AAMI IA Meeting
- Wireless Security
Introductions

Years of IT and IA Experience

Years Working with Medical

Certifications
BLUF: It’s All About Risk

“Operational Risk” ... Reality
Zero Risk ... Impossible
Some Risk ... Needed
Ignoring Risk ... Foolish
Allow or Avoid Too Much Risk ... Results in Mission Failure...
Wireless Security Challenges

1. FIPS 140-2 Requirements
2. DoD IA Requirements
   1. STIGS
   2. Scan Requirements
All About Defense in Depth

Difficult to meet every FIPS/DoD/AF Requirement on the device itself.

Layered Defenses – Layer 1: Network
- AES-256 CCMP Encryptions
- EAP-TLS Authentication
- Not broadcasting SSIDs
  - MAC Filtering
- Wireless network with WIPS, embedded firewalls, ACLs and isolation
- Secure enclave boundaries to not allow Internet browsing, etc.
All About Defense in Depth

Difficult to meet every FIPS/DoD/AF Requirement on the device itself.

Layered Defenses – Layer 2: Device
- Secure the Operating System
- An embedded firewall is NOT the only mitigating factor
- Clients need to be as bullet proof as possible so when connecting to the network the risk is mitigated or at a minimum reduced to an acceptable level
Challenges to Success

*How do We Get Past these Challenges?*

*Discussion*