Full System Security

Use of U.S. DoD imagery does not imply or constitute DoD endorsement.

Information System Security is an integral part of protecting critical data.

Our Services Include:

- Monitor and implement Information Assurance Vulnerability Alerts (IAVA)
- Apply DISA Security Technical Implementation Guides (STIGS)
- Ensure compliance with DoD standards and requirements for ports, protocols and services
- Ensure that technical and physical security controls and countermeasures are applied
- Monitor and implement anti-virus and software patch updates
- Perform a full-system security scan, including a network discovery scan to evaluate network traffic and analyze port activity

L-3 Information System Security Services - L-3 I(S)^3
L3Cybersecurity@L-3com.com 856-338-4777

L-3 Communication Systems-East

L-3 Information System Security Services L-3 I(S)^3

- Cybersecurity
- System Security
- Life-Cycle Security
- Risk Identification and Analysis
- Cybersecurity Training
- Certification and Accreditation
- Information Assurance Vulnerability Management
- Software Assurance

L-3 Information System Security Services L-3 I(S)^3

Cybersecurity

Cybersecurity is the foundation of secure Information Systems and is essential to our national security. L-3 I(S)^3 cybersecurity engineers have a comprehensive, understanding of implementing countermeasures, including technical cybersecurity controls, physical security and encryption methods. Our team has years of experience working with all branches of the Department of Defense (DoD) to ensure the confidentiality, integrity, availability, authentication, and non-repudiation of government data, while supporting our customers' need for a secure and functional system. L-3 I(S)^3 cybersecurity engineers are DoD Instruction 8570-approved, Defense Information Systems Agency (DISA) Assured Compliance Assessment Solution (ACAS)-certified and maintain proper certifications for the roles they support.

System Security

L-3 I(S)^3 can assist in selecting approved hardware/software, applying security by hardening systems and networks before development, test and evaluation begins. We ensure that IT systems comply with cybersecurity and National Institute of Standards and Technology (NIST) Risk Management Framework controls, Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG), and assist in creating policies, processes and plans. We can harden systems on-site, and provide guidance on continuously maintaining your security requirements.

Life-Cycle Security

L-3 I(S)^3 uses a balanced approach of building security into system design, engineering processes and secure coding standards for the life cycle of a program, from the beginning stages of customer requirements, all the way through building, testing and deployment. We understand the different approaches needed for building security into a new-start program and those needed for a legacy program to ensure secure and functional systems. We can provide support at any stage.

Risk Identification and Analysis

We conduct threat and vulnerability assessments, using a full set of DoD-approved cybersecurity assessment and scanning tools, to analyze systems and determine effective countermeasures. This minimizes risk and ensures information systems are operational and secure. L-3 I(S)^3 identifies cybersecurity threats and implements the appropriate controls by enabling security features. A risk analysis report is generated that provides detail of the overall security posture, status of the system and residual risks.

Certification and Accreditation

We have extensive experience with Certification and

Accreditation (C&A) processes by performing comprehensive evaluations of technical and non-technical features of an information system in its intended environment. We evaluate standard general purpose systems, enclave

systems, afloat systems, and complicated communications systems all resulting in successful accreditations.

Our team creates system accreditation packages, including all supporting documentation, and assist with submitting the completed package to the accreditation office. L-3 I(S)^3 works closely with the Designated Approving Authority from all branches of the DoD. Our team can assist with re-accreditations by scanning all system components, resulting in a Conformance Testing Report.

Information Assurance Vulnerability Management

L-3 I(S)^3 complies with the DoD Plan of Action and Milestone (POA&M), to ensure that reported vulnerabilities are mitigated in a timely manner. Cybersecurity mitigation strategies include operating system updates and service packs, application software updates, and changes to operating procedures. Timely dissemination of critical vulnerability information is vital. Security advisories are communicated to L-3 I(S)^3 through multiple channels based on the program requirements, DoD governing policies, and the regulations governing the type of data that will be processed, including classification and designation.

Software Assurance

Software Assurance builds confidence while increasing consistency, reliability, and security of applications by building software resilient to known weaknesses and vulnerabilities. L-3 I(S)^3 assists software engineers on applying

secure coding standards to ensure that the software is consistent with its allocated requirements, while identifying and mitigating any deficiencies in the software. These practices provide objective evidence throughout the development effort that the software is being developed according to plan, meets its requirements, and operates safely and securely.

Cybersecurity Training

L-3 I(S)^3 delivers instructor-led, up-to-date training on our premises and at customer sites by sharing concepts, principles, and hands-on training on cybersecurity scanning tools to enhance confidentiality, integrity and availability of DoD information, information systems, and networks.

Use of U.S. DoD imagery does not imply or constitute DoD endorsement.