

## BUSINESS CHALLENGES

The security of Government Agency IT systems, and the networks on which they run, is a critical component of our nation's overall security posture. This includes assurance that the enterprise is secured from both internal and external threats. With the continued expansion of the Global Information Grid (GIG), and the promulgation of concepts like Net-Centric Enterprise Services (NCES), security challenges become not only more complicated but more critical to the mission than ever before.

## HOW WE CAN HELP

As a seasoned Information Security and Assurance (IS&A) service provider, SuprTEK can offer a spectrum of IS&A services through a robust security service delivery framework. This framework helps guide our security services, ensuring comprehensive coverage and quality support. We fully understand the critical nature and activities required for customers' security needs and operational focus. SuprTEK's IS&A services focus on all enterprise defense layers. Our IS&A staff is comprised of veteran engineers with an average of twelve years experience in Federal Government IA focused support including:

- Certification & Accreditation
- Vulnerability Assessment
- Intrusion Prevention System (IPS)
- Computer Network Defense (CND)
- HSPD-12 and e-Authentication Support
- Incident Response Planning (IRP), Continuity of Operation and Disaster Recovery Planning (COOP-DR)
- Secure Wireless LAN (WLAN) Design and Implementation (FIPS 140-2)
- Single sign-on and Identity Management System
- Information Assurance Policy Support
- Network & Host Intrusion Detection (NID-HID)
- Firewall design and support
- System Readiness Reviews (SRR)
- Anti-virus Support

## OUR CUSTOMERS AND EXPERIENCE

SuprTEK has performed this set of services for a wide variety of both Department of Defense and Civilian Agencies as shown on the table below. Many of our staff bring extensive credentials and best practice experience including certifications such as CISSP, CISM, CISA, SAN-GISC, PMP, and ITIL. We are compliant of the DoD 8570.1-M, Information Assurance Workforce Improvement Program requirements.

Client Engagement Competency	DOJ OJP	DISA JFCOM	DC MPD	SDDC	DISA FSO	PFPA	DOJ JMD	ASD HD	INTEL	AFIT
Policy and Planning	◆	◆	◆	◆		◆		◆		◆
Program Management Support	◆		◆	◆		◆				◆
IA Operations Support	◆	◆	◆	◆			◆			◆
Certification & Accreditation	◆			◆	◆	◆			◆	◆
Vulnerability & Risk Assessments	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
Secure Wireless Management			◆		◆					◆
HSPD-12 & e-Authentication	◆									
Business Continuity & Disaster Recovery Planning			◆							◆
Software Security Analysis									◆	



## WHAT YOU CAN ACHIEVE

- A secure yet flexible computing environment
- A proactive posture to protect, monitor, analyze, detect, and respond to unauthorized activity
- Certified and Accredited systems based on DIACAP, NIACAP, NIST, and/or FISMA standards

## CASE STUDY – NO. 1:



**Engagement:** Department of Justice, Office of Justice Programs, Office of the CIO, Information Security Management Services

**Background:** Seven-person team in Washington DC, supporting the Office of the CIO on enterprise IT security management services

**Solution:** Four major areas of IT security management services:

- Certification and Accreditation Support: comprehensive evaluations of information system technical and non-technical security features
- Penetration Testing: including Denial of Service and Brute Force penetration, and attempts to circumvent system security features
- Post Accreditation Security Management: operational security for information systems and operations on a day-to-day basis. Operate and maintain all firewall technology. Ensures that system and all operational infrastructure security requirements are met.
- HSPD-12 and e-Authentication Support: provide full System Development Life-Cycle support for implementation of HSPD-12

Recognition: OJP has scored an "A" in "Trusted Agent" for FY 2006. "Trusted Agent" is the DOJ system used to report security performance metrics for all accredited IT systems. OJP was only major component within DOJ that received "A."

## CASE STUDY – NO. 2:



**Engagement:** US Army, Surface Deployment and Distribution Command (SDDC) Information Assurance Support

**Background:** SDDC required for day-to-day information assurance operations to protect, defend, report and analyze the IA status of SDDC systems and networks at 3 separate geographical locations –

- 1) Alexandria, VA, 2) Headquarters, Scott Air Force Base, and 3) Rotterdam, Netherlands

**Solution:** The SuprTEK IA Team provides the following services in support of the SDDC IA Mission:

- Network monitoring, firewall installation and maintenance
- Intrusion detection systems installation and maintenance
- Anti-virus operations
- Security configuration management
- Vulnerability assessments, incident response and auditing
- Supports multiple operating systems (Windows, Unix, and Linux) of security systems including IAVA vulnerability management, IDS sensors, log servers, Antivirus Servers, Mail Gateways, and Proxy servers
- Formulates, reviews, and revises procedures necessary to implement automated information systems security in accordance with higher-level regulatory requirements.
- Management of the perimeter security per Army AR 25-2 and DoD 8500.1 and 8500.2 guidance
- Provide IA support for C2 systems relocating to SCOTT AFB.

Recognition: In 2005, SuprTEK was awarded the Small Disadvantaged Business of the Year out of over 125 companies. Since 2003, SuprTEK received nine Letters of Commendations from the SDDC CIO and the Network Division Director for our dedication and performance.