



## Case Study: Large United States Department of Defense Agency

### Unified Wireless Threat Management

#### Challenge:

Cost-effective solution to enforce "no wireless devices" policy at secure portion of SCIF (Sensitive Compartmented Information Facility)

#### Solution:

AirPatrol's Wireless Locator System with combined WiFi / Cellular Sensors

#### Benefits:

- ¼ the expense of separate systems that detect each type of wireless device
- Operational efficiency: single management system for policy, alerts & analytics
- Addresses current cellular detection needs while providing for future expansion
- AirPatrol's open, cooperative approach lets client contribute to TSCM product requirements

### Challenged to Carry out Security Policy

Being responsible for sensitive and critical national security missions, this Agency processes and stores classified information throughout its headquarter building of 500,000 square feet. Subsequently, there is a strict policy of no wireless devices, including no cell phones. Signs are posted to state the policy but a cost-effective solution to enforce the policy did not exist. They had a sparse network of WiFi wireless intrusion detection systems (WIDS) to detect unauthorized WiFi devices, but nothing to detect unauthorized cell phones. Deploying separate sensors and management systems for various types of wireless devices for coverage of such large square footage was prohibitive financially and ongoing operationally.

Having no visibility of cell phones in the building was becoming an urgent issue. The existing WiFi WIDS was showing growing problems with onsite WiFi devices, and it was safe to assume that the number of onsite cell phones against policy was growing too. With the emerging use of a smart-phone serving as access point for multiple laptops, the security exposure was significant.

### Combined Cellular and WiFi Threat Management

The Agency deployed AirPatrol's Wireless Locator System (WLS) with combined WiFi/Cellular Sensors. They also deployed WLS Connect so that security personnel dispersed around the building could get real-time and historical playback of WLS security data. Data provided by WLS Connect was also fed into the central operations center.

### Saved Significant Time and Expense

The Agency is now enforcing their strict no-wireless device policy at a fraction of the alternative approach. Installing separate sensors and management consoles for each type of wireless communication would have meant more than 4x higher cost. Not only would they have had to purchase twice the hardware and software, they would also have needed significant professional services for wiring and the consumption of much more network switching resources. The Agency gained operational efficiency from AirPatrol's unified wireless threat management because from one console, they can set policy and get alerts and analytics for all wireless devices. Moreover, the location detection accuracy of AirPatrol was more than twice that of other products available in the marketplace.

### Security Policy Enforced

The teams from Physical Security, Technical Surveillance Counter-Measures, and Counter-Intelligence (TSCM/CI) have been impressed with the solution. AirPatrol's WLS has led to the discovery and confiscation of many unauthorized wireless devices, leading to the Agency's wireless cyber-security posture becoming strengthened multi-fold. The Physical Security team regularly demonstrates WLS to other organizations in the US Government. Going forward, they look forward to purchase of AirPatrol's next-generation sensors with narrowband scanning receivers to detect additional wireless threat vectors.