



# **502 Design Services**

***502 Design Services, Inc. High Assurance Security Engineering Professionals***

## ***Capability Overview***

502 Design Services is a small business concern providing the experience and capabilities to successfully address the current and future requirements for High Assurance Security design into new and legacy systems. 502 Design Services provides an unparalleled expertise to the DOD, IC and prime contractors. We strive to become leaders in the expanding field of communications and information security, including COMSEC/TRANSEC and Key Management technologies. Our experienced staff of subject matter experts has provided integration of critical technologies, equipment, and systems to the U.S. Government and prime contractors for secure communications. We continue to support the government agencies with security solutions that meet the demands of Next Generation Communication networks. 502 Design Services is well respected in the intelligence community, DOD and prime contractors. Our business model calls for the augmentation of government and prime contractor staff with our uniquely qualified staff of engineers.

502 Design Services consists of a High Assurance Security Engineering Subject Matter Experts (SME's) specializing in providing Security Engineering Services for NSA cryptographic solutions. The company has experienced engineers on staff that specialize in the design and product development of key management devices and End Cryptographic Units (ECUs) as well as the Cryptographic Modernization of legacy equipment. 502 Design Services consists of a well-rounded staff of engineers with extensive security design, development, and test and evaluation experience.

We have on staff Security Advocates who are uniquely qualified in the high assurance security area and are certified by the NSA. Our engineering staff have completed the NSA Certified Module Embedment (CME) accreditation process. The Security Advocates have excellent reputations within the NSA for their security expertise including development of security architectures, guidance of security designs, generation of security documentation, and the test and evaluation of security solutions.

The company also has system security engineers, one of which is a Security Advocate Candidate having successfully completed the Security Advocate training courses. The system security engineers have similar security expertise as the SAs specializing in the development of security architectures and generation of security documentation. 502 Design Services has cryptographic hardware design engineers experienced in high speed design, cryptographic key protection and algorithm development

502 Design Services uses a 50+ task high assurance security evaluation process to guide the High Assurance Security Solutions. The Security Advocates have lead Security Integrated Product Teams (IPTs) on several high assurance securities programs and have hosted Security Plan/Schedule presentations on a regular scheduled basis. The Security Advocates provide support and will lead

Security Technical Interchange Meetings, Security Preliminary Design Reviews, and Security Critical Design Reviews. The security team works closely with the prime contractor to ensure the data and documentation is complete and accurate for the reviews.

The company is well versed in the NSA Type 1 security certification process and embedded security solutions. Our Security Engineers are intimately familiar with the NSA security requirements defined in the Telecommunications Security Requirements Document (TSRD) and the Information Assurance Security Requirements Document (IASRD), which has recently replaced the Unified INFOSEC Criteria (UIC). Our Security Engineers assisted NSA with the tailoring process of the IASRD/UIC on current and past programs and completely understand each of these requirements insuring the proper allocation to the various program design elements. 502 Design Services has been involved with several Cryptographic Modernization (CM) programs and have provided guidance with algorithm selection for the protection of user data, cryptographic function and algorithm software, and NSA key material. 502 Design Services has a thorough understanding of NSA's algorithm selection and the Cryptographic Algorithm Configuration Management Board (CACMB) requirements. The Security Advocates also can provide guidance in the understanding of the interface to NSA's Electronic Key Management System (EKMS) and the newly emerging Key Management Infrastructure (KMI) from their unique experience in the development and certification of key management devices including the Really Simple Key Loader (RASKL), which is the replacement for the KYK-13.

502 Design Services understands that one of the most important documents of the Type 1 certification process is the Security Evaluation Document (SED). The purpose of this document is to provide information about the architectural design of an Information Assurance (IA) product and its intended detailed implementation throughout the development/design of the product. 502 Design Services: (1) identifies the Security Services provided by the product and defines the Security Architecture of the product including functional decomposition and mapping to the Security Services; (2) establishes the Security Boundaries including Cryptographic, INFOSEC, QUADRANT and TEMPEST; and (3) provides a compliance statement for each of the tailored IASRD/UIC requirements. Once the system security architecture and requirements have been baselined and accepted; 502 Design Services (4) provides the implementation details for each of the security critical functions used to provide the defined Security Services; (5) provides a Security Fail Safe Design and Analysis (FSDA) of the security critical design components; (6) provides an analysis of covert channels; and (7) provides an analysis of the anti-tamper design. The Security Advocates are well versed in the FSDA process and have generated several FSDAs working closely with NSA evaluators to insure that the Type 1 system/product being certified meets all FSDA requirements for the classification level of the information being protected. The Security Advocates have also provided guidance on several anti-tamper programs.

The company has a thorough understanding of Security Verification (SV) having prepared numerous SV Plans and Procedures, successfully conducted SV testing and generated SV Test Reports. The Security Advocates also have extensive experience with generating the Key Management Plan (KMP), the Final QUADRANT Report, and the production based INFOSEC Verification Test (IVT) Plan and Security Production Assurance Plans. The Security Advocates have also assisted NSA program personnel with the preparation of "The 16 Point" presentation required for the NSA Technical Review Board (TRB) and have participated in TRB meetings when requested. The Security Advocates will review and comment on all software security documentation.

502 Design Services has experience in developing security test equipment used for both cryptographic development and production module/unit testing.

The Security Advocates average over 35 years of engineering experience with a significant amount of that experience devoted to high assurance designs and evaluations. They have been involved with the designs of a variety of Department of Defense programs including KG-194 Trunk Encryption Device, Commander's Tactical Terminal (CTT), TIBS Interface Unit (TIU), CTT Receive Only (CTT/H-R), Versatile Intelligence Portable Receiver (VIPR), CTT-3 Channel, Joint Tactical Terminal (JTT) Senior, JTT-IBS, Airborne Integrated Terminal (AITG), KIV-19M Link Encryption Family (LEF), RASKL, Navy Cooperative Engagement Capability (CEC), and MUOS CAD phase. The MUOS CAD Phase provided the Security Advocates the opportunity to develop an integrated process for the system level NSA High Assurance certification and the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) accreditation for both the space and ground segments. The Security Advocates have extensive hands-on experience with over 30 different cryptographic equipment and embeddable modules including: KG-84, KIV-7, ANDVT, KGV-11 (used in the CEC USG-1 system), KGR-96, KG-94/194, TACLANE, KI-54, CTIC, CDH (used in the CEC USG-2/3 systems), RAILMAN, INDICTOR, HAYFIELD, CORNFIELD, SIERRA II, RAVEN ASIC, and AIM.

The Systems Security Engineers average over 25 years of engineering experience in the areas of high assurance design, certification and accreditation of INFOSEC products. They have an in-depth knowledge of NSA certification per the Information Assurance Security Requirements Document (IASRD) and Unified INFOSEC Criteria as well as key management, TEMPEST, QUADRANT and computer security. Their experience includes architecture definition and system engineering of secure communications systems and products for military applications. The Systems Security Engineer's experience also includes hardware and software design of cryptographic modules that utilize embedded cryptographic devices, FPGAs, and microprocessors.

The Cryptographic Hardware Design Engineers are uniquely qualified and average over 30 years of detailed design experience in several system disciplines. They are well versed in security related circuitry as well as being knowledgeable in advanced PWB (Printed Wiring Board) design techniques and FPGA implementation of algorithms and system monitoring circuitry. They are extremely proficient in the use of the NSA ARL (Algorithm Research Library) Algorithm simulation tool. 502 Design Services has the FPGA design tools and the expertise to produce a reliable and secure Single Chip Crypto application. Our approach uses a Xilinx Spartan 6 series device with the NSA approved design segregation. Both primary and redundant encryption/decryption circuits are implemented in a single device. All essential security features (e.g. key protection, tamper detection processing, etc.) are integrated into the FPGA design. Multiple algorithms can be supported by this single chip approach thus providing a flexible, low-power, low parts count, robust design platform. This platform can be easily tailored to meet the end-product requirements. The Single Chip Crypto approach gives the end-product producer a state-of-the-art, leading edge, reconfigurable and long-life design.

502 Design Services provides systems and software engineers to work with our clients from the product conception stage, through product realization, development, and deployment. Our rich background in Information Security helps clients capitalize on their current investments, while avoiding some of the pitfalls associated with new development or integration work.

Because we're involved with development of next generation communication networks our systems/software engineers provide technical expertise in developing architectural alternatives that fit our customers overall strategic goals. Once architectures are defined, we can:

- Assist with the development of system requirements
- Identify systems integration options
- Define the custom engineering to integrate hardware and software into complex systems
- Provide System Level integration services
- Provide an experienced software engineering team for application development and software module upgrades
- Provide expertise in deploying off-the-shelf technology for instant benefits without long and costly deployment cycles
- “Big Picture” capabilities ensure that your next generation communication network integrates smoothly with existing legacy systems

502 Design Services can partner and support Business Development and Translation of End-User INFOSEC Requirements. The company provides Information Assurance Authoring in support of any Proposal. Our staff provides extreme comfort in working with clients and delivering IA proposals and presentations. Our NSA Security Advocates on staff makes it a discriminator on proposal efforts and is considered a Key Proposal Staff.

Contact information:

502 Design Services, Inc.  
Oldsmar, FL 34677  
Voice: 813.852.9809  
FAX: 813.435.2201  
Web: [www.502design.com](http://www.502design.com)  
POC: Frank Tortorelli  
Email [ftortorelli@502design.com](mailto:ftortorelli@502design.com)  
Cell 727.858.7245