
**Emergency Response Interoperability Center**

**Public Safety Advisory Committee (PSAC)**

# Considerations and Recommendations for Security and Authentication

**Security and Authentication Subcommittee Report**

**May 2011**

# Contents



# List of Tables

# List of Figures

# 1 Results in Brief

## 1.1 Executive Summary

The importance of cyber security to the nationwide interoperable Public Safety Wireless Broadband Network (PSWBN) must be recognized and adequately addressed. Given the significant role of the PSWBN to provide a comprehensive communications capability to our nation's first responders and government organizations chartered to protect life and property, protecting this national asset must be a high priority. A comprehensive Security Architecture, which includes technology, policies and procedures, must be implemented to ensure protection of the PSWBN from malicious attacks in the face of evolving cyber threats and to protect information and identities from compromise.

In this report, the PSAC Security & Authentication Work Group (S&A WG) makes the following recommendations:

- Adoption of a risk-based approach to cyber security for the PSWBN – This involves (1) Analyzing the Risk Profile (balancing impact of breach with cost of protection), (2) Understanding the Threat Environment, and (3) Addressing/Eliminating Vulnerabilities.
- Acceptance of a Statement of Key Objectives of the PSWBN Security Architecture to serve as guiding principles for implementing cyber security
- Mandatory implementation of key LTE standardized security features
- Roaming to commercial networks should be supported with standardized security technologies
- Access to the Internet should be allowed, contingent on an acceptable outcome of a full Risk/Threat/Vulnerability analysis
- Support for a diversified set of applications within a varied collection of jurisdictional-specific security policies and implementations by enabling layering of security features on top of a standardized mandatory baseline

The S&A WG has provided these recommendations in a manner that is flexible with respect to an evolving governance structure. Portions of these recommendations may be codified in the *Fourth Further Notice of Proposed Rulemaking* (*FNPRM*) rule-making process[1] and portions may be further adopted, and/or modified under the oversight of a PSWBN governance entity in the future.

The S&A WG recommends that implementation of the PSWBN begins with an initial security baseline that is continually updated as:

- The Risk/Threat/Vulnerability profile continues to evolve
- Cyber security technologies continue to advance
- Public safety jurisdictions upgrade their security policies and procedures

[1] *See* Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, PS Docket 06-229, *Third Report and Order and Fourth Further Notice of Proposed Rulemaking*, 26 FCC Rcd 733 (2011) (*Third Report and Order* and *Fourth FNPRM*, respectively).

# 2 Introduction

Emergence of wireless broadband is one of the most significant technology breakthroughs of the last decade. The widespread availability of wireless broadband capabilities has impacted nearly every facet of our lives. Now, our nation's first responders and organizations that provide emergency response are poised to leverage this technology in ways that will significantly enhance their ability to perform their mission.

For more than a decade our nation has engaged in active spectrum policy initiatives to enable wireless broadband for consumers and public safety in the 700 MHz spectrum. Favorable spectrum policy and availability of commercial broadband technology provide two key ingredients that now enable construction of a nationwide interoperable broadband network for public safety. The Public Safety Wireless Broadband Network (PSWBN) will enable unprecedented capabilities to those involved in providing emergency response.

Long Term Evolution (LTE) technology is emerging as the technology of choice for implementation of fourth generation (4G) broadband networks in the 700 MHz spectrum. Recent rule-making by the Federal Communications Commission (FCC), has affirmed the use of LTE technology for building the PSWBN. On a world-wide basis, LTE is also emerging as a dominant standard for wireless broadband networks. This trend is resulting in a prolific eco-system that will propel this industry forward. By leveraging this vast eco-system, significant economies of scale will be available to the public safety community, enabling a highly innovative and competitive supply chain.

Widespread worldwide use of LTE technology and the deployment of numerous LTE-based networks will also make these networks a frequent target of cyber attacks. It is reasonable to expect the sophistication, frequency and resolve of these attacks to increase over time. It therefore becomes a prime consideration in constructing our nation's public safety broadband network to provide for its cyber security from the onset and throughout its life. Because of its particular mission, it is also reasonable to expect aggressive cyber attacks on the PSWBN will occur by those hoping to exploit vulnerabilities in order to compromise network availability or access information and/or identities for malicious purposes. The S&A WG agrees with comments provided by Northrop Grumman, "the use of open and globally deployed standards, such as Internet Protocol (IP) that forms the core of the LTE-based public safety broadband wireless networks, considerably increases the vulnerability of these networks to malicious attacks, further underscoring the need for robust security mechanisms to protect these networks".[2] To that end, the Commission has properly recognized the need to protect this strategic asset along with the information and services it conveys. The S&A WG also notes that the Commission has on-going work on the topic of Cyber Security Best Practices.[3] That body of work provides very broad recommendations of direct relevance to the PSWBN.

Local public safety agencies are also governed by several federal laws as related to security. These federal laws are further driving forces requiring a robust security scheme. The two major ones are the Health Insurance Portability and Accountability Act (HIPAA) and Criminal Justice Information Services (CJIS). HIPPA covers the privacy and security of medical records. First responder emergency medical services personnel will need to use applications and devices which can recognize and conform to HIPPA requirements. CJIS has mandates and guidelines for limiting access to criminal justice information, widely used by law enforcement practitioners.

## 2.1 Working Group Team Members

The Public Safety Advisory Committee (PSAC) was established as a Federal Advisory Committee chartered to provide recommendations to the FCC regarding best practices and actions the Commission should undertake as part

[2] Comments of Northrop Grumman Information Systems, Inc. to *Fourth FNPRM*.

[3] Communications Security, Reliability and Interoperability Council (CSRIC), Working Group 2A Cyber Security Best Practices – Final Report, March 2011

of its rule making initiatives aimed at implementation of the PSWBN.

PSAC is organized into four working groups focused on the following topics:

1. Interoperability
2. Applications and User Requirements
3. Security and Authentication
4. Network Evolution

The Security and Authentication Work Group (S&A WG) is comprised of 8 members, including a Chair and two Co-Chairs. S&A WG membership was selected from the full PSAC membership by the Commission and PSAC leadership. The Security and Authentication Working Group consists of the members listed below.

| **Name** | **Representing** |
|---|---|
| Dennis Martinez - Chair | Harris Corporation |
| Stacey Black - Vice Chair | AT&T |
| Ken Zdunek- Vice Chair | Illinois Institute of Technology |
| Michael Cline | National Emergency Management Association (NEMA) |
| Dorthy Spears-Dean | Commonwealth of Virginia |
| Leonard Edling | The InterAgency Board (IAB) |
| Arnold Hooper | Tennessee Valley Regional Communications System |
| Robert Wideman | Nevada Department of Public Safety |

# 3 Objective, Scope, and Methodology

## 3.1 Objective

The S&A WG was tasked by the PSAC leadership with providing recommendations based on the following questions:

**Short Term Question:**

> *In order to ensure that the public safety broadband network is interoperable on a nationwide basis, what security and authentication features should each network be required to implement?*

**Long Term Question:**

> *What best practices can be adopted to ensure increased security on the public safety broadband network?*

Response to these questions is provided in the context of specific security and authentication topics addressed in the *Fourth Further Notice of Proposed Rule Making* (*Fourth FNPRM*).

## 3.2 Scope

The S&A WG was created on March 15, 2011 and tasked to develop this report with its associated recommendations as part of the record in the *Fourth FNPRM* proceeding. Given time constraints associated with the rule-making process, this S&A WG report was required to be finalized and its recommendations accepted by the entire PSAC membership by May 24, 2011. A key input to the S&A WG was provided by the comments provided to the Commission on the Fourth FNPRM in the April 10 timeframe.

### 3.2.1 Governance

Comments provided to the Commission in the *Fourth FNPRM* make frequent reference to the need to address the governance structure for the PSWBN, not only in the context of Security and Authentication issues, but on a very broad range of topics. A number of entities recommend that definition of many technical and operational aspects of the PSWBN should not be addressed in the Fourth FNPRM proceedings, but rather deferred to a yet-to-be defined governance organization.[4] Although the S&A WG shares similar concerns, it also holds the view that with respect to the Objectives described above, it is essential for the S&A WG and PSAC in whole to provide specific recommendations, independent from the governance issue. As the Commission and other policy makers continue to deliberate this important topic, this body of work would remain available to the Commission as it proceeds with rule making and also to a governance entity that may be created in the long-term.

## 3.3 Methodology

The S&A Work Group work flow was based on the following largely sequential steps:

1. Catalog the Fourth FNPRM sections relevant to Security and Authentication
2. Adoption of a framework in which to conduct the work

[4] See for example Andrew Seybold, APCO, City of Mesa, Arizona, NPSTC, and the Public Safety Spectrum Trust Corporation.

3. Review of the five LTE security groups as specified in the 3GPP standards
4. Development of initial recommendations for the five LTE security groups
5. Review and catalog comments provided to the Commission in the Fourth FNPRM
6. Identification of relevant security & authentication topics in addition to the five LTE security groups based on Fourth FNPRM material (supplemental security and authentication topics)
7. Refinement of initial recommendations for the five LTE security groups based on Fourth FNPRM material
8. Development of recommendations for the supplemental security and authentication topics

### 3.3.1 Information Assurance Framework

In the *Fourth FNPRM* the Commission sought input on very specific technical aspects of the PSWBN as well as input on a very broad and open range of topics. The S&A WG holds the view that response to specific technical questions required that these recommendations be anchored within an over-arching framework. Secondarily, addressing more open questions further drives the need for a holistic or top-down view of the problem.

Because of its widespread significance to nearly every facet of our lives, the field of cyber security contains a very large eco-system of contributors both in the public and private sectors. The S&A WG developed its top-down holistic methodology by drawing on this vast eco-system. A holistic approach to security for the PSWBN has also been advocated for by Northrop Grumman and Harris:

*"The interests of the public safety community are best served by approaching the security requirements of the 700 MHz public safety broadband wireless networks in a holistic manner that addresses public safety's fundamental mission of protecting property and saving lives. As a case in point, public safety first responders depend on the 24x7 availability of their communications network to carry out their mission, inextricably linking reliability and security of the public safety networks. Weak and compromised network security undoubtedly reduces reliability and hence availability. Without the proper security measures in place no amount of reliability features, such as site hardening and backup power, can assure the highest degree of availability required of the public safety communications networks."* [5]

*"Harris believes that development of a comprehensive security architecture, driven by suitable governance structure is critical to success of the public safety broadband network. Development of the architecture and governance structure should be based on well established Information Assurance (IA) principles, driven by clearly articulated objectives."*[6]

The top-down methodology selected by the S&A WG was to view the PSWBN as an Information System, comprising the LTE network, user applications and terminal devices, with interconnection to other commercial and private networks. This motivated the S&A WG to base its work on well established principles in the field of Information Assurance (IA). The National Institute of Standards and Technology (NIST) has devoted much effort to the topic of IA and the S&A WG used the NIST compilation of Security Principles (NIST Special Publication 800-27) as providing the top-down holistic view of the problem. The 32 specific principles in NIST SP 800-27 are listed in Appendix 2. The high level groupings of these principles are:

- Security Foundation
- Risk Based
- Ease of Use
- Increase Resilience
- Reduce Vulnerabilities

[5] Comments of Northrop Grumman Information Systems, Inc. to *Fourth FNPRM*.

[6] Comments of Harris Corporation to *Fourth FNPRM*.

- Design with Network in Mind

A complete IA framework involves not only the technical aspects of the security implementation, but also the policies and procedures that form and direct the operational component of the security implementation.

After review of these generic IA principles, the S&A WG developed the following Key Objectives for basing its work. The S&A WG furthermore recommends that these objectives be carried forward as the PSWBN design, deployment and operation commence:

**Table 1: Key Objectives for the PSWBN Security Architecture**

| | |
|---|---|
| ***Availability*** | Ensure that network services are not disrupted by malicious attacks |
| ***Privacy:*** | Ensure protection and integrity of sensitive data and identities |
| ***Interoperability:*** | Ensure that security mechanisms do not inhibit interoperability |
| ***Usability:*** | Ensure that security-enabled devices and services are easy to use |
| ***Quality of Service: QoS*** | Ensure that security mechanisms are not detrimental to achieving QoS required for mission critical applications |
| ***Cost Effective:*** | Ensure that the cost of implementing security is consistent with the cost associated with security breach |
| ***Standards Based:*** | Ensure robust standards are used for implementing the PSWBN Security Architecture |
| ***Flexibility:*** | Ensure that security can be tailored to support role-based security and allow local control and management of security, consistent with the over-arching security policy |

### 3.3.2 Risk Based Methodology

In the field of IA, one of the methodologies that has emerged and is now commonly accepted is that of a Risk Based Methodology. This methodology involves three key components:

| Table 2: Risk Based Methodology | |
|---|---|
| **Risk** | • Understanding exposure to threats<br>• Assessing likelihood of attack and success<br>• Performing up-front and on-going risk assessments that attempt to quantify likelihood and cost of a breach |
| **Threats** | • Understanding source and means of particular types of attack<br>• Threat assessments are performed to determine best method(s) of defense<br>• Organizations perform penetration testing to assess threat profiles |
| **Vulnerabilities** | • Weaknesses or flaws in a system that permit successful attacks<br>• Can be policy related as well as technology related<br>• Vulnerability assessment should be performed on an on-going basis |

This methodology is used to develop and measure the effectiveness of a cyber security system. It can also be used as a litmus test for assessing the risk/benefit of introducing capabilities into a system. For example, the S&A WG recommends use of this methodology to determine if access to the Internet from the PSWBN should be allowed.

It is also worth noting that the International Telecommunication Union (ITU) has developed a standard based on this methodology. ITU-T X.805 is a standardized, risk-based framework for assessing risks/vulnerabilities and developing an end-to-end approach to securing next-gen communications systems. It is a best practice in the commercial world. The ITU-T X.805 framework is useful way to organize the complexity of security requirements into manageable requirements - covering access control, authentication, non-repudiation, data confidentiality, data integrity, availability, and privacy.

### 3.3.3 Assumptions

In applying the risk-based methodology to the PSWBN, there are some fundamental assumptions relative to the three components described above. These assumptions define the PSWBN Security Profile and are summarized in Table 3.

| Table 3: PSWBN Security Profile | |
|---|---|
| **Risk** | • Many public safety organizations rely on commercial wireless data services today – that risk profile is deemed appropriate for the types of services that utilize these networks<br>• Increased reliance of the PSWBN by first responders for mission-critical applications will increase that risk profile<br>• Public safety networks must work when nothing else does – the mission is to protect life and property – This places a very high risk/cost associated with breaches to the security system. |
| **Threats** | Many types of cyber threats will likely be present. A representative sample is:<br><br>• Denial of Service (DoS) attacks<br>• Theft of Service (TOS)<br>• IP address spoofing<br>• User ID theft<br>• Intrusion Attacks<br><br>The threat environment will continue to evolve over time with ever-more sophisticated attacks to be expected in the future |
| **Vulnerabilities** | • The LTE network will be open to many users<br>• Many applications will operate over the network<br>• Subject to debate, access to the Internet may be provided[7]<br>• Large emerging eco-system of devices with a variety of computing environments will emerge<br>• The PSWBN will be a frequent target of attack<br>• Commercial LTE networks will be a frequent target of attack. Because of their connection to a common technology, success of commercial network attack may impact the PSWBN. |

[7] Many local and state jurisdictions restrict access to the Internet for their mobile workers and responders. The ability for local jurisdictions to monitor, log and control this access to comply with local laws and policies must be accommodated.

# 4 Background

The Commission seeks recommendation on specific topics of cyber security related to the PSWBN in *the Fourth FNPRM*. In the *Third Report and Order*, the Commission mandated that all networks deployed in the 700 MHz public safety broadband spectrum adopt LTE, specifically at least 3GPP Standard E-UTRA Release 8 and associated EPC.[8] On the basis of that ruling, a significant portion of the Security Architecture is pre-determined in accordance with the 3GPP standards. Therefore, consistent with the Key Objectives described in Section 3.3.1, the S&A WG recommends adoption of the standardized LTE security framework as it relates to the five LTE Security Groups:

1. Network Access Security
2. Network Domain Security
3. User Domain Security
4. Application Domain Security
5. User Configuration and Visibility of Security

Specific recommendations relative to these security groups is contained in Section 5.1.1 of this report.

In addition to the five LTE security groups above, the S&A WG identified three other Supplemental Security & Authentication topics that warrant recommendations. Identification of these topics became evident upon review of comments provided to the Commission in response to the Fourth FNPRM.

- Roaming to Commercial Networks
- Support for varied application and security requirements associated with a diverse public safety market and the applications and software specific to individual cities, counties, regions and states
- Access to the Internet

[8] *See Third Report and Order*, 26 FCC Rcd at 738 ¶ 10.

# 5 Analysis, Findings and Recommendations

Figure 1 illustrates the network domains that define security boundaries for the PSWBN. At the core is the PSWBN, comprised of one or more regional networks interconnected to form a single nationwide interoperable network. In accordance with the architectural structure of LTE, the PSWBN consists of an LTE Core Network and an LTE Radio Access Network (RAN). At the edges of the network are Jurisdictional Network Domains located within the many participating public safety entities and the Mobile Network Domains comprised of subscriber devices and client applications. Services associated with roaming between the PSWBN and commercial networks are provided through Inter-Carrier Services interfaces. Standardized Inter-Carrier roaming capabilities are also defined in the 3GPP LTE Standards. Internet access (if allowed) is provided through fire-walls into the PSWBN.

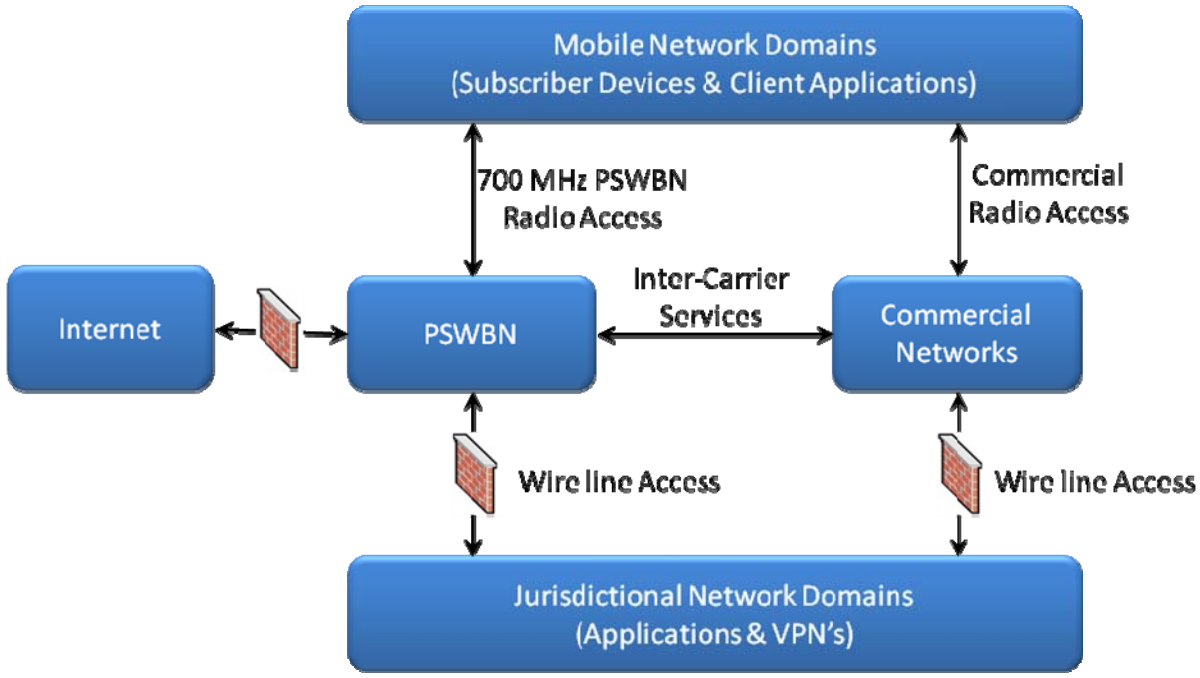


**Figure 1: Network Security Domains**

## 5.1 LTE Security Groups

As noted earlier, the Public Safety Broadband Network third Report and Order mandates LTE as the technology standard. In so doing, much of the Security Architecture becomes defined. Figure 2 illustrates the LTE Security Architecture.[9] It consists of five security groups. Each security group addresses certain threats and accomplishes certain security objectives

- (I) Network Access Security – The set of security features that provide users with secure access to services, and which in particular protect against attacks on the (radio) access link[10]
- (II) Network Domain Security – The set of security features that enable nodes to securely exchange signaling data, user data (between AN and SN and within AN), and protect against attacks on the wire line

[9] 3GPP TS 33.401 V8.7.0 (20-10-04)

[10] 3GPP TS 33.401

network[11]

- (III) User Domain Security – The set of security features that secure access to mobile stations[12]
- (IV) Application Domain Security – The set of security features that enable applications in the user and in the provider domain to securely exchange messages[13]
- (V) Visibility and Configurability of Security – The set of features that enables the user to determine whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature[14]

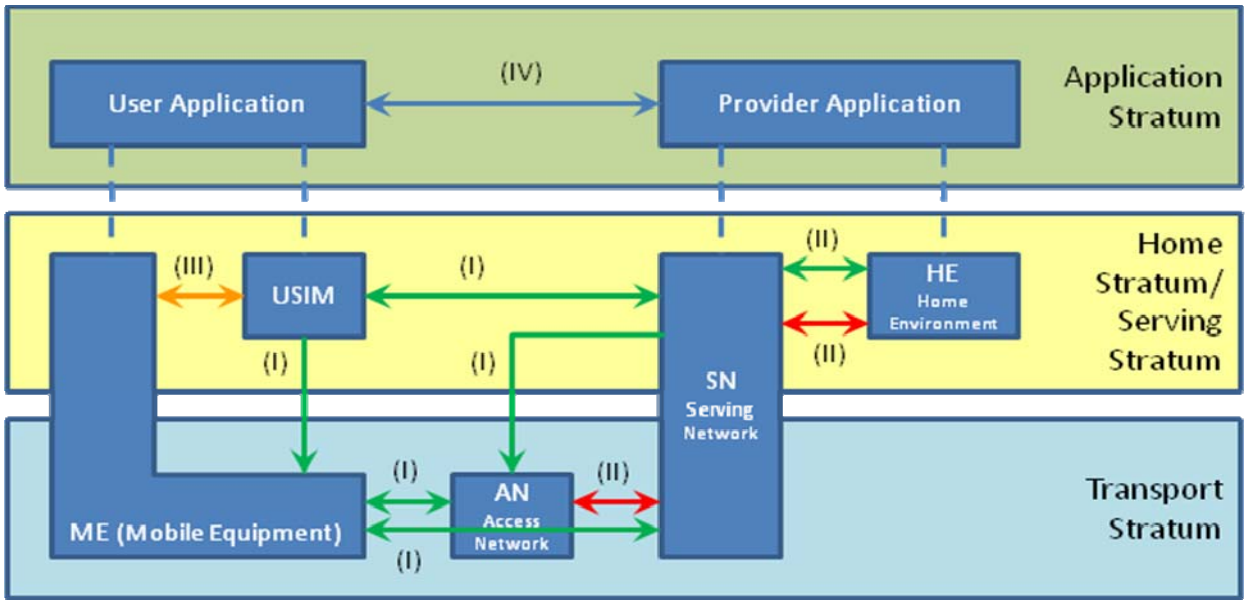


**Figure 2: LTE Security Architecture**

### 5.1.1 LTE Security Groups: Analysis, Findings & Recommendations

The recommendations described in this section were developed using the overall methodology described in Section 3.3, with the following additional guiding principles.

1. Balance the need for security and authentication processes with the need to impose as few operating requirements on users of the network as possible. The understanding developed was that if the security procedures imposed on the network users were overly burdensome, the PSWBN would not realize its value.
2. Recommend only the minimum number and type of security requirements to insure interoperability, without hindering the ability of individual jurisdictions, or a future nationwide governing entity, to go beyond the minimum. It is recognized that effective security and authentication requires an ongoing process of risk assessment and response. Any mandated requirements should be at a high enough level to

[11] 3GPP TS 33.210

[12] 3GPP TS 33.102

[13] 3GPP TS 33.102 and TS 31.111 is an optional feature

[14] 3GPP TS 33.102 and TS 22.101 is an optional feature

allow future refinement and further specification as required to deal with future threats.

3. Follow industry best-practices and utilize existing standards wherever possible, balancing the requirements of all the PSWBN stakeholders, (public safety jurisdictions, public safety users, suppliers). Where security processes are necessary, public safety should have the ability to procure standards-based approaches, allowing public safety to procure equipment from multiple suppliers
4. Recommendations should reflect a consensus (convergence) of viewpoints from the PSWBN stakeholder communities.

The following sections describe and summarize the Working Group responses to the specific questions posed by the Commission in the FNPRM with regard to Security and Authentication, within the five security domains as described in the 3GPP LTE standards: Network Access, Network Domain, User Domain, Application Domain, and Visibility and Configurability. The table contained in each section summarizes the security domain context, the FCC position and questions posed the S&A WG supplied context, PSAC SA & WG position, and additional S&A WG commentary on the position.

#### 5.1.1.1 Network Access Security

| Comments | FCC Position | FCC Questions |
|---|---|---|
| Consists of three protocol layers:<br><br>1. LTE signaling layer security features over the Radio Resource Control (RRC) protocol layer (UE and eNodeB)<br>2. EPC signaling layer security features over the Non Access Stratum (NAS) protocol layer (UE and MME)<br>3. User data/control layer security features over the Packet Data Convergence Sublayer (PDCP) protocol layer (UE and eNodeB) | FCC Tentative conclusion is that all 3 layers should be required. | Are all 3 security features for Network Access Security appropriate to ensure security of the public safety broadband network? We seek comment on this tentative conclusion. Is this sufficient to ensure network access security? Does the public safety community require additional security? If so, what is this and what are the costs incurred to achieve this? |
| **PSAC SA WG Background** | **PSAC SA WG Position** | **PSAC SA WG Comments** |
| • Reference NIST SP 800-27 Security Principles used as framework for discussion<br>• Key Objectives of PSWBN Security Architecture on which position is based (availability, interoperability, privacy, usability, QoS, cost effectiveness, standards based)<br>• IA drivers: risk, threats, vulnerability<br>• Expected Types of Attacks: DoS; Bidding down; eavesdropping | • All three layers should be required. (uE/NAS, uE/eNB (control plane) and uE/eNB (user plane)—Agree with FCC | • eNodeB part of "Trusted Environment"- contrasts with conventional PS wireless architecture<br>• Radio Access Network is the most exposed--vulnerable to attacks<br>• Uniform approach is necessary condition for enabling interoperable roaming.<br>• S&A WG position is in contrast with PS FNPRM comments that security should not be regulated. |

The consensus position of the Working Group regarding security in the (radio) Network Access domain is that the LTE security features in the Radio Resource Control (RRC) protocol layer, the Enhanced Packet Core (EPC)/Non Access Stratum, and the user data/control layer over the Packet Data Convergence Sublayer should be required, as recommended by the FCC. The justification of requiring these security provisions is that the Radio Access Network is the most vulnerable to external attacks, and unlike current public safety networks, commercially available user equipment will be available that operates according to the LTE protocols. Furthermore it is viewed that to insure interoperability, a uniform, standards-based approach is necessary. Since the 3GPP LTE standard has

already developed these security procedures, it is the view of the working group that these constitute a minimum requirement for Radio Network Access security. While the Working Group could identify no compelling reasons to require more than these security procedures, this conclusion should not be interpreted as contradicting the previously stated principle that a continuous process of risk assessment as part of the ongoing operation of the future PSWBN is required to respond to newly generated threats.

#### 5.1.1.2 Network Domain Security

| Comments | FCC Position | FCC Questions |
|---|---|---|
| | None | Should we adopt rules for network domain security? If so, what should they be? Do the optional features specified in 3GPP TS 33.210 fully serve the purpose of network domain security? Are they sufficient? Which optional features should be selected? Would there be any interoperability issues should the commission choose not to require network domain security features, or not to select them? |
| **PSAC SA WG Background** | **PSAC SA WG Position** | **PSAC SA WG Comments** |
| | • Network Security Domains should be implemented consistent with 3GPP TS 22.210 (defines IPSec and IKE profiles) | • Uniform approach a necessary condition for interworking between regional PSBB networks<br>• S&A WG position is in contrast with PS FNPRM comments that security should not be regulated |

The consensus position of the Working Group is that a consistent approach to security in the LTE Network Domain is necessary to insure seamless interworking between regional networks that may be deployed using equipment from different suppliers. Without rules governing the Network Domain Security procedures, the possibility exists that regional networks could implement non-standard (vendor proprietary) approaches that would hinder interoperability and reduce the utility of the PSWBN. Furthermore, the lack of rules requiring a standards-based approach to Network Domain Security could limit Public Safety organizations from purchasing equipment from multiple vendors, reducing competition and resulting in potentially higher infrastructure costs. Finally, without some standards for security rules, such practices could also limit the ability of transient users (public safety officers responding to an incident in a jurisdiction or passing through the jurisdiction) from using the network. The Working Group therefore concludes that Network Domain Security as specified in 3GPP TS 22.210 be required.

### 5.1.1.3 User Domain Security

| Comments | FCC Position | FCC Questions |
|---|---|---|
| Mandatory feature according to 3GPP TS 33.102 for the operation of the LTE network. See 3rd Generation Partnership Project, "3G Security; Security architecture (Release 8)," 3GPP TS 33.102 (2009). | The public safety broadband network must support it and it is not the subject of this notice. | |
| **PSAC SA WG Background** | **PSAC SA WG Position** | **PSAC SA WG Comments** |
| | • Supports this mandatory 3GPP feature according to TS 33.102. | • No overriding reason not to require this 3GPP mandatory feature.<br>• S&A WG position is in contrast with PS FNPRM comments that security should not be regulated |

While the FCC has not formulated any questions in the Fourth FNPRM regarding User Domain Security in the PSWBN, the consensus view of the Working Group is to restate its agreement with the FCC that this 3GPP mandatory feature be required.

### 5.1.1.4 Application Domain Security

3GPP standards permit executing applications on the Universal Subscriber Identity Module (USIM) based on the USIM application Toolkit as defined in TS 31.111. Application Domain Security enables secure communication with these USIM-based applications.

| Comments | FCC Position | FCC Questions |
|---|---|---|
| | None | Should the Commission adopt rules for application domain security? Do the optional features specified in these standard specifications fully serve the purpose of application domain security? Are they sufficient? Which optional features should be selected? Would there be any interoperability issues should the Commission choose not to require application domain security features, or not to select them? |
| **PSAC SA WG Background** | **PSAC SA WG Position** | **PSAC SA WG Comments** |
| • Application Domain Security may be required by certain public safety entities. Two categories of applications identified: USIM resident applications, and non-USIM resident apps.<br>• USIM resident applications create security vulnerabilities for Public Safety. (i.e. USIM access)<br>• VPNs are a key method for E2E and application domain security and interoperability. | • Application Domain Security as specified in 3GPP TS 33.102 and TS 31.111 should be mandated for USIM-based applications.<br>• VPN support should be required by PSWBN regional networks. | • While public safety may not widely employ USIM-based applications, it is necessary to protect the PSWBN from vulnerabilities causes by this type of application.<br>• If USIM-based applications are used, they should be subject to the 3GPP security procedures. |

The Working Group identified two application categories within the 3GPP LTE architecture relative to its security analysis: USIM (Universal Subscriber Identity Module) resident applications, and non-USIM resident applications. The consensus view of the Working Group is that because of the security vulnerabilities of USIM-based applications, the use of 3GPP TS 33.102 and TS 31.11 should be required for this application type. The Working Group further concludes that VPNs (Virtual Private Networks) will be the primary method that public safety jurisdictions use to establish End-to-End (E2E) application-level security. Therefore, the PSWBN should be required to support VPNs.

#### 5.1.1.5 Visibility and Configurability of Security

| Comments | FCC Position | FCC Questions |
|---|---|---|
| | None | Should the Commission adopt rules for visibility and configurability of security? Are these necessary to ensure the operability and interoperability of the public safety broadband network? Do the optional features specified in these standard specifications fully serve the purpose of visibility and configurability of security? Are they sufficient? Which optional features should be selected? Would there be any interoperability issues should the Commission choose not to require visibility and configurability of security features, or not to select them? What are the cost implications of such requirements? |
| **PSAC SA WG Background** | **PSAC SA WG Position** | **PSAC SA WG Comments** |
| • Visibility of Security as specified in 3GPP TS 33.102 is notionally consistent with certain established policies and procedures used in public safety (e.g. notification of secure/insecure link) | • 3GPP TS 33.102 and TS 22.101 should not be mandated.<br>• If a particular jurisdiction requires a Visibility function, it should be in accordance with the above specifications.<br>• PSWBN regional networks and application providers should be required to support these 3GPP capabilities. | • Allowing public safety users to set security policy parameters could compromise security. As FNPRM commenters have noted, user configurability of security parameters is not a standard practice within public safety today. |

The view of the Working Group is that while the visibility to the end user of the security status of a session or call is generally a requirement for public safety, the provisions of 3GPP TS33.102 and TS 22.101 do not reflect public safety requirements. In particular, the configurability of Security as specified in these 3GPP documents does not reflect public safety practice. For this reason, the consensus of the Working Group is that the Visibility and Configurability of Security as described in 3GPP TS 33.102 and TS 22.101 should not be mandated by the FCC. It is the further view of the Working Group, however, that if a Public Safety jurisdiction does require a Visibility of Security function, it be implemented according to the provisions of these specifications.

## 5.2 Roaming to Commercial Networks

The topic of roaming to commercial networks is an area the Commission is seeking input in the *Fourth FNPRM* proceedings. The S&A WG provides the following considerations on security matters relative to these proceedings.

User Equipment (UE), or more specifically its Universal Integrated Chip Card (UICC)[15] that is homed on the

[15] UICC (Universal Integrated Chip Card) is a mandatory secure element of the LTE environment, ensuring safe and protected access to mobile LTE and IMS networks.

PSWBN will need to be provisioned with Public Land Mobile Network (PLMN) Identifiers of the networks it is allowed to roam onto, should it leave the PSWBN as its home network. The Visited PLMN (VPLMN) list of PLMN ID's is stored in order of priority and may also list specific networks the UE should reject (forbidden VPLMNs). Once provisioned and appropriate roaming agreements with the Visiting network operator have been executed, the UE can establish a connection on the visited network.

A variety of Management/Administration and User Services will be enabled by the PSWBN-to-Commercial Carrier interface(s), including but not limited to data exchanges for billing and fraud prevention and Short Message Service (SMS).

As is common practice with inter-carrier roaming between commercial networks, a data session may terminate upon leaving the PSWBN requiring the user device to re-register and re-authenticate its session on the visited network. Under this scenario, data is not tunneled between the visited and home networks. To mitigate the adverse affect of this, it is recommended that public safety agencies employ session persistence middleware as part of a Virtual Private Networking (VPN) application (see below). This is accomplished by establishing a virtual IP address for each VPN session. As users roam, enterprise application servers always see the same, unchanging virtual IP address rather than network-specific IP addresses. With session persistence, there is no need to re-segment networks, implement Virtual Local Area Networks (VLANs) or deploy additional hardware to enable mobile workers to traverse networks seamlessly. Session persistence allows a user's session to be suspended during hand off to disparate networks and will automatically reestablish the session upon registering on the visited network. The VPNs also enable continuity of established security credentials and hence secure services across different networks.

## 5.3 Applications and Virtual Private Networks

The PSWBN will interface to IT systems from State, Local, Federal and Tribal jurisdictions.[16] In particular, applications (both infrastructure and mobile clients) reside within the domain of these jurisdictions and hence will be subject to their own IA policy manuals. The San Francisco Bay area comments "the security and encryption needs of public safety also have to conform to state and federal requirements, including FIPS 140-2, Department of Justice, and NCIC requirements."[17] It is also important to recognize that the LTE standard does not define all elements of the Security Architecture. The S&A WG recommends that these two real-world situations be accommodated by permitting layering of security features on top of the baseline security features provided within the PSWBN. The use of VPN's is an example of this layering concept. Another example is the use of end-to-end encryption techniques used to protect sensitive or perhaps possibly classified material.

With respect to potential use of the PSWBN by the Federal Government, the S&A WG refers to comments offered by Northrop Grumman:

*"Northrop Grumman also thinks that it is entirely plausible for the nationwide public safety broadband wireless network to be shared by the federal government. During an emergency event, multiple agencies from all levels of government, including federal, state, and local, will need to communicate and share information with each other in order to mount an effective and coordinated response. Northrop Grumman would like to note that the federal government follows its own standards and guidelines for exchanging and securing information as codified in the*

[16] The S&A WG recognizes that access to the PSWBN by Federal and Tribal agencies is a topic of active rule making. Depending on the outcome of that rule making process, Federal and/or Tribal jurisdiction participation may or may not occur.

[17] Comments of the San Francisco Bay Area in Response to the *Fourth FNPRM*.

*Federal Information Processing Standards (FIPS).* [18]

*FIPS 140-2 is a NIST standard that specifies security requirements for cryptographic modules within a security system protecting sensitive but unclassified information. Because LTE's encryption schemes do not adhere to these standards in all cases, FIPS validated and certified solutions will need to be integrated with the public safety network in order to meet the government requirements for secure communications. In short, use of state-of-the-art technology for securing the network must be complemented with clearly defined and documented agency specific security policies and procedures, as well as personnel who are trained in implementing, monitoring, and enforcing these policies and procedures. An important aspect of security policy and procedures that cannot be overlooked is a well thought out contingency plan describing the sequence of actions that are needed to mitigate, limit, and contain damage in the unforeseen event that a security breach does indeed happen."* [19]

The S& A WG recommends all PSWBN users implement Virtual Private Network (VPN) middleware on wireless devices and computers that will be used to access sensitive databases and other information. The S&A WG recommends that as a minimum, public safety agencies employ a strong, standards-based authentication and encryption method that meets Department of Justice requirements. Many applications feature single sign-on and inter-network roaming capabilities that make security transparent to the end user. In these applications, users only need to log in once, for the duration of their session. There are no additional steps or passwords to remember, no matter how many different networks they use. The VPN tunnel encrypts all data transmitted to guard against eavesdropping.

Two-factor authentication is federally mandated for many law enforcement agencies, and the S&A WG recommends it for all users of the PSWBN.[20] It requires a second factor — something the user has — in addition to a password to successfully authenticate the user. There are many well developed best practices that applications should support, such as RSA SecurID, smart cards or X.509v3 user certificates. By leveraging technologies such as RADIUS-EAP (Extensible Authentication Protocol) and standard Public Key Infrastructure (PKI) available from many vendors and built into Microsoft server operating systems, many VPN solutions can provide options for strong, two-factor user authentication with little or no incremental cost.[21]

The S&A WG recommends use of VPNs that have utilized FIPS 140-2 validated AES encryption modules. FIPS 140-2 is the United States government's standard for securing non-classified information which is commonly required in public safety systems.[22] End-to-end encryption provides security for all data transmitted between the

---

[18] Federal Information Processing Standards (FIPS) are standards and guidelines for information processing issued by National Institute of Standards and Technology (NIST) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.

[19] Comments of Northrop Grumman Information Systems, Inc. to *Fourth FNPRM.*

[20] For example, the FBI CJIS Advanced Authentication (AA) standard requires the replacement of weak passwords with strong authentication technology for every user that accesses the CJIS databases.

[21] The Remote Authentication Dial In User Service (RADIUS) protocol described in IETF RFC 2865 and RFC 2866 define standardized methods for carrying authentication, authorization and accounting information between a Network Access Server (NAS) and a shared Accounting Server.

[22] FIPS PUB 140-2 is a U.S. government computer security standard used to accredit cryptographic modules. This standard defines an information technology security accreditation program for cryptographic modules produced by private sector vendors who seek to have their products certified for use in government departments and regulated industries (such as financial and health-care institutions) that collect, store, transfer, share and disseminate sensitive but unclassified (SBU) information.

device and the server with FIPS 140-2 validated AES encryption, in 128-bit, 192-bit or 256-bit strengths.

## 5.4 Access to the Internet

Comments to the Fourth FNPRM are generally supportive of Internet access from the PSWBN, but express some notable misgivings.

*"This topic [Internet access] is discussed in paragraph 93-96 of the FNPRM. The required nationwide Public Safety applications need more discussion. However, I do NOT believe access to the public Internet is a required application. Indeed, I am concerned such access presents grave security and operational issues."*[23]

*"However, we also acknowledge that connectivity to the Internet to provide access to vital public safety information is increasingly important to public safety agencies. Local and incident-based use of the Internet should therefore be available, but only with proper security and Denial-of-Service attack (DoS attack) preventative measures put in place to ensure the on-demand access for information from the public Internet will not interfere or have an impact on the core of the public safety broadband network. Further, appropriate provisions are needed within the public safety network governance structure to ensure that network managers have the ability to disconnect any and all connections from the Internet in case of cyber aggression on and over the Internet."*[24]

*"The PSWBN will have to be connected to the public internet to access it, and thus through routers, firewalls, and other means establishing demarcation, part of it. However, the State does not feel that routing mission-critical traffic through the public internet is appropriate, and that no enterprise customer – public of private – would be comfortable doing so regardless of the security of data exchange afforded through VPN with AES or comparable isolation and security."*[25]

There are many examples where Internet access is used in public safety operational missions. Within the S&A WG membership, it was noted that in the course of performing their mission, public safety personnel may have need to access to weather sites such as the National Weather Service. Traveling Urban Search and Rescue (US&R) teams must be able to do Open Source Intelligence (OSINT) research on where they are responding to. Local HAZMAT teams perform Internet-based research on chemicals in route to an incident. Officers in cruisers must have a way to exploit Twitter, Ustream, Face book and other social media sites during their response. The goal of the PSWBN must be to enable these types of real-world applications without compromising security.

By way of best practices:

- The S&A WG recommends that all users of the PSWBN employ suitable firewalls, virus and intrusion detection, spam filtering, and Denial of Service (DoS) monitoring tools within their specific local area network enclaves. Regardless of the measures of protection the PSWBN ultimately employs, each IT department should be prepared to protect itself from any number of attacks regardless of the originating end point.
- PSWBN users should be employing custom Access Point Names (APNs) to direct UE session traffic to specific servers. Additionally, custom IP addresses may be employed to limit certain users to within an intranet domain, and only provide access to the public Domain Name Service (DNS) upon specific permissions.

---

[23] Andrew Seybold - Comments And Petition For Reconsideration, reply comments to *Fourth FNPRM.*

[24] Comments of APCO in Response to *Fourth FNPRM*.

[25] Comments of Minnesota Department of Public Safety in response to *Fourth FNPRM*.

The S&A WG recommends that it should be the responsibility of the PSWBN governing body(s) to decide on the level of security precautions and investments that should be applied to the access networks. Working with industry partners, as well as the Commission and the Department of Homeland Security, a best practices document should be provided to the PSWBN governance leadership with recommendations.

The tentative recommendation of S&A WG is that access to the Internet should be allowed, contingent on an acceptable outcome of a full Risk/Threat/Vulnerability analysis.

# 6 Conclusions

The PSWBN will bring unprecedented capabilities to our nation's first responders and government agencies that support the public safety mission. Built on the latest broadband standards and supported by a large emerging eco-system, the PSWBN will enable nation-wide interoperability to become a reality. While providing this unprecedented capability, the PSWBN will also experience unprecedented cyber threats. Providing for comprehensive cyber security is of vital importance to ensure the PSWBN remains viable when it is needed most by first responders and government organizations responsible for providing emergency response. Simply put, the PSWBN must work when nothing else does – especially in the face of malicious attacks to this vital asset.

The S&A WG has made recommendations in this report relative to both short-term and long-term issues related to cyber security for the PSWBN. These recommendations are provided independent of the evolving governance structure.

There are important facets of implementing the PSWBN Security Architecture that this report does not include which must be addressed in the future.

- Defining requirements for securing the management systems used to monitor, configure and control the PSWBN network is an open issue that should be addressed in the future.
- Defining requirements for transaction logging and analytics that enable implementation of the on-going functions associated with a security architecture built on risk-based methodology.
- Development and distribution of applications (an "apps store") will pose particular vulnerabilities and must receive full treatment under the risk-based methodology.

Ensuring Cyber Security for the PSWBN is not an end-point, it is a process. This process must begin early in the design and implementation phases and must continue throughout the lifecycle of the PSWBN.

# Appendix 1: List of Acronyms

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| AN | Access Network |
| AS | Access Stratum |
| CJIS | Criminal Justice Information Services |
| DoS | Denial of Service |
| EAP | Extensible Authentication Protocol |
| EPC | Enhanced Packet Core |
| FCC | Federal Communications Commission |
| FNPRM | Further Notice of Proposed Rule Making |
| HAZMAT | Hazardous materials |
| HE | Home Environment |
| HIPPA | Health Insurance Portability and Accountability Act |
| IA | Information Assurance |
| IT | Information Technology |
| ITU | International Telecommunication Union |
| LTE | Long Term Evolution |
| ME | Mobile Equipment |
| NAS | Non Access Stratum |
| OSINT | Open Source Intelligence |
| PKI | Public Key Infrastructure |
| PLMN | Public Land Mobile Network |
| PSAC | Public Safety Advisory Committee |
| PSWBN | Public Safety Wireless Broadband Network |
| QoS | Quality of Service |
| RAN | Radio Access Network |
| RRC | Radio Resource Control |
| S&A WG | Security & Authentication Work Group |
| SMS | Short Message Service |
| SN | Serving Network |
| UICC | Universal Integrated Chip Card |
| UE | User Equipment |
| US&R | Urban Search and Rescue |
| USIM | Universal Subscriber Identity Module |
| VLAN | Virtual Local Area Network |
| VPLNM | Visited Public Land Mobile Network |
| VPN | Virtual Private Network |

# Appendix 2: Security Principles (NIST SP 800-27)

The NIST compilation of Security Principles is reproduced here for convenience.[26]

**Security Foundation**

- Principle 1. Establish a sound security policy as the "foundation" for design
- Principle 2. Treat security as an integral part of the overall system design
- Principle 3. Clearly delineate the physical and logical security boundaries governed by associated security policies
- Principle 4. Ensure that developers are trained in how to develop secure software

**Risk Based**

- Principle 5. Reduce risk to an acceptable level
- Principle 6. Assume that external systems are insecure
- Principle 7. Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness
- Principle 8. Implement tailored system security measures to meet organizational security goals
- Principle 9. Protect information while being processed, in transit, and in storage
- Principle 10. Consider custom products to achieve adequate security
- Principle 11. Protect against all likely classes of "attacks"

**Ease of Use**

- Principle 12. Where possible, base security on open standards for portability and interoperability
- Principle 13. Use common language in developing security requirements
- Principle 14. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process
- Principle 15. Strive for operational ease of use

**Increase Resilience**

- Principle 16. Implement layered security (Ensure no single point of vulnerability)
- Principle 17. Design and operate an IT system to limit damage and to be resilient in response
- Principle 18. Provide assurance that the system is, and continues to be, resilient in the face of expected threats
- Principle 19. Limit or contain vulnerabilities
- Principle 20. Isolate public access systems from mission critical resources (e.g., data, processes, etc.)
- Principle 21. Use boundary mechanisms to separate computing systems and network infrastructures
- Principle 22. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations
- Principle 23. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability

**Reduce Vulnerabilities**

---

[26] For more details refer directly to NIST Special Publication 800-27.

- Principle 24. Strive for simplicity
- Principle 25. Minimize the system elements to be trusted
- Principle 26. Implement least privilege
- Principle 27. Do not implement unnecessary security mechanisms
- Principle 28. Ensure proper security in the shutdown or disposal of a system
- Principle 29. Identify and prevent common errors and vulnerabilities

**Design with Network in Mind**

- Principle 30. Implement security through a combination of measures distributed physically and logically
- Principle 31. Formulate security measures to address multiple overlapping information domains
- Principle 32. Authenticate users and processes to ensure appropriate access control decisions both within and across domains