



**Technical Support Working Group  
Combating Terrorism Technology Support Office  
Technical Brief**

## Airborne Boundary Integrated Security System (ABISS)

### Background

Currently, airborne and special operations networks lack the ability to monitor and control intentional or unintentional cyber security threats. Cyber threats or unauthorized activities into airborne and special operations networks could originate from a number of activities including foreign intelligence gathering, terrorism, state-sponsored probing, hackers, and unintentional threats.



Dell PE1950

The TSWG and the Cryptologic Systems Group (CPSG) co-sponsored the development of the Airborne Boundary Integrated Security System (ABISS) for airborne applications within the Air Force and U.S. Department of Transportation. Both seek to implement an airborne boundary integrated security system/solution for specific security domains. The final report from the Phase One, Volpe Center Support to the Airborne Network (AN) Information Assurance (IA) Program, Sept 2007 reports gaps and specific security domains that ABISS implementation help.

The ABISS is a prototype DoD capability that provides a suite of COTS information assurance (IA) products in a small physical footprint through the use of virtualization technologies. It was developed to provide boundary protection for airborne and ground-based platforms. The device leverages existing DoD and AF approved and enterprise licensed COTS products to minimize cost and maximize support for Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) considerations.

The ABISS provides computer network defense (CND) per CJCSI 6510.01D and is intended to protect systems residing on a LAN and systems residing on an optional demilitarized zone (DMZ). The ABISS provides boundary services for Size, Weight and Power (SWaP) limited nodes. The ABISS also enforces network layer security policies for ports, protocols, and services (PPS) traffic. Also, the ABISS supports post-mission forensics through event logging.

### Requirement or Problem

ABISS has to be robust, securable, certifiable, and meet compliance standards of established policies and guidelines:

- Compliance with the architecture considerations of the Global Information Grid (GIG)
- Provide a Defense-in-Depth Strategy
- Joint Airborne Network Services Suite (JANSS) IA Strategy Guideline

- Policy mandates of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01E, Information Assurance (IA) and Computer Network Defense (CND)
- IA Goals, Objectives and Functional IA Requirements
- National Security Telecommunications and Information Systems Security Policy (NSTISSP) 11 - National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products

### Technical Description

The ABISS is a suite of boundary security tools that can be used to protect a security domain. The tools consist of firewalls, application proxies, anti-virus, and intrusion detection. The ABISS was implemented consistent with virtual machine technology. The software tools include components of the Host Based Security System (HBSS) which is being installed DoD-wide. The McAfee's ePolicy Orchestrator (ePO) version 3.6.1 is used and is also in the HBSS. McAfee's Intrusion Prevention System (IPS) module is version 7.0.1. The hardware/software list is provided in the Characteristic Statements and Specification section.

### Advantages & Limitations

By employing virtualization technologies such as VMware, ABISS software installation is only constrained by instantiation on an Intel-based hardware platform.

The use of DoD and AF approved and enterprise licensed COTS products reduces acquisition, maintenance, training costs, and leverages the security investments made in the HBSS.

### Characteristics Statements and Specifications

Software Components:

Category or Type	Manufacturer	Software	Version
Operating System	Microsoft	Windows 2003 Enterprise Server	SP2
Operating System	VMware	ESXi	3i
Operating System	University of CA, Berkley	BSD	7.0.1
Firewall	McAfee	Sidewinder Firewall	7.0.1
Intrusion Prevention System	McAfee	IPS Module	7.0.1
Gateway Anti-Virus	McAfee	Anti-Virus Module	7.0.1
Host Based Management	McAfee	Enterprise Policy Orchestrator	3.6.1
Management Dashboard Portal	CNF Technologies	ABISS Portal	1.5
Vulnerability Detection	eEye Digital Security	eEye Retina	1.0.0.4
Web Service	Microsoft	Internet Information Server	6.0
Database Server	Microsoft	SQL Server 2005 Standard Edition	SP1
Management Software	VMware	VMware Client	2.5.0

### Size, Weight, and Power (SWaP)

The hardware requirements are for an Intel-based computer capable of supporting VMWare. ABISS is currently implemented on a Dell 1950 server. The current hardware was selected to meet mounting requirements of aircraft electronic equipment racks. Thus the particular current implementation uses the Dell 1950. Operational and environmental requirements will vary the hardware requirements. For example, the ABISS virtual machine image could be installed in an Intel-based militarized or personal computer.

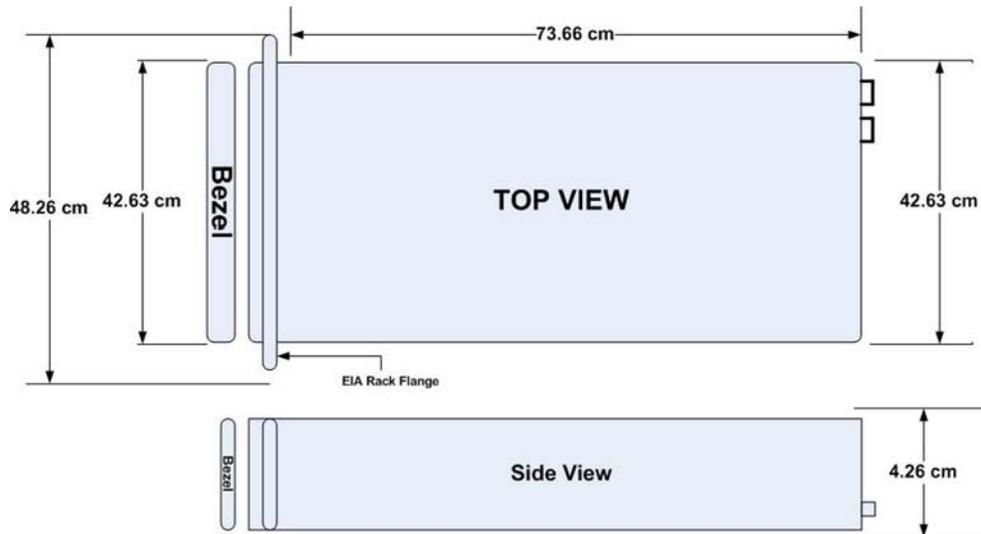
#### Model PE1950 1 Unit Rackable

##### Size

Depth = 73.6 cm

Width = 42.63 cm

Height = 4.26 cm



##### Weight

Max system Weight = 16.3 Kg

##### Input Power

Autoranged

47-63 Hz

100-120V ~ 10A

200-240V ~ 4.8A

##### Output Power

670W Max

+12V/54.4A

+3.3VSB/5.25A

## Test and Evaluation Results

The ABISS has been functionally tested for compliance with the requirements.

The functional verification testing included:

- VMware Integration;
- Management & Active Appliances (VMware);
- Firewall functionality (Sidewinder);
- Server 2003 functionality (Logging/Manager);
- Intrusion Prevention System (IPS) functionality (Sidewinder);
- Gateway Anti-Virus (AV) functionality (Sidewinder)
- Host-Based Security System (HBSS) Manager (ePO)
- Vulnerability Detection (ePO and eEye Retina);
- Asset Discovery (ePO and eEye Retina);
- Database (Microsoft SQL Server 2005);
- Internal and External Connectivity;

The test report is available for review.

## ABISS Certifications and Approvals

Rapid transition of capability to the warfighter, cost minimization, and DOTMLPF considerations were key elements in the development of the ABISS prototype. To support all three of these factors, COTS IA products that have been Common Criteria (CC) validated or designated as DoD/AF approved products were selected as a foundation. This selection was also done with potential certification of a productized ABISS capability in mind. Employing IA tools that have already been through a rigorous approval process is expected to substantially mitigate any potential certification and accreditation (C&A) effort.

Several components are “virtualized” versions of approved or CC validated COTS IA products. These versions are expected to be placed on the same path for Common Criteria validation as their predecessors. While the use of virtualization is becoming more commonplace for network management functions, it has not been widely used for IA capabilities. The ABISS effort is an early effort in the arena of virtualizing IA capability.

The table below reflects the ABISS software suite as currently configured on the prototype being tested at Bold Quest 2009 on-board the MIT Lincoln Lab’s Paul Revere 707 aircraft. Performance metrics will be captured to measure ABISS throughput, latency, and its IA effectiveness in protecting the aircraft boundary.

## UNCLASSIFIED

<b>Manufacturer / Product Name</b>	<b>Version#</b>	<b>Date</b>	<b>Approval</b>	<b>Notes</b>
McAfee ePolicy Orchestrator (ePO)	3.6.1	17 May 07	EAL3	
Retina Network Security Scanner	5.9.0.1795	25 May 07	EAL2, iTRM	Version 5.4.21.53 approved at EAL2
Microsoft Windows Enterprise Server	2003	7 Feb 08	EAL4, iTRM	
Microsoft SQL Server 2005	9.00.2047	21 Mar 07	EAL1, iTRM	
McAfee Virtual Firewall (Sidewinder)	7.0.1			Software Virtual Firewall pending CC/EAL validation
VMware ESXi Server	3.5 Upd4			pending CC/EAL validation
McAfee IPS Module	7.0.1	17 May 07	EAL3	
McAfee Anti-Virus Module	7.0.1	17 May 07	EAL3	
Host-Based Firewall/IPS (HIP)	6.0.2	17 May 07	EAL3	Part of ePO
Host-Based Anti-Virus (HIP)	6.0.2	17 May 07	EAL3	Part of ePO
Microsoft Internet Information Server	6.0	7 Feb 08	EAL4, iTRM	Included in Windows Enterprise Server 2003 CC TOE

Table Legend:

CC Common Criteria  
EAL Evaluated Assurance Level  
iTRM (Air Force) Infrastructure Technology Reference Model  
TOE Target of Evaluation

## Acquisition and Support Pricing

Preliminary Rough Order of Magnitude, unit cost estimates are listed below:

McAfee's integrated Firewall/IPS/Gateway Antivirus Software Licenses for each unit (includes 1 year of Maintenance)	~\$ 3,000
<p>The other Enterprise Licenses are available per the Host Based Security System (HBSS) purchase.</p> <p>VMware is supplied via an evaluation license. VMware players are open sourced and free.</p>	
Dell PE 1950 Unit Rackable, 4G (1)	~\$ 2,500
4G memory module (1)	~\$250
Optional Aircraft Hardened Unit (1)	TBD

On the GSA Schedule?	TBD
On the DHS Approved Equipment List?	TBD
On the DHS Responder Data Base?	TBD
Designated as a Homeland Security Product?	TBD

Note: Since the ABISS implemented on virtual machines the hardware costs are avoidable by installing the Virtual ABISS image on currently available Intel-based computers.

## Contacts at using Departments and Organizations

*USAF AFMC CPSG/NID*

**Robert Flores, GG-13**

[robert.flores2@lackland.af.mil](mailto:robert.flores2@lackland.af.mil)

(210) 925-0716

The MITRE Corporation

**Eugene Berger**

[eugene.berger.ctr@lackland.af.mil](mailto:eugene.berger.ctr@lackland.af.mil)

(210) 925-0774

## System Integrator Information:

*CNF Technologies*

*415 Oak Village Drive*

*San Antonio, Texas 78253*

(210) 957-2800

<http://www.cnftech.com>