

Enabling a Secure Mobile Environment for the State of Illinois



GOVERNMENT PUSHING THE MOBILE FRONTIER



SPACE PROGRAM



LAW ENFORCEMENT



LAW ENFORCEMENT



MILITARY



FUTURE CAPABILITIES



FUTURE CAPABILITIES



FUTURE CAPABILITIES



MOBILE APPLICATIONS



Photo by Sean Gallup/Getty Images

MOBILE APPLICATIONS



Photo by Rick Garrison/Getty Images

MOBILE APPLICATIONS



MOBILE APPLICATIONS



MOBILE APPLICATIONS



MOBILE APPLICATIONS



MOBILE APPLICATIONS



MOBILE APPLICATIONS

The image displays two side-by-side screenshots of the FCC Broadband.gov mobile application. Both screens show the same basic layout with different content.

Top Bar: Shows signal strength (AT&T), Wi-Fi icon, battery level (55% or 57%), and time (8:43 PM or 8:40 PM).

Header: FCC Federal Communications Commission logo and BROADBAND.GOV BETA logo.

Left Screen (Test Mode):

- Section Title:** Mobile Broadband Test In Progress...
- Download Speed:** 3.01 Mbps (yellow bar)
- Upload Speed:** 0.50 Mbps (green bar)
- Latency:** 0 ms (grey bar)
- Icons:** Home, Network, and Globe.

Bottom Navigation: Test, Settings, Results, About.

Right Screen (Results View):

- Section Title:** Results
- Table:** A list of test results with columns for Date/Time, Download Speed (Mbps), Upload Speed (Mbps), and Latency (ms). Each row includes a 'Details' icon (orange arrow).

Date/Time	Download Speed (Mbps)	Upload Speed (Mbps)	Latency (ms)
3/11/10 8:40 PM	0.90	0.31	>
3/11/10 8:39 PM	0.30	0.34	>
3/11/10 8:38 PM	4.90	3.62	>
3/11/10 8:38 PM	4.70	3.63	>
3/11/10 8:37 PM	1.01	0.23	>
3/11/10 8:35 PM	2.15	0.12	>
3/11/10 5:05 PM	0.21	0.01	>

Bottom Navigation: Test, Settings, Results, About.

ILLINOIS – MOBILE FRONTIER



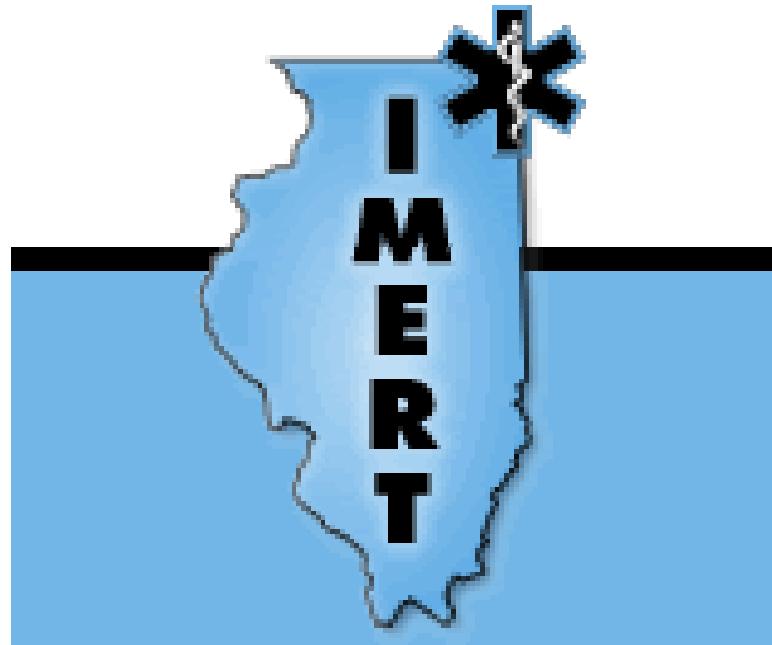
ILLINOIS – MOBILE FRONTIER



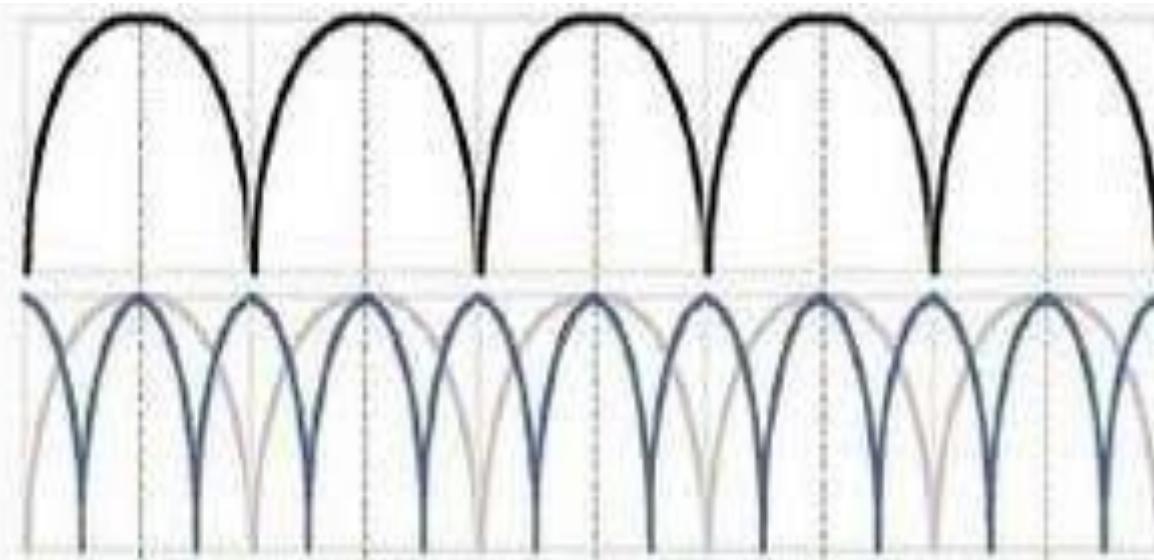
Illinois Terrorism Task Force



ILLINOIS – MOBILE FRONTIER



ILLINOIS – MOBILE FRONTIER



Legacy
25KHz
Channels

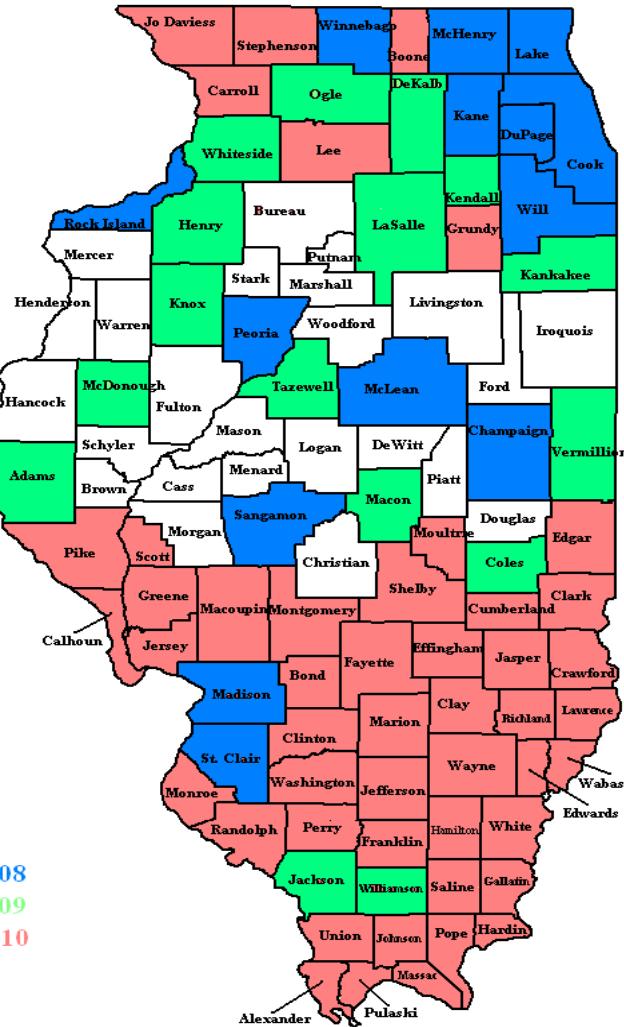
Narrowband
12.5KHz
Channels
Phase1

All 25 KHz
systems
MUST
be 12.5 KHz
systems by
Jan 1st,
2013

ILLINOIS – MOBILE FRONTIER



ILLINOIS – MOBILE FRONTIER



MOBILE SECURITY IS DATA SECURITY



DATA IS EVERYWHERE

data

standard deviation median
hypothesis test
normal distribution histogram pie chart response
confidence interval mean
scatterplot variability explanatory

MOBILE MALWARE

Malware Goes Mobile

The acceleration of mobile threats

It will take 2 years for mobile threats to do what PC threats evolved to in 15 years.



* Source: Lookout Mobile Security Data
** Source: Mary Meeker Report, September 2010

@lookout

facebook.com/mylookout

mylookout.com

lookoutTM
MOBILE SECURITY

A NEW MODEL FOR MOBILE RESILIENCY



MOBILE SECURITY CONCERNS

- Lost/stolen devices
- Penetration of our corporate Wi-Fi networks
- Mobile malware on applications from public app stores
- Users forwarding corporate information to cloud-based storage services
- Security at public hotspots
- Users forwarding email to personal accounts
- Interception of over-the-air transmissions
- Malware exploiting vulnerabilities on internally developed mobile apps
- Devices jailbroken or rooted by end users
- Penetration of users' home Wi-Fi networks

MOBILE POLICIES

- 62% organizations allow personal devices at work,
- IT's juggling laptop policies and Wi-Fi policies and BYOD policies
- 80%, require only passwords for mobile devices that access enterprise data/networks
- 14% require hardware encryption
- 40% of organizations limit the range of devices supported and require that users connect them with an MDM system.

SECURING DATA IN TRANSIT

- VPN secure tunnel
- Secure HTTP
- BlackBerry secure email
- Virtual desktop (e.g., VMware, Citrix)
- Other secure email
- MDM technology

AUTHENTICATION MECHANISMS

- User name/password
- Power-on device password
- On-device certificates
- Secure token
- Image or pattern
- Biometrics
- Cellular call-back verification (e.g., PhoneFactor)
- Facial recognition
- Grid card (e.g., Entrust IdentityGuard)

AUTHENTICATION MECHANISMS

- Securing the data residing on mobile devices
- Securing data in transit from the network to mobile devices
- Securing the network perimeter
- Securing devices themselves using antivirus/anti-malware, MDM client software, etc.
- Preventing phone/SMS fraud

MOBILE SECURITY AWARENESS



PREPAREDNESS



MOBILE PREPAREDNESS ASSESSMENT

- Business and technical requirements analysis
 - Review of your existing wireless LAN architecture
 - Review of your existing RF design
 - Wireless LAN configuration review
 - Gap analysis and recommendations

WIRELESS CONFIGURATION REVIEW

- Wireless LAN security
- Quality of service
- Wireless multicast
- RF planning
- Client mobility
- High availability

MOBILE SECURITY “ART OF WAR”

“IF YOU TRULY KNOW THE ENEMY AND YOURSELF, YOU NEED NOT FEAR THE RESULT OF A HUNDRED BATTLES. IF YOU KNOW YOURSELF BUT NOT THE ENEMY, FOR EVERY VICTORY GAINED YOU WILL ALSO SUFFER A DEFEAT. IF YOU KNOW NEITHER THE ENEMY NOR YOURSELF, YOU SHALL SUCCUMB IN EVERY BATTLE.”

~ SUN TZU, THE ART OF WAR