security Professional (CISSP) with over 25+ years in the cybersecurity field with a broad and comprehensive knowledge executing assessment & authorization processes (NIST, CMMC, RMF, NISPOM, DAAPM, JSIG) across multiple government (DoD, DOJ) Missile and Defense programs, enterprise business systems, national security systems, collateral and Special Access Programs (SAP) with hands-on Windows, HP UNIX, Linux, Solaris, IRIX, SUSE, and MAC operating systems hardening, vulnerability scanning, auditing, assessment, and authorization responsibilities. Excellent team-builder, innovative thinker with a proven track record devoted to process excellence.

SUMMARY

- ★ **Government Cybersecurity Specialist**
  - ○ *CMMC Technical Manager, American Bureau of Shipping - Quality Evaluations*
  - ○ *Enterprise Information System Security Manager, Aerojet Rocketdyne*
  - ○ *Supporting Multiple DoD Programs, The Boeing Company*
- ★ **Cyber Integration Information Security Manager**
  - ○ *ARMY, PEO IEW&S, TSS PdL: ARMY Civilian (NH-03)*
  - ○ *ARMY, Space and Missile Defense Center (SMDC), Radiance Technologies*
- ★ **Supervisor Information Systems Security Professional (ISSP)**
  - ○ *Defense Security Service (DSS), Government Civilian, (GG-14)*
- ★ **Information Security Consultant**
  - ○ *NASA, Marshall Space Flight Center for Hewlett Packard Enterprise (HPE)*
- ★ **Information System Security Manager (ISSM)**
  - ○ *ARMY, PEO Missiles and Space, JACOBS*
  - ○ *MDA, Ground-based Midcourse Defense (GMD), The Boeing Company*
- ★ **Information System Security Officer (ISSO)**
  - ○ *FBI, Terrorist Explosive Device Analytical Center (TEDAC), SPRY Methods*
  - ○ *MDA, Terminal High Altitude Area Defense (THAAD) for Lockheed Martin*
- ★ **United States Navy Submariner (Veteran)**
  - ○ *USS Kamehameha (SSBN-642), Ballistic Missile submarine*
  - ○ *USS Bremerton (SSN-698), Los Angeles-class submarine.*

CLEARANCE

- **Clearance Level:** TS SCI-ICD704
- **Granting Agency:** DoD CAF
- **Date Granted:** 2020-03-03

EDUCATION/CERTIFICATIONS

- Bachelor of Science in Information Systems, GPA 4.0, 2008
- Certified Information Systems Security Professional (CISSP) - In Good Standing: 2008, 2011, 2014, 2017, 2020, 2023 Certification #314520
- Certified CMMC Assessor (CCP), 2024
- Certified CMMC Professional (CCA), 2024
- Certified CMMC Provisional Instruction (PI), 2024

PROFESSIONAL EXPERIENCE

ADIRA Solutions LLC

Madison, AL
July 2024 - Present

Co-Owner Services and Training Provider - CCP, CCA, PI

As a co-owner of Adira Solutions I provide Cybersecurity Maturity Model Certification (CMMC) expert services for:

- Assessments
  - Certification
  - Mock
  - Readiness
- Consultation and Advisory Services
- Assessor Training
  - Provide training through an approved Licensed Training Provider (LTP) network and ensure assessors understand the CMMC framework, assessment procedures, and relevant guidelines.

ABS-Quality Evaluations

American Bureau of Shipping
Spring, TX 77389
July 2023 - Present

CMMC Technical Manager

As a CMMC Technical Manager within a Cybersecurity Maturity Model Certification (CMMC) Third-Party Assessment Organization (C3PAO), I specialized in coordinating assessments by leveraging my in-depth technical knowledge of cybersecurity and CMMC requirements.

Responsibilities

- **Assessment Planning and Coordination:** Coordinate with internal and external stakeholders to ensure a smooth and efficient assessment process.
- **Communication and Reporting:** Prepare comprehensive assessment reports that clearly outline areas of compliance and non-compliance with CMMC requirements.
- **Client Relationship Management:** Maintain positive relationships with client organizations undergoing CMMC assessments.

Competencies

- <u>Communication</u> – I effectively shared information both verbally and nonverbally to other parties inside and outside the organization.
- <u>Executing leadership</u> – I mentored, trained, and provided performance development.
- <u>Technical</u> – I maintained an updated body of knowledge and skills required to scope and assess situations and find effective solutions.

Skills

- Performing DoD DIB risk analysis, mitigations and assessments
- Coordinating and conducting GAP and mock assessments
- Self-inspections, security control assessments, readiness reviews
- CMMC Scoping, cybersecurity technical assistance and collaboration

Aerojet Rocketdyne

Cummings Research Park
Huntsville, AL
September 2020 - July 2023

Enterprise Information System Security Manager (ISSM)

Responsible for overseeing and supporting contractual compliance in enterprise classified processing environments. I lead cross functional teams in planning new systems, security plans, and operating environments. I managed multiple site ISSMs on the creation and submission of authorization packages to Cognizant Security Agencies (CSAs). I conducted periodic self-assessments of site level compliance and the overall security program. Promulgated and maintained contingency, disaster recovery, spill response, and other security related plans and standard operating procedures.

Responsibilities

- Operated autonomously as the information systems subject matter expert.
- Determined and implemented approaches to objectives set by leadership.
- Served as the lead coordinator with Program Management, Engineering, and IT on all new enterprise level classified systems/initiatives to meet program and customer requirements.
- Monitored quality and timeliness of program deliverables, identify best practices and opportunities for improvement, standardization, and increased efficiency
- Maintain the Enterprise Mission Assurance Support Service (eMASS) for all site ISSMs
- Developed, facilitated, and monitored security education, training, and awareness.
- Provided compliance status reports to leadership on all assessments and self-assessments.

Competencies

- <u>Communication</u> – I work with clients, coworkers and managers to keep them informed.
- <u>Time management</u> – I develop timelines and complete projects on time and within budget.
- <u>Problem-solving</u> – I evaluate situations and find effective solutions.

Skills

- Managing/Supervising teams across multiple locations
- Working autonomously.
- Project Management
- Communication; oral and written

The Boeing Company

Boeing JetPlex
Huntsville, AL
May 2019 - September 2020

Government Cybersecurity Analyst

Author, direct and assess the implementation of security procedures and mitigate system security threats/risks throughout the information system life cycle. Responsible for supporting contractual compliance within classified processing environments. Subject Matter Expert SME for new information systems authorization packages under the Risk Management Framework (RMF). I utilize my direct experience in validating system security requirements, analysis, and establishing documentation to ensure compliance through self-governance. Very familiar with the DAAPM, JSIG, and Special Access Programs (SAP), and performing system and program auditing to ensure and verify requirements; perform information system certification and authorization planning, testing, assessing and liaison activities.

Responsibilities

- Co-Chair National Industrial Security Program (NISP) for the Boeing Huntsville site
- Conduct and author Risk Assessment Reports
- Obtain formal Assessment & Authorization to Operate (ATO) of systems.
- Implement government policies, authoring policies and procedures
- Maintain the Enterprise Mission Assurance Support Service (eMASS)
- Interpret and mitigate vulnerability scans

Competencies

- <u>Results Driven</u> – I develop and communicate goals dedicated towards positive customer outcomes.
- <u>Team Dynamics</u> – I build trust relationships with diverse team members to leverage their expertise across all functional areas.
- <u>Managing Change</u> – I demonstrate and support innovation, and personally develop new methods and processes.

Skills

- Performing IT risk analysis, mitigation and implementing strategies
- Coordinating information security inspections, tests, and reviews
- Oversight and execution of a continuous monitoring program
- Self-inspections, security control assessments, scanning

ARMY Civilian (NH-03)

PEO IEW&S, TSS PdL

Huntsville, Alabama

May 2018 to May 2019 *Note: (I stayed in place when I was selected as a government civilian.)

Cyber Integration ISSM

The Cyber Integration ISSM appointed by the Army Space and Missile Defense Command (SMDC) I provided support to the Tactical Space Superiority Program Office. I managed and coordinated various defense contractors' on the design, testing, and implementing state-of-the-art secure operating systems, networks, database products, firewalls, and network architectures to meet government classified Cyber resilience requirements.

Responsibilities

- Managed a team of Systems Engineering and Technical Assistance (SETA) and Cyber Information Systems Security (CISS) Professionals.
- Established control processes to ensure mitigation of risks and support obtaining formal Assessment & Authorization to Operate (ATO) of systems.
- Implemented government policies, authoring policies and procedures in line with the JSIG, CIO G/6 SAP policies and memorandums.
- Voting member on the Change Control Board (CCB) with veto authority.
- Chaired the Cyber Integration Integrated Product Team (IPT)
- Communicated and coordinated program management teams, vendor teams, and security control assessor (SCA) teams.

Skills

- Experienced in communicating with both Program and senior leaders: ARMY 05-08, CIO, CISO, Corporate Presidents, Vice Presidents.
- Prior experience in leadership and management roles: DSS ISSP, ISSM, Consultant.
- Diverse classified information systems security/information assurance background: Business, mission/tactical, platform IT).

Radiance Technologies

Army - Space and Missile Defense Command (SMDC)
Huntsville, Alabama
March 2017 to May 2018 *Note: (I stayed in place when I was selected as a government civilian.)

Information Security Manager

Provided cyber integration support to the PdD TSS Office at Army Space and Missile Defense Command (SMDC) as the principal advisor to the Cyber Integration Team Leader in effectively integrating cybersecurity across all functional domains.

Responsibilities

- Provided coordination and oversight with vendor Information Systems Security Officers (ISSO) and Facility Security Officers (FSO).
- Performed CDRL (Contract Data Requirements List) reviews and provided feedback to the Cyber Integration Team Lead.
- Led the Cyber Integration Working Integrated Product Team (WIPT) meetings.
- Engaged with internal and external customers (i.e. AOs, DAOs, SCAs, Program Managers, etc.), to include negotiating controls/requirements.
- Performed risk assessments, SSP and STIG reviews
- Vulnerability assessment scans, SCAP Scans.

Competencies

- <u>Self-Motivation</u> – I am motivated in my work by learning and sharing information which helps others understand the cyber environment and the threats against it.
- <u>Executing leadership</u> – I mentor, train, and provide performance development.

Skills

- Cyber Security acquisition support to a Program Management Office (PMO).
- Ensuring security policies, standards and procedures are established and enforced.
- Coordinating information security inspections, tests, and reviews.
- Oversight and execution of a continuous monitoring program.
- Self-inspections, security control assessments, scanning.

SPRY Methods

Federal Bureau of Investigation (FBI)
Huntsville, Alabama
November 2016 to March 2017

Security Consultant

Provided cybersecurity expertise and guidance to the FBI's Terrorist Explosive Device Analytical Center (TEDAC) in Huntsville, Alabama. Assigned as a SPRY Methods Information System Security Officer (ISSO) to the TEDAC Operations, Plans, and Policy (TOPPs) Office. I worked closely with the Project Manager in developing and implementing classified cyber security operations across multiple classified and unclassified technology platforms, and business environments for the TEDAC enterprise.

Responsibilities

- Authored policies and procedures for Risk Management Framework (RMF).
- Performed Personal Identifiable Information (PII) Impact Assessments.
- Approval authority for users' access to the TEDAC FBI and SIPRnet websites.
- Approved classified document uploads to the TEDAC website on SIPRnet.
- Authored system security plans for the Department of Justice (DOJ) utilizing Risk Vision.

Competencies

- <u>Solving problems and making decisions</u> – I quickly resolved problems and created projects for open issues. As the sole cybersecurity professional, I leaned upon my years of experience to make many decisions on accreditation actions, processes, and procedures.

- <u>Understanding and Navigating the Organization</u> - My Department of Defense experience enabled me to ramp-up quickly and navigate the FBI Department of Justice (DOJ) Policies and Instructions.

Skills

- Agile methodology for System Development Life Cycle
- Security/Document classification and marking
- Risk Vision accreditation system
- Security Controls Review, Vulnerability Management

Hewlett Packard Enterprise (HPE)

NASA - Marshall Space Flight Center
Huntsville, Alabama
August 2016 to November 2016

Security Consultant

As an Information Security Consultant, I was in daily contact with high level program management, engineering staff, and NASA cybersecurity team to resolve cyber security related issues. I was personally responsible for managing multiple projects in a dynamic environment spanning over 11 NASA centers, to include Marshall Space Flight Center, Johnson, Stennis, Kennedy, and seven others across the nation.

Utilizing my prior experience in authoring security plans and processes, and maintaining accreditations with the Department of Defense, I created and maintained technical and operational documentation, which included system security plans (SSP), Plan of Action and Milestones (POA&M) management, threat and vulnerability assessments, as well as managed the vulnerability tracking and mitigation activities.

Responsibilities

- Authored policies for Risk Management Framework (RMF).
- Performed risk analysis and recommended mitigation implementation strategies.
- Functioned as Security Point of Contact for internal projects.
- Coordinated with internal and external customers in a demanding environment to close out over 100 Plan of Action and Milestones (POA&M) vulnerabilities.

Competencies

- <u>Influencing Others</u> – I address issues with win-win solutions.
- <u>Customer Orientation</u> – Customers know I am willing to work with them to meet their needs.
- <u>Foster Innovation</u> - I developed and supported the introduction of new and improved methods, products, and procedures.

Skills

- Policy writing for RMF, Mitigation techniques, Risk Response Strategies
- Security Controls Review, Vulnerability Management
- System Development Life Cycle, RMF, NIST 800-53 Controls

Jacobs Technology

Army - PEO Missiles and Space
Huntsville, Alabama
November 2015 to August 2016

Senior Information Assurance Specialist

As the Senior Information Assurance Specialist I worked with the Army as an Information Systems Security Manager (ISSM) conducting accreditation actions under the DoDI 8510.01 Risk Management Framework (RMF) for both classified (SIPR) and unclassified (DREN) enterprise networks.

Responsibilities

- Authored Policy and Standard Operating Procedures for RMF solutions.
- Maintained the Enterprise Mission Assurance Support Service (eMASS).
- Conducted Security Content Automation Protocol (SCAP) scans.
- Migrated DIACAP accreditation packages to RMF.

Competencies

- <u>Implementing Strategy</u> – I interpret goals and requirements into working plans of action.
- <u>Technical & Business Solutions</u> – I manage, recommend, and promote changes that arise during the migration of DIACAP controls to RMF.

Skills

- Policy writing for RMF, Disaster, Contingency Planning
- DIACAP migration to RMF, Application Development, DISA STIGs
- Security Controls Review, Vulnerability Management
- System Development Life Cycle, Continuous Monitoring
- RMF, DFARS, CUI, NISP, NISPOM, NIST 800-53 Controls

Defense Counterintelligence Security Agency (DCSA)
Formally known as: Defense Security Service (DSS)

Government Civilian (GG-14)
Huntsville, Alabama
August 2010 to November 2015

Supervisory Information Technology Specialist

Managing out of the Huntsville, Alabama Field Office, I supervised a team of Information Systems Security Professionals for the Southern Region. I was responsible for certifications/accreditations and vulnerability assessments for the Cybersecurity Program across four (4) States and 100 cleared defense contractors.

Under my leadership, my team and I provided cybersecurity oversight across multiple security environments to include reviewing and assessing facilities under FOCI (Foreign Ownership, Control or Influence), approving Technology and Electronic Control Plans (TCP/ECP) under the National Industrial Security Program (NISP). I lead assessment teams, providing advice and counsel on risk levels, security posture and implications of new technologies or technology upgrades. Interfaced and disseminated necessary cyber event information to appropriate internal & external organizations and audiences.

My responsibilities covered all facets of the Authorizing Official (AO) responsibilities to include hiring, developing and retaining cyber security talents performing the DCSA classified cyber security mission.

Responsibilities

- Supervised, provided technical guidance and policy direction.
- Created metrics and project planning.
- Lead Assessment Teams.
- Collaborated and partnered with Industry.
- Trained and mentored ISSPs, ISSMs, and ISSOs.

Competencies

- <u>Establishing Focus</u> – I develop and communicate goals in support of the mission.
- <u>Empowering Others</u> – I convey confidence in others, allowing them to grow professionally.

Skills

- Managing Projects
- Managing/Supervising teams across multiple locations
- Performing IT risk analysis, mitigation and implementing strategies