

# EXPLORING CYBERSPACE WITHOUT FEAR



Our nation invests billions of dollars annually discovering, developing, and deploying advanced technology. This technology is the critical enabler of the powerful and precise capabilities our military now enjoys - and our forces rely on these capabilities to accomplish their mission. Our enemies understand this and attempt to exploit our capabilities by acquiring critical DoD technology. Historical evidence indicates that unprotected technology is easily stolen and replicated.

Whatever your organization's role in developing critical technology, the ATSPI Technology Branch can assist you in identifying your critical technology and provide protection solutions tailored to the value of the Intellectual Property and your specific use case.



ATSPI Technology Branch

AFRL/Rywa

2241 Avionics Circle

WPAFB, OH 45433-7320

ATSPI\_outreach@wpafb.af.mil

<http://spi.dod.mil>

Sponsored by:



Deputy Under Secretary for Defense  
**Science & Technology**

28 November 2007

PA # WPAFB-07-0557

# SOFTWARE PROTECTION INITIATIVE



<http://spi.dod.mil>

IDENTIFYING AND PROTECTING  
CRITICAL INTELLECTUAL  
PROPERTY

---

# SAFE COLLABORATION THROUGH TECHNOLOGY



## SPI MISSION:

The SPI Program, established by USD (AT&L), was founded on the principal focus to protect critical DoD intellectual property (ostensibly application software including executables, source code, and data) from piracy, tamper, and exploitation by nation-state class threats.

The SPI Program addresses the need of an alternative approach to implementing security in depth for Information Technology (IT) systems that will provide cost effective defenses against nation-state class threats and can be built from commercial components available today.

## THREATS TO DoD IP: RECENT HEADLINES

### Russian Cyberthief Case Illustrates Security Risks for U.S. Corporations

Anti-virus programs only catch viruses that were created in the past. For the most part, they can't catch what is sent out that day.

"The threat is all of your intellectual property — gone."

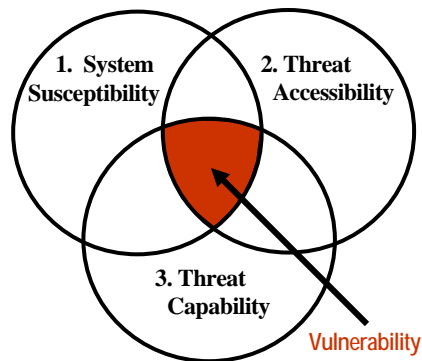
Every computer in a company's system may be targeted. They don't have to go after "crown jewels," Warner said. They can gather a little bit of data from all of the computers and put together a picture.



## THREAT-DRIVEN DEFENSES

- Anti-Piracy - Protected development, distribution, and execution
- Code Integrity - Trusted execution
- Anti-Reverse Engineering - Intellectual Property (IP) protection

## THE THREAT MODEL



## THE SOLUTION: ATSPI TENETS

SYSTEM VULNERABILITY IS DEFINED TO BE THE INTERSECTION OF A SYSTEM SUSCEPTIBILITY OR FLAW, ACCESS TO THE FLAW, AND THE CAPABILITY TO EXPLOIT THE FLAW. IMPLEMENTATION OF THE ATSPI THREE TENETS REDUCES VULNERABILITIES BY REDUCING ANY OR ALL OF THESE AREAS.

FAITHFUL ADHERENCE TO THE ATSPI TENETS WILL PRODUCE IT SECURITY SYSTEMS THAT PROVIDE SUPERIOR MITIGATION OF NATION-STATE CLASS THREATS WHILE BEING COMPATIBLE WITH DoD IT SYSTEMS DEPLOYED ACROSS THE ENTERPRISE

### Tenet 1. Focus on What's Critical: (shrinks susceptibility)

- Enumerate system access points and associated security elements
- Reduce access points to only those necessary to accomplish the mission

### Tenet 2. Move It Out-of-Band: (restricts threat access)

- Make critical access points and associated security elements less accessible to adversary

### Tenet 3. Detect, React, Adapt: (deny threat capability)

- Impose appropriate penalties when attack is detected
- Reaction occurs inside threat's OODA loop
- Fight through the attack!

## SPI PRODUCTS

**LPS-Public**— Boot CD for safer, CAC-enabled, no-local-trace browsing; as seen on AF Portal login page and discussed in <http://www.wpafb.af.mil/news/story.asp?id=123189629>.

**LPS-Remote Access** — Boot CD for remote desktop access to your DoD enterprise from a personal PC, CAC enabled, approved by the DoD CIO for COOP telework DoD wide.



**Encryption Wizard**— Encrypt and send FOUO files safely with the FIPS 140-2 compliant version, easy to deploy, no cost to US Government and contractors, widely used by Air National Guard; compliments data at rest (DAR).



**Secure Launcher**— Designed to mitigate nation-state class threats by locking the executable to a preconfigured, tamper-resistant system. Allows users to protect and process data on networks they don't control.

**Secure Mobile Device (SMD)** — A secure, zero-maintenance netbook for safe remote NIPRNet desktop access and Internet browsing.

**Cross Fabric Internet Browsing System (CFIBS)** — For unrestricted, safe Internet browsing and file transfers to and from the DoD GIG.

**Cyber Sensing Station (CSS)** — Grants the freedom to configure your own computing hardware, provides secure command and control of your system while allowing full and open internet access with strict egress control.



Use "COTS parts with government smarts" to shrink adversary's playing field.