



**FOR IMMEDIATE RELEASE**

**AirPatrol Enforces Cell Phone Security Policies in Enterprises and Government Agencies where Wireless Devices are Prohibited**

*Enterprises and Government Agencies Use AirPatrol's Wireless Locator System to Keep Cell Phones from Infiltrating Sensitive Areas of Buildings*

**Columbia, MD—September 1, 2009**—AirPatrol Corporation, a leading mobile and wireless threat management solutions company, today announced that its **Wireless Locator System (WLS)** is the only wireless intrusion detection system which allows security administrators to keep cell phones out of mission critical areas by detecting, locating and characterizing both Cellular and 802.11 WLAN devices on a 24 x 7 basis.

Recent news reports have detailed serious vulnerabilities in the A5/1 encryption standard which protects worldwide Global System for Mobile Communications (GSM) cellular communications. GSM security vulnerabilities are significant since cellular devices are routinely used to transmit large volumes of confidential data and voice communications in today's 'always connected' world. As smart phones and cellular broadband devices become increasingly widespread, the need for robust security practices in government agencies and blue chip corporations becomes increasingly critical due to the threat of security compromises via cellular modes.

GSM is used by roughly 80 percent of global cell phones, leaving many enterprises wondering what preventative measures can be taken to protect employees' conversations and sensitive data transmitted via unsecured cellular devices. AirPatrol is the only company that can prevent wide scale problems by rooting out cell phones in buildings and areas that have no wireless policies.

"GSM is not secure and if researchers are successful in their attempts to crack the code within 6-12 months, IT administrators will have a new world of headaches in attempts to protect unsecured data such as medical records, bank account information and conversations on their employees' smart phones," said Ozzie Diaz, president and CEO, AirPatrol Corporation. "Enterprises and government agencies turn to AirPatrol to enforce wireless policies and our WLS is the only wireless security product that roots out cell activity in areas deemed to be off limits to cell phones."

AirPatrol's WLS also features a new Forensic Database plug-in that records and archives both 802.11 WLAN device and cellular device event information. The WLS Forensic Database gives security administrators the ability to revisit wireless threat events that occurred hours, days or months ago. Collected security data can be used directly or can be correlated with other security data such as video surveillance, identity management and physical access control information to provide a full understanding of security incidents. To review a flash narrated demonstration of the WLS, log onto:

[http://www.airpatrolcorp.com/video\\_wls\\_overview.php](http://www.airpatrolcorp.com/video_wls_overview.php).

### **About AirPatrol Corporation**

AirPatrol Corporation is the most trusted authority on mobile and wireless threats to enterprises. The company's comprehensive suite of location-based products enable security administrators in the government, financial, healthcare, corporate enterprise and retail industries keep pace with the expanding requirements of an increasingly mobile world. For more information, please visit the company's website at [www.airpatrolcorp.com](http://www.airpatrolcorp.com).

### **Media Contact**

Bill Keeler  
Schwartz Communications  
781 684-6542  
[billk@schwartz-pr.com](mailto:billk@schwartz-pr.com)

###