

Information Assurance (IA)



Securing the Privacy of your Data

When transmitting sensitive information, insist on the assurance that your communications network has not been compromised by an intruder. TCS' Information Assurance (IA) suite of services manages the risk associated with data transmission, and provides the peace of mind needed when sending and receiving critical communications.

TeleCommunication Systems, Inc. (TCS) Information Assurance services provide Information Systems Security Lifecycle Management; Vulnerability Assessment and Evaluation; and Certification & Accreditation Service for DIACAP or NIACAP. Together these services ensure that all communication transmission modes in systems and enterprises are able to maintain operational integrity.

TCS IA services are superior at providing the technical and administrative controls designed to enforce confidentiality, integrity, and availability of data on information systems. TCS' IA services offer more than just security; they fill the gap between information operations and physical security, encompassing issues relating to privacy, regulatory compliance, audits, business continuity, and disaster recovery.

Key Features

Information Systems Security Lifecycle Management (ISSLM)

TCS manages systems through the entire lifecycle with our proven methodology using the following techniques to provide Information Assurance support:

- ISSE (Information Systems Security Engineering)
- Systems Implementation (TCS III Step Implementation Process)
- Certification and Accreditation Activities for DIACAP/NIACAP support
- SDIM (Security Documentation Implementation and Maintenance Process)
 - Configuration Control management
 - Information Assurance Vulnerability Alert Management (IAVAM)
 - Training
- Systems Baselines
- Installation, repairs, or Backups
- Information Systems Security Lifecycle Management supports any integrated system, such as the TCS SwiftLink® deployable communications suite, and is a useful tool in applying a sound information assurance practice to systems provided by other vendors.

Get started Now

For more information, call 1.888.728.8797 or e-mail sales@telecomsys.com. Learn about TCS' complete line of products and services at www.telecomsys.com.

Your Established Partner

TeleCommunication Systems, Inc. (TCS) (NASDAQ: TSYS) is a world leader in high availability and secure mobile communication technology. TCS infrastructure forms the foundation for market leading solutions in E9-1-1, text messaging, commercial location, and deployable wireless communications. TCS is at the forefront of new mobile cloud computing services providing wireless applications for navigation, hyper-local search, asset tracking, social applications, and telematics. Millions of consumers around the world use TCS wireless apps as a fundamental part of their daily lives. Federal government agencies depend on TCS' cyber security expertise, professional services, and highly secure deployable satellite solutions for mission-critical communications. Headquartered in Annapolis, MD, TCS maintains technical, service and sales offices around the world. To learn more about emerging and innovative wireless technologies, visit www.telecomsys.com.

TeleCommunication Systems, Inc.
275 West Street
Annapolis, MD 21401 USA
Toll Free: 1.888.728.8797
Outside US: +1.410.263.7616
www.telecomsys.com

Enabling Convergent Technologies® is a registered trademark of TCS. All other trademarks are the property of their respective companies. Information subject to change without notice. | NasdaqGM: TSYS | 110712



Vulnerability Assessment

The TCS Vulnerability Assessment Team (TVAT) provides Information Security (INFOSEC) Assessments, INFOSEC Evaluations, Penetration Testing, and/or Remediation through processes derived directly from the National Security Agency's Information Assessment Methodology/ Information Evaluation Methodology (IAM/ IEM) guidance. Through this multi-level process, TCS examines an organization's security posture and provides solutions to address deficiencies.

- Level 1: Assessment
 - A high level review of the INFOSEC posture of any organization
 - Conduct Information / Mission Critically Analysis
 - Review of policies, procedures, information systems and the network architecture
 - No vulnerability scanning or testing tools are used at this level
- Level 2: Evaluation
 - Based on completed Assessment, the Evaluation validates the findings of the Assessment, and the organizations policies and procedures
 - Diagnostic tools, scanners, and light penetration testing are used
- Level 3: Penetration Testing / Red Teaming
 - TVAT will use simulated attacks for identified vulnerabilities according to the ROE (Rules of Engagement) for the organization. These methods can be conducted from outside or inside the organization's perimeter
 - Heavy penetration testing is conducted by exploring avenues of attack to include logical, physical, and social

- Level 4: Remediation
 - TCS provides remediation and training for vulnerabilities found through any stages of the Assessment/Evaluation

Certification & Accreditation (C&A) Services

C&A Services are provided by TCS for DIACAP and NIACAP to enable Federal Government Agencies such as the Department of Defense to meet FISMA (Federal Information Security Management Act) Requirements. Our process also aids in the transition to provide support throughout all DIACAP/NIACAP phases. Examples of the DIACAP activities support by TCS include:

- Phase I: Initiate and Plan IA C&A
 - Systems Identification Profile (SIP)
 - Assign IA Controls through ISSE
- Phase II: Implement and Validate Assigned IA Controls
 - Validate IA Controls through ST&E
 - Execute the DIACAP Implementation Plan (DIP)
 - IT Security Plan of Action & Milestones (POA&M)
 - Prepare (POA&M)
 - Compile Validation or results in DIACAP Scorecard
- Phase III: Make Certification Determination and Accreditation Decision
- Phase IV: Maintain Authorization to Operate and Conduct Reviews
 - Annual DIACAP scorecard
 - Configuration Control Management
 - Maintain the Systems Security Posture
 - Periodic Reviews and Scans performed on a quarterly basis
- Phase V: Decommission