Course ID
**WNETSEC**
Course Duration
**5 days**

Course Title

# Wireless Communications, Networking, and Security for US Federal Government Personnel

## Related Courses

- 5G Wireless: State-of-the-art of Research, Policy, and Standards (5GCOMP, 4 days)
- 5G Wireless: A Fast-Paced Tutorial (5GTUTE, 1 day)
- 5G Wireless: Federal and Defense Applications and Implications (5GSEC, 1 day)
- LTE: A Comprehensive Tutorial (LTE-CT, 3 days)
- LTE: A Comprehensive Three Day Course (LTE-C3DC, 3 days)
- WIMAX: A Comprehensive Three Day Course (WIMAX-C3DC, 3 days)
- Cyber Security and Cyber Warfare (CYBERSEC, 2 days)
- Cyber Space and Cyber Conflict Policy (CYBERPOL, 2 days)

## Aimed At

This course is aimed at the Government personnel in national security and telecommunications policy space.

## Group Size

5-25

## Prerequisites

Those wishing to take this course should have a basic knowledge of telecommunications and exposure to national security and/or policy issues.

## Course in a Nutshell

This is a comprehensive course on telecommunications, with focus on 4G/5G wireless technologies, aimed at the specific needs of US government personnel. This course seeks to build up the participants' understanding of the 5G/4G technologies starting with a discussion of the underlying telecommunications technologies, with the national security and/or policy issues serving as the backdrop.

## Customize It!

We can customize this course at little to no additional cost to your own issues and concerns, whether related to defense, homeland security, or telecommunications policy. The "tech-level" of the course can be raised or lowered to meet the needs of the participants. Variations and subsets of this course, focusing on security, policy, or other concerns are also available.

**Course Outline**

## Day 1 – Software Defined and Cognitive Radio

- Software Defined Radio
  - Radio Architectures
  - Reconfigurable Embedded Processing
  - Hardware/Software Architectures
  - Signal Processing
  - Protocol Processing
  - Research Challenges: Latency, Scalability, Management
- Cognitive Radio
  - Planning Algorithms
  - Machine Learning
  - Policy Radios
  - Learning Radios
  - Radio Parameter Optimization
  - Spectrum Sensing
  - Dynamic Spectrum Access
- Emerging Spectrum Policy
  - TV Whitespace
  - National Broadband Plan
  - Role of Spectrum Sharing

## Day 2 – Emerging Communications Technologies

- RF Channel Models
  - Fading
  - Mobility
  - Link Budgets
- Orthogonal Frequency Division Multiplexing (OFDM)
  - Time-Frequency Diversity
  - Frequency-Domain Modulations
  - OFDM Basics
  - Multiple Access Protocols
  - Performance Analysis
- Multiple Input Multiple Output (MIMO)
  - Spatial Diversity
  - Beamforming
  - Spatial Multiplexing
  - Space-Time Coding

## Day 3 – Cellular/Broadband Standards and Protocols

- Cellular Technology History
  - 1G AMPS
  - 2G GSM/EDGE/IS-95

    - 2G CDMA/1xRTT
- 3G Cellular Technologies
    - 3GPP UMTS
    - 3GPP HSPA/HSPA+
    - 3GPP2 CDMA2000
    - 3GPP2 EV-DO
- IEEE Broadband Standards
    - IEEE 802.11 (WiFi)
    - IEEE 802.16 (WiMAX)
    - IEEE 802.22 (WRAN)
- 4G Cellular Technologies
    - 3GPP Long Term Evolution (LTE)
    - 3GPP LTE Advanced
    - IEEE 802.16m (WiMAX2)
- 5G Technologies
    - Femtocells
    - Cognitive Radio
    - Dynamic Spectrum Access

**Day 4 – Wireless Networking Security**

- IEEE 802.11 Security
    - Wired Equivalency Protocol (WEP)
    - Cryptographic and Protocol Attacks
    - IEEE 802.11i (WPA/WPA2)
    - Extensible Authentication Protocol (EAP)
- Cellular Network Security Architectures
    - Subscriber Identity Modules (SIMs)
    - Authentication and Roaming
    - Authorization and Accounting
    - Core Network Security
- Physical-Layer Security
    - RF Jamming Threats
    - Intelligent Jamming
    - Network-Layer Jamming
    - Next-Generation Electronic Warfare

**Day 5 – Emerging Mobile Security**

- Changing Threat Model
    - Emergence of Smartphones
    - Military Applications of Smartphone Technologies
    - Threats against Smartphones
    - Mobile Applications

- Handset Security Challenges
    - Hardware Security
    - Operating System and Kernel Security (Linux)
    - Mobile Distribution Security (Android, iOS)
    - Mobile Application Security
- Network Security Challenges
    - Mobile Device Management (MDM)
    - Provisioning and Accounting
    - Hardened App Stores
- Evolving DoD Policies
    - Management of MDM
    - Mobile Virtual Network Operators (MVNOs)
    - Hardened COTS/GOTS Handset Programs
    - DoD and Federal Mobility Strategies

Course Wrap-up

- Course Recap and Q/A
- Evaluations

## How You Will Learn

- A highly qualified instructor will present this course in interactive lecture format.
- Along with the lecture, we will use discussion and group activities to enrich the instruction and drive home the essential points.
- If you already know something about the technology, we will build on that. We'll compare and contrast what's familiar with what's new, making the new ideas easier to learn as well as more relevant.
- If your background is less technical, we will use meaningful and ingenious examples and analogies to simplify the complex subject matter.
- You will receive a printed Participant Handbook which will help you remember and retain what you learned in class and apply it on your job.

*Revised* *2Pr-f*