

**SBIR Topic Number:**  
AF05-106

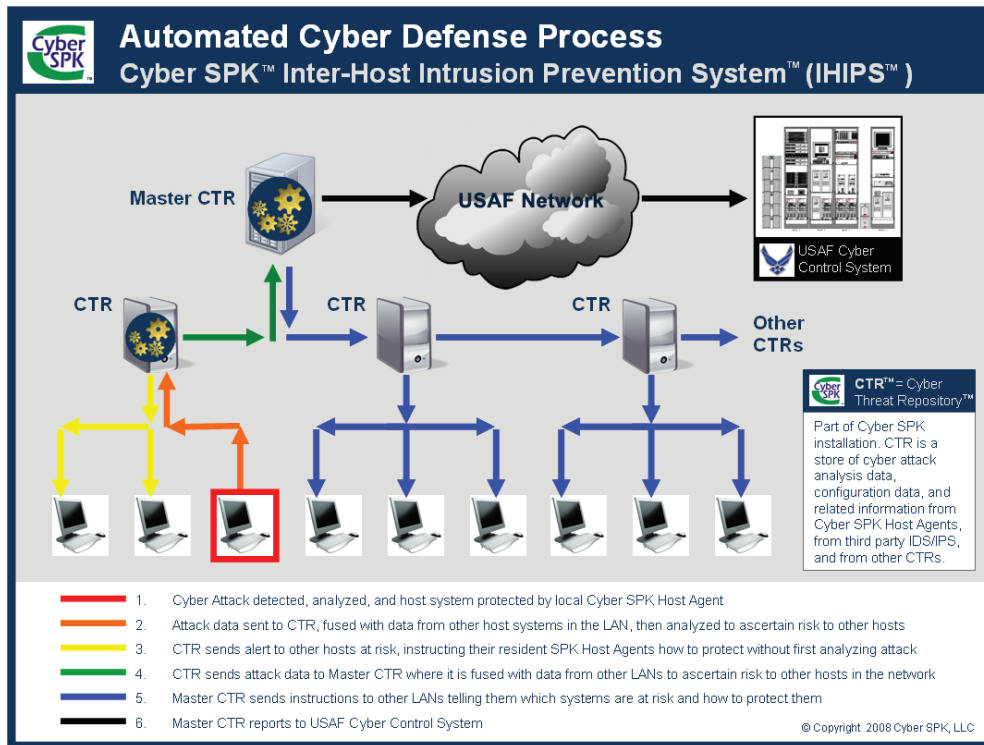
**SBIR Title:**  
Cyber Operations

**Contract Number:**  
FA8750-06-C-0031

**SBIR Company Name:**  
Cyber SPK, LLC  
Nashua, NH

**Technical Project Office:**  
AFRL Information  
Directorate, Rome, NY

This Air Force SBIR/STTR Innovation Story is an example of Air Force supported SBIR/STTR technology that met topic requirements and has outstanding potential for Air Force and DoD.



## Defending Against Zero-Day Cyber Attacks with Inter-Host Intrusion Prevention System™

- In spite of multiple layers of security, cyber attacks still threaten both general and mission operations
- Cyber SPK, LLC developed its Cyber SPK System Protection Kit, the first Inter-Host Intrusion Prevention System™ (IHIPS™)
- Cyber SPK Host Agents prevent attacks by blocking and terminating malicious behavior, thereby preventing that code from running again at a later time
- While this technology has now been proven for Windows desktops, servers, and other host systems, Cyber SPK can be ported to other environments, including secure embedded systems for the cockpit

20080318

**A**

DISTRIBUTION A:  
Approved for public  
release; distribution  
unlimited.

## Air Force Requirement

Our nation's defense is increasingly dependent upon its rapidly-growing, network-centric computing environment. But in spite of multiple layers of security, cyber attacks still threaten both general and mission operations. In particular, zero-day malware and Trojan code are often able to enter military installations without being detected. Once the malware is planted on a victim machine, the attacker has a software sentinel inside the target organization, which can be used to control that system, take over other systems, and exfiltrate sensitive information. Existing signature and rules-based solutions are not able to defend against this type of attack.

To solve this, the Air Force Cyber Operations Branch sought the capability to gather and mine digital information from multiple sources so as to better assess and defend against cyber threats. In this way, the function of their networks can be assured, resulting in full and proper support of Air Force operations.

## SBIR Technology

Developed by Cyber SPK, LLC, the Cyber System Protection Kit™ (Cyber SPK™) is the first Inter-Host Intrusion Prevention System™ (IHIPS™). Without human intervention, SPK Host Agents™ detect attacks, even zero-day attacks, by intercepting inappropriate data access, control, registry and file permission changes and network-related activities. It also correlates operating system and application-related process actions based on their real-time behavior.

SPK Host Agents prevent attacks by blocking and terminating malicious behavior, and preventing that code from running again at a later time. Data from each attack is forwarded to the Cyber SPK Cyber Threat Repository™ (CTR™) for inter-host data mining. This unique inter-host data mining process correlates data from other host systems in the local area network (LAN) as well as from third-party Network Intrusion Prevention Systems (NIPS) resources. SPK then automatically instructs all other SPK Host Agents in the LAN how they can protect their host systems from the attack.

As an Inter-Network Intrusion Prevention System™ (INIPS™), Cyber SPK can be scaled beyond an individual LAN to provide a broad spectrum of host protection, thereby protecting multiple networks across the Air Force domain.

## Potential Air Force Application

While Cyber SPK will protect Air Force systems at the host and inter-host level, it could also feed critical attack data to the Cyber Control System and ultimately into the Global Information Grid. Key features that impact the Air Force include:

- Individual Air Force host computer systems will be protected proactively; SPK does not rely upon historical attack signature information or human intervention to detect and prevent cyber attacks.
- The remainder of the Air Force network will be protected through automated inter-host mining, preventing the attack from spreading.

As a result, an attack upon a single Air Force host system or upon a single air base could be correlated automatically with attacks upon seemingly unrelated host systems at remote locations in other defense agencies, thus revealing – and preventing – coordinated and/or staged attacks on a massive scale.

While this technology has now been proven for Windows desktops, servers, and other host systems, Cyber SPK can be ported to other environments, including secure embedded systems for the cockpit. Additionally, variants of this technology could be developed that would enable (1) testing of Air Force host systems in order to identify weaknesses prior to attack, and (2) a cybercraft to retaliate against cyber adversaries

## Company Impact

The Air Force SBIR program enabled Cyber SPK, LLC, to take a new concept – an idea – and develop it into the Cyber System Protection Kit. As a result, a critical security challenge in the Air Force's Cyber Operations Branch has been resolved. Additionally, the SBIR program has brought the company into partnership opportunities with prime defense contractors as well as other Department of Defense organizations. It has also caused both revenues and staff at the firm to grow.

Cyber SPK develops software that enables information technology staffs to prevent, recover from, and diagnose system failures and cyber threats. In January 2008, Cyber SPK was invited to take part in a Commercialization Pilot Program workshop, sponsored by the Air Force, wherein the company met with prime defense contractors to move towards transitioning its R&D achievements to commercial deployment.



# SBIR/STTR

Air Force SBIR Program  
AFRL/XP  
1864 4th Street  
Wright-Patterson AFB OH 45433

AF SBIR/STTR Program Manager: Steve Guilfoos  
Website: [www.sbirsttrmall.com](http://www.sbirsttrmall.com)  
Comm: (800) 222-0336  
Fax: (937) 255-2219  
e-mail: [afrl.xppn.dl.sbir.hq@wpafb.af.mil](mailto:afrl.xppn.dl.sbir.hq@wpafb.af.mil)

