



*Public Safety WINS
Policy Solutions—Security*

FINAL

July 2002

Policy Solutions Introduction

The recent acts of domestic terrorism have elevated and highlighted the importance of public safety wireless interoperability. As such, seamless interoperable communications between public safety related agencies, across all levels of government, has become a top priority. Seamless interoperability can be achieved only when stakeholders work together to address the key policy issue areas identified by the Public Safety Wireless Network (PSWN) Program. The PSWN Program has worked to understand the importance of each policy issue and has identified actions and approaches to meet current and future interoperability challenges. Our solutions offer insight, guidance, and resources for stakeholders in their efforts to improve interoperability. This section also provides a detailed review of the impact of each issue on interoperability and what constitutes success in addressing the issue.

Security—Relevance to Interoperability

Security is an often overlooked but critical component of interoperable systems development. Without the presence of secure, interoperable communications, the lives and property of citizens protected by public safety responders are put at significantly greater risk. Consequently, the security of public safety communications infrastructures is a national priority and is essential for successful public safety operations.

Specifically, as a result of the events occurring on September 11, 2001, the need to protect our national infrastructure has become even more evident. Secure communications, especially during emergency situations, is fundamental to ensuring homeland security. When security is not built into the system design process, wireless communications systems are at risk. They become susceptible to electronic intrusion by outsiders and damaging physical attacks. Interception or jamming of transmissions can also become a problem when wireless systems security is not adequately addressed.

When interconnected, or otherwise linked together to improve interoperability, wireless communications systems are susceptible to additional security vulnerabilities. These vulnerabilities increase as the number of access points to the system increases. An increase in system “entry points” can result in the unauthorized interception of unencrypted sensitive network traffic, and allow the number of unauthorized people masquerading as system users to increase.

Different approaches for securing wireless systems can also cause problems when coordinating policies and procedures during the development of interoperable systems. Therefore, it is important to focus resources on developing secure modes of communication that are viable in an interoperable environment. Public safety agencies should also be aware that interconnections can provide redundancy and system backup, reducing the possibility of a single point of failure within their own system.

Success in the area of security will manifest as advancement to a higher level of overall system security. The following matrix illustrates the common stages that public safety agencies may exhibit as they progress towards that desired end state—

New	Developing	Established	Mature
<ul style="list-style-type: none"> • Identifying and minimizing security risks • Researching specifications of security requirements • Addressing the lack of security standards and guidelines • Addressing the lack of adequate approaches to system security • Researching national-level strategies 	<ul style="list-style-type: none"> • Addressing immediate security risks • Developing security policy and plan • Incorporating successful security policies into standards and guidelines • Developing approaches to system security • Addressing relevant national-level strategies 	<ul style="list-style-type: none"> • Ensuring that a strong security policy is in place that encompasses several new security technologies • Adhering to security policies and plans • Testing security standards and guidelines • Implementing best practices for system security • Enacting relevant national-level strategies 	<ul style="list-style-type: none"> • Maintaining the highest security technology available • Operating systems in accordance with security policy • Implementing security standards and guidelines • Sharing best practices among the public safety community • Ensuring national-level strategies for infrastructure protection and assurance are widely used

Target Audiences Introduction

The PSWN Program understands that it cannot resolve the five policy challenges alone and that many people must assume the responsibility to achieve success in each policy area. These five challenges must be addressed by local, state, federal, and tribal public safety entities and the broader set of public safety communications stakeholders, including the U.S. Congress, regulatory agencies, civic leadership forums, and equipment manufacturers. These key public safety entities and stakeholders are jointly responsible for the resolution of interoperability issues. This section is designed to allow members of each group to identify specific actions they can take related to each issue area that can ultimately lead to the successful development of an interoperability solution.

Relevance to State Decision Makers

State decision makers must understand the importance of security and its effect on public safety wireless communications systems. When public safety personnel are not supported by reliable, uninhibited (i.e., interference-free) communications capabilities, the lives of citizens and responding public safety personnel may be at risk, especially in times when the domestic security of the Nation is threatened. In turn, the assurance of secure communications can ease interoperability among all levels of public safety providers within the state and can encourage co-jurisdictional incident response for both day-to-day and emergency operations.

The protection of public safety communications infrastructure is a national priority. In 1998, this infrastructure was designated as critical in Presidential Decision Directive 63 and reaffirmed as such in 2001 as part of the Critical Infrastructure Protection in the Information Age executive order. As so designated, public safety communications infrastructure must be protected from physical and electronic risks and vulnerabilities. Critical infrastructure assurance refers to efforts to ensure that critical infrastructure can withstand the effects of hostile events and continue to fulfill its mission. Additionally, the development of secure public safety communications systems can help the state combat domestic terrorism.

Overall, secure wireless systems can increase the mission effectiveness of the public safety community. The confidential information that is transmitted on wireless systems must be protected. In addition to saving lives, the use of secure systems would reduce the number of unauthorized eavesdroppers (e.g., civilians and the media) during major incidents.

Actions/Solution Steps for State Decision Makers

State decision makers can take numerous steps to ensure that security is adequately addressed to meet interoperability requirements. They can educate the state's public safety agencies about the relevance of wireless systems security by raising awareness of the security risks and vulnerabilities of the state's communications system through the use of publications and videos.

The following resources will prove useful to state decision makers in educating the state's public safety agencies about the relevance of wireless systems security—

- *Public Safety Wireless Communications Security Awareness Guide*
- *Digital Land Mobile Radio (DLMR) Security Problem Statement*
- *Public Safety Communications Security Briefing*
- *The Role of the States in Public Safety Wireless Interoperability*

State decision makers can provide leadership regarding the importance of systems security in several ways. They can support proof-of-concept solutions in the state that test encryption or other features, ensure adequate funding is available to improve the security in the state's existing communications systems, and address security in any new system development. State decision makers can ensure that provisions for public safety wireless systems security are requirements in any request for proposals (RFP) for new systems and can also monitor national-level security issues regarding protection of critical infrastructure such as Homeland Security initiatives.

The following resource will prove useful for state decision makers providing state-level leadership on the importance of systems security—

- *Critical Infrastructure Protection in the Information Age*
(<http://www.ciao.gov/News/EOonCriticalInfrastructureProtection101601.html>)

State decision makers can also require use of a consistent approach to security for state-owned public safety wireless systems. This consistent approach can include a security policy and plan for state wireless communications systems, as well as a comprehensive emergency management plan and contingency/business reconstitution plan for the state.

The following resources will prove useful to state decision makers in identifying and requiring a consistent approach for statewide wireless systems security—

- *Land Mobile Radio System Recommended Security Policy*
- *Land Mobile Radio System Security Planning Template*
- *Digital Land Mobile Radio (DLMR) System Security Guidelines Recommendations*

Relevance to Regional Decision Makers

Regional decision makers must understand the importance of security and its effect on public safety wireless communications systems. When public safety personnel are not supported by reliable, uninhibited (i.e., interference-free) communications, the lives of citizens and responding public safety personnel may be at risk, especially when the domestic security of the Nation is threatened. In turn, the assurance of secure communications can ease interoperability among all levels of public safety providers within the region and can encourage co-jurisdictional incident response for both day-to-day and emergency operations.

The protection of public safety communications infrastructure is a national priority. In 1998, this infrastructure was designated as critical in Presidential Decision Directive 63 and reaffirmed as such in 2001 as part of the Critical Infrastructure Protection in the Information Age executive order. As so designated, public safety communications infrastructure must be protected from physical and electronic risks and vulnerabilities. Critical infrastructure assurance refers to efforts to ensure that critical infrastructure can withstand the effects of hostile events and continue to fulfill its mission. Additionally, the development of secure public safety communications systems can help the region combat domestic terrorism.

Overall, secure wireless systems can increase the mission effectiveness of the public safety community. The confidential information that is transmitted on wireless systems must be protected. In addition to saving lives, the use of secure systems would reduce the number of unauthorized eavesdroppers (e.g., civilians and the media) during major incidents.

Actions/Solution Steps for Regional Decision Makers

Regional decision makers can take numerous steps to ensure that security is adequately addressed to meet interoperability requirements. They can educate the public safety community within the region about the relevance of wireless systems security by raising awareness of the security risks and vulnerabilities of the region's communications system through the use of publications and videos.

The following resources will prove useful to regional decision makers in educating the regional public safety community about the relevance of wireless systems security—

- *Public Safety Wireless Communications Security Awareness Guide*
- *Digital Land Mobile Radio (DLMR) Security Problem Statement*
- *Public Safety Communications Security Briefing*
- *The Role of the States in Public Safety Wireless Interoperability*

Regional decision makers can provide leadership regarding the importance of systems security in several ways. They can support proof-of-concept solutions in the region that test encryption or other features, ensure adequate funding is available to improve the security in the region's existing public safety communications systems, and address security in any new system development. Regional decision makers can ensure that provisions for public safety wireless systems security are requirements in any request for proposals (RFP) for new systems, and can also monitor national-level security issues regarding protection of critical infrastructures.

Regional decision makers can also require use of a consistent approach to security for regional public safety wireless systems. This consistent approach can include a security policy and plan for regional public safety wireless communications systems, as well as a comprehensive emergency management plan and contingency/business reconstitution plan for the region. The security policy and plan will also capture the region's best practices addressing security.

The following resources will prove useful to regional decision makers in identifying and requiring a consistent approach for regional wireless systems security—

- *Land Mobile Radio System Recommended Security Policy*
- *Land Mobile Radio System Security Planning Template*
- *Digital Land Mobile Radio (DLMR) System Security Guidelines Recommendations*
- *Critical Infrastructure Protection in the Information Age*
(<http://www.ciao.gov/News/EOonCriticalInfrastructureProtection101601.html>)

Relevance to the Public Safety Community

The public safety community must understand the importance of security and its effect on public safety wireless communications systems. When public safety personnel are not supported by reliable, uninhibited (i.e., interference-free) communications, the lives of citizens and responding public safety personnel may be at risk, especially in times when the domestic security of the Nation is threatened. In turn, the assurance of secure communications can ease interoperability among all levels of public safety providers and can encourage co-jurisdictional incident response for both day-to-day and emergency operations.

The protection of public safety communications infrastructure is a national priority. In 1998, this infrastructure was designated as critical in Presidential Decision Directive 63 and reaffirmed as such in 2001 as part of the Critical Infrastructure Protection in the Information Age executive order. As so designated, public safety communications infrastructure must be protected from physical and electronic risks and vulnerabilities. Critical infrastructure assurance refers to efforts to ensure that critical infrastructure can withstand the effects of hostile events and continue to fulfill its mission. Additionally, the development of secure public safety communications systems can help combat domestic terrorism.

Overall, secure wireless systems can increase the mission effectiveness of the public safety community. The confidential information that is transmitted on wireless systems must be protected. In addition to saving lives, the use of secure systems would reduce the number of unauthorized eavesdroppers (e.g., civilians and the media) during major incidents.

Unfortunately, current and emerging system technologies may introduce additional system vulnerabilities. While new digital communications systems allow sharing and interconnection with different systems, they also introduce network-related security vulnerabilities. To address these new computer-based threats, the public safety community must receive proper training and adequate financial resources.

Actions/Solution Steps for the Public Safety Community

The public safety community can take numerous steps to ensure that security is adequately addressed to meet interoperability requirements. Its members can continue to learn about the relevance of wireless systems security. They can also review existing security standards, become aware of the security risks and vulnerabilities of communications systems, promote the importance of security during attendance at outreach forums and conference events, and support pilot and proof-of-concept solutions that test encryption or other security features.

The following resources will prove useful to the public safety community in understanding the relevance of wireless systems security—

- *Public Safety Wireless Communications Security Awareness Guide*
- *Digital Land Mobile Radio (DLMR) Security Problem Statement*
- *Public Safety Communications Security Briefing*

The public safety community can actively participate in the development of security standards. Its members can review and provide comment on suggested security standards as they relate to

the public safety community. The public safety community can also support the adoption of security standards that enable interoperability among secure systems.

The public safety community can develop a consistent approach to security for regional public safety wireless systems, as well as develop security policies and plans for wireless communications systems. The public safety community can also develop or update a comprehensive emergency management plan and contingency/business reconstitution plan for their jurisdictions.

Specifically, the public safety community can outline the protection of physical sites (e.g., communications centers, tower sites, maintenance facilities, and communications equipment) from threats such as unauthorized site access and radio frequency signal interference. Its members can also provide network security to the systems' hardware, software, and associated interfaces. Overall, the public safety community can ensure the confidentiality and integrity of a system's transmitted communications by using encryption techniques, properly managing and reprogramming encryption keys, and safeguarding key codes and software.

The public safety community can also implement administrative security procedures, such as policy statements. These statements can provide information about security documentation, security training, system life cycle controls, and personnel security. The public safety community can implement the policy statements to ensure the confidentiality, integrity, and availability of the system. In turn, the public safety community can identify best practices addressing security in the region's communications systems and monitor national-level security issues regarding protection of critical infrastructures.

The following resources will prove useful to the public safety community in developing a consistent approach to security—

- *[Land Mobile Radio System Recommended Security Policy](#)*
- *[Land Mobile Radio System Security Planning Template](#)*
- *[Critical Infrastructure Protection in the Information Age](#)*
[\(<http://www.ciao.gov/News/EOonCriticalInfrastructureProtection101601.html>\)](http://www.ciao.gov/News/EOonCriticalInfrastructureProtection101601.html)
- *[Digital Land Mobile Radio \(DLMR\) System Security Guidelines Recommendations](#)*

By documenting the security risks of communications systems, the public safety community can further develop design phase risk assessment plans to identify potential vulnerabilities and the preferred risk-mitigation strategies that can be adopted. Its members can also develop security test and evaluation plans to verify the security strategy and identify any components that require improvement.

The following resources will prove useful to the public safety community in documenting security risks of public safety wireless communications systems—

- *[Security Field Data Collection and Analysis, #1](#)*

- *Security Field Data Collection and Analysis, #2*
- *Security Field Data Collection and Analysis, #3*

Addressing wireless systems security using a system life cycle approach will ensure that security is adequately addressed to meet interoperability requirements. Namely, the public safety community can ensure that security is a requirement in any request for proposals (RFP) for new systems, continually test and evaluate the existing systems' security, and participate in security training to raise awareness of all possible threats and to learn risk-mitigation strategies.

The following resource will prove useful to the public safety community in addressing security using a system life cycle approach—

- *Roadmap for Systems Development*

Relevance to Civic Leadership Forums

Civic leadership forums must understand the importance of security and its effect on public safety wireless communications systems. When public safety personnel are not supported by reliable, uninhibited (i.e., interference-free) communications, the lives of citizens and the responding public safety personnel may be at risk, especially in times when the domestic security of the Nation is threatened.

Civic leadership forums provide a venue for dialog that enhances active and informed citizenship. Through these forums, citizens gain knowledge about the effect secure systems, or lack thereof, has on public safety. Additionally, civic leadership forums can serve as an effective organizational tool to obtain security standards for public safety communications systems.

Civic leadership forums have the influence to significantly contribute to public problem solving. As such, civic leaders play a key role in bringing to light issues of public concern. Advocating and other awareness efforts led by civic leadership forums can heavily influence key decision makers to recognize the importance of wireless systems security and to actively promote measures that address these concerns.

Actions/Solution Steps for Civic Leadership Forums

Civic leadership forums can take numerous steps to ensure that security is adequately addressed to meet interoperability requirements. Civic leadership forums can obtain a general understanding of the relevance of public safety wireless systems security standards.

The following resources will prove useful to civic leadership forums in understanding the importance of public safety wireless systems security—

- *Public Safety Wireless Communications Security Awareness Guide*
- *Digital Land Mobile Radio (DLMR) Security Problem Statement*
- *Public Safety Communications Security Briefing*

Understanding the relevance of public safety wireless communications security standards will enable civic leadership forums to effectively promote the importance of security during attendance at outreach forums and conference events, and to educate the state's legislators about the benefits of implementing wireless communications security standards and guidelines.

Relevance to the U.S. Congress

The U.S. Congress must understand the importance of security and its effect on protecting citizens across the Nation. When public safety personnel are not supported by reliable, uninhibited (i.e., interference-free) communications, the lives of U.S. citizens and the responding public safety personnel may be at risk, especially in times when the domestic security of the Nation is threatened.

The protection of public safety communications infrastructure is a national priority. In 1996, the President identified public safety infrastructure as so important to the United States that an interruption in service would have a severe impact on the security of the country. As a result, in 1998, the President created the Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, stressing the need to protect these infrastructures from physical and electronic risks and vulnerabilities. This policy was reaffirmed in 2001 as part of the Critical Infrastructure Protection in the Information Age executive order. Critical infrastructure assurance refers to efforts to ensure that critical infrastructure can withstand the effects of hostile events and continue to fulfill its mission. Additionally, the development of secure public safety communications systems can help combat domestic terrorism.

After the attacks against America on September 11, 2001, the President created the Office of Homeland Security to ensure domestic preparedness. This office will develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks. Vital to the Homeland Security Office's mission, communications security and un-impeded interoperable communications need to be fully realized to keep America safe.

Actions/Solution Steps for the U.S. Congress

The U.S. Congress can take numerous steps to ensure that security is adequately addressed to meet interoperability requirements. Understanding the relevance of and recognizing the threats to public safety wireless systems security will enable the U.S. Congress to effectively advocate the use of secure wireless systems. Identifying any security challenges facing their home district's public safety wireless communications system and understanding the security standards requirements for the public safety community across the Nation will help members of the U.S. Congress recognize the public safety need for secure wireless communications systems.

The following resources will prove useful to the U.S. Congress in understanding the relevance of public safety wireless systems security—

- *Public Safety Wireless Communications Security Awareness Guide*
- *Digital Land Mobile Radio (DLMR) Security Problem Statement*
- *Public Safety Communications Security Briefing*
- *The Role of the Federal Government in Public Safety Wireless Interoperability*

The U.S. Congress can provide leadership regarding the importance of public safety communications systems security in several ways. It can continue to fund efforts to study problems and design solutions to improve the security in the Nation's public safety communications systems. It can also include regulations for security in any rulemaking or policy

development, and reevaluate the critical infrastructure protection policy to stress the need to protect these infrastructures from attack.

The following resource will prove useful for the U.S. Congress in providing leadership on the importance of public safety communications systems security—

- *Critical Infrastructure Protection in the Information Age*
(<http://www.ciao.gov/News/EOonCriticalInfrastructureProtection101601.html>)

Relevance to the Federal Communications Commission (FCC)

The FCC must recognize the importance of security and its effect on public safety wireless communications systems. In 1998, public safety infrastructure was designated as critical in Presidential Decision Directive 63 and reaffirmed as such in 2001 as part of the Critical Infrastructure Protection in the Information Age executive order. As so designated, public safety communications infrastructure must be protected from physical and electronic risks and vulnerabilities. Critical infrastructure assurance refers to efforts to ensure that critical infrastructure can withstand the effects of hostile events and continue to fulfill its mission. Because the protection of public safety infrastructure is a national priority, the development of secure public safety communications systems can help combat domestic terrorism and mitigate other national-scale emergencies.

As a regulatory entity, the FCC can influence public safety wireless communications systems development. By endorsing approaches to security in rulemakings, the FCC can promote the benefits of secure public safety communications systems with state and local public safety communities, and indirectly, with the federal public safety community. Overall, security is a public safety wireless communications systems requirement, and secure communications are critical to successful interoperability.

Actions/Solution Steps for the Federal Communications Commission (FCC)

The FCC can take the following steps to ensure that security is adequately addressed to meet interoperability requirements. By recognizing the threats to public safety wireless communications systems, the FCC can raise awareness of the security risks and vulnerabilities of the Nation's communications systems, thereby stressing the importance of security across the Nation.

The following resources will prove useful to the FCC in understanding the importance of public safety wireless communications security—

- *Public Safety Communications Security Awareness Guide*
- *Digital Land Mobile Radio (DLMR) Security Problem Statement*
- *Public Safety Communications Security Briefing*
- *The Role of the Federal Government in Public Safety Wireless Interoperability*

The FCC can also include regulations for security in any rulemaking or policy development. By promoting the development of security standards, the FCC can encourage the public safety community to actively participate in the security standards process while supporting the adoption of security standards that enable interoperability among secure systems. The FCC can also monitor national-level security issues regarding protection of critical infrastructures.

The following resource will prove useful to the FCC in monitoring national-level security issues—

- *Critical Infrastructure Protection in the Information Age*
(<http://www.ciao.gov/News/EOonCriticalInfrastructureProtection101601.html>)

Relevance to Equipment Manufacturers

Equipment manufacturers must recognize the importance of security and its effect on public safety wireless communications. In 1998, public safety infrastructure was designated as critical in Presidential Decision Directive 63 and reaffirmed as such in 2001 as part of the Critical Infrastructure Protection in the Information Age executive order. As so designated, public safety communications infrastructure must be protected from physical and electronic risks and vulnerabilities. Critical infrastructure assurance refers to efforts to ensure that critical infrastructure can withstand the effects of hostile events and continue to fulfill its mission. Because the protection of public safety communications infrastructure is a national priority, the development of public safety communications systems incorporating security standards and features can help combat domestic terrorism.

Public safety customers require security in their wireless communications systems. Secure communications are critical not only to the effectiveness of the public safety community but also to successful overall system interoperability. Because public safety officials depend on quality secure equipment, the demand for secure radio communications technology is high. These additional security requirements can provide equipment manufacturers with an opportunity to develop new markets and expand existing ones, thus sustaining long-lasting business partnerships.

Actions/Solution Steps for Equipment Manufacturers

Equipment manufacturers can take the following steps to ensure that security is adequately addressed to meet interoperability requirements. They can support the public safety community concerning the relevance of wireless systems security. Equipment manufacturers can promote the importance of system security during outreach forums and conference events. They can also support pilot and proof-of-concept solutions by providing equipment that tests encryption or other security features.

The following resources will prove useful to equipment manufacturers in supporting the public safety community concerning the relevance of wireless systems security—

- *Public Safety Communications Security Awareness Guide*
- *Digital Land Mobile Radio (DLMR) Security Problem Statement*
- *Public Safety Communications Security Briefing*

Equipment manufacturers can also actively participate in the development of security standards. By reviewing and providing comment on suggested security standards as they relate to the public safety community, equipment manufacturers can best support the adoption of security standards that enable interoperability among secure systems.

Once equipment manufacturers are fluent in public safety security requirements (e.g., encryption, radio inhibiting for lost or stolen equipment, over-the-air rekeying), they will be better able to design and manufacture subscriber units and infrastructure components compliant with existing security standards. Equipment manufacturers can also advertise security features of product offerings to the public safety community while providing research and development funding for enhanced security features.

Relevance to the Federal Law Enforcement Wireless Users Group (FLEWUG)

The FLEWUG must recognize the importance of security and its effect on public safety wireless communications systems. When public safety agencies are not supported by reliable, uninhibited (i.e., interference-free) communications, the lives of U.S. citizens, including public safety officials, may be at risk. In turn, the assurance of secure communications can ease interoperability among all levels of public safety providers and can also encourage co-jurisdictional incident response for both day-to-day and emergency operations, especially in times when the domestic security of the Nation is threatened.

In 1996, the President of the United States stated that an interruption in public safety service would have a severe impact on the security of the country. In 1998, he created the Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, stressing the need to protect these infrastructures from physical and electronic risks and vulnerabilities. In 2001, following the September 11th attacks on America, the President created the Office of Homeland Security to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats and attacks. In this same security-conscious vein, the President, on October 21, 2001, issued the Critical Infrastructure Protection in the Information Age executive order, reaffirming the underlining policies put forth in Presidential Decision Directive 63. Both presidential acts on critical infrastructure protection underscore the fact that the development of secure public safety communication systems is critical in combating domestic terrorism and mitigating other national-scale incidents.

Overall, secure wireless systems can increase the mission effectiveness of the public safety community. Secure wireless systems can increase the mission effectiveness of the FLEWUG members' organizations, making critical the need for confidential information transmitted on wireless systems to be protected. In addition to saving lives, the use of secure systems would reduce the number of unauthorized eavesdroppers (e.g., civilians and the media) during major incidents.

Actions/Solution Steps for the Federal Law Enforcement Wireless Users Group (FLEWUG)

The FLEWUG can take the following steps to ensure that security is adequately addressed to meet interoperability requirements. Its members can continue to educate others within their department or agency about the relevance of wireless systems security. They can review existing security standards and raise awareness of the security risks and vulnerabilities of communications system(s) among senior decision makers within their department or agency. The FLEWUG can also raise the awareness of security through the use of publications and videos and by promoting the importance of security during attendance at outreach forums and conference events.

The following resources will prove useful to the FLEWUG in educating department and agency personnel about the relevance of public safety wireless communications systems security—

- *Public Safety Communications Security Awareness Guide*
- *Digital Land Mobile Radio (DLMR) Security Problem Statement*
- *Public Safety Communications Security Briefing*
- *The Role of the Federal Government in Public Safety Wireless Interoperability*

The FLEWUG can also actively participate in the development of security standards. It can review and provide comment on suggested security standards as they relate to the public safety community. The FLEWUG can also support the adoption of security standards that enable interoperability among secure systems.

The FLEWUG can require a consistent approach to security for federal wireless systems. It can also require security policies and plans for departmental or agency wireless communications systems. The FLEWUG can also require a comprehensive department or agency-level emergency management plan and contingency/business reconstitution plan for each of its member agencies that includes communications systems and capabilities.

Specifically, the FLEWUG can outline the protection of physical sites (e.g., communications center, tower sites, maintenance facilities, and communications equipment) from threats such as unauthorized site access and radio frequency signal interference. It can also require network security for the systems' hardware, software, and associated interfaces. Overall, the FLEWUG can ensure the confidentiality and integrity of a system's transmitted communications by mandating the use of encryption techniques, the proper management and reprogramming of encryption keys, and the safeguarding of key codes and software.

The FLEWUG can also implement administrative security procedures, such as policy statements. These statements can provide information about security documentation, security training, system life-cycle controls, and personnel security. The FLEWUG can design the policy statements to ensure the confidentiality, integrity, and availability of the system. In turn, the FLEWUG members can identify best practices addressing security in their department's or agency's communications systems and monitor national-level security issues regarding protection of critical infrastructures.

The following resources will prove useful to the FLEWUG in requiring a consistent approach to security—

- *Land Mobile Radio System Recommended Security Policy*
- *Land Mobile Radio System Security Planning Template*
- *Critical Infrastructure Protection in the Information Age*
<http://www.ciao.gov/News/EOonCriticalInfrastructureProtection101601.html>
- *Digital Land Mobile Radio (DLMR) System Security Guidelines Recommendations*

FLEWUG members can document the security risks of their department's or the agency's communications system. They can require a design phase risk assessment plan to identify potential vulnerabilities and the preferred risk-mitigation strategies that can be adopted. A security test and evaluation plan can also be required to verify the security strategy and identify any components that require improvement.

The following resources will prove useful to the FLEWUG in documenting security risks of their department's or agency's communications system—

- *Security Field Data Collection and Analysis, #1*
- *Security Field Data Collection and Analysis, #2*
- *Security Field Data Collection and Analysis, #3*

Relevance to Federal Decision Makers

Federal decision makers must recognize the importance of security and its effect on public safety wireless communications systems. A lack of secure wireless communications across the Nation endangers the lives and property of citizens as well as those within public safety agencies. In turn, the assurance of secure communications can ease interoperability among all levels of public safety providers and can also encourage co-jurisdictional incident response for both day-to-day and emergency operations, especially in times when the domestic security of the Nation is threatened.

In 1996, the President of the United States stated that an interruption in public safety service would have a severe impact on the security of the country. In 1998, he created the Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, stressing the need to protect these infrastructures from physical and electronic risks and vulnerabilities. In 2001, following the September 11th attacks on America, the President created the Office of Homeland Security to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats and attacks. In this same security-conscious vein, the President, on October 21, 2001, issued the Critical Infrastructure Protection in the Information Age executive order, reaffirming the underlining policies put forth in Presidential Decision Directive 63. Both presidential acts on critical infrastructure protection underscore the fact that the development of secure public safety communication systems is critical in combating domestic terrorism and mitigating other national-scale incidents.

Overall, secure wireless systems can increase the mission effectiveness of the public safety community. The confidential information that is transmitted on wireless systems must be protected. In addition to saving lives, the use of secure systems would reduce the number of unauthorized eavesdroppers (e.g., civilians and the media) during major incidents.

Actions/Solution Steps for Federal Decision Makers

Federal decision makers can take the following steps to ensure that security is adequately addressed to meet interoperability requirements. Federal decision makers can recognize the threats to public safety wireless communications systems. By raising awareness of security risks and vulnerabilities of the Nation's public safety communications systems, federal decision makers can stress the importance of public safety wireless systems security across the Nation.

The following resources will prove useful to federal decision makers in recognizing the threats to public safety wireless communications systems—

- *Public Safety Communications Security Awareness Guide*
- *Digital Land Mobile Radio (DLMR) Security Problem Statement*
- *Public Safety Communications Security Briefing*
- *The Role of the Federal Government in Public Safety Wireless Interoperability*

Federal decision makers can also provide leadership regarding the importance of secure critical infrastructure. They can educate the U.S. Congress and other federal decision makers about the need for secure wireless communications systems. Federal decision makers can continue to fund

programs that study problems and design solutions to improve the security of the Nation's public safety communications systems. Federal decision makers can include regulations for security in any rulemaking or policy development and can also monitor national-level security issues regarding protection of critical infrastructures.

The following resource will prove useful to federal decision makers in proving leadership on the importance of secure critical infrastructure—

- *Critical Infrastructure Protection in the Information Age*
(<http://www.ciao.gov/News/EOonCriticalInfrastructureProtection101601.html>)

Relevance to the National Telecommunications and Information Administration (NTIA)

The NTIA must recognize the importance of security and its effect on public safety wireless communications systems. In 1996, the President of the United States stated that an interruption in public safety service would have a severe impact on the security of the country. In 1998, he created the Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, stressing the need to protect these infrastructures from physical and electronic risks and vulnerabilities. In 2001, following the September 11th attacks on America, the President created the Office of Homeland Security to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats and attacks. In this same security-conscious vein, the President, on October 21, 2001, issued the Critical Infrastructure Protection in the Information Age executive order, reaffirming the underlining policies put forth in Presidential Decision Directive 63. Both presidential acts on critical infrastructure protection underscore the fact that the development of secure public safety communication systems is critical in combating domestic terrorism and mitigating other national-scale incidents.

The NTIA, as a regulatory entity, can influence public safety wireless communications systems development. They can influence the federal public safety community and indirectly, the local and state public safety community on the benefits of secure public safety communications systems. The NTIA can also endorse approaches to security in the rulemakings.

Actions/Solution Steps for the National Telecommunications and Information Administration (NTIA)

The NTIA can take the following steps to ensure that security is adequately addressed to meet interoperability requirements. They can effectively raise the awareness of the security risks and vulnerabilities of wireless communications systems across the Nation. Additionally, the NTIA is in position to monitor national-level security issues regarding protection of critical infrastructures.

The following resources will prove useful to the NTIA in ensuring that security is adequately addressed to meet interoperability requirements—

- *Public Safety Communications Security Awareness Guide*
- *Digital Land Mobile Radio (DLMR) Security Problem Statement*
- *Public Safety Communications Security Briefing*
- *The Role of the Federal Government in Public Safety Wireless Interoperability*

The NTIA can also promote the development of security standards. By encouraging the public safety community to actively participate in the security standards process, the NTIA can influence others to support the adoption of security standards that enable interoperability among secure systems.

The following resource will prove useful to the NTIA in promoting the development of security standards—

- *Critical Infrastructure Protection in the Information Age*
(<http://www.ciao.gov/News/EOonCriticalInfrastructureProtection101601.html>)

Relevance to the Public Safety Wireless Network (PSWN) Program

The PSWN Program must recognize the importance of security and its effect on public safety wireless communications systems. Overall, the program has identified, promoted, and is now working toward developing solutions to several key security-related issues. These issues include the need to increase local, state, and federal public safety agency awareness of the security issues associated with evolving communications infrastructures while promoting the inclusion of security considerations in the systems development life-cycle process.

The PSWN Program is currently involved in several discrete activities to help resolve public safety security related issues. They are developing “how-to” guides that provide public safety officials with an overview of key issues affecting system security and how to incorporate security concerns into new communications system designs. The program also monitors ongoing security issues and provides security studies and analyses of existing wireless communications systems that help the public safety community better understand the security issues affecting them. In addition, the program should address necessary security issues identified by the Office of Homeland Security as it works to develop and implement a national strategy to secure our Nation against future domestic attacks.

Actions/Solution Steps for the Public Safety Wireless Network (PSWN) Program

The PSWN Program can take the following steps to ensure that security is adequately addressed to meet interoperability requirements. They can continue the process of educating decision makers and the public safety community on the relevance of security through the program’s many activities. These activities include PSWN Program-sponsored outreach forums and conference events, meetings with equipment manufacturers, and pilot or proof-of-concept solutions that test encryption or other security features. In addition, the Program should stand prepared for the possibility of a future Federal Agency communications network merger and/or a Federal to State communications network merger.

The PSWN Program can also continue to identify common security standards, guidelines, and recommendations, as well as sharing best practices for system security among the public safety community. They can also support the development and enactment of national strategies for infrastructure protection and assurance. The PSWN Program can prepare and distribute publications, videos, and how-to guides that help public safety agencies incorporate security best practices and approaches into their wireless communications systems. Additionally, the program must keep the public safety community informed of recent events in the security arena.

The PSWN Program can also actively participate in the development of security standards. By reviewing and providing comments on suggested security standards as they relate to the public safety community, the program can support the adoption of security standards that enable interoperability among secure systems. The PSWN Program is also in a position to monitor, on behalf of the public safety community, national-level security issues regarding protection of critical infrastructures.