



CEXEC, Inc. performs information systems security (INFOSEC) assessments (IA) in accordance with established methodologies developed by the National Security Agency (NSA) and in compliance with Presidential Decision Directive 63 – Critical Infrastructure Protection. In our approach, we will review the INFOSEC posture of a specified, operational system for the purpose of identifying potential vulnerabilities. After completing our assessment, CEXEC will provide recommendations for the elimination or mitigation of vulnerabilities. We also have experience and certified personnel that utilize NIACAP and DITSCAP standards and methodology.

We utilize a standardized INFOSEC Assessment Methodology (IAM) that is endorsed by the National Security Agency (NSA) and complies with Presidential Decision Directive (PDD) 63. INFOSEC assessments comply with Federal Law that requires automated information systems operating at a security level of sensitive but unclassified (SBU) or above to be appropriately secured. Our assessments may provide system owners a level of confidence that their information is protected or may emphasize where additional security safeguards are necessary. Periodic IA by an independent party is a good security, engineering, and management practice and is a direct response to suspected threats and security incidents. Our IA may validate internal reviews and will provide a baseline for INFOSEC posture.

CEXEC will identify system information criticality, system configuration, INFOSEC posture and provide findings and recommendations. We utilize the three phased approach depicted below.

3 Phased Approach with Typical TimeLine		
Pre-Assessment	On-Site	Post-Assessment
Pre-Assessment Visit ➤ 2 Weeks Team Assignments and Coordination ➤ 2 – 4 Weeks	On-Site Visit ➤ 1 – 2 Weeks	Analysis and Report Generation ➤ 2 – 6 Weeks

In the **Pre-Assessment phase**, we will refine our customer needs and gain an understanding of the criticality of the customer's information. CEXEC will identify the pertinent systems and system boundaries, coordinate logistics with the customer and develop an assessment plan.

During the **On-Site phase**, CEXEC explores and confirms the information and conclusions made during the Pre-Assessment phase. We will gather and validate data by interviewing appropriate personnel, reviewing system documentation, and observing system demonstrations, and also perform and provide a preliminary analysis and feedback to the customer our findings.

In the **Post-Assessment phase**, CEXEC will complete the IA analysis and prepare, coordinate, and present a final report. Our comprehensive IT experience and certified INFOSEC Assessment Methodology (IAM) staff uniquely qualify us to perform this work in a standardized and industry proven manner. We can leverage our IT and security experience with Government, Military, and commercial organizations. The engineers who perform this work have certifications that include: CISSP, WatchGuard Systems Security Professional, Internet Security Systems products, MSCE, and CNE.