What is a SCIF? A Sensitive Compartmented Information Facility is an enclosed area within a larger building used by military and national defense officials to share, process and digest classified information with each other.

Officials required to perform regular SCIF security audits, and preventative sweeps must ask themselves at least 3 questions:

- ***Can SCIFs be secured from wireless threats?***
- ***Can security personnel detect and locate hidden bugs and other sources of wireless espionage?***
- ***How can you prevent spying devices from entering SCIFs?***

No single solution will solve these issues but an array of high-tech wireless threat detection solutions combined with the proper procedures can ensure that no sensitive information will be leaked or stolen from a SCIF.

BERKELEY VARITRONICS SYSTEMS is a 50 YEAR OLD WIRELESS ENGINEERING and PRIVATELY OWNED FAMILY BUSINESS headquartered in METUCHEN, NJ

ALL PRODUCTS MADE IN THE USA

Berkeley Varitronics Systems
Wireless Detection

732-548-3737
sales@bvsystems.com
www.bvsystems.com

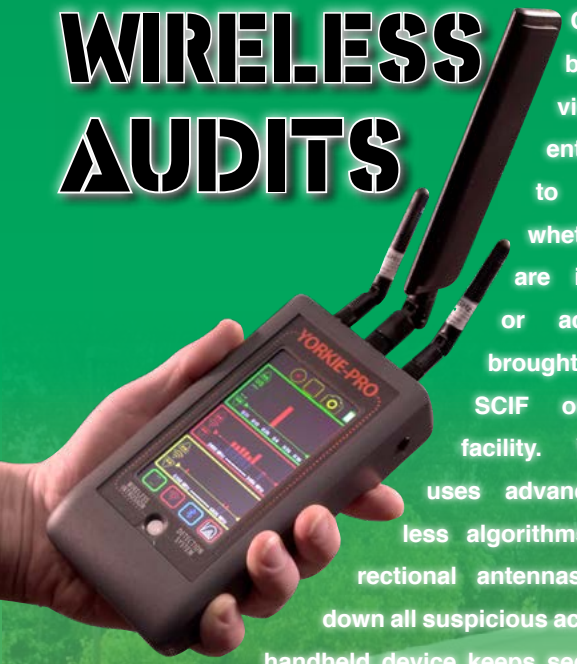
SENSITIVE COMPARTMENTED INFORMATION FACILITY

Securing SCIFs from Wireless Threats

Berkeley Varitronics Systems
Wireless Detection

732-548-3737
sales@bvsystems.com
www.bvsystems.com

WIRELESS AUDITS



Contraband devices present a danger to infosec whether they are intentional or accidentally brought into a SCIF or secure facility. Yorkie-Pro uses advanced wireless algorithms and directional antennas to hunt down all suspicious activity. This handheld device keeps security personnel on their feet allowing instant detection and location of hidden wireless bugs, RF transmissions and any devices that communicate wirelessly. Yorkie-Pro can also record all RF activity and allows whitelisting to distinguish between friendly and unknown devices.

SCAN FOR BUGS, ROGUE DEVICES AND UNAUTHORIZED WIRELESS ACTIVITY

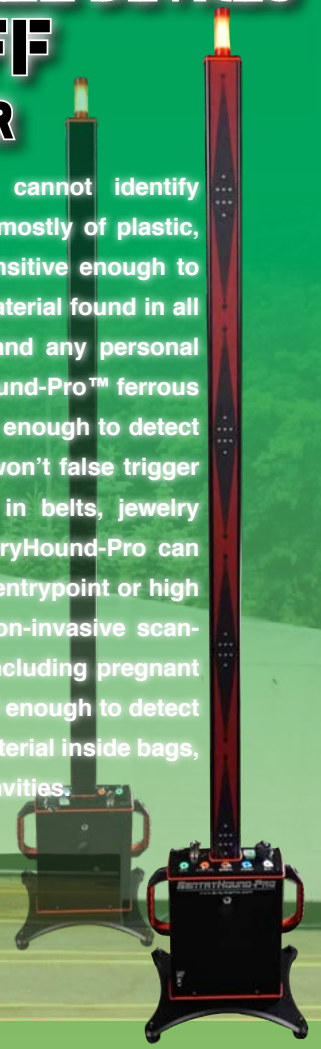
DETECT AND ALERT SECURITY PERSONNEL TO ALL WIRELESS DEVICES

Wireless threat detection for SCIFs requires a balance of effective offense with strong defense. WallHound-Pro offers comprehensive wireless detection for all active devices all day long. It also offers customizable bright and loud alerts to remind visitors and staff that there is no such thing as a benign wireless device. WallHound-Pro supports whitelisting, physical and digital security, auto and manual thresholding and even directional finding antennas to pinpoint wireless threats down specific corridors or entrypoints.

24-7 WIRELESS MONITORING AND ALERTS

STOP ALL DEVICES ON OR OFF AT THE DOOR

Standard metal detection cannot identify modern smartphones built mostly of plastic, but ferrous detection is sensitive enough to identify trace amounts of material found in all phones, tablets, wearabls and any personal electronic device. SentryHound-Pro™ ferrous detection portal is sensitive enough to detect any P.E.D. ON or OFF, but won't false trigger on common metals found in belts, jewelry and medical implants. SentryHound-Pro can be deployed quickly at any entrypoint or high foot traffic area for safe, non-invasive scanning of staff and visitors (including pregnant women) but is also powerful enough to detect trace amounts of ferrous material inside bags, briefcases and even body cavities.



Pro Tip: The element of surprise...
Unannounced wireless sweeps of SCIFs can be very effective in maintaining compliance of personnel regarding prohibited use of personal electronic devices in the SCIF. It is suggested not to announce a wireless sweep in advance in order to maintain the element of surprise!

Pro Tip: Detection overhead...
Use optional directional (DF) antennas to isolate detection areas by mounting them overhead (pointing downward) in front of the SCIF door rather than mounting them to WallHound-Pro unit itself. For hallway detection prior to SCIF entry, mount DF antennas atop WallHound-Pro and aim them down the hallway. In either case, locate WallHound-Pro antennas as far away as possible from the cell phone lockers to reduce false positives.

Pro Tip: Start with decoys...
Optimize detection sensitivity by perforing decoy tests using a variety of brands/models of cell phones. Hide each phone (one at a time) under clothing in various locations to establish the proper setting of the sensitivity control and distance between the scanning poles.