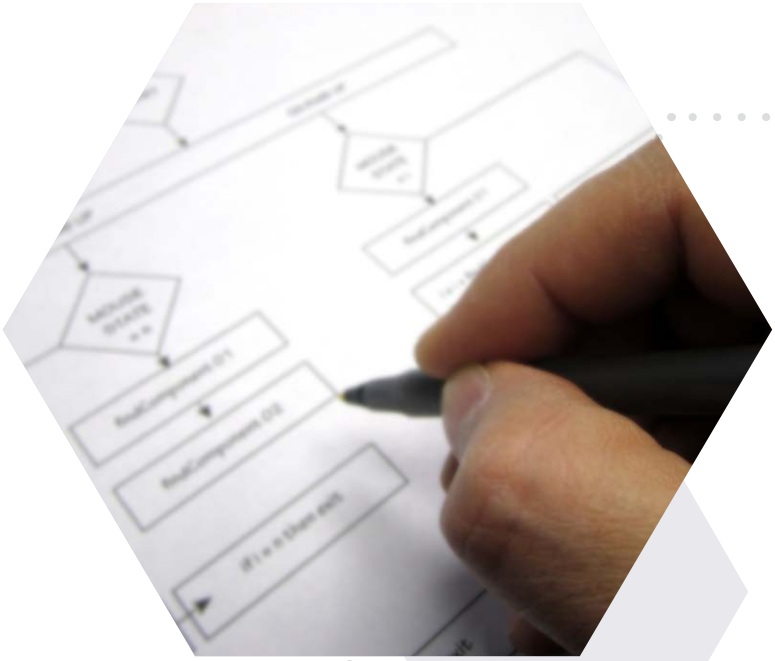
Application Software Assurance Services

- Protect your investment in software development and procurement
- Fix flaws and vulnerabilities before they become an expensive problem
- Strengthen your cybersecurity posture at the code level

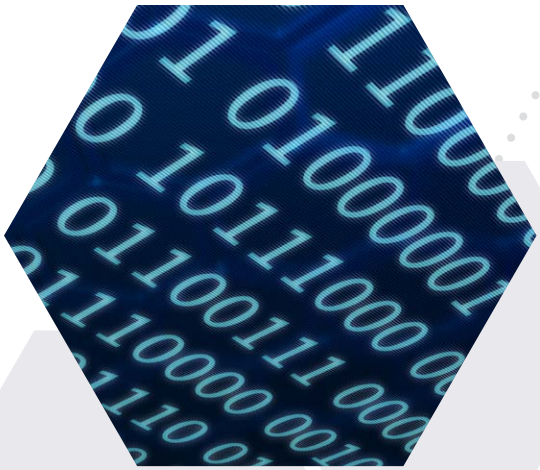
The first line of your cyber defense is software assurance.



Today's software and applications often contain flaws and errors that can be exploited by attackers to compromise the software's security and performance. It's estimated that up to 90 percent of reported IT security incidents result from defects in the design, architecture, or insecure coding practices of software.

The resulting vulnerabilities can be exploited through a variety of attack vectors depending on the specific type of application in question. From desktop to server applications, Web applications, and even embedded applications, each have their own set of attack vectors.

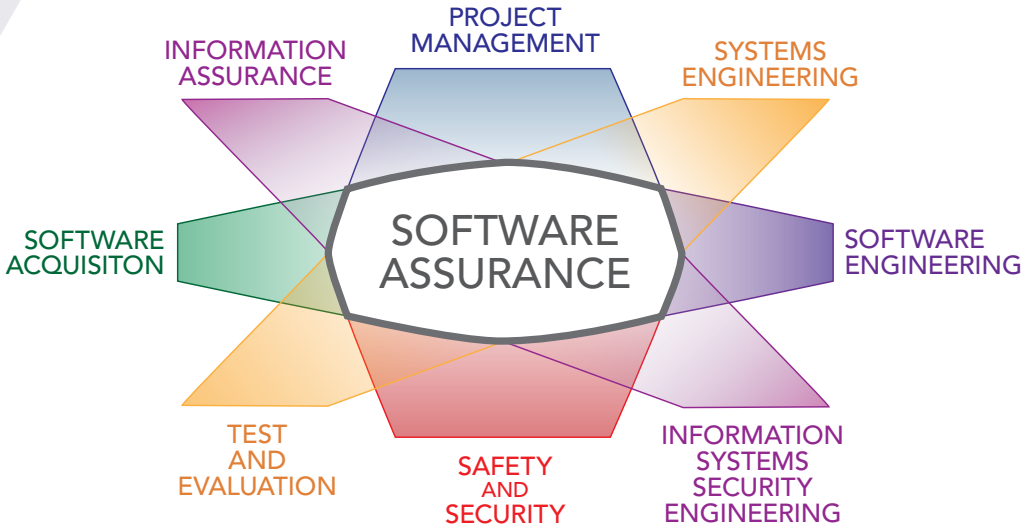
Software that is not built using secure coding practices introduces significant risks to the organization deploying and/or using that software. The first, and often last, line of defense for applications lies in the code itself.



Telos: Helping assure the security of your software and applications.

Telos Corporation is a leading provider of services, solutions and training that make security an essential element of your software development and procurement processes. Our experience extends across a variety of environments, including defense and federal agencies, all branches of the armed forces, and major commercial enterprises.

Our corps of software assurance personnel provides the foundation for secure, vulnerability-free applications. We apply a rigorous yet flexible regimen of processes for testing and validating your existing software and for assuring the secure production and operation of new software throughout the development and acquisition lifecycles.



Vulnerabilities make software assurance essential.

One of the key reasons Telos software assurance services are so essential is because all applications are potentially vulnerable, regardless of any defensive measures that may be in place. For example, Web applications cannot be 100% protected by perimeter defense mechanisms such as network firewalls, intrusion prevention systems (IPS), or even Web application firewalls (WAFs).

Once an application is deployed, it becomes a potential target. If an application is remotely accessible, such as a Web application, the potential for exploitation increases dramatically. Which means software needs to be built secure from the start in order to protect IT infrastructure and to reduce overall risk from cyber attacks. Telos helps ensure your development practices will result in sound, secure applications.

Software development lifecycles (SDLC) with security built in.

Time-to-market deadlines and the pressure to deploy applications quickly mean that security is often overlooked during software development and acquisition. The resulting flaws and vulnerabilities can lead to disastrous results and are costly to fix after-the-fact.

Telos helps you reduce risk and save time and money by ensuring that security measures are included in each phase of the software development lifecycle (SDLC). These measures include security requirements development, threat modeling, design and code review, security testing, penetration testing, training, documentation, and ongoing security enforcement during and after deployment.

WHY TELOS FOR SOFTWARE AND APPLICATION ASSURANCE?

- Telos co-established the ASACoE with the Air Force in 2007 – the first and only such organization in the DoD
- Telos has the experience and expertise necessary to secure your current and future applications
- Telos has developed best practices and repeatable processes that can be easily adapted to any development environment or organization
- Telos is a proven leader in SwA efforts and fully understands the wide range of obstacles that must be overcome for your organization to develop secure applications
- Telos maintains relationships with industry leading SwA tool vendors that can be leveraged to provide you with best-of-breed tools for your environment
- Telos was instrumental in the ASACoE being nominated for the 2010 Air Force Chief of Staff Awards for program excellence

Use of established SwA models and frameworks.

With Telos, you benefit from proven approaches to software assurance through our use of established software security models and frameworks such as the OWASP Open SAMM, CLASP, BSIMM, Capability Maturity Model Integration (CMMI), and others. These frameworks provide a consistent and repeatable series of activities that ensure the integrity, security, and reliability of software and applications during their development or acquisition and throughout their lifecycle.

Use of automated tools for speed and efficiency.

Human insights and manual steps in software assurance can be effectively complemented by tools that streamline and automate tasks during development, testing, and operation. Telos personnel deploy and provide training in the use of tool suites for application security and penetration testing, source code review, database scanning, bug tracking, and others, tailored to your particular technology environment and likely cyber attack scenarios. Reports generated from these tools also provide insights for auditors and senior management.

BSIMM Software Security Framework (SSF)			
Governance	Intelligence	SSDL Touchpoints	Deployment
Strategy and Metrics	Attack Models	Architecture Analysis	Penetrations Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

Telos software security experts apply the leading SwA models and frameworks in accordance with the customer's requirements, including the BSIMM Software Security Framework (shown above), the OWASP Software Assurance Maturity Model (SAMM), SEI's Capability Maturity Model Integration (CMMI), and others. *(BSIMM SSF is licensed under the Creative Commons Attribution-Share Alike 3.0 License. www.bsimm.com | www.creativecommons.org/licenses/by-sa/3.0)*

TELOS IN ACTION / Application Software Assurance Center of Excellence

The U.S. Air Force asked Telos to establish the Application Software Assurance Center of Excellence (ASACoE) at Maxwell AFB-Gunter Annex in Montgomery, Alabama.

The Telos-led contractor team provides tools, training and services to assist the center in establishing application security best practices Air Force-wide, fostering security throughout the software development and maintenance life cycles, and identifying and mitigating existing vulnerabilities.

The center has conducted software assurance assessments on over 1,000 applications, discovering and mitigating numerous exploitable vulnerabilities. In recognition of the advances made by the center in securing Air Force applications, the ASACoE was selected to represent AFMC for the 2010 Air Force Chief of Staff Team Excellence Award.

TELOS IN ACTION

Security Assertion Certifier for Air Force's STAX-based Applications

The clouds have been a familiar operating environment for the United States Air Force for more than six decades. Today, as Air Force computing enters the cloud, the service is taking measures to assure the security of their cloud-based applications.

The Air Force has named the Application Software Assurance Center of Excellence (ASACoE) the security assertion certifier for Air Force applications and services hosted in the Secure Technology Application eXecution (STAX) environment.

STAX is a cloud capability offered by Defense Information Systems Agency (DISA) for hosting Java and Microsoft .NET Web services for the Department of Defense. STAX provides development, test, and production environments for computing, storage, network infrastructure, and software from a secure facility and under a single pricing model.

As the security assertion certifier, the Telos-led ASACoE team will apply its stringent software assurance assessment processes to the STAX environment, ensuring the development and implementation of SwA best practices for applications moving to or being developed in STAX.

Telos Application Software Assurance Services include:

- Standards and policies development
- Security architecture reviews
- Coding best practices
- Source code analysis
- Threat modeling
- Vulnerability and penetration testing
- Documentation of best practices
- Application shielding
- Database monitoring
- Remediation of legacy systems
- Implementation services
- Post-implementation maintenance
- Training and education
- Regulatory compliance

Start taking steps now to protect your critical operations.

The security of your application is critical to the effective operation of your organization. Let Telos assure the integrity, security, and reliability of the software you rely on for mission success.

Telos®

Contact Telos for More Information

Telos Corporation | 19886 Ashburn Road, Ashburn, VA 20147-2358 | 1.800.70.TELOS | 1.800.708.3567 | Fax 703.724.3865 | www.telos.com