



ato

AIR TRAFFIC ORGANIZATION

# PROPOSED FAA WIRELESS SYSTEM ARCHITECTURE

ACB-250 William J. Hughes Technical Center

Department of Transportation, Federal Aviation Administration

Atlantic City International Airport, NJ 08405

Anthony Stevens (609) 485 6527 [anthony.stevens@faa.gov](mailto:anthony.stevens@faa.gov)

David Ingegneri (609) 485 8197 [david.ingegneri@faa.gov](mailto:david.ingegneri@faa.gov)

Jamie Chappell (609) 582 5777 x18 [Jamie.CTR.Chappell@faa.gov](mailto:Jamie.CTR.Chappell@faa.gov)



a t o

AIR TRAFFIC ORGANIZATION

# WLAN Challenges

- 1) The FAA has not begun to implement Wireless LANs, but it will.
- 2) Window to architect future wireless systems, and ensure that security is in place.
- 3) Testing the wireless security characteristics.
- 4) Integrating wireless systems into the FAA's wired network infrastructure without impacting security.



# Current FAA Position on Wireless Networks

- The FAA has been operating under a Wireless Moratorium since February 2, 2004.
- The FAA Wireless Policy was signed February 3, 2005.
- A Wireless Waiver process has existed since the Moratorium, but the available guidance is geared toward filling out the Waiver, not in getting it approved.
- FAA Designated Approving Authorities (DAAs) are the final authority on approving wireless implementations.
- Currently there is no uniform process for Designing, Securing and Documenting Wireless Networks prior to submission to a DAA.



a t o

AIR TRAFFIC ORGANIZATION

# System Engineering

- Now is the time to provide a System Engineering approach to Wireless Networks Planning.
- Risks of not designing Wireless Networks from an Enterprise Perspective.
  1. Spectrum Congestion.
  2. Loss of Mobility of Users across the agency.
  3. Security Risk to Facility Wired Networks.
  4. Risk of Network Infection by existing FAA laptop users.



a t o

AIR TRAFFIC ORGANIZATION

# Risk Factor #1

## Spectrum

- Unlike wired networks, wireless networks have a finite bandwidth which must be shared. Wired networks can be enlarged by pulling more cable, upgrading to fiber, etc.
- If 2 adjacent business, departments, etc. establish wireless networks on the same channel. They will both operate, but at greatly reduced bandwidth.
- If every group in FAA Headquarters were to establish it's own wireless network without coordination, everyone's bandwidth would be greatly reduced.
- At the very least, wireless networks in each building need to be centrally managed.



a t o

AIR TRAFFIC ORGANIZATION

# Risk Factor #2

## Mobility of Users

- Government standards and policy mandate encryption that is certified to NIST FIPS 140-2. At this time, most FIPS certified solutions require software to be installed which replaces portions of the Microsoft OS.
- In our experience, once a solution is installed a second solution cannot be installed, and the first solution cannot be removed.
- What does this mean? Let's say that FAA Headquarters (HQ) deploys Vendor #1 and the FAA Technical Center (TC) deploys Vendor #2. An HQ employee that brings their laptop to the TC will not be able to use the TC Wireless network. The HQ laptop cannot have the driver for Vendor #2 installed without reinstalling the Operating System.
- The Agency needs to choose a single encryption solution to ensure user mobility!



a t o

AIR TRAFFIC ORGANIZATION

# Risk Factor #3 Security of Facility Networks

- Despite the Moratorium, unauthorized Wireless Access Points (Rogues) are connected to FAA networks.
- Every laptop with built-in wireless has the capability to be used as a bridge into the wired network.
- Uniform standards for detecting and shutting down wireless devices in FAA buildings need to be developed.



a t o

AIR TRAFFIC ORGANIZATION

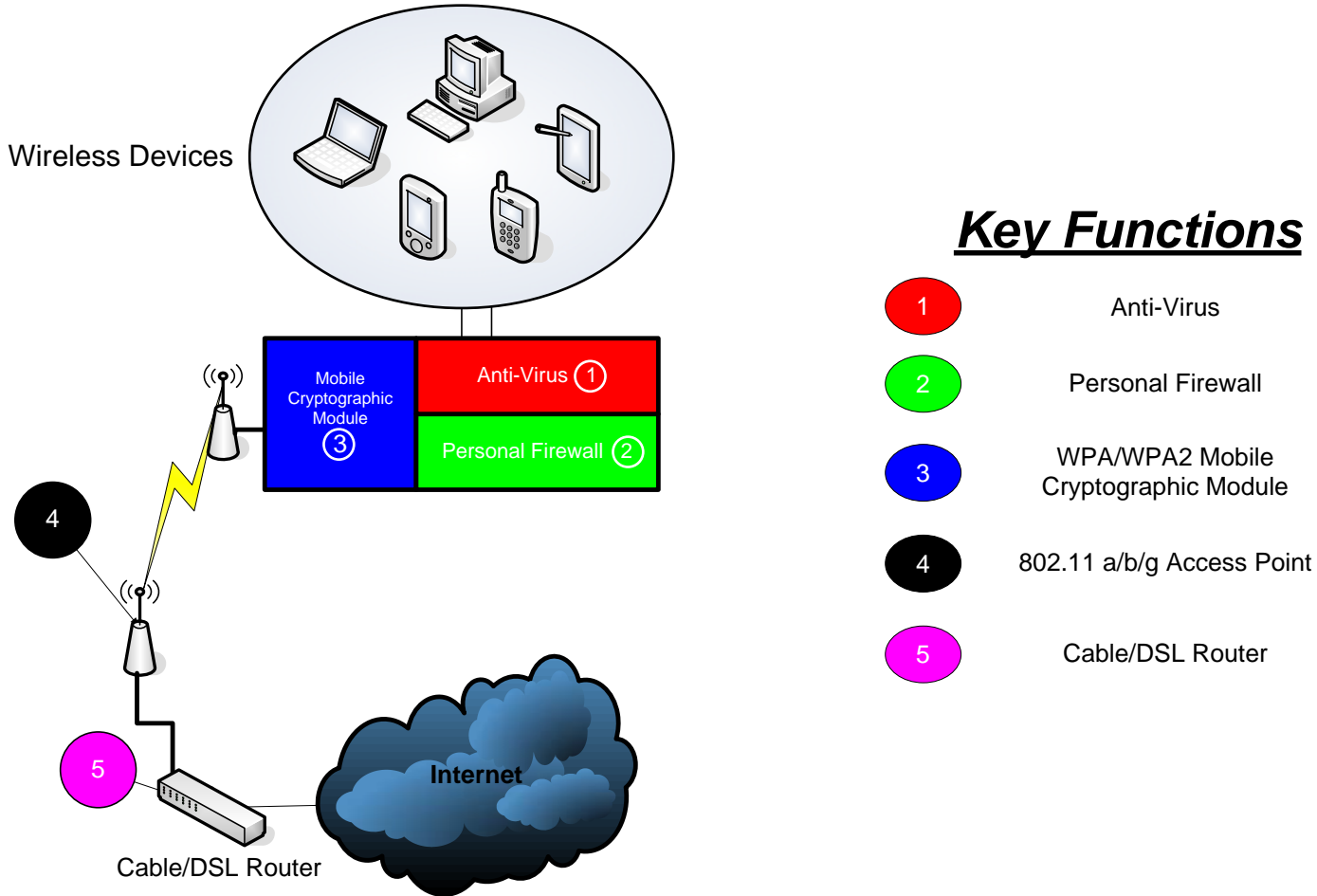
# Risk Factor #4

## Infection by FAA laptops

- Many FAA employees and contractors have portable devices.
- Many of these devices have wireless capability.
- Traveling FAA employees use wired and wireless services at hotels, hotspots, etc.
- Upon return to the FAA network, these devices are not flagged as “Mobile” devices and no special scans are performed.



# Typical Small Office/Home Office Wireless (SOHO) Network



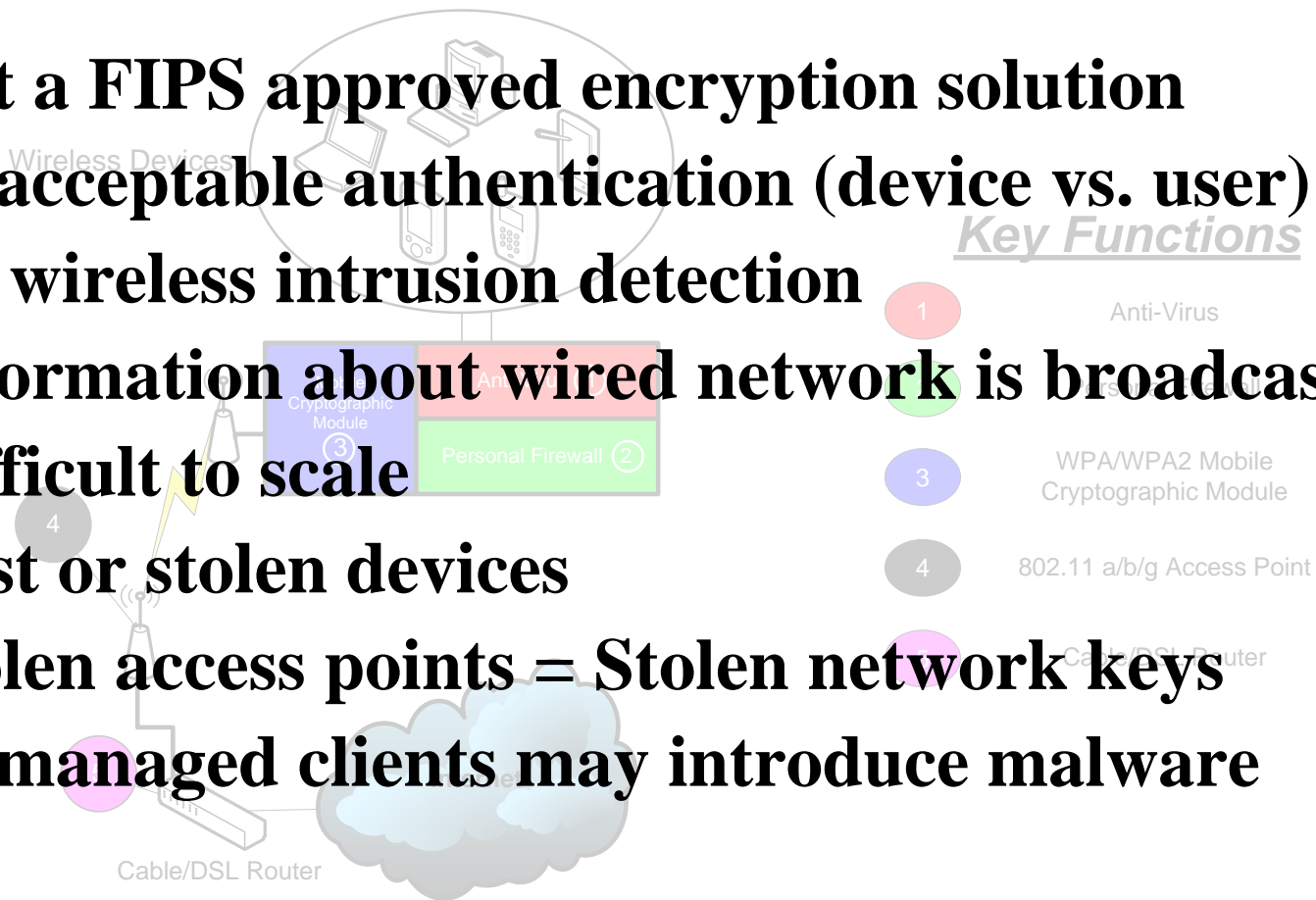


a t o

AIR TRAFFIC ORGANIZATION

# Limitations of SOHO Style Wireless Network

- ➔ Not a FIPS approved encryption solution
- ➔ Unacceptable authentication (device vs. user)
- ➔ No wireless intrusion detection
- ➔ Information about wired network is broadcast
- ➔ Difficult to scale
- ➔ Lost or stolen devices
- ➔ Stolen access points = Stolen network keys
- ➔ Unmanaged clients may introduce malware



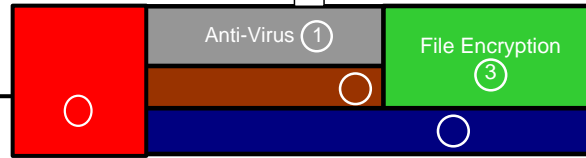
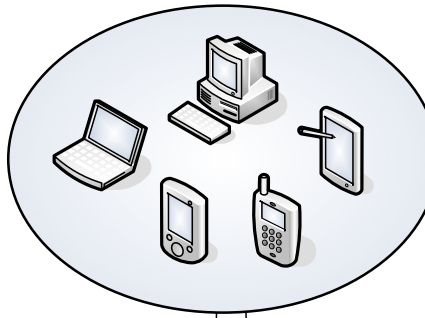


ato

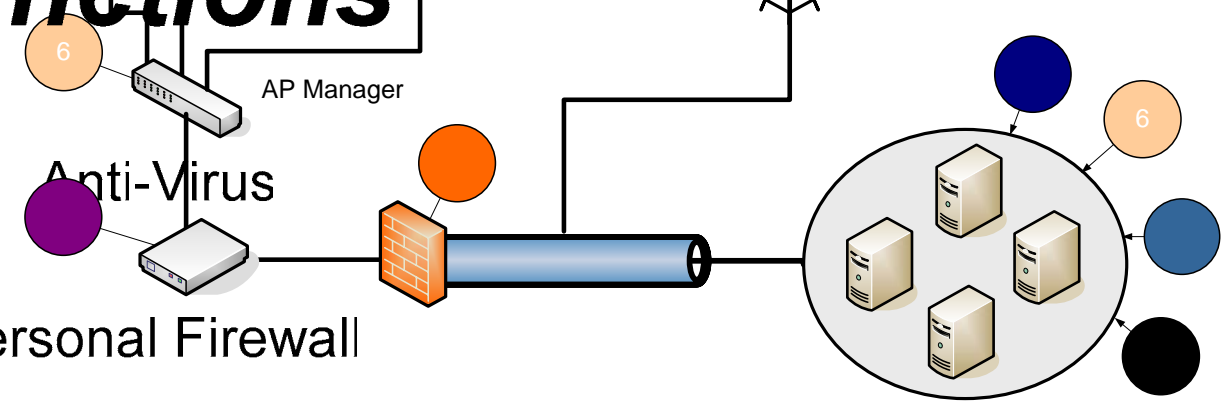
AIR TRAFFIC ORGANIZATION

# Proposed FAA Wireless System Architecture

Wireless Devices



## Key Functions



Personal Firewall

File Encryption



ato

AIR TRAFFIC ORGANIZATION

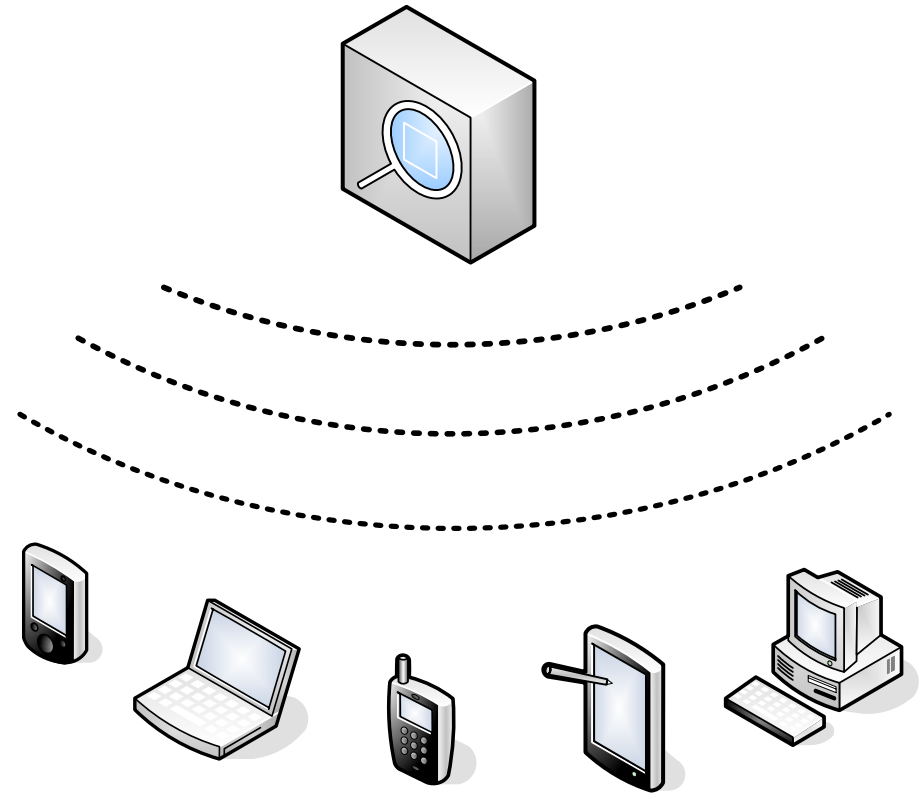
# Anti-Virus

## Problem:

- Mobile devices may roam to unprotected and/or unmonitored networks

## Solution:

- Ensure that mobile devices do not infect the network assets by using proven anti-virus software
- Ensure that the devices are running the proper anti-virus software through the use of policy management software





ato

AIR TRAFFIC ORGANIZATION

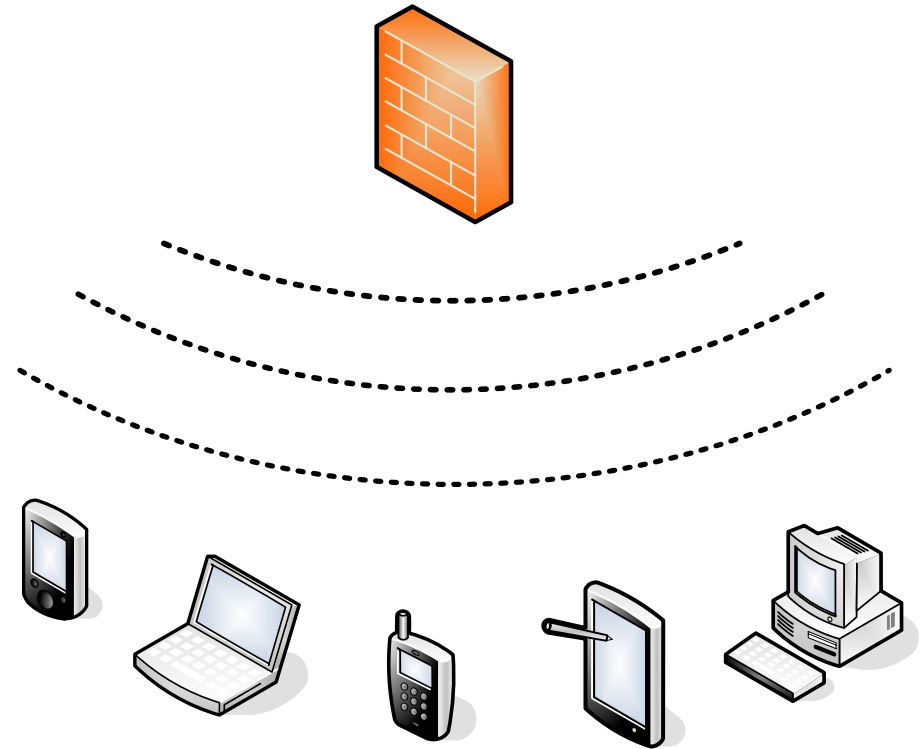
# Personal Firewall

## Problem:

- Mobile device(s) may roam to unprotected and/or unmonitored networks

## Solution:

- Ensure that the mobile devices do not become targets for network-based attacks, e.g. worms, hackers, etc by implementing proven personal firewall protection software
- Ensure that the devices are running the proper personal firewall protection software through policy management





ato

AIR TRAFFIC ORGANIZATION

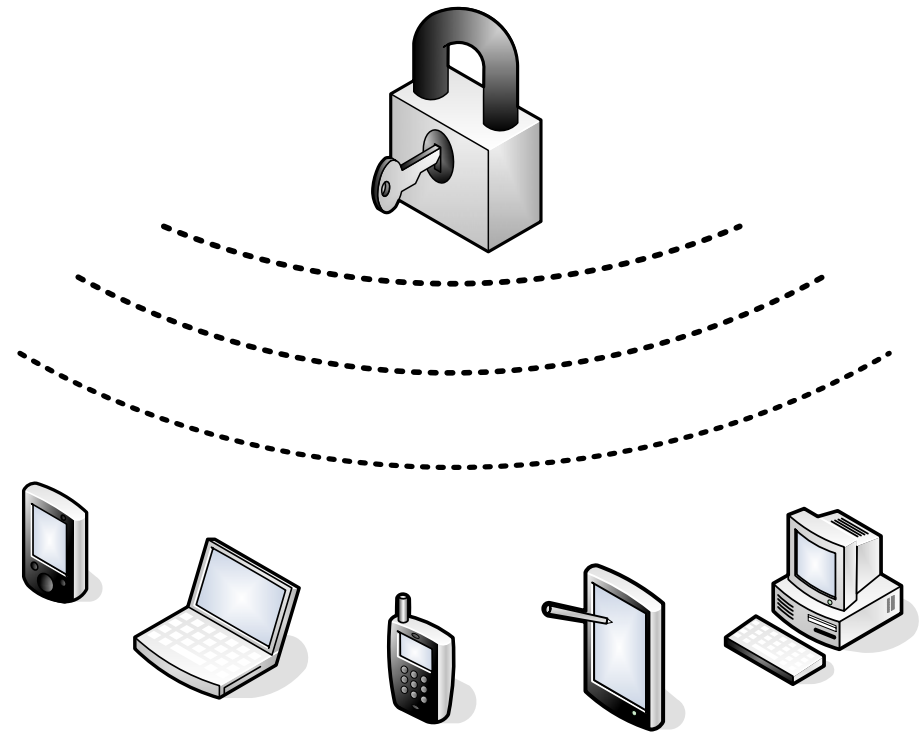
# File Storage Encryption

## Problem:

- Mobile devices may be lost or stolen resulting in disclosure of sensitive data

## Solution:

- Implement proper file/folder encryption to ensure data confidentiality
- Ensure that file storage encryption mechanism uses approved cryptographic modules, e.g. FIPS 140-2
- Ensure that the devices are running the proper file storage encryption software through the use of policy management software



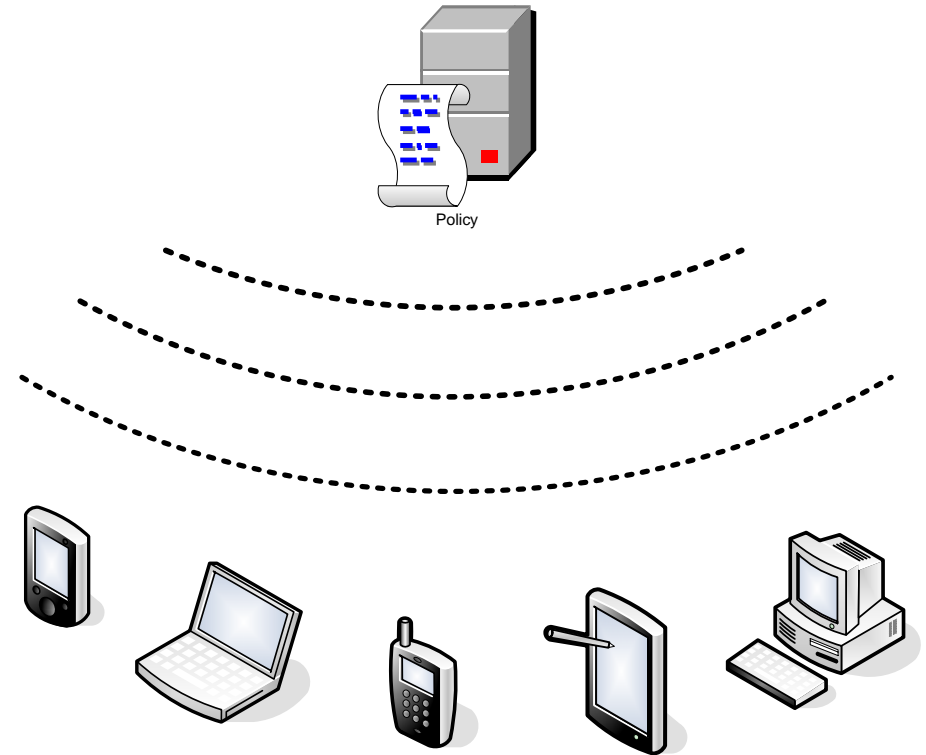


ato

AIR TRAFFIC ORGANIZATION

# Policy Management

- Controls features of mobile clients (Anti-Virus, File Encryption, etc.)
- Manage and publish policy changes through a central policy server.
- Allows for special scans of Mobile devices
- Manages and Controls Access between Wired and Wireless Networks:
  - Allowable Ports, Applications
  - Devices, Traffic, Bandwidth





ato

AIR TRAFFIC ORGANIZATION

# Radio Function

## Problem:

- What are the user's requirements?
- Conventional 802.11 is not the only option.
  - 802.11a/b/g vs. Cellular
  - Public spectrum vs. custom radios using FAA controlled spectrum.
  - Small vs. Enterprise

## Solution:

- Bandwidth, Cost/Benefit, Range, Spectrum, resistance to jamming, and security must all be factors in the decision making process
- Ensure that the spectrum chosen leaves enough overhead for security
- Physical security of the radios must be considered if the radio stores cryptographic keys





ato

AIR TRAFFIC ORGANIZATION

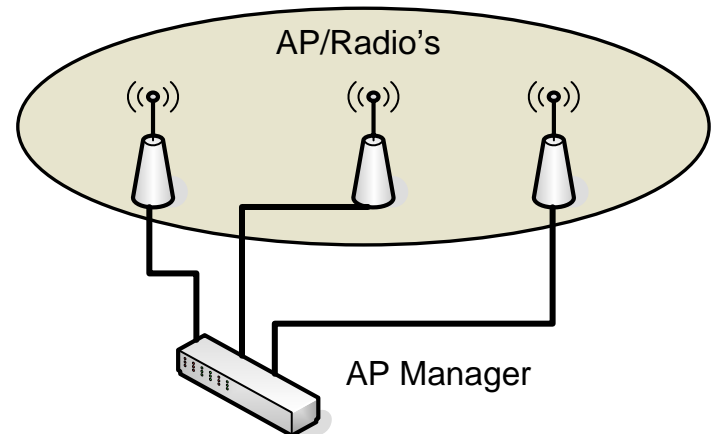
# Radio Management

## Problem:

- An 802.11b access point has a functional range of up to 300 ft. Good for small applications.
- In a large facility, dozens of access points may be required. Adjacent APs must be on non-overlapping frequencies.

## Solution:

- Enterprise Access Point Systems
  - “Light” access points – Simpler, less expensive radios. No Crypto Keys stored locally.
  - Controller is locked in a LAN closet and can handle many Light APs.
  - Central management of APs, Channel selection, automatic power adjustment.





ato

AIR TRAFFIC ORGANIZATION

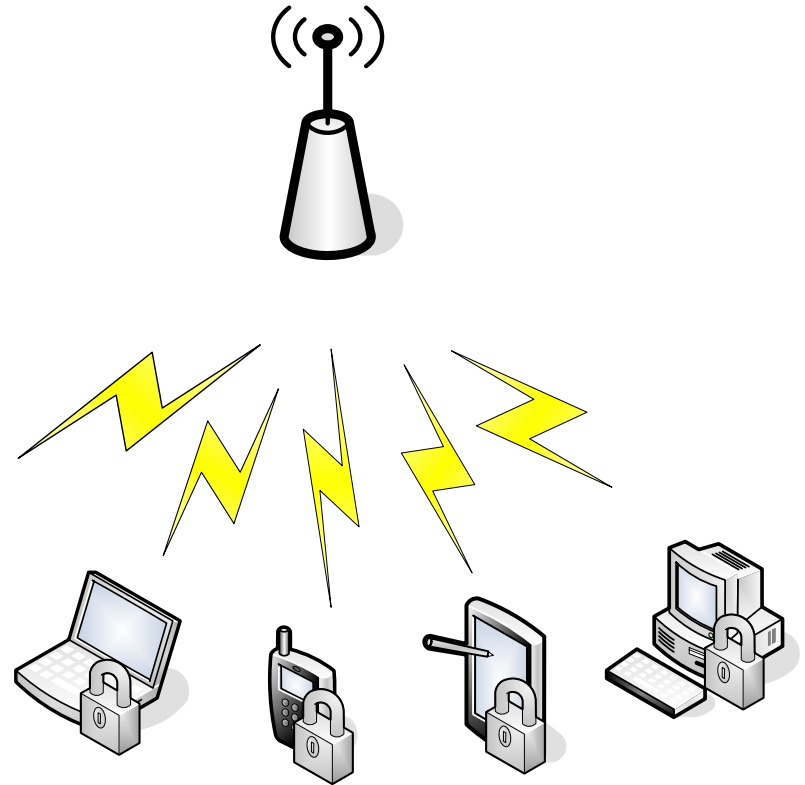
# Mobile Cryptographic Module

## Problems:

- Every packet send wirelessly needs to be secured!
- FIPS 140-2 approved cryptographic modules are required.
- Mixing vendors could effect mobility.

## Solution:

- Purchase FIPS 140-2 certified hardware/software and ensure that the clients are certified.
- Standardize upon the mobile cryptographic modules.





ato

AIR TRAFFIC ORGANIZATION

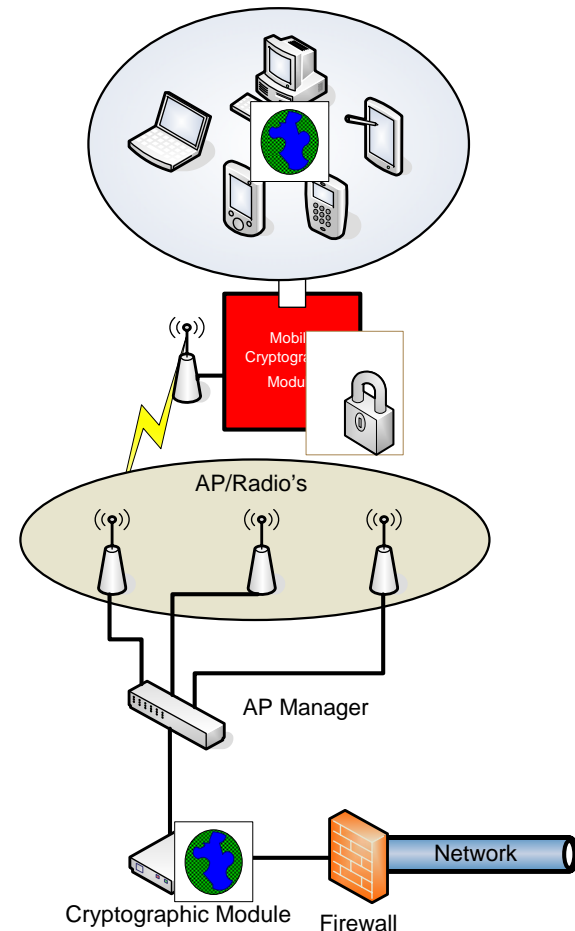
# AP/Wired –Side Encryption/Decryption

## Problems:

- Every packet sent wirelessly needs to be secured!
- FIPS 140-2 approved cryptographic modules are required.
- Most SOHO APs don't have the processing power for the required AES-128 Encryption.

## Solutions:

- Today, all FIPS approved solutions are Gateway devices added behind Access Points – adds to cost.
- In the future, APs may perform this function.





a t o

AIR TRAFFIC ORGANIZATION

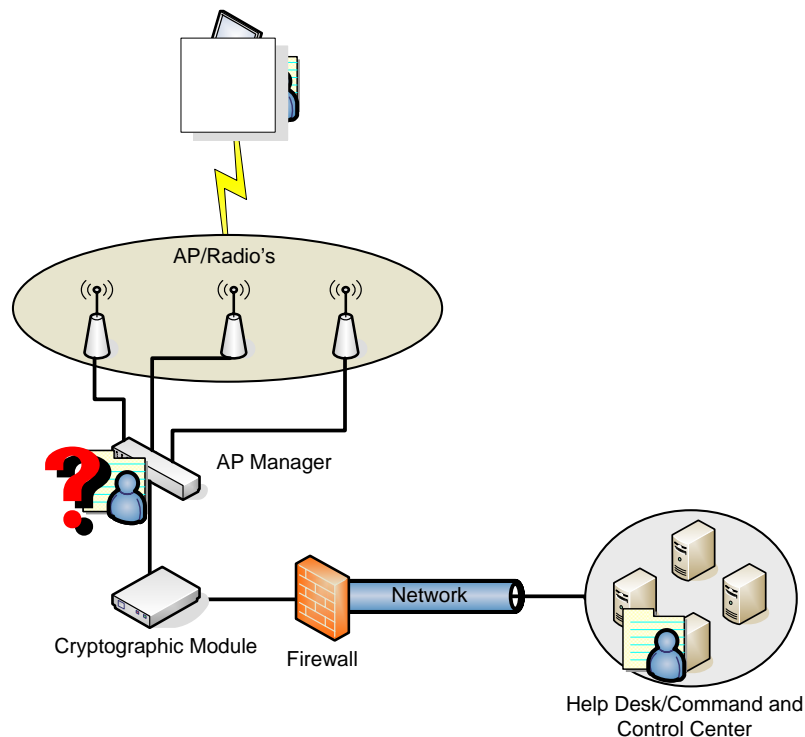
# Authentication, Authorization, and Accounting

## Problem:

- How do you authenticate wireless users? How do you keep out unauthorized users?

## Solution:

- Unlike wired networks, all wireless users must authenticate.
- A new user/password database could be created for wireless users. It is better to leverage or merge existing user databases (badge, email, network resources)
- E-Authentication – Presidential Directive HSPD-12 – Oct. 2005





a t o

AIR TRAFFIC ORGANIZATION

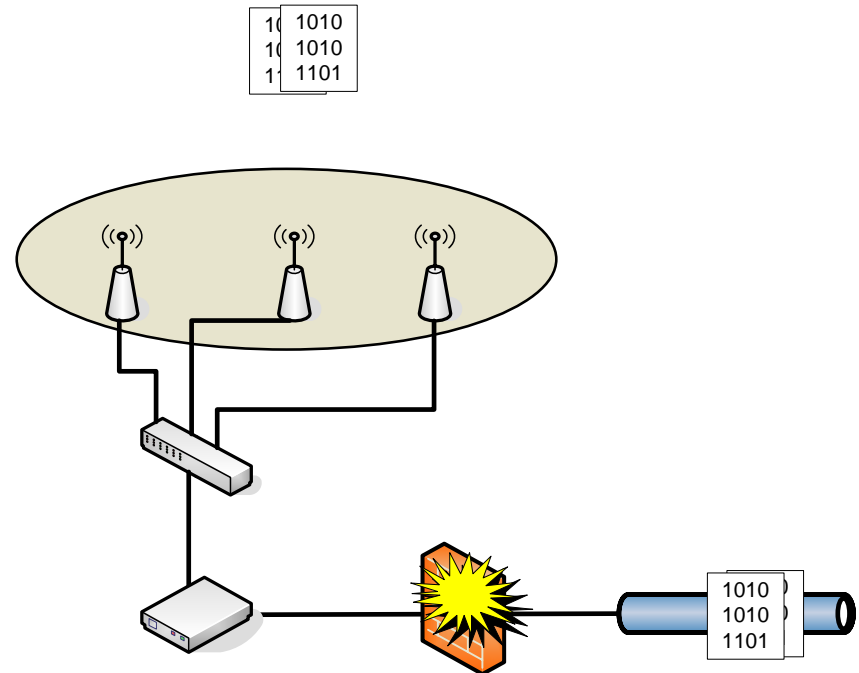
# Firewall

## Problem:

- Packets from the wireless-side need to be inspected before entering the protected wired-side network
- We can't allow packets not destined for wireless users to leak to radios

## Solution:

- Use a firewall to filter unauthorized traffic between the wired and wireless network segments.





ato

AIR TRAFFIC ORGANIZATION

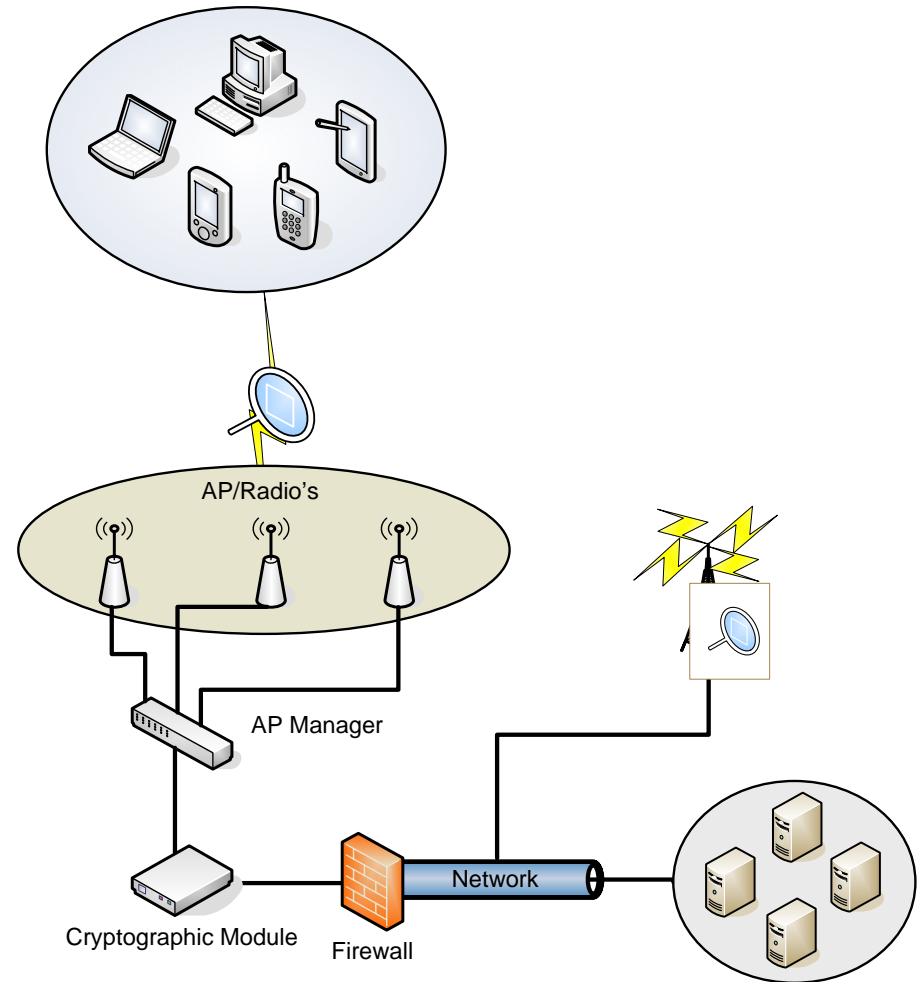
# Intrusion Detection / Security Monitor

## Problems:

- Need to monitor the spectrum for intruders and other unauthorized wireless devices, e.g. Rogue APs
- Need to monitor trusted users to ensure they are operating securely

## Solutions:

- Scan and monitor the wireless spectrum using Wireless Intrusion Detection systems
- Intrusion Prevention systems are coming.



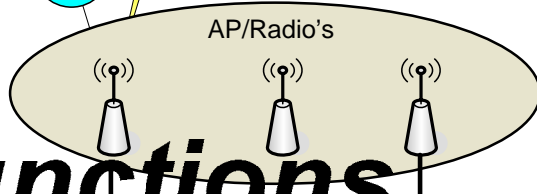
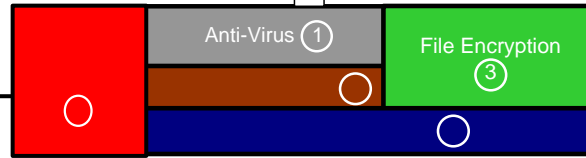
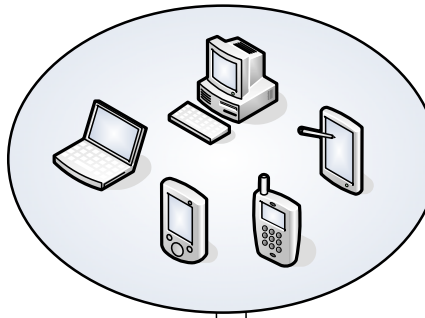


ato

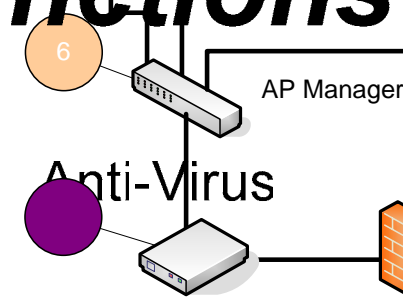
AIR TRAFFIC ORGANIZATION

# Proposed FAA Wireless System Architecture

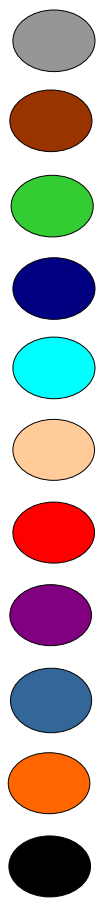
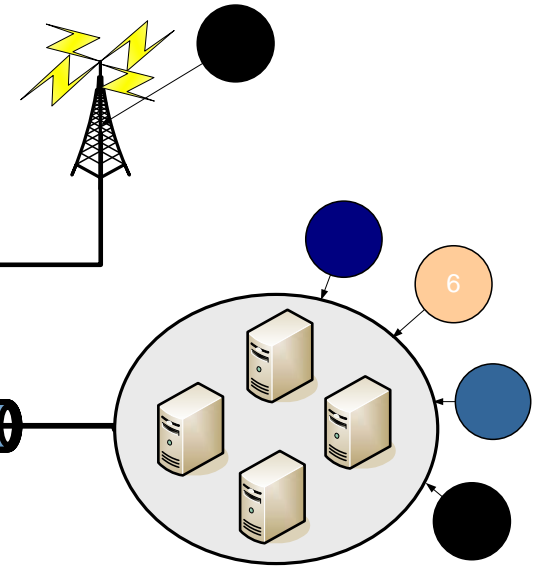
Wireless Devices



## Key Functions



Personal Firewall



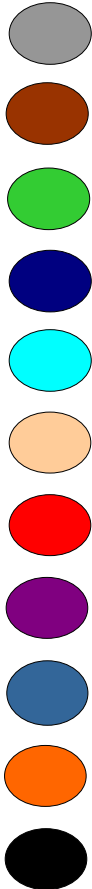
File Encryption



ato

AIR TRAFFIC ORGANIZATION

# THE PROCESS FOR DEVELOPING WIRELESS REQUIREMENTS



1. In designing a system to meet a specific FAA need, all 11 of these elements must be captured in the final system.

## *Key Functions*

2. This does not mean purchasing 11 systems. Many COTS systems are capable of meeting several of these functions.

Anti-Virus

Personal Firewall

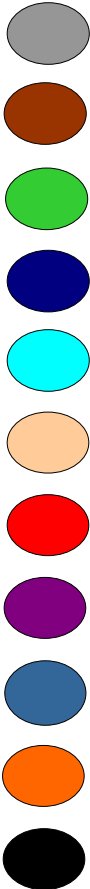
File Encryption



ato

AIR TRAFFIC ORGANIZATION

# THE PROCESS FOR DEVELOPING WIRELESS REQUIREMENTS



## Key Functions

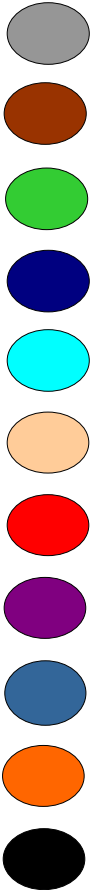
3. All of the requirements from NIST/DOT/FAA high-level policies apply to wireless networks.
4. 802.11 Wireless networking is an extension of 802.3 ethernet wired networking. The FAA has extensive experience with building **Anti-Virus** wired networking.
5. Wireless networking requires a **Personal Firewall** more rigorous application of existing security practices.  
**File Encryption**



a t o

AIR TRAFFIC ORGANIZATION

# THE PROCESS FOR DEVELOPING WIRELESS REQUIREMENTS



- 6. Further work is required to verify that existing COTS systems are suitable for FAA use.

## *Key Functions*

- 7. Once a preliminary designed is complete, a Security Certification and Authorization Package (SCAP) must be prepared.

File Encryption



ato

AIR TRAFFIC ORGANIZATION

# Questions?

