Assessment & Authorization (A&A) – Risk Management Framework (RMF)

Perform Assessment & Authorization (A&A) efforts in order to obtain Authorization to Operate on DoD/DoN networks in support of target activities. Scope shall include the following:

- Support policies and procedures related to cybersecurity, including appropriate certification and system testing, and achieving an authorization. A&A shall be performed per Risk Management Framework (RMF) and the Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation ICD 503 requirements. The effort shall develop the documentation required to meet RMF requirements. Supporting A&A documents may include:
    - Security Plan (SP)
    - Security assessment Plan (SAP)
    - System Level Continuous Monitoring (SLCM) Strategy
    - Security Assessment Report (SAR)
    - Risk Assessment Report (RAR)
    - RMF Validation Plan and Procedures
    - Validation (ST&E) Report/ ST&E Plan and Results
    - Plan of Action and Milestones (POA&M)
    - Contingency Plan

- The effort shall determine and identify applicable Cybersecurity A&A procedures, controls and develop the appropriate ST&E Test Plan and Risk Analysis.

- The effort shall provide but is not limited to requirements determination, A&A strategy development, policy research and documentation, to include addressing mission description; user descriptions; operating and computing environment; physical security needs; threat analysis; security roles; system architecture diagrams; external interfaces and data flows, Ports, Protocols and Services (PPS); and developing a contingency plan. The effort shall provide DISA Secure Technical Implementation Guide (STIG) software images of all systems in the architecture.

- Cybersecurity System Owner Support and Implementation - The effort shall manage and provide all A&A tasks and services to include A&A collaboration, Platform IT (PIT), Platform IT Interface (PITI), and RMF package generation, eMASS upload and management, security controls implementation and validation, and supporting security documents generation. The effort shall prepare the A&A schedule highlighting the major phases and identify potential risks with recommended actions and mitigations. The effort shall support government development of program POA&M documentation.

- The effort shall manage the A&A validation process and collaborate with designated certification authorities. These services shall include review of RMF documentation, validation reports, risk assessment, and POA&M. The effort shall discuss with certification authorities the mitigation and remediation of outstanding vulnerabilities. The effort shall proactively identify and remediate any A&A issues to avoid unscheduled collaboration with certification authority.