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
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