

## **Ensuring Compliance with DoD Wireless Policies**



| White Paper

## Ensuring Compliance with DoD Wireless Policies

*The purpose of this whitepaper is to summarize the wireless policies defined by DoD Directive 8100.2, dated April 14, 2004, and the supplemental policy issued on June 2, 2006. This paper also describes how AirDefense's patented, Common Criteria certified, deployed and tested 24x7 wireless monitoring solution provides the required security and policy compliance in DoD networks.*

### DoD Wireless Policy

The Department of Defense (DoD) Directive Number 8100.2 was issued on April 14, 2004. The Directive covers the use of commercial wireless devices, services, and technologies in the DoD Global Information Grid (GIG). The Directive spells out policies for deploying secure wireless networks, and requires monitoring of those wireless networks for compliance. Additionally, the Directive states that wireless networks are banned from use in certain areas, and it covers policies for banned and authorized wireless networks.

On June 2, 2006 the DoD issued a supplemental policy and guidance to 8100.2 with the objective of enhancing overall security guidance and to create a foundation and roadmap for increased interoperability that embraces open standards regarding Wireless LAN (WLAN) technologies. This policy applies directly to IEEE 802.11 based WLAN devices, systems and technologies and excludes cellular, Bluetooth, WiMax and proprietary RF communication standards.

### Scope

The DoD 8100.2 Wireless Directive applies to all DoD organizations, including the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Command, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other DoD organizations. The Directive refers to these agencies collectively as DoD Components and applies to all commercial wireless devices, services, and technologies, including voice and data capabilities. This includes, but is not limited to, commercial wireless networks and Portable Electronic Devices (PEDs) such as laptop computers with wireless capability, cellular/Personal Communications System (PCS) devices, audio/video recording devices, scanning devices, remote sensors, messaging devices, Personal Digital Assistants (PDAs), and any other commercial wireless devices capable of storing, processing, or transmitting information.

### Responsibilities

The Assistant Secretary of Defense for Networks and Information Integration, as the DoD Chief Information Officer, shall monitor and provide oversight and policy development of all DoD wireless activities. The supplemental DoD policy requires heads of the DoD Components to:

1. Ensure that all WLAN procurements comply with the set policies starting in FY 2007.
2. Submit to the DoD CIO within 180 days specific migration plans for legacy systems.
3. Ensure interoperability through standards based products.
4. Prepare and execute incident response plans for wireless intrusion detection.

## **Summary of WLAN Policy Requirements**

The DoD has explicitly specified the following requirements for WLAN in its June 2, 2006 memorandum.

### ***Standards Based Technology***

All DoD Components must ensure that WLAN devices, systems and technologies are compliant with the IEEE 802.11 standard.

### ***Certifications and Validations***

All DoD Components must ensure that WLAN products are certified and validated for secure end-to-end communications and interoperability.

1. FIPS Compliance: Any cryptographic functionality must be National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 140-2 overall Level 1 validated at a minimum.
2. Common Criteria Certified: WLAN products must be National Information Assurance Partnership (NIAP) Common Criteria (CC) validated.
3. Wi-Fi/WPA2 Certified: WLAN devices must be Wireless Fidelity (Wi-Fi) Alliance certified and Wi-Fi Protected Access 2 (WPA2) Enterprise certified for security.
4. Firewalls/Antivirus: WLAN enabled PEDs must use personal firewalls and antivirus software that are NIAP CC validated.

### ***WLAN Security Standards***

Starting FY 2007, DoD Components must implement WLAN solutions that are IEEE 802.11i compliant and WPA2 Enterprise certified that implement 802.1x access control with EAP-TLS mutual authentication and a configuration that ensures exclusive use of FIPS 140-2 (minimum overall Level 1) validated Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code Protocol (AES-CCMP) encrypted communications.

### ***WLAN Intrusion Detection***

Wireless Intrusion Detection Systems (WIDS) were not directly specified in the original 8100.2 Directive. However, the new supplemental policy lays down the following explicit requirements:

1. WIDS is required for all DoD wired and wireless networks.
2. WIDS must continuously scan for and detect authorized and unauthorized devices. Continuous scanning is defined as 24 hours/day, 7 days/week.
3. WIDS must have location sensing capability.

4. WIDS must be validated under NIAP CC.

## **Need for the DoD Wireless Policy - Risks of WLANs**

Along with the many conveniences and cost saving advantages to WLANs, there are also many inherent risks and vulnerabilities. These exist in the nature of the wireless medium, and in insecure WLAN devices and configurations.

### ***Wireless Medium is Uncontrolled and Shared***

Traditional wired networks use cables to transfer information, which are protected by the buildings that enclose them. To gain access to a wired network, a hacker must bypass the physical security of the building or breach the firewall. On the other hand, wireless networks use the air, an uncontrolled medium. WLAN signals can travel through the walls, ceilings, and windows of the building. This renders the entire network accessible from another floor of the building, from an adjoining building, from the parking lot, or from across the street. Radio signals from a single access point can travel thousands of feet outside of the building walls.

Wireless networks use a shared medium, i.e., any wireless device in the network can “see” all the traffic of all other wireless devices in the network. WLAN risks are increasing with the advent of readily available hacking tools. A variety of specialized tools enable hackers to “sniff” data and applications, and to break both encryption and authentication.

### ***Insecure WLAN Devices***

Insecure WLAN devices, such as Access Points (AP) and user stations, can seriously compromise both the wireless network and the wired network, making them popular targets for hackers. APs can be insecure due to improper user configuration or operating with default settings which do not have strong encryption or authentication. They become gateways that hackers use to access both the wireless and the wired network.

Insecure wireless user stations pose even a bigger risk than insecure access points. These devices, which often have either no security configuration or are using an insufficient default configuration, easily come and go in the enterprise. Hackers can convert laptops into “soft” access points (soft APs) by either using a variety of software programs, such as HostAP, Hotspotter, or Aircrack-ng, or, by simply using a USB wireless adapter. By inserting a soft AP into a wireless network, a hacker can cause legitimate users in the network to connect to hacker’s soft AP, compromise the user laptop, and use it as a bridge to breach the network backbone.

### ***WLANs Allow Easy Access***

Accidental association takes place when a wireless laptop running the networking friendly Windows® XP OS or a misconfigured client automatically associates and connects to a neighboring wireless network. This enables intruders to connect to innocent user’s computers often without their knowledge, compromise sensitive documents on the user station, and expose it to even further exploitation. This danger is compounded if the station is connected to a wired network, which is also now accessible.

Ad hoc networks are peer-to-peer connections between devices with WLAN cards that do not require an AP. While these ad-hoc networks can be convenient for transferring files between stations or to connect to network printers, since they lack security, they enable hackers to easily compromise an innocent user's station or laptop.

## Overview of the AirDefense Solution

The AirDefense solution meets all the DoD stipulated requirements and was the first WIDS to receive the stringent CC certification from the NIAP program, as mandated by the DoD. Figure 1 shows the CC certificate awarded to AirDefense in July-2005. At the highest level, the AirDefense solution provides two necessary DoD functions:

1. Wireless Intrusion Detection and Prevention (WIDS/WIPS)
2. DoD WLAN Policy Enforcement

The AirDefense solution is designed to provide total wireless intrusion protection, regardless of location. The system provides centralized visibility and control of the DoD air space as well as mobile PEDs. It actively protects the DoD infrastructure against all known and potentially unknown wireless threats and extends this protection to laptop PEDs even when they are outside the secure DoD perimeter. In addition, the system can be used for centralized policy enforcement and compliance management of the entire WLAN infrastructure.



Figure 1: AirDefense was the first wireless IIDS/PS to be Common Criteria Certified

Figure 2 illustrates the top level components of the AirDefense solution. AirDefense Enterprise provides the most comprehensive detection of all wireless threats and intrusions. AirDefense Enterprise analyzes existing and day zero threats in real-time against historical data to accurately detect all attacks and anomalous behavior originating inside or outside the organization. AirDefense allows DoD Components to customize policies for each device as part of its centralized policy manager which defines, monitors and enforces the device-centric policies. In addition, it allows organizations to manage several standardized compliance requirements.

AirDefense Personal protects mobile DoD laptops from wireless-specific risks that could expose private data and transactions. It allows centralized DoD Component wide wireless access policies to be enforced across all wireless laptops.

RF Rewind™ allows DoD Components to trace any suspicious device by rewinding and reviewing minute-by-minute records of connectivity and communication with the network, to improve network security posture, assist in forensic investigations and ensure policy compliance.

AirDefense products scale to accommodate the largest DoD WLAN deployments, with minimal bandwidth requirements without sacrificing centralized management and easy of use. Our deployment and planning tools, along with industry leading WIPS accuracy, provide the lowest TCO and the highest ROI.

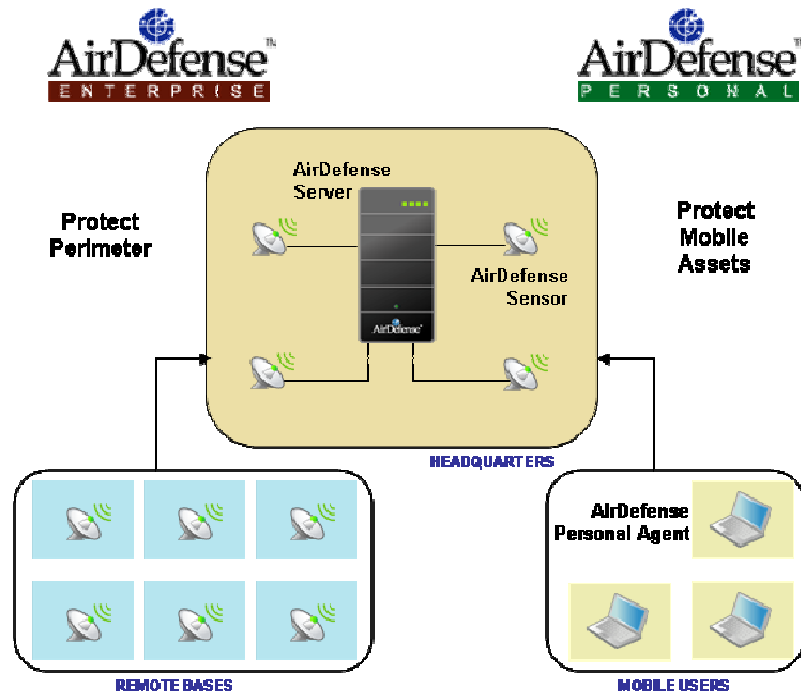


Figure 2: AirDefense provides comprehensive wireless intrusion detection and policy enforcement

### WLAN Intrusion Detection

AirDefense utilizes its 24x7, real-time monitoring of 802.11 networks for the most accurate intrusion detection of known and unknown attacks. With stateful monitoring of all WLAN activity based on attack signatures, protocol analysis, statistical anomaly and policy violations, AirDefense identifies network reconnaissance activity, suspicious WLAN activity, impending threats and attacks against the WLAN. AirDefense Enterprise has over 200 alarms.

**Detection of All Rogue WLAN Devices and Activity** - AirDefense recognizes all WLAN devices, which include APs, WLAN user stations, “soft APs” where stations function as APs and specialty devices such as wireless bar code scanners for shipping or inventory applications. AirDefense also identifies rogue behavior from ad-hoc or peer-to-peer networking between user stations and accidental associations from user stations connecting to neighboring networks.

**Reconnaissance Activity** - AirDefense recognizes multiple forms of WLAN scans including scans from NetStumbler, Wellenreiter, AirMagnet, Windows XP, etc.

**Suspicious Activity and Impending Threats** - AirDefense correlates information from all remote sensors over time to identify suspicious activity, such as:

- A user station on the watch list entering the airspace

- A single station repeatedly attempting to connect with multiple APs (this could be a sign of an intruder looking for the weakest link of a WLAN)
- Anomalous traffic from unusual off-hours activity or large downloads to a station.
- Clear-text leakage

**Attacks Against WLANs** - AirDefense draws upon the most sophisticated WLAN intrusion detection technologies with correlation across all sensors to identify attacks. Because similar attacks can take on various forms, attacks are then grouped into subcategories. With these subcategories, AirDefense provides the information that security personnel need to know, without getting into unnecessary detail. AirDefense alerts them to a range of attacks which include:

- Identity thefts used when an attacker impersonates a valid wireless device
- Out-of-sequence communication triggered by session hijacking or Man-in-the-Middle (MITM) attacks
- Multiple forms of Denial-of-Service (DoS) attacks
- Dictionary attacks from excessive failed attempts to authenticate to an AP from a single station

**Detection Accuracy** -

AirDefense reduces false positives with correlation among its four key detection technologies and by factoring in historical context instead of just looking at the present snapshot. AirDefense recognizes documented and undocumented (day-zero) attacks, because it does not rely solely on attack signatures.

**Active Defenses** -

Intrusion prevention systems are not only responsible for detecting the existence of threats but also for mitigating those threats. AirDefense offers real-time wireless and wired attack mitigation.

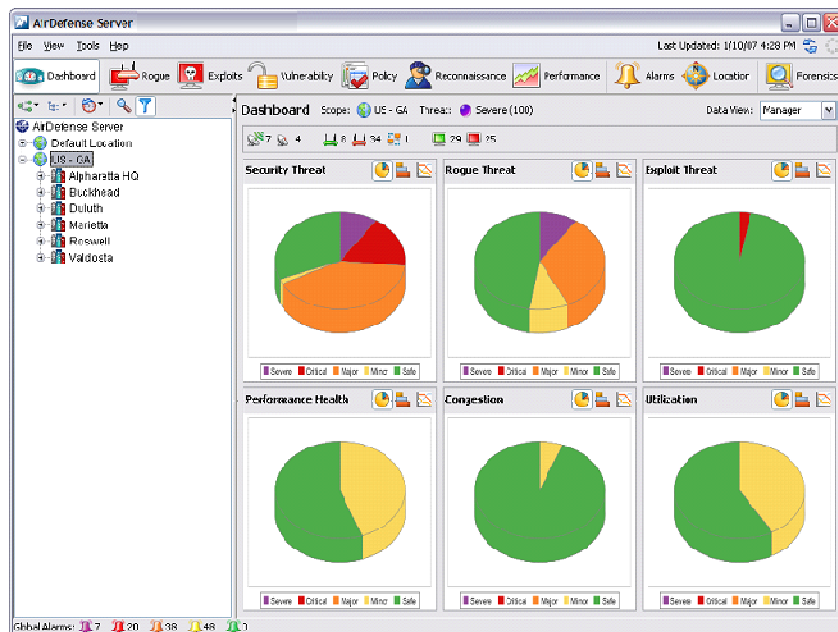


Figure 3: AirDefense Enterprise dashboard

- AirTermination - This patented feature enables the DoD administrators to terminate a connection between an authorized device and an unauthorized wireless device over the air.
- Wired-side Termination - The wired-side port suppression feature enables the administrator to suppress the communications port for any network device.
- On-command - The IT administrator can proactively terminate a device through the central web console.
- Policy-based - Automatic termination through pre-defined policies is needed for the temporary mitigation of wireless threats. When a threat is discovered at two o'clock in the morning, administrators can count on AirDefense to discover and terminate the threat. Accurate detection is a key requirement to prevent paralyzing the network as a result of false positives.

### ***Policy Enforcement***

Well-defined wireless policies and their enforcement is a crucial requirement for wireless security. Fortunately, the DoD WLAN policy has already been defined. AirDefense allows DoD Components to manage and enforce these policies centrally.

**Configuration Policies** - AirDefense allows organizations to set policies for how all WLAN devices should be configured and then monitors all WLAN devices to identify when any device deviates from that policy. AirDefense can define and monitor for all DoD specific configuration policies:

- Encryption and Authentication - Define policy for WLAN encryption and authentication from 802.11 standards (WPA2, 802.1x, EAP-TLS, AES-CCMP).
- Unauthorized "Open" Authentication - While WPA2 or another form of encryption and authentication are enabled, some APs have a "backdoor" vulnerability where the AP may also accept other lesser secure forms of authentication, which contradicts the defined policy.
- "No-Wireless" Zones: AirDefense can be used very effectively to block out all WLAN activity in a specified zone and notify administrators should any suspicious activity occur.
- VLANs - For APs configured for virtual LANs or multiple SSIDs on a single AP, AirDefense recognizes the varying policies for each VLAN segment.
- Approved Data Rates - The various 802.11a/b/g standards offer varying data rates and AirDefense allows DoD Components to define and monitor actual data rates being used.
- Improper Network Names - AirDefense recognizes default service set identifiers (SSIDs) or names of an AP or network, which often sends an inviting message to outsiders that the WLAN is not secure.

**WLAN Device and Roaming Policies** - AirDefense allows DoD network managers to define policies for authorized user stations, their configuration, how stations connect to the WLAN and recognized threats. WLAN device and roaming policies supported by AirDefense include:

- Authorized User Stations - AirDefense allows managers to set policy for authorized user stations whereby all other stations are unauthorized (a list of authorized user stations can be imported into AirDefense).
- Network Roaming - AirDefense allows DoD Components to define the appropriate APs for every user station and recognizes roaming policy violations when a user station tries to connect with unapproved APs. In addition, AirDefense can prevent stations from roaming between VLANs that they are not supposed to access.
- Ignore Lists - For DoD Components with neighboring WLANs, AirDefense can ignore activity from APs and stations on an “ignore” list until one of those devices attempts to communicate with an authorized user station or AP.
- Watch Lists - For DoD Components that recognized repeated suspicious activity from the same suspicious user station, AirDefense can put such stations on a “watch” list to alert IT personnel the minute that the suspicious station enters the airspace even if the suspicious station has not connected to anything or scanned the airwaves.

**Performance Policies** - Upon deploying a WLAN, DoD Components have an expectation for how the network should perform. AirDefense allows network managers to define these expectations for performance and monitor for performance policies that are specifically applied in the areas of individual APs, single user stations and a collective group of user stations. These performance policies set a threshold for health monitoring in the areas of:

- Maximum Number of Stations Connected to an AP - Network performance decreases dramatically when too many stations connect to the same AP and AirDefense allows DoD Components to define how many stations should be connected at any one time to a single AP.
- Traffic Thresholds allowed between an AP and the Wired Network - AirDefense allows DoD Components to protect the wired network from excessive bandwidth drain from the WLAN by defining a threshold for maximum traffic between the AP and the wired network.
- Traffic Thresholds Allowed Between an AP and a Single Station - AirDefense allows DoD Components to protect an AP from being overwhelmed from the traffic of a single station by defining a threshold for traffic between an AP and station.
- Thresholds for transmitting and receiving data frames, management frames and control frames for a single user station, a single AP, or collective stations connecting to an AP.
- Thresholds for total fragmented frames and decrypted error frames observed from a single user station or AP.

**Channel Policies** - AirDefense allows DoD Components to establish channel policies for approved channels of operation, ad hoc networks and approved hours of operation.

- Ad Hoc Networks - AirDefense allows DoD Components to set a policy for ad hoc and peer-to-peer networking between stations and specify the channels for authorized ad hoc networks
- Authorized Channels - With AirDefense, DoD Components can define channels for each AP and identify all WLAN traffic on unsanctioned channels
- Off-Hours Traffic - For DoD Components with defined work hours, IT managers should designate appropriate hours for use of the WLAN. AirDefense monitors these policies on a channel by channel basis and alerts IT security personnel to WLAN activity outside of the allowed hours.

**Vendor Policies** - Because enterprise WLANs should be deployed using enterprise-class infrastructure, AirDefense allows IT managers to define approved hardware vendors for devices using the WLAN. With a list of accepted vendors, AirDefense then recognizes all hardware from unapproved vendors when they enter the enterprise airspace.

**Policy Enforcement** - While AirDefense allows IT managers to define WLAN policies and monitor the network for compliance, AirDefense also provides the capability to enforce policies across an enterprise-class WLAN. Using SNMP from the wired side of the network along with wireless AirTermination, AirDefense can help organizations strictly enforce corporate wireless policies.

### ***Anywhere Protection***

AirDefense Personal is a Windows-based software agent that protects the mobile DoD laptops when they are outside the 24x7 monitored wireless airspace. Because today's networks are virtual with mobile employees extending the edge of corporate networks to homes, hotspots and airports, AirDefense has expanded its anywhere, anytime monitoring solutions to include AirDefense Personal. Residing on mobile users' laptops, AirDefense Personal monitors for malicious or accidental wireless activities and misconfigurations that may cause security exposures or policy violations. AirDefense personal can be used to centrally enforce wireless access policies as well as ensure that proper Firewalls, Antivirus and VPNs are enabled and running when DoD laptops are in use.

AirDefense Personal is integrated with the AirDefense Enterprise system. Policy profiles that are centrally defined on AirDefense Enterprise are automatically transferred to each mobile user when they connect to the corporate LAN. If threats are discovered, AirDefense Personal notifies the user and sends the logs to AirDefense Enterprise for central reporting and notification.

### ***Forensics and Reporting***

By statefully monitoring all WLAN activity, AirDefense maintains a historical database that powers robust forensic analysis and historic trending, as well as incident investigation. AirDefense stores over 300 statistics for every wireless device on a minute-by-minute basis. With a single click

AirDefense can display the time of attack, what entry point was used, the length of the exposure, how much data was transferred and which systems were compromised, etc.

**Drill-Down Alarms** - From the console dashboard, AirDefense allows IT personnel to view a summary of recent alarms and drill down for specific information as to when this alarm first appeared on the network, which devices are involved in the alarm, the location of the alarm, a detailed explanation and suggested remedies.

**Historical Data for Trending and Forensic Analysis** - AirDefense provides report templates for historical network analysis and allows for customized reports for specific trends and forensic analysis.

**Device-Centric Reports** - AirDefense provides standard device-centric reports for missing devices, ad hoc networks, probing stations, individual AP snapshots, single user station snapshots, most active user stations and most active APs.

**DoD Compliance Reports** - DoD policy compliance specific reports are built into AirDefense Enterprise. The reports are available in several formats and can be automatically scheduled and sent to appropriate personnel or manually generated. The reports have executive summaries and details related to specific DoD policies and current compliance status. In addition, AirDefense allows the generation of fully-customizable reports that leverage the forensic data stored by the system.

## WLAN Location Tracking

To find the location of any WLAN device, AirDefense provides accurate location tracking using signal strength triangulation and fingerprinting techniques. Location tracking enables the administrator to locate and track rogue devices or any other device of interest in real-time. Location determination is also available in AirDefense Mobile, a complementary product to AirDefense Enterprise, which allows administrators to locate and track down rogue devices during walk around tests.

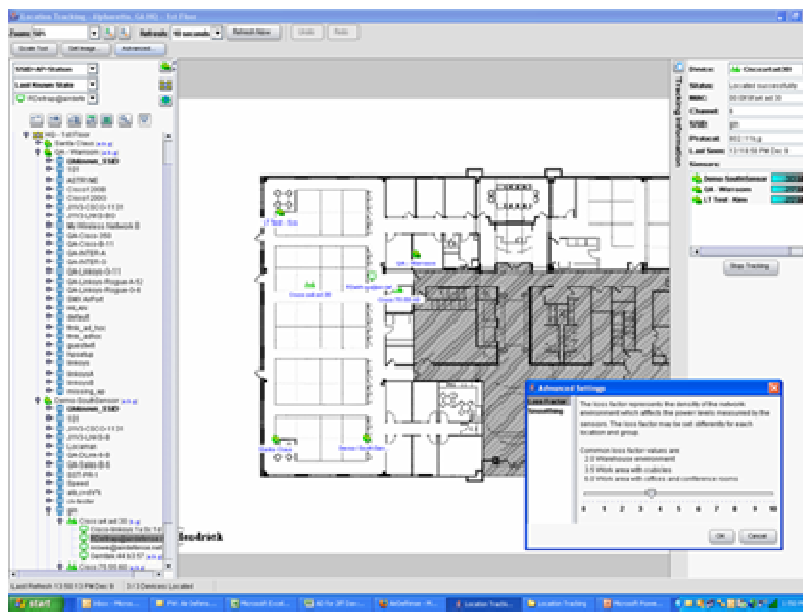


Figure 4: AirDefense Enterprise location tracking

## Summary

The new DoD policy has made WIDS mandatory for all DoD wired and wireless networks. WIDS must provide 24x7 monitoring of the airwaves, have location tracking capabilities and must be Common Criteria validated. AirDefense Enterprise meets all the DoD stipulated requirements. AirDefense Enterprise has been broadly adopted for deployment throughout the DoD. Current DoD customers include the US Army, Navy, Marine Corps, unified combatant commands, defense agencies and intelligence community organizations. In addition to its large presence in DoD, AirDefense's solutions are utilized by dozens of Federal civilian agencies to protect network data, detect unauthorized devices, mitigate threats and to monitor wireless activity.

## ***About AirDefense***

**AirDefense**, the market leader in anywhere, anytime wireless security and monitoring, is trusted by more Fortune 500 companies, healthcare organizations and high-security government agencies for enterprise wireless protection than any other wireless security provider. Ranked among Red Herring's Top 100 Private Companies in North America, AirDefense products provide the most advanced solutions for rogue wireless detection, policy enforcement and intrusion prevention, both inside and outside an organization's physical locations and wired networks. Common Criteria-certified, AirDefense enterprise-class products scale to support single offices as well as organizations with hundreds of locations around the globe.

**AirDefense Enterprise**, the flagship product, is a wireless intrusion prevention system that monitors the airwaves 24x7 and provides the most advanced solution for rogue detection and mitigation, intrusion detection, policy monitoring and compliance, automated protection, forensic and incident analysis and remote troubleshooting. As a key layer of security, AirDefense Enterprise complements wireless VPNs, encryption and authentication. Using a monitoring architecture of distributed smart sensors and a secure server appliance, the AirDefense Enterprise system provides the most comprehensive detection of all threats and intrusions. Unlike any other solution on the market, AirDefense Enterprise analyzes existing and day zero threats in real time against historical data to more accurately detect threats and anomalous behavior originating inside or outside the organization. The system automatically responds to threats according to appropriate business process and compliance requirements on both wireless and wired networks, making AirDefense Enterprise the industry's most secure and cost-effective wireless intrusion prevention and troubleshooting solution.

**AirDefense Personal**, the industry's first end-point security solution, provides uninterrupted protection for all mobile employees and their enterprise wireless assets, regardless of location – at work, home, airports or other wireless hotspots. Policy profiles are defined centrally on AirDefense Enterprise and automatically downloaded to each mobile user. If threats are discovered, AirDefense Personal notifies the user and sends the alerts to AirDefense Enterprise for central reporting and notification. This unique solution allows the network administrator to enforce corporate policies and provide complete protection for the mobile workforce, regardless of location.

**The AirDefense InSite Suite** is a collection of powerful tools available today for network architects to design, install, maintain and troubleshoot wireless networks. Tools included in the suite are: AirDefense Mobile, complementary to AirDefense Enterprise allows administrators to perform wireless assessments, security audits, locate and manage rogues. AirDefense Architect provides complete design and 3D RF simulation of WLANs based on building-specific environments. AirDefense Survey provides real-time, in-the-field measurements of Wi-Fi RF environments for site-specific surveys.

For more information or feedback on this white paper, please contact [info@airdefense.net](mailto:info@airdefense.net) or call us at 770.663.8115. All trademarks are the property of their respective owners.