

**W**hen 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.

Information Assurance (IA) 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.

## Information Assurance: Securing the Privacy of your Data

TCS Information Assurance services are superior at providing the technical and administrative controls designed to enforce confidentiality, integrity, and availability of data on information systems. TCS' Information Assurance 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.

## 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



- IAVAM (Information Assurance Vulnerability Alert Management)
- 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.

## Vulnerability Assessment and Evaluation

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 Criticality 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 a 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 stage of the Assessment / Evaluation

## Certification & Accreditation 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 from DITSCAP to DIACAP. TCS has the ability to provide support throughout all DIACAP/ NIACAP phases. Examples of the DIACAP activities supported 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 and Milestones
  - Prepare the Plan of Action & Milestones (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

## Your Established Partner

TCS is a leading provider of software and solutions to government customers requiring high reliability and security. TCS has been providing premier IT and wireless communications solutions to the U.S. Government since 1987. SwiftLink is a branded TCS family of products and services that are proven through use by U.S. government agencies, including the Department of State, Department of Defense, and Department of Homeland Security.

## Get Started Now

For additional information about TCS Information Assurance call 1.800.307.9489 or e-mail us at [SwiftLink@telecomsys.com](mailto:SwiftLink@telecomsys.com). Learn more about TCS' complete line of products and services at [www.telecomsys.com](http://www.telecomsys.com).



TCS • 275 West Street, Annapolis, MD 21401 USA • Toll Free: 1.800.307.9489 • Outside US: +1.410.263.7616 • [www.telecomsys.com](http://www.telecomsys.com)

Copyright © 2009 TeleCommunication Systems, Inc. (TCS). All rights reserved. Enabling Convergent Technologies® and SwiftLink® are registered trademarks of TCS. All other trademarks are the property of their respective companies. Information subject to change without notice. | NasdaqGM: TSYS | 071509