

# Comprehensive Security Assessments (CSA)

---

## Intro

In order to protect your computer environment it is critical to periodically survey the architecture, collect, research and analyze any vulnerabilities and develop mitigation strategies. With the sophistication of security attacks and the number of “black hat” hackers increasing, a strong network security plan is crucial. Security is an ongoing process, the purpose of which is to ensure the continuity of the network and the systems connected to it. WareOneEarth’s Comprehensive Security Assessments can be an integral part of your dynamic security process.

## WCI’s Extensive Experience

- Security design and configuration
- Identification and authentication
- Enclave and computing environment
- Enclave boundary defense
- Physical and environmental
- Personnel
- Continuity
- Vulnerability and incident management
- Site-specific requirements

## Advantages of a CSA by WCI

The WCI CSA team is comprised of individuals who think like hackers, but act like professionals. The WCI CSA team understands the concept of acceptable risks in order to minimize degraded operations, and can offer ways to circumvent any security holes through the use of other means approved by the customer. The CSA is a formal evaluation of the site for information, information systems, and communications systems security, as well as increasing the site awareness of physical, administrative, and personnel security. The WCI CSA team makes it very clear they are there to HELP the site. WCI CSA team members work closely with the customer to review and explain each finding giving the client a first hand look at the respective strengths and weaknesses of the existing security posture. Additional advantages of a CSA include:

- Provides an independent, objective view of the site security posture.
- Heightens site security personnel awareness of current security issues.
- Provides an opportunity for external validation of site security documentation:
  1. Current network diagrams showing current network configurations and hardware
  2. Memorandums of Agreement
  3. Site accreditations
  4. SSAA’s, standard operating procedures, contingency plans, risk assessments, etc.

## WCI's CSA Methodology Includes

- Physical Inspection
- Examination of Documentation
- Personnel Interviews
- Technical Testing
- External Scans
- Diagnostic Scripts (CSA UNIX and Windows Scripts)
- Ad Hoc Testing

## CSA Tools

The WCI CSA team approaches each site with the understanding that each network is unique and has different requirements. After a review of the site's architecture and mission the WCI CSA team will use the most appropriate tools to collect and analyze system and network vulnerabilities. Some of the tools used are:

- ISS and Nessus
- NMAP
- Password Crackers
- Custom system configuration scripts for Unix (AIX, Solaris, IRIX, HPUX, and Linux variants)
- Custom system configuration scripts for Windows (98, ME, 2000, XP, 2003)
- Ad-hoc Testing

## CSA Safeguards

Scan results and script issues are verified through vulnerability testing, analysis of OS versions and patch levels, and thorough checks of OS and common network application configurations. The assessment scripts are information gathering tools only, and make no changes to assessed systems other writing output results (And these can be redirected if necessary). All scripts and scan configurations are thoroughly tested prior to deployment on a CSA.

WCI CSA team scanning systems are accredited and re-loaded clean for each assessment. At the site's discretion, scanning system results can be purged prior to the CSA team's departure. If arrangements are made in advance, the hard drives can be wiped and left with the site.

## Training and Awareness

Security is an ongoing process rather than a static event. WCI knows that one of the most effective methods for addressing security is through training the on-site staff. With that in mind the WCI CSA Team encourages participation by site personnel during system and network assessments and results analysis. WCI CSA teams can also conduct onsite training sessions with specific security administrative staff on their own equipment.

## Our Contracts:

Government Agencies may use the following Contract Vehicles to do business with WCI:

- GSA IT Schedule GS-35F-0076R
- SPAWAR IA N65236-02-D-7838
- DISA ENCORE DCA200-02-D-5010 (ENCORE-SC-02-052)
- DISA IASSURE DCA200-00-D-5018 (S2246D3168)
- USAF NETCENTS FA8771-04-D-0003 (SUB04-018)
- USAF ITS F01620-02-A-0003 (ITS-SC-02-042)
- SPAWAR CISS N65236-01-D-3818 (NDO-SC-0033)

## Contact Us

Julia Settle

Director, Business Development  
WareOnEarth Communications, Inc.

Email: [jsettle@wareonearth.com](mailto:jsettle@wareonearth.com)

Cell: (703) 517-1327

