



207 Tremont Street

Rochester, New York 14608

[www.nexusisr.com](http://www.nexusisr.com)

# Concept Commentary

# Ruggedizing and Securing Cellular Datacard Services

## Introduction

An often-asked question is, “*Can’t I just plug a cellular data card into my*

*laptop?*” While doing so may be fine for many uses, there is an entire market segment that requires stronger security, enhanced connectivity assurance, greater bandwidth, asset track-ability and a higher degree of ruggedness.

The Nexus Hawk™ is a mobile router and IP gateway that addresses each of these issues, head-on while still utilizing cellular data cards in an enhanced and rugged way, as part of the solution.

As an added benefit, the Nexus Hawk can IP-link devices that are not connected to computers (therefore, have no place to insert a datacard natively). This includes IP-based remotely-mounted surveillance cameras and Supervisory Control And Data Acquisition (SCADA) appliances.

## Stronger Datacard Security

The Nexus Hawk was engineered with today’s privacy and governance mandates in mind; it is a perfect fit for organizations addressing FIPS 140, HIPAA and ISO 270001 issues for the non-brick-and-mortar workforce.

The Nexus Hawk can serve as a Virtual Private Network (VPN) endpoint. No software needs to be loaded on the laptop(s). As an added benefit, a VPN *server* is provided as well! Users without an existing VPN can implement one at no additional cost. Of course, the Nexus Hawk can pass-through any VPN whose client software is loaded on the local laptop(s), too.

The Nexus Hawk faces the Internet, with all ports closed by default. The cellular

datacard's public IP address is hardware-firewalled by the Nexus Hawk. Local Nexus Hawk devices are provided non-routable IP addresses via a Network Address Translation (NAT) server and are protected by Stateful Packet Inspection (SPI). Local devices are effectively "invisible" to the Internet unless overridden by an administrator.

The Nexus Hawk supports Secure Sockets Layer (SSL), natively. Additionally, the Nexus Hawk's SSL module is compiled in a FIPS 140-2 compliant way.

Users may wish to connect to the Nexus Hawk using Wi-Fi (801.11) rather than by cable. This allows many people or appliances to share the same connections. The Nexus Hawk presents *rock-solid, governance-compliant strategies* here, as well.

Wi-Fi traffic can be securely encrypted! The Nexus Hawk includes several Wi-Fi encryption schemes to assure that communication between it and local users remains private and secure. The most secure strategy is called WPA2/PSK, which relies on a 256-bit AES key. Unlike WEP, this WPA2/PSK strategy has *never* been reported to have been compromised.

Wi-Fi cloaking suppresses the wireless network from identifying itself when interrogated. Users must already know its name; otherwise they will neither see it on a "search for available network" scan nor be able to attach to it.

Wi-Fi LAN-user white- and black-listing further secures the connection between laptop(s) and Nexus Hawk. If white-listing is invoked, only devices with authorized MAC addresses will be allowed to connect. If black-listing is invoked, devices with particular MAC addresses would be rejected, while passing all others.

Wi-Fi on the "a-channel" (5.8 GHz) is a high-security selection. "War drivers" (Wi-Fi exploiters) focus on the b/g-channels (2.4 GHz) because there are so many easy targets there. Operating on the a-channels is the best strategy, if your laptop(s) can support doing so.

### **Assured Connections**

Once users begin to rely on remote connectivity, they expect it to be available when they need it.

Optional signal-enhancing external gain antennas and signal boosters can be employed. This is especially important in fringe and rural installations. With these strategies, the Nexus Hawk often enjoys cellular data connectivity even when traditional cell phones have no usable signal!

A "throughput-quality watchdog" is included. It can reset the datacard, if circuit errors exceed a user-defined threshold. Often times, a simple "hang-up-and-redial" will re-establish a higher quality session.

The Nexus Hawk allows the concurrent use of multiple cellular datacards and other pathways. This can provide additional bandwidth via link load-balancing or static routing. Otherwise, the Nexus Hawk can auto fail-over from one provider to another when needed. The Nexus Hawk additionally supports private & 700MHz

datacards, Wi-Fi hotspots and satellite service providers as part of these strategies

### **Future-safety and Longevity**

The state-of-the-art in cellular and wireless networking is constantly advancing. Because these datacards are removable, your investment in the Nexus Hawk solution allows you to upgrade as service providers release new cards with new services offerings.

Cellular datacard drivers are embedded within the Nexus Hawk; there is nothing to load on your local device(s); it's all plug-and-play. Additionally, the Nexus Hawk can provide cellular datacard services even to legacy computers that lack drivers from the datacard manufacturer!

### **Rugged and Damage Resistant**

The Nexus Hawk is designed for use in a rugged environment. Its heavy-gauge steel case also provides protection for cable terminations. Reclaim real-estate by using case-top mounting holes for other equipment.

Thanks to the Nexus Hawk, Cellular datacards may now be mounted in the trunk or under / behind seats, etc. Cables can be properly dressed and hidden.

### **Trackable**

Knowing where your mobile asset is, is easy with the optional embedded GPS. The Nexus Hawk can send NMEA-0183 or TAIP formatted GPS data to *multiple* target AVL systems at the same time.

Because the GPS is in the Nexus Hawk, and not reliant on a powered-up laptop for data connectivity, the asset's location can be determined, even if the laptop isn't functioning!

If data services are interrupted while the Nexus Hawk is being tracked, its GPS information will be cached, auto uploading it when service is restored.

The Nexus Hawk's GPS stream continues to be delivered even when laptops are "off".

This is especially advantageous if laptops may be powered "off" or otherwise removed from the operational environment.

### **In Summary**

The Nexus Hawk enhances the traditional "in-the-laptop" datacard use by providing...

- **Stronger security**
  - VPN (IPsec, OpenVPN w/embedded server)
  - All-ports-closed hardware firewall
  - NAT with Stateful Packet Inspection
  - FIPS 140-2 SSL compliant
  - 256-bit AES Wi-Fi encryption
  - Wi-Fi Cloaking
  - Wi-Fi White- and Black-listing
  - 802.11a (in addition to b and g) Wi-Fi
- **Assured connectivity**
  - GPS delivered even when laptop is "offline"
  - Connect external gain antennas and boosters
  - Throughput quality watchdog circuitry
  - Multiple concurrent datacard use
  - Supports private, 700 MHz, Wi-Fi hotspot and satellite
- **Future Safety and Longevity**
  - Replace old cards with new ones for new services
  - Datacard drivers are embedded (nothing to load)
  - Serve legacy computers with old operating systems
- **Rugged and Damage Resistant**
  - Heavy-gauge steel case or optional stainless-steel injected ABS (if low weight is needed)
  - Mounting in trunk, under/behind seats, etc

The Nexus Hawk squarely addresses HIPAA, ISO 270001, FIPS 140-2 issues. The following chart may be used as a guideline in meeting your organization's

compliance strategy. Each of these functions are native to the Nexus Hawk.

- Use encrypted VPN for all traffic.
- Use a hardware firewall to face the Internet.
- Use Secure Sockets for web traffic (https://)
- Secure Wi-Fi through encrypted connections
- Secure Wi-Fi through cloaking
- Secure Wi-Fi through white-listing
- Secure Wi-Fi by using 802.11a (if supported by laptop's WiFi)

-end

Author: Evhen Tupis, Executive Director