DOD Wireless Policies and Requirements

Timothy J. Havighurst
V34, NSA

Policies DOD Deals With

- Global Information Grid Policy (Wired and Wireless)
- DOD Overarching Wireless Policy
- Pentagon Area Common Information Technology Wireless Security Policy
- FCC Policy
- Coalition Partner Country Policies

GIG Policy

- Not specific to wireless, but specific about Information Technology and Protection
- Carries the weight of law
- Gives specific roles to different DOD Agencies
- Brought DOD more in line with Intelligence Community and NSTISSP 11

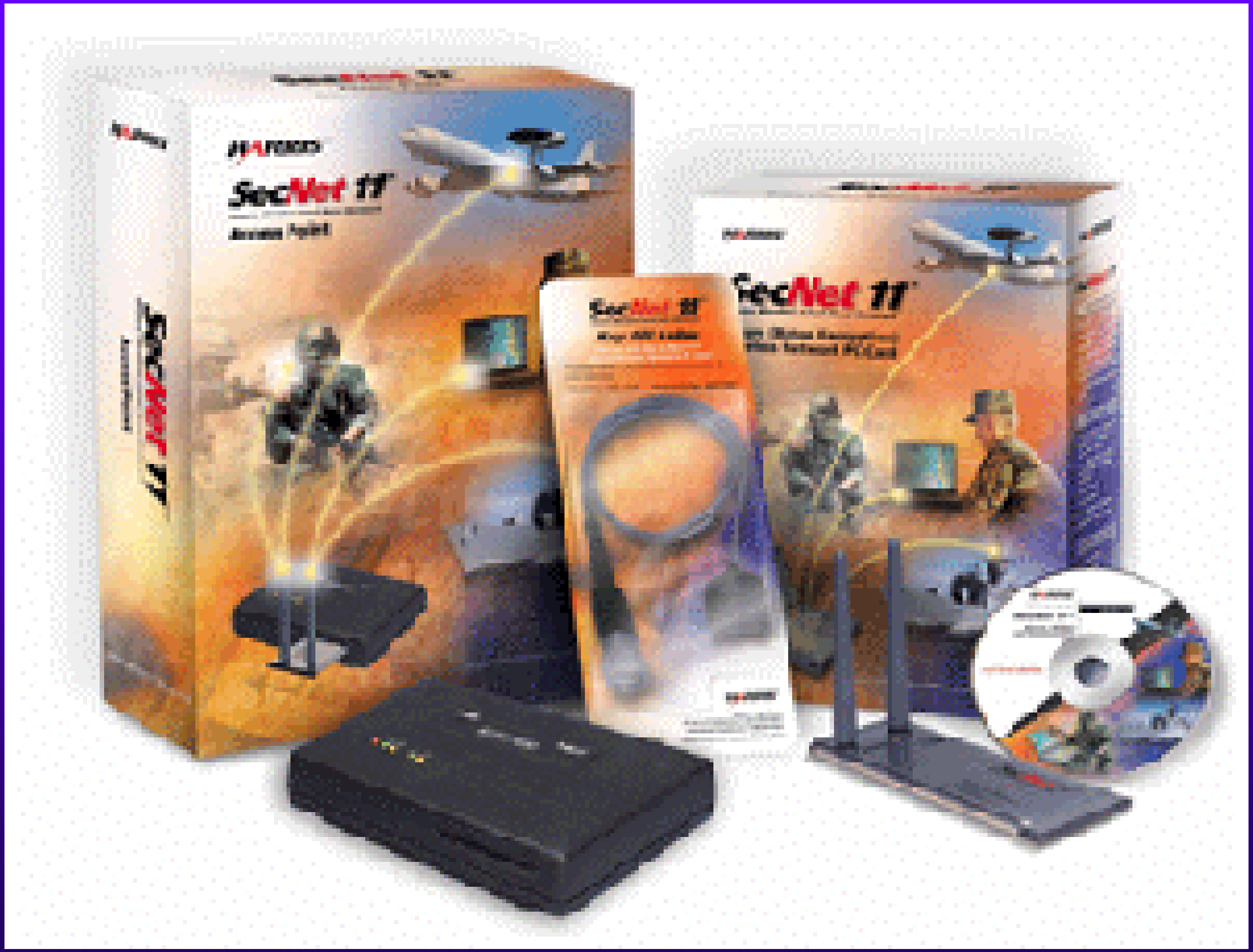
DOD Overarching Wireless Policy

- Written for the Designated Approval Authority (poor guy who has to worry about all these wireless products)
- Written for DAA who didn’t even know that he was buying a wireless product
  - 802.11
  - Bluetooth
  - IR
- In Review (SD-106) again

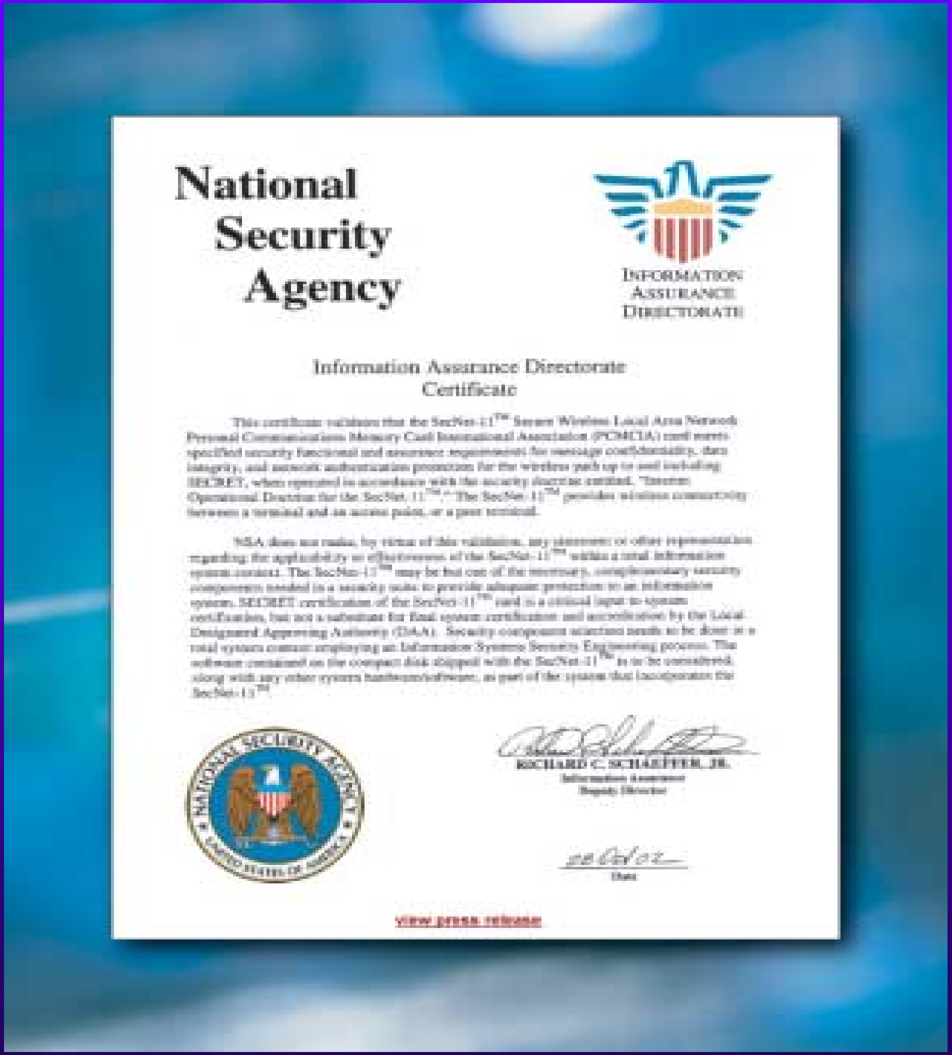
Classified? That’s Easy!

- SECRET and TOP SECRET data must be protected with a Type I algorithm
  - BATON
  - AES (sufficient key length)
  - SKIPJACK
- Must be NSA approved / certified

Type I Product



Certification Isn’t Easy



National
Security
Agency

INFORMATION
ASSURANCE
DIRECTORATE

Information Assurance Directorate
Certificate

This certificate validates that the SecNet-11™ Secure Wireless Local Area Network Personal Communications Memory Card International Association (PCMCIA) card meets specified security functional and assurance requirements for message confidentiality, data integrity, and network authentication protection for the wireless path up to and including SECRET, when operated in accordance with the security doctrine entitled, "Interim Operational Doctrine for the SecNet-11™." The SecNet-11™ provides wireless connectivity between a terminal and an access point, or a peer terminal.

NSA does not make, by virtue of this validation, any statement or other representation regarding the applicability or effectiveness of the SecNet-11™ within a total information system context. The SecNet-11™ may be but one of the necessary, complementary security components needed in a security suite to provide adequate protection to an information system. SECRET certification of the SecNet-11™ card is a critical input to system certification, but not a substitute for final system certification and accreditation by the Local Designated Approving Authority (DAA). Security component selection needs to be done in a total system context employing an Information Systems Security Engineering process. The software contained on the compact disk shipped with the SecNet-11™ is to be considered, along with any other system hardware/software, as part of the system that incorporates the SecNet-11™.

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

RICHARD C. SCHAEFFER, JR.
Information Assurance
Deputy Director

28 Oct 02
Date

view press release

SBU, FOUO? OOOOOH….

- What are you trying to protect?
  - Personnel Data
  - Logistics
  - Medical
  - Financial
- Who are you trying to protect it from
  - Hackers
  - Enemies

Better to Light a Candle…

- FIPS 140-1 or 2 MUST be used
- VPN? Traffic Protection?
- Accounting for products
- Unclassified in total?

Pentagon Wireless Policy

- Pentagon and any network that is interdependent of a Pentagon Network
- Moratorium placed on new wireless products
- NSA to produce a database for wireless vulnerabilities

Pentagon Wireless Policy (cont.)

- Does not apply to SCIFs (covered under DCID policy already)
- No connectivity to Classified networks

FCC

- Still beholdin’ to FCC
  - Can request waivers, and usually get them, but we have to coexist
- Must maintain separate rules for Wireless Products (WLANs are Class 3, Microwave lights are class 2….)
- Often neglected in the coverage maps of wireless products

Coalition Compliance

- Special Products may not be usable in foreign countries
  - Not just frequency
  - By design
  - By accident
- Products may have to be approved
  - Result could be confiscation of platform

Homeland Security

- Coalition Partners we never imagined
  - First Responders
  - ONS
  - Coast Guard
  - DOJ, DOT, DOS, DOWhatever
- Need to have a single, trusted thread from beginning to end

Brave New Government

- Much like the old Soviet model (but arrived at completely differently)
- Dependence on partners, vendors, local law enforcement
- Institutional awareness of vulnerabilities
- New emphasis on security
- Must keep pace with technology