



System Inventory

We provide Information Assurance Engineering support to the Customer's Applications Engineering Division for implementation at an Enterprise level. Our IA Engineers work with each division's Project Team to ensure their projects successfully complete the security-related CIO Project Management Process control gates as well as managing the systems within the Enterprise Architecture, and utilizing configuration management to ensure project success.

Risk Management and Threat Analysis

We provide agency-specific or National level risk and vulnerability assessments. Our team also provides risk and vulnerability assessments following the NIST SP 800-26, NIST SP 800-30, NIST SP 800-53, and Critical Infrastructure Protection (CIP) guidelines. We have developed comprehensive security control assessments for desktops, servers, embedded devices, and mainframes in accordance with agency-wide policies. In addition, Our security professionals also provide Blackbox and/or Whitebox penetration testing. We also provide consultation on penetration testing techniques along with policy training.

Certification and Accreditation

Our highly trained engineers and security professionals are well trained and experienced in all certification and accreditation standards to include NIST, DCID 6/3, DITSCAP, and commercial requirements. We are also providing services for meeting the FISMA and Independent Verification and Validation (IV&V) requirements. Our security professionals assist and develop System Security Plans (SSP) and other associated documentation. In addition, our professionals work through the entire process of establishing COOP and Disaster recovery plans. From the development, implementation, testing and training we can ensure that our customer meets all federal requirements. We also ensure that if for any reason the organization finds a need to utilize the COOP or disaster recovery plan all information will be promptly and accurately available.

Security Monitoring and Incident Response

Compumatics Information Assurance Professionals provide security engineering support to the certification and accreditation process. Functions include gathering evidence on systems, analysis, and evaluation of threats and vulnerabilities. In addition, they provide functional support for the mitigation of vulnerabilities and system threats, technical guidance and support for “best practice” approaches towards threat and vulnerability mitigation, functional support for the creation and maintenance of associated security documentation packages and balance operational policy and information assurance requirements into effective and logical solutions. Some of our services include: In-depth security analysis and risk assessments; security hardening of Operating Systems; multi-vendor firewall implementation and designs; protocol and ports reviews; compliance with multiple x.500/509 directory structures; Intrusion Detection Systems; router/switch access controls; and Enterprise Systems Management.

Regulatory Review and Guidance

Responsible for assisting in the control and management of information security and its implementation across the business. Knowledge of risk assessment elements of policies, standards, frameworks and processes to effectively control the risk associated with the compromise, loss or damage of the Groups information and/or the technology used to store and process information.

General and Specialized Awareness Training

Our work in this area was done in compliance with approved DoD and Intelligence Community standard communications, specialized security requirements, data and other defined technical specifications, standards and architectures. Tasks within this area include but are not limited to planning, controlling, overseeing and conducting successful installation, development and/or conduct of initial training, conversion and acceptance testing of migration applications.

Partner Liaison and Technical Representation

Compumatics Group provides Sr. Information Systems Security (INFOSEC) Engineering support. Our INFOSEC Engineers ensure supported projects roll properly coordinated with Security Center/Information Security Center. This support begins when the systems or application(s) is in the planning phases all the way through the project lifecycle. We provide security-related recommendations to the projects during requirements gathering and coordinates with the ISC to ensure the applications and systems go through the proper C&A process. We review the projects’ documentation for completeness based on DCID 6/3, FISMA (and other Agency specific) requirements and the C&A Tier assigned by the Information System Security Manager (ISSM).

Lifecycle Support of Security Technologies

Compumatics Group provides INFOSEC Engineering support to a Multi Level Security (MLS) system accredited at PL4. This single workstation, single NIC card, single wire solution has revolutionized the MLS community. Our INFOSEC Engineer also serves as the Cross Domain Federated Search security architect. This effort involves all of the previously stated efforts plus multi-agency coordination at a National level. C&A documentation reviews involve technical and procedural security compliance to include:

In-depth security analysis and risk assessments; security hardening of Operating Systems; multi-vendor firewall implementation and designs; protocol and ports reviews; compliance with multiple x.500/509 directory structures; Intrusion Detection Systems; router/switch access controls; and Enterprise Systems Management.

Technical, Operational and Logistical Support for Global, Regional and Local Security Management

Compumatics Group provides comprehensive System Integration, Systems Engineering Project Management support solutions to our customer on this effort. Most notably our team plans, implements, tests, and documents local and enterprise-wide solutions and subsystems using internally created and/or off the shelf products. We analyze and identify all or part of a company's existing or new peripheral, network, and telecommunications systems requirements, taking into consideration their special technology, personnel, and security needs. We establish functional and technical specifications and standards, solve hardware/software interface problems, define input/output parameters, and ensure integration of their entire system and subsystems.

Technical Security Studies, Analysis, Tests, and Reviews

Compumatics Group personnel provide technical planning, verification and validation, cost and risk analysis, and overall system effectiveness. Analyses are performed at all levels of systems including concept, design, fabrication, test, installation, operation, maintenance, and disposal. Our personnel ensure the logical and systematic conversion of a customer and/or products requirements. Our personnel perform functional analysis, timeline analysis, detail trade studies, requirements allocation, and interface definition studies to translate our customer's requirements into hardware and software applications. Implementing quality standards that establish procedures for monitoring cost, schedule, and performance across the system are a couple of ways that we assist our customers in determining future budgetary concerns.

Program Management

As the customer's fiduciary, Compumatics Group personnel analyze business and technical processes to formulate and develop new and modified business information processing systems, such as production and work flow systems, financial tracking systems, and human resources systems. In coordination with our customer, our Program and Project Managers represent the customer to define requirements and business cases for the technology developments. With this oversight, many of the customers rely on our experience and thorough understanding of Requirements Management to define specific, rather than generic requirements. Further, we coordinate with external business and technology teams to ascertain system requirements, such as program functions, output requirements, input data acquisition, and system techniques and controls. Our personnel perform data analysis of data in a centralized repository which assists our customers with monitoring support of data. In addition, several of our Program Managers are PMP certified and some are certified as Lean Six Sigma Blackbelts.

Compumatics Group (CG) Information Assurance Professionals provide security engineering support to the certification and accreditation process. Functions include

gathering evidence on systems, analysis, and evaluation of threats and vulnerabilities. In addition, they provide functional support for the mitigation of vulnerabilities and system threats, technical guidance and support for “best practice” approaches towards threat and vulnerability mitigation, functional support for the creation and maintenance of associated security documentation packages and balance operational policy and information assurance requirements into effective and logical solutions.

Responsible for assisting in the control and management of information security and its implementation across the business. Knowledge of risk assessment elements of policies, standards, frameworks and processes to effectively control the risk associated with the compromise, loss or damage of the Groups information and/or the technology used to store and process information.

Provide Certification and Accreditation (C&A) support for federal agencies and DoD clients throughout the system development life cycle. Liaise with the client on a one-on-one basis and during team meetings on the completion of C&A documents.

Some examples of our experience in the area of Cross Domain Solutions and Multi-Level Security:

"CG provides the following support to IC Cross Domain Solutions (CDS)/ Multi Level Security (MLS) Systems, as exemplified:

1. Sr. Network Engineer for a Cross Domain Search effort in support of NCTC.
2. Sr. INFOSEC Engineer with oversight over all of CIA's Cross Domain Solutions.
3. Represented the “Agency” at Unified (DoD/IC Level) Cross Domain Management Office.
4. Configuration Manager for Multi Level Security (MLS) project in support of the “Agency”. MLS was to be incorporated across the entire Agency.
5. Senior PM served as Acting Deputy PM for Agency's Controlled Interface Program Office.