

# ***Public Safety Communications Security Briefing***

***June 2001***

## **USING MODIFIED TWO-WAY RADIO EQUIPMENT, ACCESS HAS BEEN GAINED TO PUBLIC SAFETY RADIO SYSTEMS, FABRICATING CALLS AND CAUSING CONFUSION**

Recently the following items were posted on the Internet:

- In Omaha, Nebraska, a radio hacker broadcasted a rock song for two minutes over a police radio, interfering with officers activities to negotiate with a man who was attempting suicide. (February 3, 2001)
- In Burnsville, Minneapolis, a ham radio operator had broadcast misleading information on police, fire and ambulance radios for almost two years by using personal two-way radio equipment. (February 6, 2001)

**RISK: If criminals have two-way access to public safety radio channels, they could listen to police activities and transmit false information on police channels thus interfering with or impeding law enforcement activities**

## **THE TECHNOLOGY TO INTERCEPT PUBLIC SAFETY COMMUNICATIONS IS READILY AVAILABLE TO THE GENERAL PUBLIC**

- An active group of scanner enthusiasts in the Washington, DC, area operates an internet site to further their hobby
- Recently the following items were posted on this site:
  - Highly detailed logs of Covert Drug Operations in the Washington, D.C.
  - Logs of the comings and goings of presidential aircraft at Andrews AFB
  - Complete listings of radio frequencies used by law enforcement and type of activities occurred on these frequencies

**RISK: Clear communications can be monitored not only by scanner enthusiasts as a hobby but also by criminals, potentially jeopardizing the safety of our public safety officials**

## **CRIMINALS CAN MONITOR UNENCRYPTED POLICE RADIO BROADCASTS AND USE THE INFORMATION TO ESCAPE FROM OR AMBUSH RESPONDING OFFICERS**

### **THE PLAIN DEALER**

#### **Considers Adding Encryption To Radio Systems** The Plain Dealer, January 28, 1999

The report of a burglary on Bainbridge Rd. crackled out over the police scanners. Bainbridge Township officers started scrambling. So did the would-be thieves. Carrying portable scanners, the two suspects heard the broadcast over the air and fled. If a patrol car had not been just half a block away, Bainbridge Police Chief James Jimison said, the suspects would have escaped...[further] if criminals could listen to police radio broadcasts, they could escape or, even worse, wait and ambush his officers.

**In Ohio, burglars used scanners to break into a home, monitored police communications, and planned their escape just before officers arrived.**

**RISK: Clear communications are being monitored by criminals and can be used to counter public safety responses**

## **HACKERS ATTACKS ON GOVERNMENT COMPUTER SYSTEMS ENDANGER INTERCONNECTED RADIO SYSTEMS**

### **BUSINESS WIRE**

#### **Hacker Disrupts Service At Airport Business Wire, March 19, 1998**

At approximately 9:00 a.m., [a] juvenile computer hacker intentionally, and without authorization, accessed the [phone] system servicing the Worcester Airport...Public health and safety were threatened by the outage which resulted in the loss of telephone service [to the] FAA tower at the Worcester Airport, to the Worcester Airport Fire Department, and to other related concerns such as airport security, the weather service, and various private airfreight companies.

Further, as a result of the outage, both the main radio transmitter ... and a circuit which enables aircraft to send a signal to activate the runway lights on approach were not operational for this same period of time.

In Massachusetts, an attack on the phone system at the Worcester Airport caused communications outage and affected all interconnected systems, including the radio system

**RISK: Interconnected systems can be more vulnerable without proper protection because when one part of the system is compromised, the rest of the system can be affected**

## **ATTACKS ON PHYSICAL INFRASTRUCTURE CAN WEAKEN THE MAIN NODES IN A PUBLIC SAFETY RADIO NETWORK**

In Scott County, Iowa, vandals severed a 295-foot tower using a hacksaw.

The fallen tower caused a loss of communications with half the county until alternate arrangements could be made.

**RISK: Unprotected communications equipment is vulnerable to vandalism and terrorism that may cause large-scale communications outages**

**Public Safety**  
Communications  
Magazine

### **Snapped Off! How one agency maintained communications and made repairs after vandalism took out its tower APCO Bulletin, April 1999**

At 3:47 a.m. on Dec. 17, 1998, communications received a microwave transmit alarm...the tower had fallen down...the anchor rod, which was 1 1/2 inches in diameter, had been cut twice with what appeared to be a hacksaw...it was the primary tower for the both the sheriff's frequencies and county fire...The DEA also had an antenna on the tower...44 days after we received the first alarm, at a cost of \$125,000 installation of a new tower was completed...Not only did this act of vandalism cost a considerable amount of money, it jeopardized the safety of both the perpetrators and the public...the safety of half the county was compromised while the site was down...What happens to you if you lose one of your towers -- or your only tower?

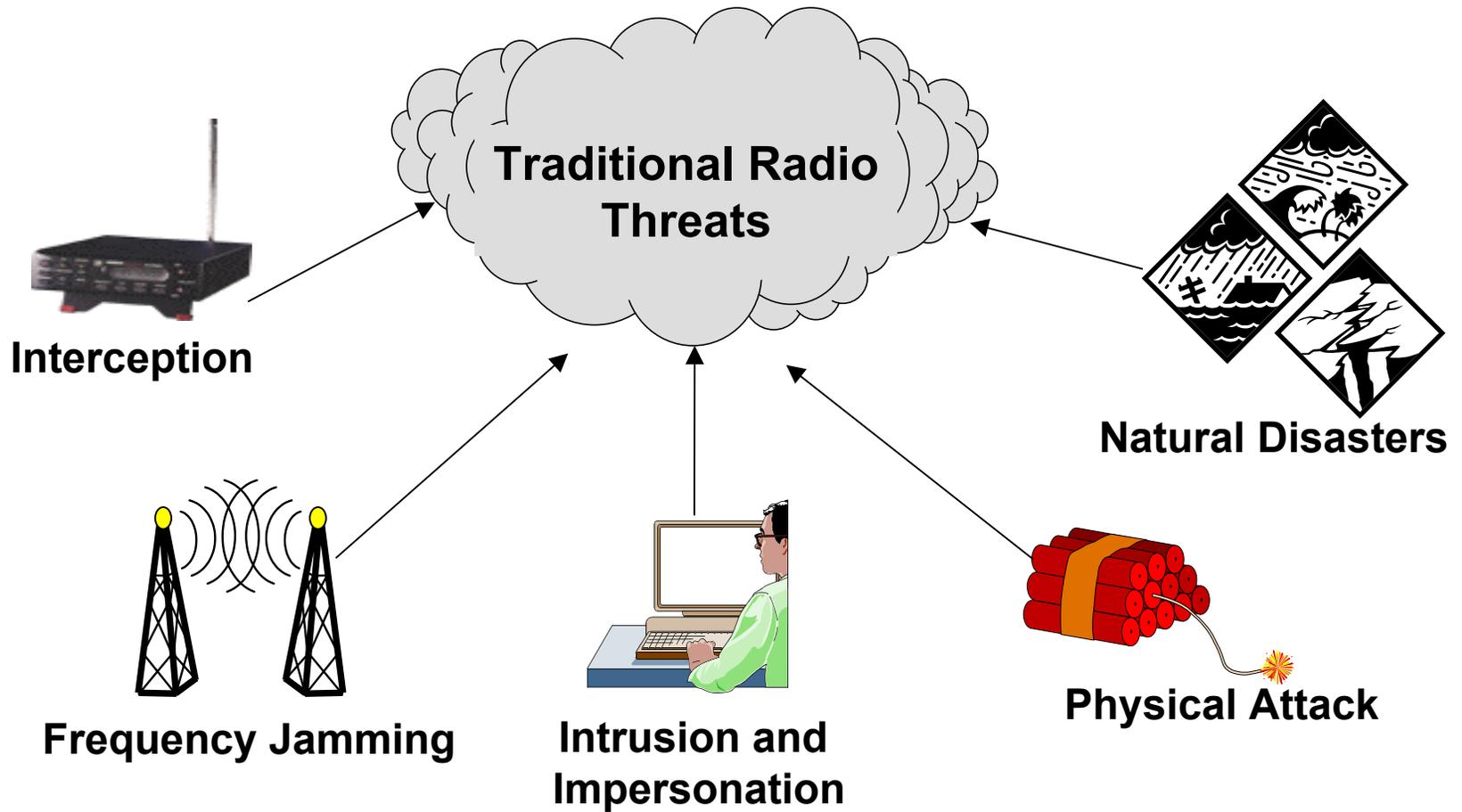
***THESE INCIDENTS HIGHLIGHT THE NEED FOR AGENCIES TO UNDERSTAND AND ADDRESS VULNERABILITIES THAT THREATEN THEIR RADIO SYSTEMS' SECURE COMMUNICATIONS***

This briefing will address the following —

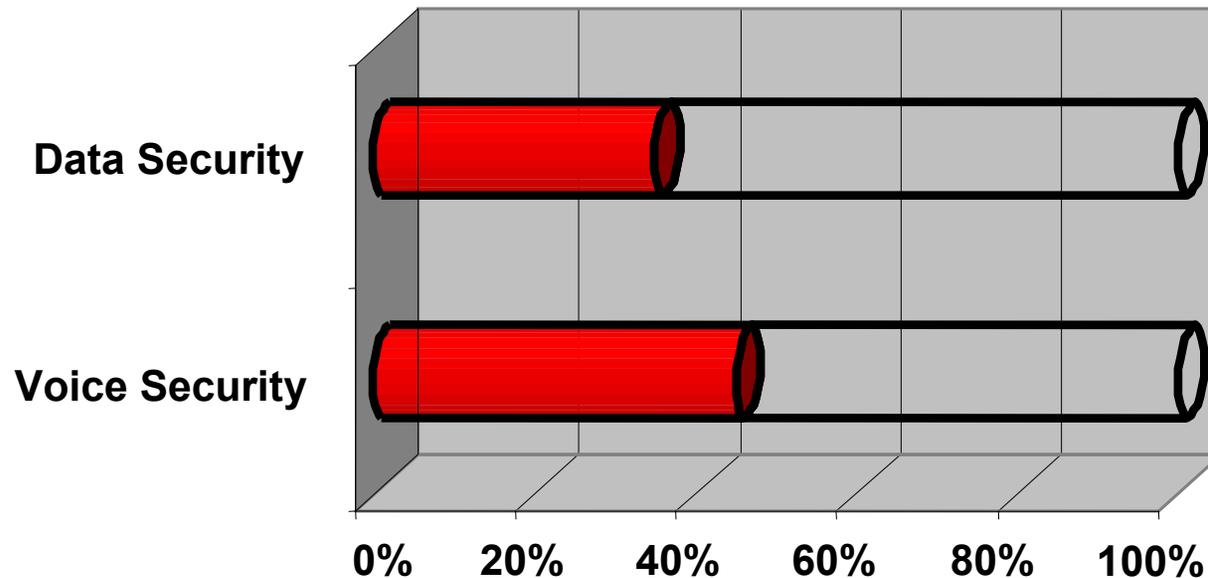
- Security Challenges
- Near-Term Solutions
- Long-Term Solutions

# ***Security Challenges***

**FOR YEARS, PUBLIC SAFETY AGENCIES HAVE CONTENDED WITH SECURITY RISKS TO THEIR WIRELESS COMMUNICATIONS SYSTEMS**



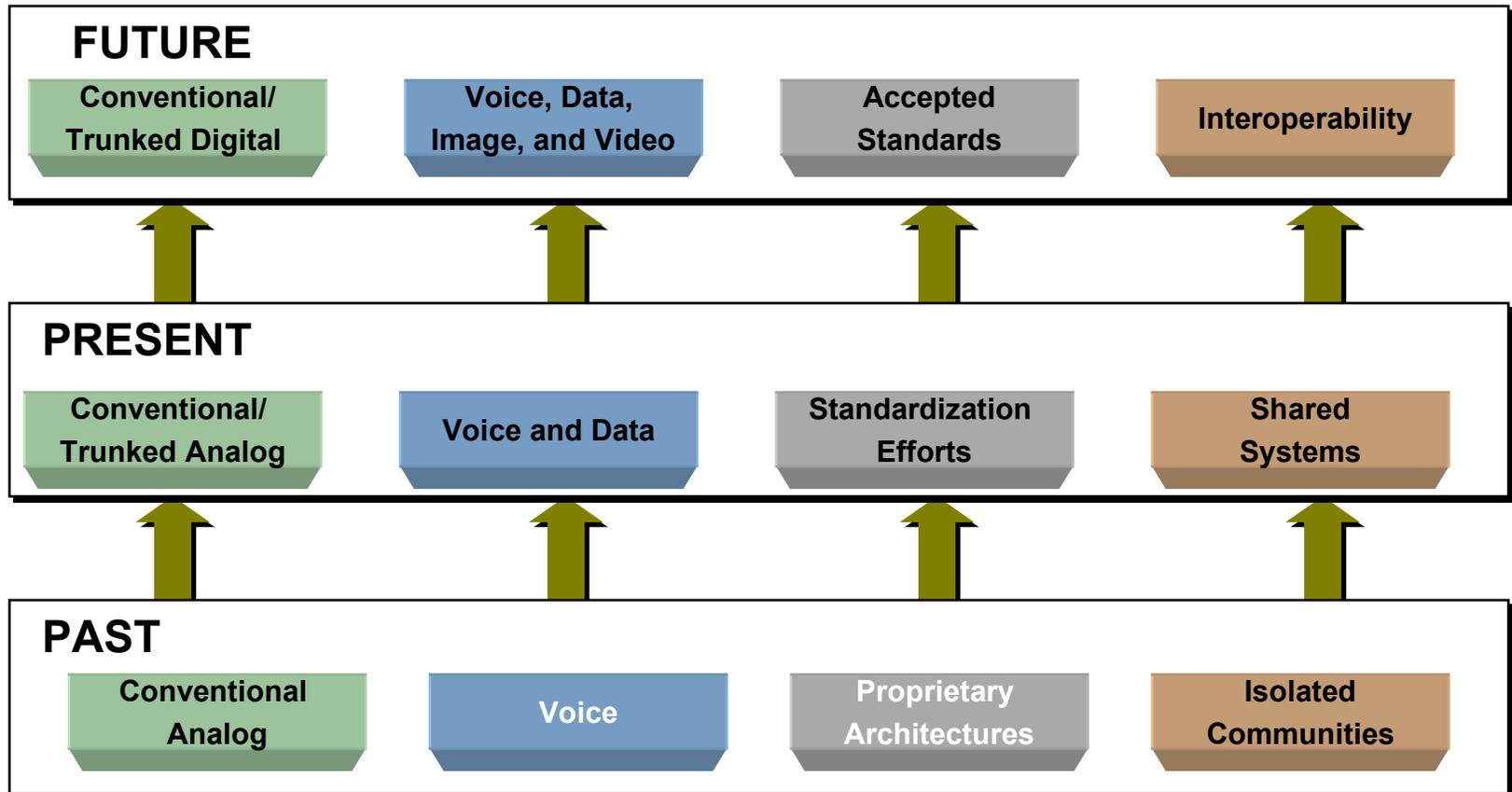
**MOST LAW ENFORCEMENT AGENCIES DO NOT EMPLOY VOICE OR DATA SECURITY PROTECTION TO COUNTER EXISTING THREATS**



- Thirty five percent of responding law enforcement agencies use data security protection\*
- Forty five percent of responding law enforcement agencies use voice security protection\*

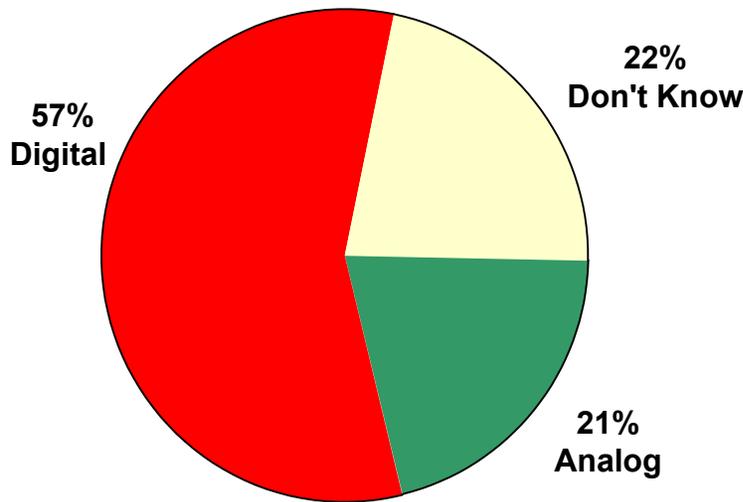
\* Based on a sample size of 1,334 agencies

***PUBLIC SAFETY COMMUNICATIONS INFRASTRUCTURES ARE NOW EVOLVING INTO SOPHISTICATED, DIGITAL, COMPUTER-BASED SYSTEMS***

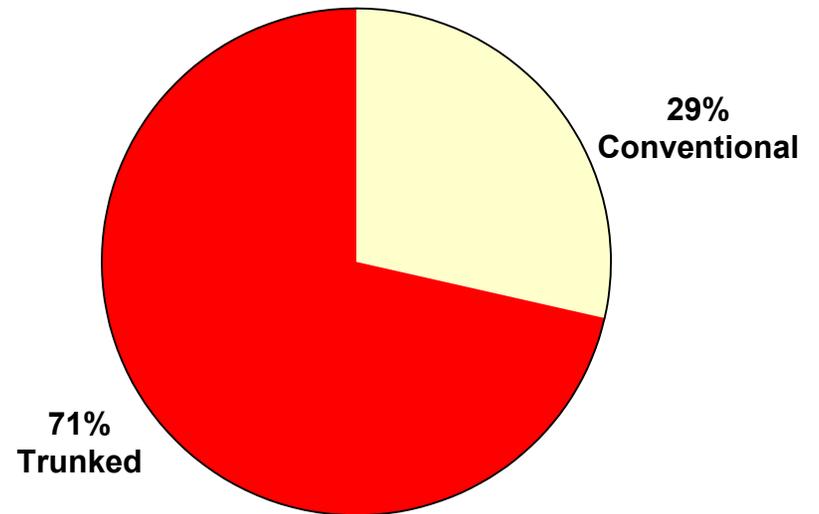


**STUDIES INDICATE THAT THIS EVOLUTION WILL ACCELERATE OVER THE NEXT 10 YEARS**

Fifty four percent of all public safety agencies plan to upgrade their communications systems within the next 10 years



**Fifty seven percent plan to upgrade to digital systems**



**Seventy one percent plan to upgrade to trunked systems**

\* Based on a sample size of 2,379 agencies

## **AS PUBLIC SAFETY COMMUNICATIONS SYSTEMS EVOLVE, SECURITY ISSUES AND THREATS ALSO PROLIFERATE**

### **CHALLENGES**

- Greater interconnectivity causing an increase in system “entry points”
- Interoperability among all levels of government
- Increased network data transfer
- Unspecified security requirements
- Increased sophistication of “bad guys”
- Increased public safety information availability to public
- Storage of critical radio resources on computer-based systems
- Increased encryption use
- Proper inventory control of radio equipment

### **THREATS**

- Interception of unencrypted sensitive network traffic
- Unauthorized people masquerading as system users
- Malicious people disabling radio subscribers
- Re-mapping talk groups to different channels
- Transmission of false information over the system
- Inadvertent release of sensitive information
- Password guessing and random dial-in modem attacks
- Improper encryption and system key management

## ***SECURITY RISKS ARE ASSOCIATED WITH EVOLVING PUBLIC SAFETY COMMUNICATIONS SYSTEMS***

**The PSWN Program assessed several communications systems at the following locations:**

- An Emergency Communications Center that operates on an analog, trunked, voice system as well as a mobile data system
- A Communications Center, a transmit-receive site, and a maintenance facility operating on an analog, trunked voice system as well as a mobile data system
- A Communications Center for police and fire departments that will operate on a digital, simulcast, and trunked voice radio system (currently in a design phase)
- A Network Control Center for statewide public safety agencies operating on a digital, trunked voice radio system as well as a mobile data system (being implemented)

***PUBLIC SAFETY RADIO SYSTEMS ARE SUBJECT TO VARIOUS THREATS IN THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF RADIO COMMUNICATIONS***

- **Confidentiality**—The protection that ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity**—The protection that ensures that data have not been altered, repeated, or destroyed in an unauthorized manner, either accidentally or maliciously
- **Availability**—The accessibility and usability of service upon demand by an authorized entity.

**The following are representative findings regarding the confidentiality of the information being transmitted over their radio systems:**

- Sensitive information is being transmitted in clear mode on primary radio channels
- Trunked analog and digital communications are becoming more susceptible to scanners
- Radios with encryption capability are generally not used in the encrypted mode
- Encryption keys are not changed regularly
- Key management guidelines are not developed to secure encryption keys

**The following are representative findings regarding the integrity of information that systems store and process:**

- Radio systems connected to agencies' local area networks (LAN) and wide-area networks (WAN) are increasingly susceptible to intruders that can access the systems through insecurely configured network systems
- Stringent password constraints are not used to prevent unauthorized access to communications systems
- Agencies generally do not have methods (e.g., Secure ID, token) to restrict remote access to system resources via modems
- Security features of computer-based systems are not properly configured for user account policy, privilege assignment, and auditing
- System servers are not located in a secure environment, which could lead to unauthorized access to critical system resources

The following are representative findings regarding the availability of radio communications

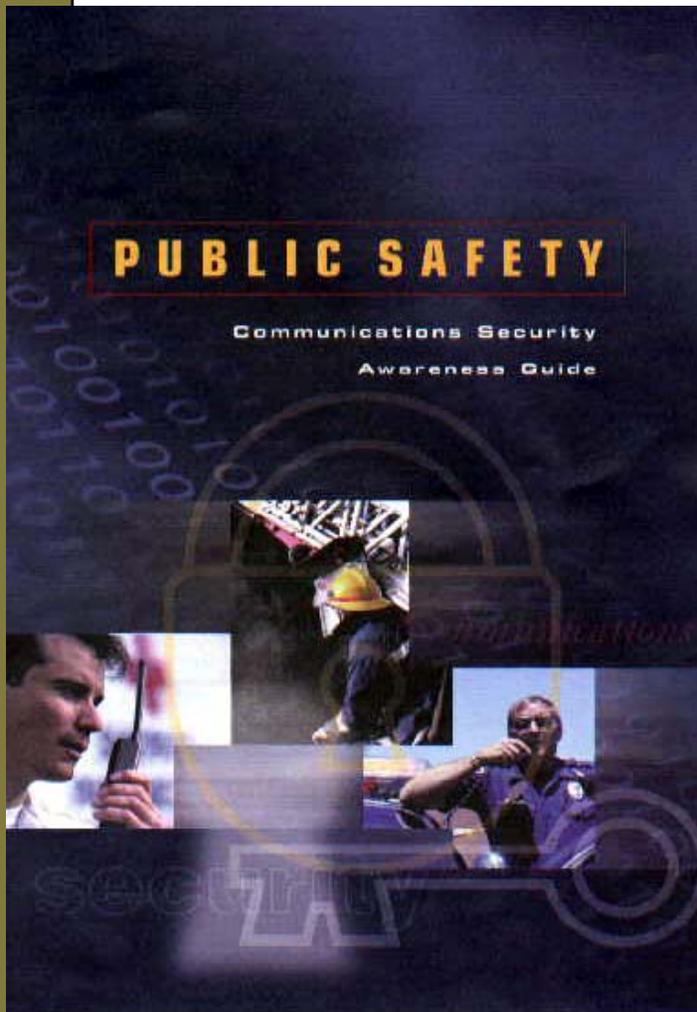
- Agencies are beginning to realize the need for implementing of redundant communications paths
- Physical security at some radio sites and dispatch centers is inconsistent and relatively weak
- Agencies' contingency plans do not consider changes made to the radio communications systems
- Critical system components are often located at the same facility
- An off-site storage facility is not designated to store system data backup tapes

## ***THE FEDERAL GOVERNMENT HAS RECOGNIZED THE NEED TO SAFEGUARD CRITICAL NATIONWIDE INFRASTRUCTURES***

- **Emergency services (i.e., law enforcement, fire, and EMS) is considered one of the Nation's critical infrastructures**
- **Public safety radio communications systems should be protected from physical and electronic threats**
- **National-level policies have been set forth to address security problems of public safety communications systems**
  - Executive Order 13010 (July 1996) stresses the need to protect critical infrastructures from physical, electronic, radio frequency, and computer attacks
  - Presidential Decision Directive (PDD) 63 (May 1998) states that addressing these vulnerabilities would require flexible, evolutionary, and coordinated approaches that span both the public and private sectors
  - Classified PDD 67 (October 1998) deals with the continuity of government operations

# ***Near-Term Solutions***

## **AGENCIES' SENIOR DECISION MAKERS MUST BE AWARE OF SECURITY THREATS AND APPROPRIATE COUNTERMEASURES**



**The PSWN Program has created a guide that explains public safety security issues in clear terms. The guide–**

- Highlights security vulnerabilities of legacy and developing public safety communications systems
- Identifies actions that governmental leaders and public safety agencies can take to address security problems

**This guide has been endorsed by the PSWN Executive Committee**

## ***AGENCIES CAN TAKE STEPS TO ENSURE SECURE TRANSMISSION OF SENSITIVE INFORMATION ON THEIR RADIO SYSTEMS***

-  **Understand that the private call feature on the radio does not offer voice security**
-  **Provide encryption capability for all equipment on the system**
-  **Use end-to-end encryption to lower the probability of compromising intercepted communications**
-  **Ensure that users receive proper training in the importance of encryption use**
-  **Ensure that key management guidelines are developed such that all keys are handled in a secure and controlled manner**
-  **Store encryption key loaders in a secure environment**

## **AGENCIES CAN TAKE STEPS TO PROTECT THE INTEGRITY OF DATA IN COMPUTERIZED PORTIONS OF THEIR COMMUNICATIONS SYSTEMS**

- Provide security requirements and guidelines to system and database administrators**
- Configure security mechanisms of system software properly**
- Implement stringent password constraints to restrict access to system resources**
- Limit access to systems to only a limited number of people**
- Separate functions between system/database administrators and security officers**

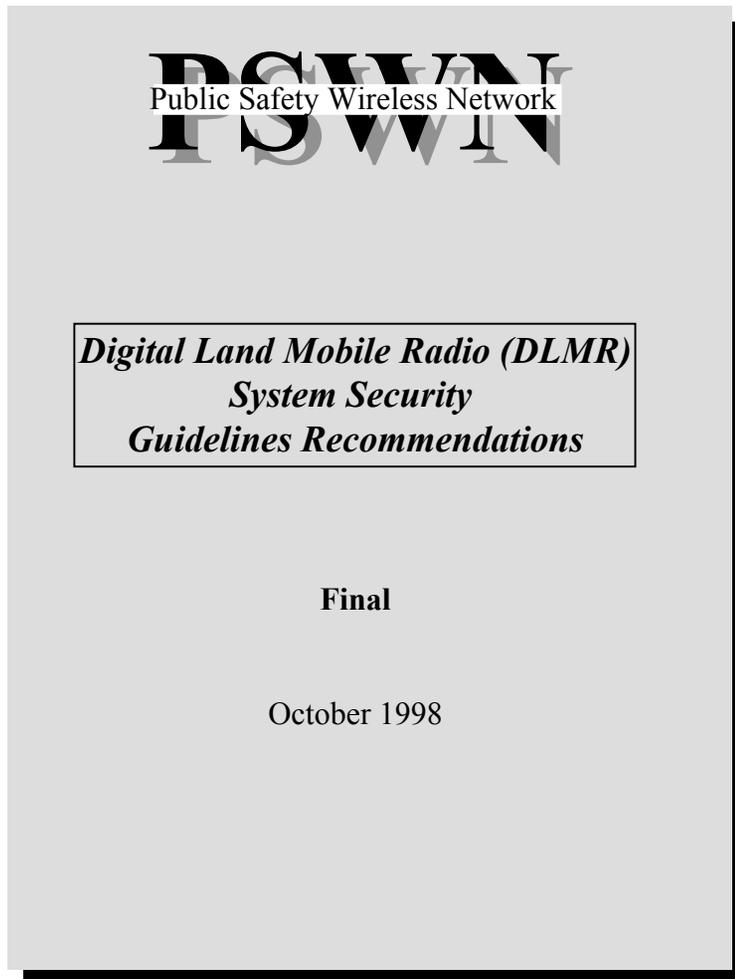
***AGENCIES CAN TAKE STEPS TO PROTECT THE INTEGRITY OF DATA IN COMPUTERIZED PORTIONS OF THEIR COMMUNICATIONS SYSTEMS (cont'd)***

-  **Establish configuration controls for evaluating, approving, and tracking changes made to the system**
-  **Separate wireless radio communications systems from the Agency's information technology systems and networks**
-  **Generate and review audit reports regularly**
-  **Provide internal maintenance departments for most repairs, limiting the potential contact with people outside of the organization**

## ***AGENCIES CAN TAKE STEPS TO ENSURE THE AVAILABILITY OF THEIR SYSTEMS DURING DISASTROUS EVENTS***

-  **Control access to radio equipment by implementing some form of physical access controls (especially for those sites collocated with other organizations)**
-  **Use alarm and monitoring systems to detect unusual activities at radio sites**
-  **Provide redundant infrastructure to ensure system reliability and availability**
-  **Back up system data regularly and store the backup tapes in a secure environment (off-site storage facility)**
-  **Provide adequate environmental controls to protect system components**
-  **Do not advertise locations of communications centers and radio sites**

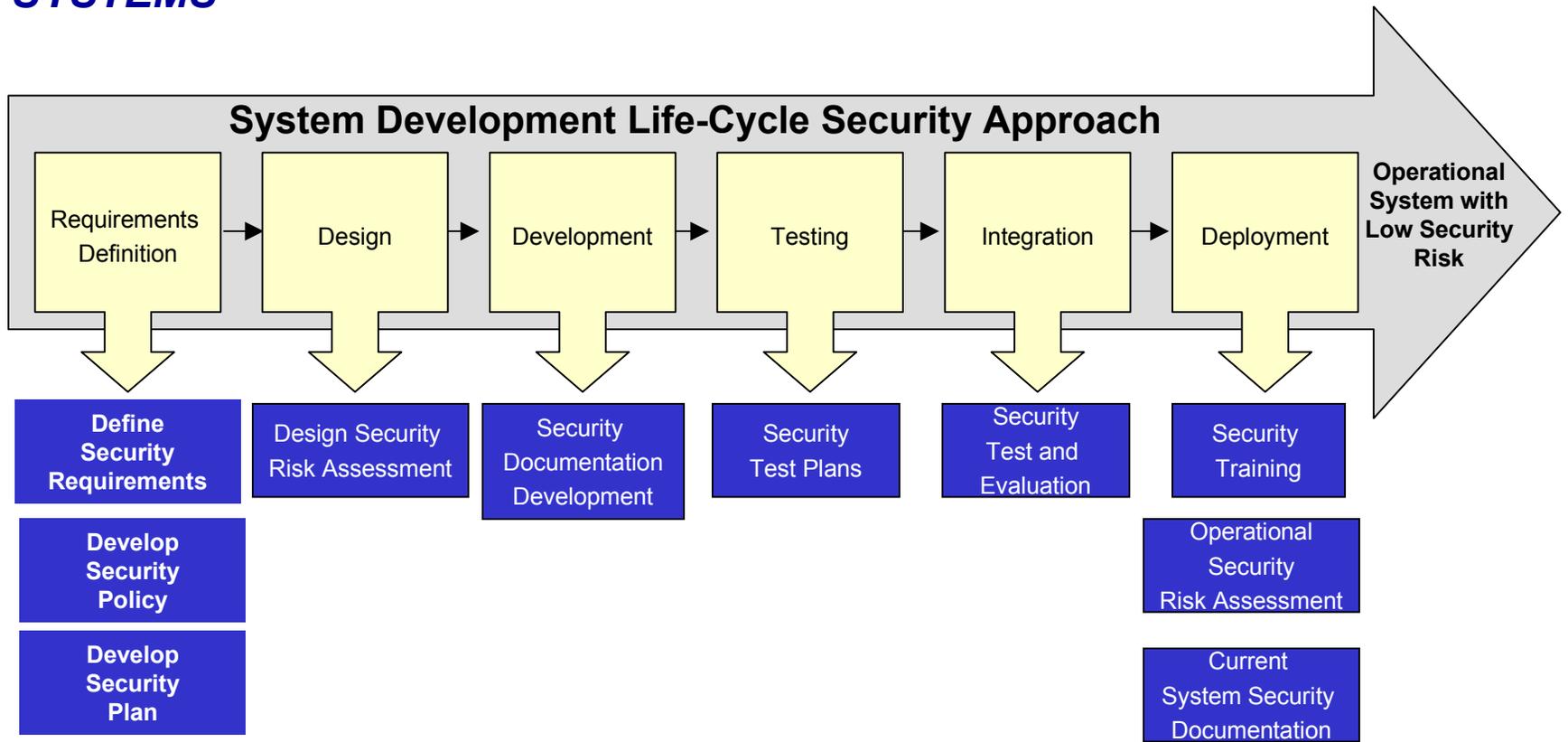
## ***ESTABLISHING SECURITY GUIDELINES IS A FIRST STEP IN INCORPORATING SECURITY CONTROLS INTO THEIR SYSTEMS***



- **The PSWN Program has developed a recommended security guidelines designed for digital land mobile radio (DLMR) systems**
  - **The guidelines are applicable to both planned and operational DLMR systems**
  - **Guidelines are presented in the areas of administrative, physical, computer, communications, radio, and mobile data terminal/mobile computer terminal (MDT/MCT) security**

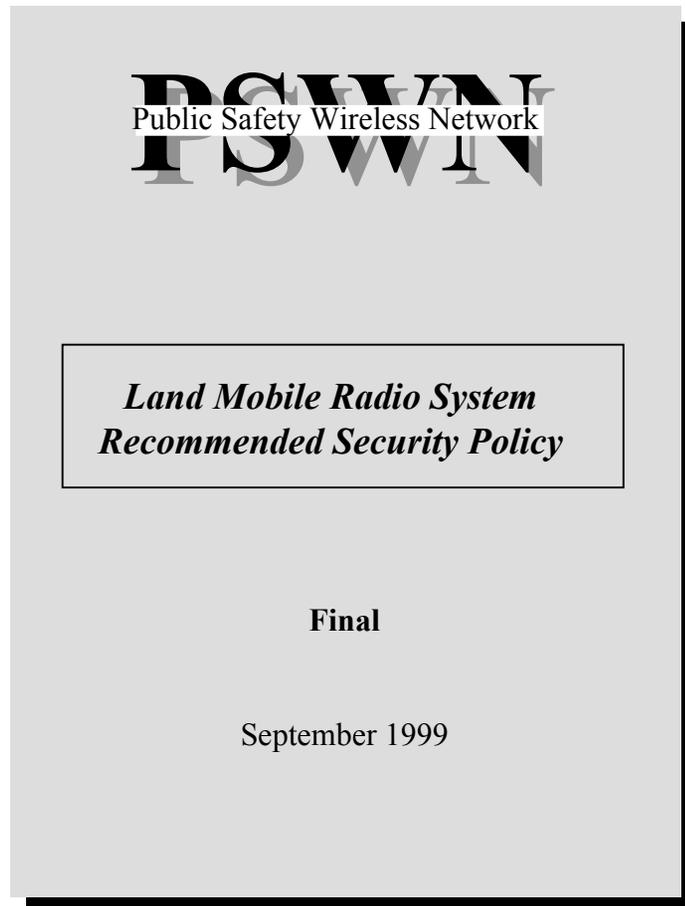
# *Long-Term Solutions*

**PUBLIC SAFETY AGENCIES SHOULD SUBSCRIBE TO A LIFE-CYCLE APPROACH TO SECURITY AS THEY DESIGN AND IMPLEMENT NEW SYSTEMS**



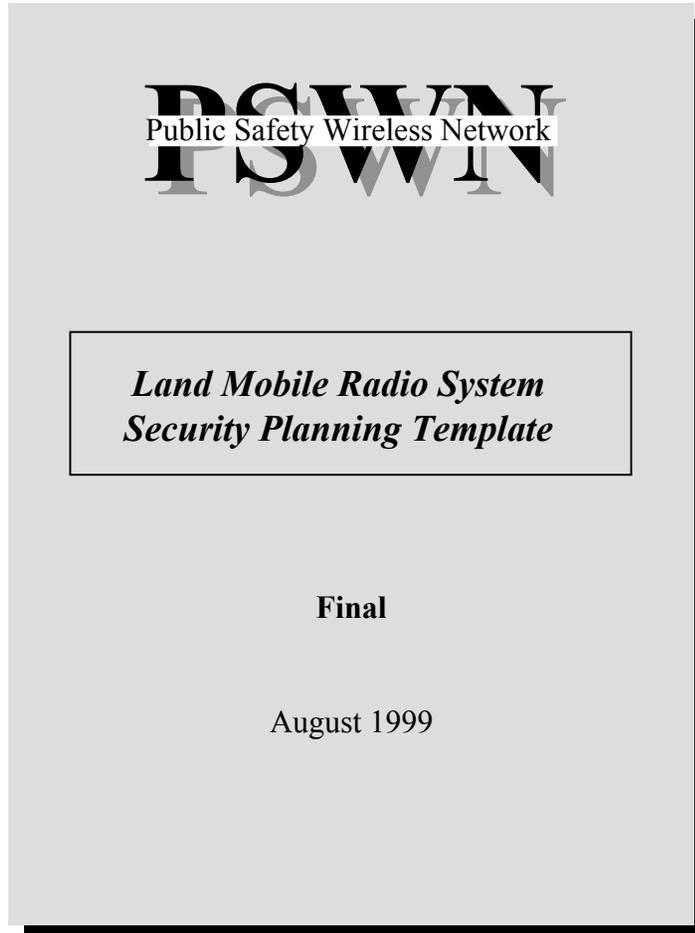
**... FOR THE LIFE-CYCLE APPROACH TO BE SUCCESSFUL, SECURITY MUST BE CONSIDERED BY STANDARDS ASSOCIATIONS, VENDORS, AND THE COMMUNITY**

**THE PSWN PROGRAM HAS DEVELOPED A TOOL TO HELP AGENCIES  
IN DEVELOPING THEIR OWN SYSTEM SECURITY POLICY**



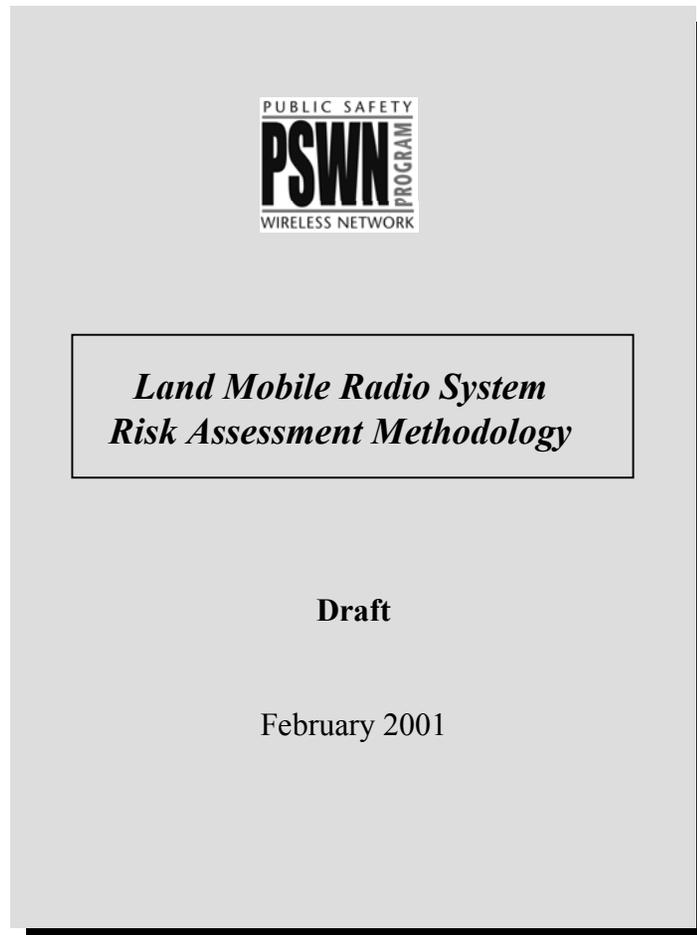
- **Developing a security policy is the first step in developing a long-term security program**
- **This document introduces a representative set of rules and practices to protect radio-related sensitive information**
- **The document is scalable and can be tailored to any public safety wireless system (whether planned or operational)**

**THE PSWN PROGRAM HAS DEVELOPED A TEMPLATE TO HELP AGENCIES IN DEVELOPING THEIR OWN SYSTEM SECURITY PLAN**



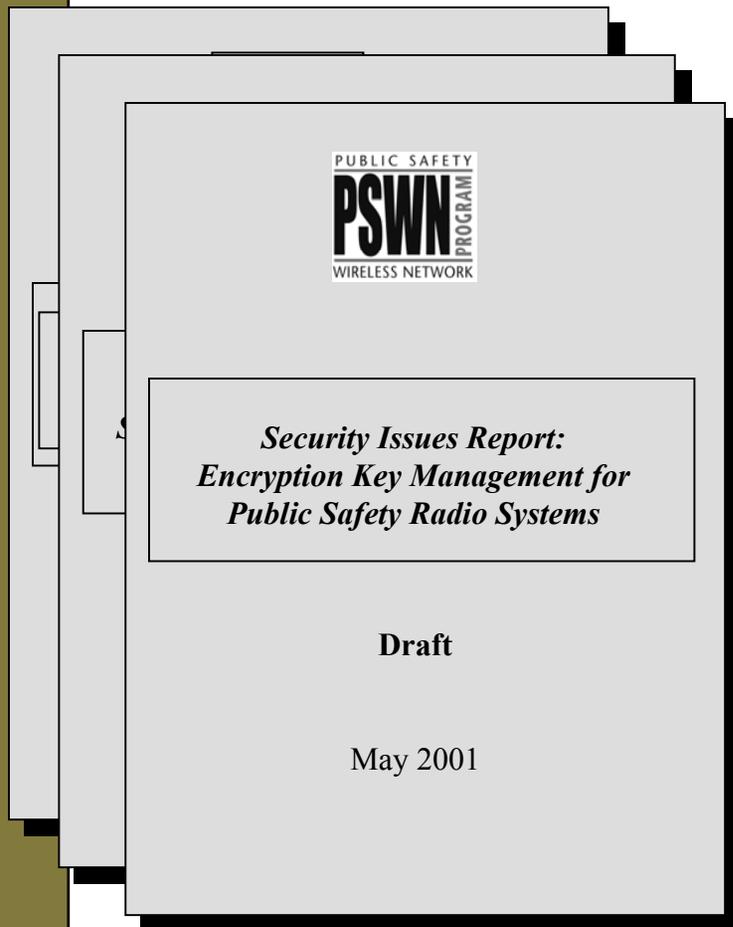
- **Security plans provide public safety agencies with the information necessary to understand the security status of their radio systems**
- **These documents are “living” and require periodic reviews and updates to reflect changes made to the system security**
- **The security plan helps radio managers identify existing and future security controls that protect radio communications**

***THE PSWN PROGRAM HAS USED A SPECIFIC METHODOLOGY TO IDENTIFY RISKS ASSOCIATED WITH EVOLVING DLMR SYSTEMS***



- The document provides public safety agencies a “how-to” guidance to perform a risk assessment for a radio system
- The document is scalable and can be tailored to any public safety wireless system that is being developed or that has been operational
- The document helps radio managers identify vulnerabilities of and threats to their radio systems

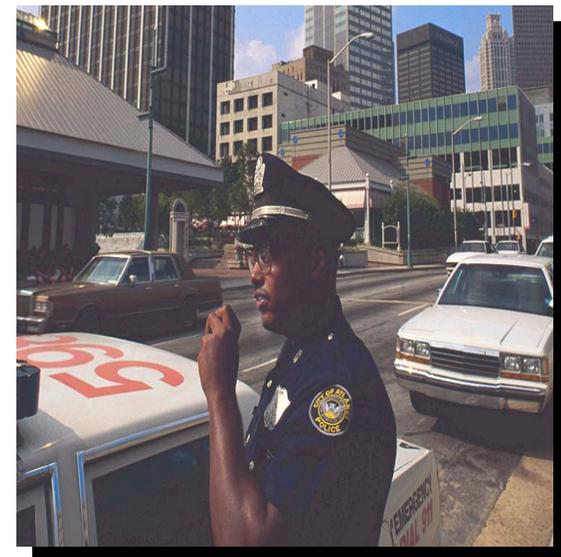
***THE PSWN PROGRAM HAS INITIATED THE DEVELOPMENT OF SECURITY ISSUES REPORTS ON VARIOUS SECURITY SUBJECTS***



- **A Security Issues Report (SIR) on Encryption Key Management was developed**
- **The purpose of the document is to:**
  - Raise security awareness on the importance of key management
  - Address security issues on encryption key management associated with public safety radio systems
  - Provide recommendations to establish a proper key management

**Additional security topics  
for SIRs are to include :**

- **Computer-Controlled  
Radio Communications  
Systems**
- **Impediments and Issues  
on Using Encryption on  
Public Safety Radio  
Systems**



## ***THE SECURITY OF OUR NATION'S PUBLIC SAFETY COMMUNICATIONS INFRASTRUCTURE AFFECTS ALL OF US***

- Radio communications systems must support secure communications (encryption) to protect lives of public safety officers and the lives and property of America's citizens
- Physical and system security measures must be provided to help public safety agencies effectively and efficiently carry out their critical operations
- Agencies must keep their operating and security policies up to date to protect their systems from newly introduced threats
- There must be significant coordination among leaders from all levels of government and public safety officials
  - Government leaders ensure adequate funding is available to secure existing systems and strive to fund new systems
  - Public safety agencies can incorporate security measures into their existing systems to the greatest extent possible and take a life-cycle approach to building security into their new systems



***Julio “Rick” Murphy***  
***PSWN Program Manager–***  
***Treasury***

***Derek M. Siegle***  
***PSWN Program Manager–***  
***Justice (FBI)***

***www.pswn.gov***  
***Information@pswn.gov***  
***1-800-565-PSWN***