Clarrissa Darden

Personal Profile

- I am a Subject Matter Expert on the FISMA Risk Management Framework and NIST (800-53), FISMA, FIPS 199, HIPAA standards with the adaptability to work as a team player or independently to progress vertically through any organization, while having the expertise to grasp technical nuances and effectively communicate. I have specialized experience, which includes performing RMF work in support of analysis to evaluate and or improve the efficiency, effectiveness, and productivity of organizations. I have experience with tools like ACAS, XACTA, ServiceNow Tenable Nessus and AWS security monitoring. I am extremely interested in learning new and advanced skills and abilities within the ever-evolving IT field. I am a professional with cybersecurity and IT audit experience with proven abilities to work and excel in highly stressful environments while still achieving positive results.

Education

- Northern Virginia Community College (Cybersecurity associate degree)
- Old Dominion University (Cybersecurity Bachelor's degree (graduate in August 2026)

Certification

- Top Secret Clearance SCI
- CompTIA Security+ Certification
- Network Administration Certification

Professional Experience

Rite-Solutions Inc.| Department of Navy
06/2023 – Present
Cyber Security Analyst

- Implement Cybersecurity Program strategy.
- Apply information security in accordance with Navy/DOD directives security policy including, but not limited to, NIST SP.
- Assess entire system’s lifecycle requirements and network security impacts.
- Support creation of, and ensure approval for, Department of Defense (DOD) Risk Management Framework (RMF) Assess and Authorize (A&A) Process for development and sustainment projects.
- Support program and customer management, and government Authorizing Official (AO) for all information security status, policies, and procedures.
- Document DOD RMF Security Implementation Plan artifacts. Coordinate and assist development team with application artifact documentation.
- Assist government personnel in preparing and presenting Information Assurance Compliance System (IACS) packages to the

Clarrissa Darden

Control Assessor (SCA) Assess and analyze the current threat environment.

- Enhance – Implement Cybersecurity vulnerability/A&A hardening testing.
- Optimize – Cybersecurity development environment certification.
- Architect & Engineer security – develop security goals, capabilities, controls, and architecture.
- Design & Implement security – vulnerability management, build security into development.
- Integrate & Test Security – test patches and settings, document A&A artifacts.
- Validate & Verify security – validate patch status and software control status.
- Implement security – apply patches and security settings, performance incident handling and remediation.
- Maintain security posture – audit security settings, track security training, monitor threats, track reaccreditation.
- Enable assurance for information security during all phases of agile software development and deployment.
- Continuously evaluate and recommend innovative proven best business practices and tools to enhance defense-in-depth.
- Identify, assess, and recommend zero-day cyber threat remediation.
- Address Cybersecurity issues to help maintain Continuity of Operations Plans (COOP)
- Perform information security vulnerability testing and mitigate any nonconformance.
- Supports reviews and audits of continuous system monitoring and contingency planning. Updates associated documentation as needed.
- Create and manage Plan of Action & Milestones (POA&M)
- Implement and validate Security Technical Implementation Guide (STIG) requirements for all development and implementation projects.
- Understand and assist developers with static code analysis processes.
- Report and help investigate security-related incidents and security violations as requested by the Computer Security Incident Response Center (CSIRC)
- Monitor and inspect for approved software usage and implementation of approved antivirus and other security related software.
- Develop and maintain security training programs are developed and maintained.
- Initiates Enterprise Mission Assurance Support Service (eMASS) registrations, prepares, processes, updates and monitors RMF Assessment and Authorization (A&A) packages; ensures A&A packages are evaluated and maintained in a compliant status; implements and validates A&A packages to ensure security controls and vulnerabilities meet DON RMF authorization compliance requirements.

Clarrissa Darden

Softek International Inc./ Department of Homeland Security (DHS/NSS)
01/2021 –06/2023
Cybersecurity Specialist

- Ensure and enforce quality assurance of security authorization documentation submittal such as Local CRs, ATOs, ATCs, IATTs, etc., to the DHS Document Review team. In addition, I performed risk analyses to identify appropriate security countermeasures and NIST Compliance
- Creating dashboards, Save Searches, Daily Scores, etc., for NSS Systems using Splunk.
- Enforces NSS systems compliance and assessment in line with the RMF Framework
- Initiates Enterprise Mission Assurance Support Service (eMASS) registrations, prepares, processes, updates and monitors RMF Assessment and Authorization (A&A) packages; ensures A&A packages are evaluated and maintained in a compliant status; implements and validates A&A packages to ensure security controls and vulnerabilities meet DON RMF authorization compliance requirements.
- by scheduling artifact delivery from the ISSO to Federal Compliance Managers and
- the SCA team and ensuring the successful completion of the Security Authorization process.
- Reporting the status of POA&M using Exacta 360, CSAM, and other predetermined
- government priorities and deliverables for all systems to the Compliance Manager and the Task Area Lead.
- Provide oversight and are the primary escalation point for Site Security Plan (SSPs) requirements and the Annual Physical Security Assessment compliance for over 3000 DHS SharePoint Sites.
- Informing stakeholders of system-related compliance activities, i.e., FISMA scorecard, POA&M resolution issues, Authority to Operate (ATO), Contingency and Contingency Test Plan, and Privacy Threshold Analysis (PTA) expirations.
- Support improvement for the OA Program and monitor DHS NSS systems OA requirements. Provides guidance, reviews, and tracks POA&M.
- Consolidation and Remediation Plans for NSS Systems to ensure proper remediation.
  planning and POA&M consolidation.
- Create, reviews and updates NSS policy and SOP.

DHS/FPS Paragon Systems Inc.
February 2016/2021
SOC Analysis

Clarrissa Darden

- Prepared Excel spreadsheets and Word documents to report information to end users.
- Analytical and solutions-oriented personnel with successful career leading cross- functional teams to meet milestones and solutions for operation projects. In kick off meetings for annual assessments worked with independent assessors and system owners to provide a smooth pathway to providing evidence throughout the assessment.
- Highly skilled in building strong relationships with business partners and communicating effectively across all organizational levels. Always have an open-door policy to all organizations to ensure that if there are any questions, comments, and concerns that need to be addressed I'm here to answer or find the right answer to address and resolve.
- Planning projects to meet quality, scope, and schedule milestone deliverable for process management. Tracking schedule deliverable with the CSAM tools and staying in constant communication with stakeholders and system owners to verify that items are being addressed in with the proper procedures and in the allotted period.
- Develops and constructs departmental reports within the RMF process. (SSP, SAR, RAR, ST&A, SRTM, SIA, CM Memo, Clearance Sheets, PIA, PTA, E-Authentication, Request of ATO, and ATO). Workflow processes ensures agency requirements are met and all processes are followed.
- Analyzing raw scans outputs using Tenable' s Nessus (.csv files). Mapping scan findings to applicable controls, providing suggested implementation for the proper resolution.
- Check and assess security controls per NIST SP 800 53 and NIST SP 800 53A.
- Worked independently and as a team to make remediation on information security management for use by those responsible for initiating, implementing, or maintaining information security management systems (ISMS).

Supervisory Correctional Officer **CCA D.C. Jail**
June 2010-August 2016

- Evaluates and verifies employee performance through the review of completed work assignments and work techniques.
- Identifies staff development and training needs and ensures that training is obtained.
- Maintains records, prepares reports, and composes correspondence relative to the work.
- Responsible for preparing and analyzing transport routes that maintained a high level of confidentiality in order to ensure a safe transport to and from the U.S. Marshall Service.

Clarrissa Darden

- Communicates, interprets, and applies departmental policies, facility regulations, and Department of Correction rules to subordinates.
- Observes inmates' activities to detect unusual or prohibited behavior, which might be a threat to the security of the facility or the safety of other inmates, employees, or visitors.
- Observes and appropriately respond personally and through subordinates to "critical incidents" such as assaults on employees, inmates, disturbances, or other situations threatening facility security; response may require use of firearms.
- Corresponded with government agency to ensure the exchange of confidential documents and data was properly entered into the system for the transporting of witness protection and high-profile inmates.
- Review and ensure that inmates data was entered into the (OMS) Offender Management Systems properly.
- Provided armed security escort into the public.
- Maintain cooperative working relationships with other law enforcement agencies.

Correctional Officer **CCA D.C. Jail**
October 2003-June 2010

- Corresponded with government agency to ensure the exchange of confidential documents and data was properly entered into the system for the transporting of witness protection and high-profile inmates.
- Observe inmate activities to detect unusual or prohibited behavior, which might be a threat to the security of the facility or safety of others.
- Review and ensure that inmates data was entered into the (OMS) Offender Management Systems properly.
- Communicate, interpret and apply departmental policies and facility rules and regulations.
- Provided armed security escort into the public.
- Maintain cooperative working relationships with other law enforcement agencies.
- Maintain records, prepare reports and compose correspondence relative to the work.
- Provide firearms and restraint equipment training for new employees.
- Monitor alarms closed circuit television (CCTV)

REFERENCES AVAILABLE UPON REQUEST