

Systems Engineering Disciplines

Risk Management
 Training Curriculum
 Professional Reference
 Requirements Management
 Web Tools

> Systems Security Engineering

Program Experience

Over 60 years combined experience performing systems security work on the following programs:

Defense Meteorological Satellite Program (DMSP)
 Air Force Satellite Control Network (AFSCN)
 Global Positioning System (GPS)
 National Reconnaissance Office (NRO)
 Space Operations
 Global Command & Control Systems (GCCS)
 Theater Battle Management Core Systems (TBMCS)
 Joint Tactical Ground Station (JTAGS)

About bd Systems

bd Systems is a woman-owned small business that provides engineering and information technology services for government and private industry. Based in Torrance, California, bd Systems has over 20 operating locations nationwide.

bd Systems, Inc.
 385 Van Ness Avenue, Suite 200
 P.O. Box 2707
 Torrance, CA 90509
 P 310.618.8798
 F: 310.782.5757

info@bdsys.com
 www.bdsys.com

Systems Security Engineering

bd Systems employs an experienced multi-discipline technical engineering team providing System Security Engineering (SSE) expertise for important government programs. Our SSE staff focuses on the protection of sensitive and classified information and the systems and networks that process and store that information. From design and acquisition through operations and sustainment, our personnel can assist in developing secure systems, help solve system security problems, guide analyses of operational systems, assist in the secure operation of systems and interface with the appropriate Government security representatives and other contractors to provide the best possible security support and expertise. Our understanding and demonstrated capabilities are summarized here.

- **Information Assurance (IA):** Our staff is experienced in the protection of systems, the information embedded in those systems and the assurance of information availability, integrity, confidentiality and accountability. IA also includes secure design support that provides detection and restoration capabilities. The SSE's stay abreast of new regulations such as the Defense Information Assurance Certification and Accreditation (C&A) Program (*DIACAP*) and support the legacy C&A process driven by the Defense Information Technology Security Certification and Accreditation Process (*DITSCAP*), and by AF requirements for Certificates of Net worthiness (CoN) and Certificates to Operate (CtO). Examples of security features that must be designed into systems include user identification and authentication, passwords, memory overwrite, access controls, and public key or certificate based encryption.
- **Emanations Security (EMSEC),** and its more well-known representation, *TEMPEST*, are short names given to the investigation, study, and control of compromising emanations associated with information systems. EMSEC is also the study and control of spurious electrical signals emitted by electrical equipment. We are experts in the definition, documentation and implementation of EMSEC requirements. We determine the need for TEMPEST testing on a case-by-case basis considering such factors as threat, other emanations and positive control zone measures and establish and maintain interfaces with users to resolve issues.
- **Anti-Tamper (AT)** is specifically intended to prevent and/or delay exploitation of critical technologies in weapon systems. Our staff use AT techniques as required depending on the technology being protected; examples include integrated circuit protective coatings, and hardware access denial systems.
- **Communications Security (COMSEC)** includes measures and controls taken to ensure authenticity of telecommunications and to deny unauthorized persons access to said material. Our staff support the development and integration of crypto systems into the AF system using National Security Agency endorsed measures and/or using NSA crypto systems. Crypto systems can also support computer security (*COMPUSEC*) functions.
- **Information Support Plan (ISP),** which was formerly known as C4ISP, is a requirement for IT systems and National Security System programs that interface with the DoD Non-Secure Internet Protocol Router Network (NIPRNet). Our engineers grandfather legacy C4ISP and develop ISP documentation to identify potential information support short fall in IT systems and National Security System programs. The ISP is required to obtain a Certificate of Net worthiness (CoN) and Certificate to Operate (CtO) for connection to Global Information Grid.
- **Secure Systems Integration:** We apply engineering and management principles to develop security objectives, requirements and implementation approaches; define and maintain programs that are designed for maximum security and survivability of a program throughout its life cycle; and ensure security functions are effectively integrated into the total program effort. Our experts analyze known threats against program protective measures to determine shortfalls/ vulnerabilities, maintain threat protection vulnerabilities assessments, define and document measures to address vulnerabilities and establish/maintain interface with users to resolve issues.
- **Physical, and Operations Security:** To maintain secure operational environments, our experts define and document physical and operations security requirements and implementation measures. Measures are designed to protect designated sensitive, high value and/or classified resources from unauthorized access, physical damage, theft, compromise or sabotage. We analyze operations to identify intelligence indicators that can be used to degrade or compromise the operation, then define and document OPSEC techniques to eliminate, minimize or control those indicators.