



Information Assurance Program

Ensuring Critical Security Capabilities through Comprehensive Engineering, Implementation, Operations, Analysis, and Research

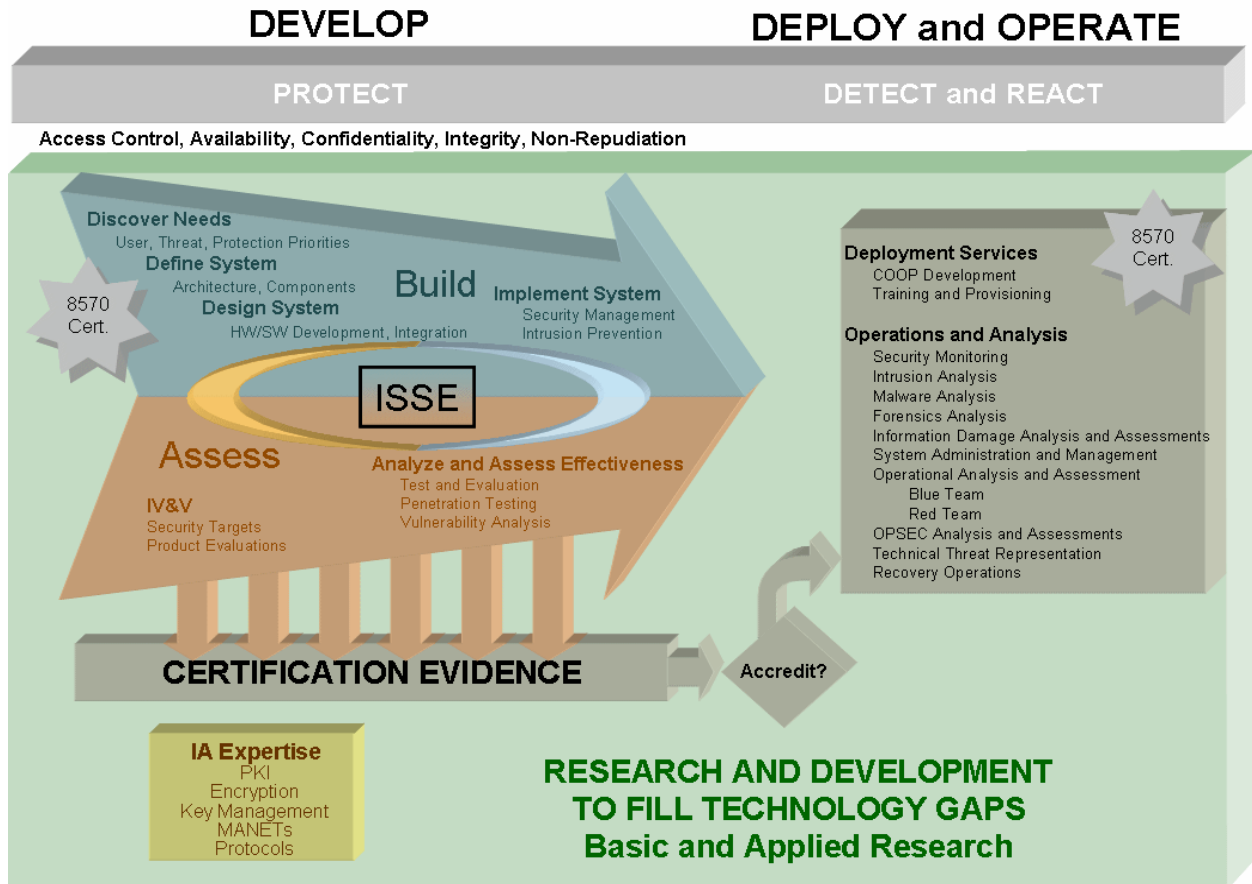
The SPARTA Approach

At SPARTA, we believe Information Assurance (IA) functions need to be built in, tested and maintained throughout lifecycle of a system. We bring certified IA expertise with a long history of successfully addressing hard-to-solve issues. Our lifecycle approach covers all aspects of IA from advanced research to system concept to, vulnerability analysis, security architecture, security controls design, development, security system integration, certification & accreditation and deployment; 24X7 analytical operations. We take advantage of the insight we gain through our advanced research and our previous solution oriented successes to bring state-of-the-art solutions, using **IA as an enabler** rather than a roadblock, to today's information sharing

problems. From a technical perspective we operate three distinct lines of business.

Information System Security Engineering

SPARTA has been an innovator and leader in the engineering of security into information systems for over three decades. Through our program support and long established relationships with the intelligence community, the Department of Defense, and commercial customers we have evolved into strong advocates for and definers of the practice of Information Systems Security Engineering (ISSE). SPARTA integrates ISSE as information Systems Engineering (SE) so that security is a functional requirement of the system. For maximum benefit our ISSEs are an integral part of the SE team. We place great emphasis on





Information Assurance Program

Ensuring critical security capabilities through comprehensive engineering, implementation, operations, analysis, and research

working with customers to understand which parts of their business or mission require information protection. We coordinate with customers at every step in the development to ensure Security concepts, architectures, and implementations reflect their information protection needs. Because of our domain experience in the building blocks of IA, we are uniquely positioned to integrate new systems and capabilities with existing security infrastructures. SPARTA and NSA defined the SE/ISSE process to include the activities of **Discover Needs, Define System, Design System, Implement System, and Assess Effectiveness**. The process is documented in NSA's Information Assurance Technical Framework (IATF), to which SPARTA made significant contributions. Artifacts of our approach provide certification evidence to support accreditation decisions. When using our process, accreditation is a smooth transition from development to operations. The key to our success is our unique, disciplined approach to security requirements throughout the system's lifecycle. Customers take advantage of our ISSE approach by either charging us with the responsibility to develop the system or component, or by acting as a trusted assessor of an ongoing development. In both cases our ISSE processes provide the foundation for customers to make sound security decisions.

Implementation, Operations, and Analysis

As an accreditation decision for the system nears, we prepare systems and organizations to implement and operate the system in the most secure way possible. Our implementation steps prepare the facility, administrators, and users to take maximum advantage of new system capabilities. Cornerstones of this phase involve training, provisioning, and continuity of operations planning (COOP). These preparations are augmented with active assurance operations such as **system administration, management (patches and upgrades), monitoring, and intrusion prevention and detection**. Our assessment services of BLUE TEAM testing (cooperative vulnerability scanning) and full spectrum Operational Security (OPSEC) assessments routinely examine and analyze the efficacy of the implemented defenses. As appropriate, we assume the role of an adversary (**RED TEAM**) to test the entire system (hardware, software, processes, procedures, and people) and its

response to unauthorized activities. RED TEAM testing identifies gaps in the system design, promotes user awareness, and provides opportunities to evolve and enhance security procedures. These testing services also facilitate periodic system re-accreditation. Inevitably, anomalies occur. SPARTA brings the analytical skills and services in the areas of **failure, intrusion, malware, and forensics analysis** to understand what is happening, what might happen, and what did happen. In the event of catastrophic occurrence, we bring the capability to restore operations quickly, introduce new security controls, if required, and update security certification documentation. Our broad set of operational security services keeps systems running effectively, and enables rapid and continuous post-fielding accreditation decisions.

Research

To respond to our customers continuous evolving information technology needs and choices, we at SPARTA leverage our experience in analyzing vulnerabilities of new and emerging IT solutions, and our experience in developing and operating systems to identify continuing security needs, and apply basic and

applied research to fill the hard technology gaps limiting high robustness system deployment and operation. A significant portion of our staff (>30%) hold advanced technical degrees relevant to addressing hard IA problems. We combine our broad IA domain expertise with the rigor of systems engineering, systems and software development, and test and evaluation to prototype technologies to address full spectrum IA requirements such as host system security, host intrusion prevention, network intrusion prevention, wireless intrusion prevention, network infrastructure security, malicious code defense, and provide timely solutions to current IA issues such as **worm quarantine, distributed denial of service attacks, Domain Name Service Security, high assurance operating systems, and object security**. Significant portions of our research are now cornerstones of best practice IA approaches around the world. Through our program support and long established relationships with the members of the IA R&D community we can take full advantage of emerging technologies to provide comprehensive IA solutions.