Compendium of Emergency Communications and Communications Network Security-related Work Activities within the Telecommunications Industry Association (TIA)

ABSTRACT

This document identifies standards, or other technical documents and ongoing Emergency/Public Safety Communications and Communications Network Security-related work activities within the TIA, and is presented for information, coordination and reference. TIA is accredited by the American National Standards Institute (ANSI) and recognized under the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) Recommendations A.5 and A.6. These Recommendations, respectfully involving, the referencing of other organizations, including TIA technical documents[1], in ITU-T work (*i.e.*, draft and mature Recommendations) and in the cooperation and exchange of information between ITU-T and other Standards Development Organizations (SDOs). ITU-Radiocommunication Sector (ITU-R) Recommendations also normatively reference TIA work. In addition to Engineering Committee work, TIA continues to be active in matters involving national and international Public Safety, Homeland Security, National Security and Emergency Preparedness (NS/EP), and Critical Infrastructure Protection (including international partnership projects).

INTRODUCTION

This compendium summarizes Emergency/Public Safety Communications and Communications Network Security-related work, within TIA. Currently, technical work is mainly being developed under TR-8 (Mobile & Personal Private Radio Standards), TR-30 (Facsimile Terminal Equipment and Systems), TR-34 (Satellite Equipment and Systems), TR-41 (User Premises Telecommunications Requirements), TR-42 (User Premises Telecommunications Infrastructure) and TR-45 (Mobile and Personal Communications Systems) Engineering Committees (TRs). In addition, this document encapsulates areas of activities, involving national and international Public Safety, Homeland Security, Network Security and Emergency Preparedness, and Critical Infrastructure/Asset Protection, which do not fall under a specific TR. For the purpose of this document, the terms Public Safety and Disaster Response are synonymous with the terms Public Protection and Disaster Relief. As an ANSI-accredited SDO, TIA develops consensus-based, voluntary industry standards for a wide variety of national and global telecommunications products and systems. TIA_standards and their descriptions can be searched and accessed at: http://www.tiaonline.org/standards/search_n_order.cfm.

TIA Standards and Technology (S&T) Department: http://www.tiaonline.org/standards/

NOTE: **Clarification regarding TIA documents:** Most documents included in this compendium involve American (ANSI-approved) National Standards (ANS), Interim Standards (IS), Telecommunications Systems Bulletins (TSB) and TIA-only standards. An ANS has been approved through the TIA and the ANSI balloting process and is indicated, in the title, by the prefix ANSI/TIA/EIA-XXX. Note that the term “standards” implies voluntary, consensus-based development and does not specifically indicate an industry or national mandate, but more aligns with the international SDO term “Recommendation,” unless mandated by governmental rules and regulations (*i.e*., FCC in the USA, etc.). Note that as of August 2, 2002, any newly published TIA ANS will NOT include the EIA (*e.g*., TIA/EIA) in its standards designation number. The document title will indicate status as an ANS (*i.e.*, ANSI/TIA-XXX) or a TIA-only standard (*i.e.*, TIA-XXX).

[1] Includes published documents or work currently being developed under various TIA Engineering Committees.

TIA Contact: David Thompson
Tel: +1.703. 907.7749
Fax: +1.703. 907.7727
E-mail: dthompson@tiaonline.org
www.tiaonline.org

TABLE OF CONTENTS

1. Work Activities of TIA TR-8 Engineering Committee, *Mobile and Personal Private Radio Standards*

The Engineering Committee and its Subcommittees[2] develop and maintain standards for private radio communications systems and equipment for both voice and data applications. TR-8 addresses all technical matters for systems and services, including definitions, interoperability, compatibility and compliance requirements.

Project 25, *Standards for Public Safety Radio Communications*

Recognizing the need for common standards, representatives from the Association of Public Safety Communications Officials International (APCO), the National Association of State Telecommunications Directors (NASTD), selected Federal Agencies and the National Communications System (NCS) established Project 25 (P25), a steering committee for selecting voluntary common system standards for digital public safety radio communications. TIA TR-8 facilitates such work through its role as the ANSI-accredited Standards Development Organization (SDO), and has developed in TR-8 the 102-series of technical documents.

The P25 suite of standards and TSBs allow compliant systems a high degree of equipment interoperability and compatibility. Specifically, P25 systems involve digital Land Mobile Radio (LMR) services for local, state and national (federal) public safety organizations and agencies. P25 is applicable to LMR equipment authorized or licensed, in the U.S., under the National Telecommunications and Information Administration (NTIA) or Federal Communications Commission (FCC) rules and regulations. However, use of such equipment is not limited to public safety, and P25 equipment has also been selected and used in other private system applications, for example, to serve the needs for a high-quality, secure digital radio system for a railroad system, including rolling stock, personnel, and transportation vehicles.

The P25 series enables compliant radios to communicate in analog mode with legacy analog radios and in either digital or analog mode with other P25 radios. In addition, P25 systems can be maintained and upgraded cost effectively over the system's life cycle, thus meeting user requirements, achieving interoperability and security, promoting committed manufacturers to provide compliant products, fostering competition and achieving cost-effective emergency/safety communication solutions. In light of recent worldwide terrorist activities, interoperability among first responders is a key initiative of many countries.

Phase I Implementation: The P25 Phase I documents described below, define the services and facilities for a P25 Phase I-compliant system and ensures that any manufacturer's compliant subscriber radios have access to the services described in such documents (including other systems, across system boundaries, backward compatibility, etc.), regardless of system infrastructure. In addition, the P25 system provides an open interface to the Radiofrequency (RF) subsystem to facilitate interlinking of different vendor's systems. The table in **Annex 1** shows the availability of P25 system services:

System and Standards Definition Document:

- **TIA/EIA/TSB-102-A, *"APCO P25, Systems and Standards Definition."*** This document addresses the structure needed to relate the various documents used in the description and definition of the P25 systems. It presents not only an overview of the P25 concept but also guidelines for locating information essential to other specific requirements.

[2] Overall, 1,300 individuals from nearly 20 countries participate in TIA's 8 product-oriented Engineering Committees (TR/FO), with over 70 subcommittees and working groups. Formulating groups' representation includes representatives from academia, manufacturers, service providers and end-users, including the government.

- **ANSI/TIA/EIA-102.AAAD-02, "*P25* - Block Encryption Protocol."** This ANS was published in July 2002 and defines the means for P25-compliant equipment to securely (including Advanced Encryption Standard -- AES) send and receive digital information, in the form of either voice or data (*i.e*., non-voice) messages. Noting that the functions of encryption and decryption generally take place near the end points of a system's message path, the encryption/decryption functions can be provided at points were voice information is coded with Improved Multi-Band Excitation (IMBE), such as MR (mobile or portable radio) or a console (CON), or at points where data information enters the system, such as an RFG (RF system gateway). This document aligns with advanced, not initial, P25 Phase I implementation.

P25 Service Category Standard Documents: Defines features that a P25 Phase I compliant system might have.

- **ANSI/TIA/EIA-102.AAAA-A-2001, "*DES Encryption Protocol.*"** This Digital Encryption Standard (DES) encryption protocol document defines the operation (voice and the data modes) of encryption and decryption in a way that is compatible with information transfer through an P25 standard system, especially, through the Common Air Interface (CAI) of such a system.
- **ANSI/TIA-102.AAAB-02, "Digital Land Mobile Radio, *Security Services Overview.*"** This recently approved ANS provides an overview of the security services available in LMR systems and provides the context in which to understand why security services are required and gives a general high-level description of how they are provided. In the context of this document, the specific security requirements are generalized into three security topics: 1) confidentiality, 2) authentication and integrity and 3) key management. These three categories correspond to the security services available to LMR systems. The definition and detail of how security services are provided is outside the scope of this document. Specific instances of these security services are given in appendices to this document.
- **ANSI/TIA/EIA-102.AAAC-2001, "*Conformance Test for the P25 DES Encryption Protocol.*"** This Digital Encryption Standard (DES) protocol document describes the following items that are necessary for P25 conformance: encryption algorithm, operating mode, key variable, initialization vector and message indicator. This protocol is compatible with either voice or data messages and can be transported through a radio network using CAI. Additionally, this ANS provides a series of conformance tests for the DES Encryption Protocol to ensure the equipment conforms to the formats specified in the DES Encryption Protocol.
- **TIA/EIA/TSB-102.AABA, "*Trunking Overview.*"** Provides a high-level overview of P25 trunked systems, including commonality with conventional systems, mixture of services, registration, voice services, secondary control, voice or data control and protected trunking.
- **ANSI/TIA/EIA-102.AABB-2000, "*Trunking Control Channel Formats*."** This ANS defines the format of trunking control channel transmissions for P25 systems, compatibility with the CAI, and both encrypted formats.
- **ANSI/TIA/EIA-102.AABC-2000, "*Trunking Control Channel Messages*."** This ANS defines all messages constructed from formats further identified by the trunking control channel formats, including messages for telephone interconnect channel grant updates and a revision for the group affiliation response.
- **ANSI/TIA/EIA-102.AABC-1-01, "*Trunking Control Channel Messages - Addendum 1 - SNDCP* [*SubNetwork Dependent Convergence Protocol*] *Trunking Control Channel Messages*."** This document updates ANSI/TIA/EIA-102-AABC to include information on SNDCP Trunking Control Channel Messages.
- **TIA/EIA/TSB-102.AABD, "*P25 Trunking Procedures*."** This document details the procedures for accessing the control channel and working channels for both trunked subscriber units (mobile, portable and fixed) and the trunked system to which the subscriber units are connected, including procedures that are required to permit interoperability. In addition, a proposed revision **[Project Number (PN)-3-3629-URV-1]** is in committee development, as **TIA-102.AABD** (to become a proposed ANS).

- ***"Trunking Conformance"*** Potential output involving this topic is in committee development. If progressed, output could be proposed as **TIA/EIA/TSB-102.AABE**, and will define conformance tests, ensuring that equipment is compatible with the specified trunking procedures.
- **TIA/EIA/TSB-102.AABF, "*Link Control Word Formats and Messages*."** Defines all link control words for voice transmissions, including both trunking and conventional modes on P25 systems.
- **TIA/EIA/TSB-102.AABG, "*Conventional Control Messages*."** Defines the control messages of trunking that may be applied to conventional systems. These control messages are extensions to the basic CAI.
- **TIA/EIA-102.AACA, "*Over-The-Air-Rekeying (OTAR) Protocol*."** Covers OTAR protocol for unclassified sensitive government communications (readers should have knowledge of the main P25 standard). OTAR is a method of encrypting and sending the encryption keys securely through the CAI. This document defines protocols and procedures to implement OTAR in radios conforming to P25 standards, including key management functions (described at conceptual level).
- **TIA/EIA/TSB-102.AACA-l, "*OTAR Protocol*."** Defines the messages and basic procedures for providing OTAR and related key management services. The document includes methods of encrypting and sending encryption keys and other related key management messages through the CAI in a way that protects them from disclosure, and in some cases, from unauthorized modification.
- **TIA/EIA/TSB-102.AACB, "*OTAR Operational Description*."** This document is a supplement to the Key Management and OTAR Protocol describing the operational procedures as sequences of messages and basic procedures, defined in the Link Control Word Formats and Messages (TIA/EIA/TSB-102.AABF), for performing key management and OTAR functions.
- **ANSI/TIA/EIA-102.AACC-02, "*Conformance Tests for the P25 OTAR Protocol*."** This ANS was published in July 2002 and provides a series of conformance tests for the P25 25 OTAR protocol. These tests are intended to assure that the equipment conforms to the message formats specified in the OTAR protocol document and that the equipment is interoperable with other equipment conforming to the standard. These tests provide for the encryption of keys and the generation of the Message Authentication Code (MAC) that may be part of a Key Management Message (KMM).
- **TIA/EIA/TSB-102.CABA, "*P25 - Interoperability Test Procedures - Conventional Voice Equipment*."** The purpose of this recently published document is to define procedures for testing the interoperability of subscribers/repeaters between different manufacturers, different models of the same manufacturer, and different firmware upgrades of the same model.
- **PN-3-0060, "*P25 - Interoperability Test Procedures –OTAR*"** (Publication expected soon): This document, proposed as **TIA/EIA/TSB-102.CABB**, will define procedures for testing the interoperability of data, specifically, OTAR commands between RF subsystems and mobile radio subscribers of different manufacturers and models.

P25 System Category Description Documents: These system category documents define the core part of the P25 Phase I standard. Technically, they can be divided into six subcategories: CAI, vocoder, Inter-RF Subsystem Interface (ISSI), telephone interconnect, data, and network management interface.

- **ANSI/TIA/EIA-102.BAAA-98, "P25 Frequency Division Multiple Access (FDMA) *CAI*."** This ANS defines the over-the-air interface configurations between a mobile subscriber unit functional group and one or more base radio functional groups at a site, at multiple sites within an RF subsystem, and within any RF subsystems in which the subscriber unit might roam. It also defines the reference configuration between mobile and portable subscriber units in a talk-around configuration. Specifically, this document provides an overview of the standardized set of data communication services such that data connectivity will operate in accordance with any P25 radio and across any P25 digital radio system, describing all of the parts of a system for public safety LMR communications. These systems have subscriber units (which include portable radios for hand held operation and mobile radios for vehicular operation), base stations (for fixed installations), and other fixed equipment (for wide-area operation and console operator positions), as well as computer equipment (for data communications). There are interfaces between each of these equipment items. The CAI allows these radios to send and receive digital information over a radio channel and ref.3 involves formats for transmission of information over such CAIs.

- **TIA/EIA/TSB-102.BAAB-A, "*CAI Conformance Testing*."** Lists a series of conformance tests for the CAI to ensure that equipment conforms to the formats specified in the CAI standard and is interoperable with other equipment conforming to the standard.
- **ANSI/TIA/EIA-102.BAAC-2000, "*CAI Reserved Values*."** This ANS defines the messages to control trunking system operation on the CAI for P25.
- **ANSI/TIA/EIA-102.BAAC-1-2001, "*CAI Reserved Values - Addendum 1*."** This document involves Service Access Point (SAP) values that are used by the data system to distinguish services for different data packets.
- **TIA/EIA/TSB-102.BAAD, "*CAI Operational Description*."** This supplement to the CAI describes simple operational procedures sufficient for basic operation in conventional systems.
- **ANSI/TIA/EIA-102.BABA-98, "*Vocoder Description*."** This ANS describes the functional requirements for the transmission and reception of voice information using the digital communication media described in the CAI documents. The vocoder standard was intended to define the conversion of voice from an analog representation to a digital representation. The digital format consists of a net bit rate of 4.4 kilobits per second (kbps) for voice information and a gross bit rate of 7.2 kbps after error control coding.
- **ANSI/TIA/EIA-102.BABB-99, "*Vocoder Mean Option Score (MOS) Conformance Testing*."** This ANS employs MOS testing to evaluate an implementation of a P25 vocoder. This document provides a method for testing interoperability of an implementation of a P25 vocoder with the P25 reference vocoder.
- **ANSI/TIA/EIA-102.BABC-99, "*Vocoder Reference Test*."** This ANS provides a method of testing an implementation of a P25 vocoder with respect to the P25 Vocoder Reference Description document. This test method requires proprietary test equipment.
- **TIA/EIA/TSB-102.BABD, "*Vocoder Selection Process*."** Provides a historical reference to the selection of the P25 vocoder, along with the method of testing candidate vocoders, evaluation metrics, and test results for the candidate vocoders.
- **TIA/EIA/TSB-102.BACA, "*ISSI Message Definition*."** Defines the messages to be used between an RF subsystem gateway functional group in one RF subsystem and a corresponding RF subsystem gateway functional group in other RF subsystems.
- **TIA/EIA/TSB-102.BACB, "*ISSI Conformance*."** Lists a series of conformance tests for the RF subsystem interface to ensure that equipment not only conforms to the formats specified in the RF subsystem interface but also is interoperable with other equipment conforming to the standard.
- **TIA/EIA/TSB-102.BACC, "*ISSI Overview*."** Provides a high-level overview of the P25 ISSI, summarizing the protocol and message structure, mobility management, and intervening network adaptation.
- **ANSI/TIA/EIA-102.BADA-2000, "*Telephone Interconnect Requirements and Definitions*."** Defines the interface between a RF subsystem and a public or private switched telephone network. Specifically, this ANS defines the requirements for telephone voice interconnect for LMR systems. This document only applies to those features of a telephone interconnect service which are necessary for basic telephone functionality.
- **ANSI/TIA/EIA-102.BAEA-2000, "*P25 Data Overview*."** This ANS provides an overview of the data services in a P25 system, including circuit and packet data. The document also specifies requirements to transport multiple packet protocols, including Transmission Control Protocol/Internet Protocol (TCP/IP), X.25, and Systems Network Architecture (SNA). Overall, the P25 system standard specifies two categories of data services in three categories of data configurations, for six distinct service/configuration combinations. A P25-compliant data system should support one or more of the service/configuration combinations.

- **ANSI/TIA/EIA-102.BAEA-1-2002, "P25 Data Overview - Addendum 1 - USB/PPP - New Technology Standards Project - Digital Radio Technical Standards."** This ANS is an addendum to ANSI/TIA/EIA-102.BAEA-2000 (above) and introduces a new physical layer standard option and a new link layer standard option on the A Reference Point in the P25 General System Model found in TIA/EIA/TSB-102-A. Specifically, this addendum (P25 Phase I upgrade) defines the application of the Universal Serial Bus (USB) specification and the Point-to-Point Protocol (PPP) to the physical and link layers, respectively, of the A Reference Point between the Mobile Data Peripheral (MDP) and the Mobile Radio Controller (MRC) in the P25 General System Model. It should be noted that inherent in the natures of the Open Systems Interconnection (OSI) seven layer architectures and the IP four layer architecture is the opportunity to implement any four configurations of the Serial Line Internet Protocol (SLIP)/Point to Point Protocol (PPP), Universal Serial Bus (USB) and the RS-232 protocols in the link layer and the physical layer.
- **ANSI/TIA/EIA-102.BAEB-2000, "*Packet Data Specification*"** and **ANSI/TIA/EIA-102.BAEC-2000, "*Circuit Data Specification*."** These ANS documents define the detailed interfaces, protocols, and procedures involved in interfacing with a data-capable P25 standard radio unit via the standard mobile data peripheral interface and the end-system interface. The data services may be provided across conventional or trunked service channels. The packet data bearer service allows two or more fixed or mobile end terminals (i.e., hosts} to communicate via the wireless network and/or Ethernet. The service is characterized as an Internet Protocol (IP) [*e.g.*, Internet Engineering Task Force (IETF) Request for Comment (RFC)-791] bearer service that provides connectionless, best-effort datagram delivery between bearer service access points.

  Error correction and detection, and encryption services are provided across the air interface by elements of the radio subnetwork. The circuit data bearer service allows two fixed or mobile end terminals (*i.e.*, hosts) to communicate in a point-to-point configuration via the wireless network and/or the intervening PSTN network. Nontransparent two-way communications are supported between bearer service access points in wireless networks and the Public Switched Telephone Network (PSTN).
- **ANSI/TIA/EIA-102.BAEB-1-2001, "*Packet Data Specification - Addendum 1 - Subnetwork Dependent Convergence Protocol*."** This document updates information contained in ANSI/TIA/EIA-102.BAEB-2000 (above). These enhancements are presented in order to optimize the capabilities and present enhancements, which will optimize the capabilities, of a trunked P25 data system.
- **TIA-102.BAEB-2, "*Packet Data Specification - Addendum 2 – USB/PPP*."** This addendum defines the application of the USB and the PPP to the physical and link layers, respectively, of the A Reference Point between the Mobile Data Peripheral (MDP) and the Mobile Radio Controller (MRC) in the P25 General system model in TIA/EIA/TSB-102-A; includes the introduction of a new Physical Layer Standard option on the A Reference Point.
- **TIA/EIA-102.BAEE, "*Radio Control Protocol (RCP)*."** Defines the Radio Control Protocol (RCP) for use in P25 digital radio systems for packet data communications services. The current packet data service specification is defined in the Packet Data Specification TIA/EIA102.BAEB. "RCP," along with the Internet Control Message Protocol (ICMP), defines the control signaling protocol across the A interface. Control signaling refers to transactions that are not directly concerned with the transfer of user information between the mobile host and destination host. In addition, a proposed ANS revision [**Standards Project (SP)-3-4631-AD1**] is in development and due to be published in 2003 as **ANSI/TIA-102.BAEE-1-2002, "*RCP – Addendum 1 – USB/PPP,*"** involving enhancements relating to the application of USB and PPP to the physical and link layers, respectively, of the A Reference Point between the MDP and the MRC.
- **TIA/EIA/TSB-102.BAFA, "*Network Management Interface Definition*."** Defines the interface between one or more RF subsystems and an attached network manager or other interconnect network management system. This part of the P25 standard defines the interface between a RF subsystem gateway functional group within one RF subsystem and a network management end system.

- **PN-3-XXXX, "*Network Management Interface Conformance*"** (PN not determined; in committee development): This proposed standard, **TIA/EIA/TSB-102.BAFB**, lists a series of conformance tests for the network management interface to ensure equipment conformance to the formats specified in the Network Management Interface Definition (above) and ensures that equipment is interoperable with other equipment conforming to the standard.

Equipment Category Description Documents: The equipment category documents define measurement methods to verify that all CAI signaling conforms to the standard.

- **ANSI/TIA/EIA 102.CAAA-1999, "*Digital C4FM/CQPSK Transceiver Measurement Methods*."** Standardizes parameter titles, definitions, test conditions and methods for measuring the performance of P25 transceiver equipment, within the scope of the standard. The transceiver measurement methods also ensure a meaningful comparison of the results of measurements made by various observers on different equipment.
- **ANSI/TIA-102.CAAB-A-2002, "*Digital Radio Technology, C4FM/CQPSK Modulation*."** This recent revised ANS is to serve as a performance level benchmark for assessing interoperable digitally modulated radio equipment compliant with ANSI/TIA-102.BAAA-98 using measurement methods defined in companion document ANSI/TIA/EIA-102.CAAA-1999, and selected federal documents. Two performance levels have been distinguished within this document. Also note that that this document may be applicable to applications other then those specifically addressed in P25. The original TIA/EIA/IS-CAAB established minimum specifications for P25 transceiver equipment performance measured in accordance with ANSI/TIA/EIA/IS-102.CAAA; specifically, physical layer performance standards under general conditions for the transmission of voice or circuit switched data (*i.e*., 12.5 kHz channelization digitally modulated radio equipment with a maximum operating frequency of 1 GHz or less in the Private (Dispatch) Land Mobile Services that employ compatible 4 Level Frequency Modulation (C4FM) or Compatible Differential Offset Quadrature Phase Shift Keying (CQPSK) digital modulation).

Phase II Implementation Documents: The primary difference between Phase I and II is the modulation schemes, which will involve TDMA and FDMA, with the goal of improved spectrum utilization of one voice channel per 6.25 kHz of channel bandwidth. Attention is also paid to interoperability with legacy equipment, roaming capacity and spectral efficiency/channel reuse. In addition, Phase II may undertake activity involving console interfacing, interfacing between repeaters and other subsystems (e.g., trunking system controller), and man-machine interfaces for console operators that would facilitate centralized training, equipment transitions and personnel movement. Published documents include (other documents expected by 2003):

- **TIA/EIA/TSB-102.BAAB-A-1, "*P25 - FDMA CAI Conformance Test - Addendum 1*."** The purpose of this addendum is to update information contained in TIA/EIA/TSB-102.BAAB revision A for P25 Phase II.
- **ANSI/TIA/EIA-102.BAAA-1-99, "*P25 FDMA CAI – Addendum 1*."** This document updates the information contained in TIA/EIA-102.BAAA for P25, Phase II.
- **ANSI/TIA/EIA-102.CAAA-1999, "*Digital C4FM/CQPSK Transceiver Measurement Methods*"** (also noted in above Section): This standard provides definition, methods of measurement and performance standards for radio equipment used in the private (dispatch) land mobile services that employ C4FM or CQSK modulation for transmission and reception of voice or data using digital techniques, with or without encryption, with a maximum frequency of 1 GHz or less.
- **PN-3-0044, "*Two-Slot TDMA Common Air Interface, Physical Layer*"** (expected publication in 2003): This document, proposed as **TIA-905.BAAA**, will define the physical layer specifications for Phase II TDMA systems.
- **PN-3-0073, "*Two-Slot TDMA Common Air Interface, Media Access Control (MAC) Layer*"** (expected publication in 2003): This document, proposed as **TIA-905.BAAC**, will define the MAC layer specifications for Phase II TDMA systems.

- **PN-3-0074, "*Two-Slot TDMA Common Air Interface, Logic Link Control (LLC) Layer*"** (expected publication in 2003): This document, proposed as **TIA-905.BAAD**, will define the LLC layer specifications for Phase II TDMA systems.
- Other documents for **TDMA systems** are in the early stages of drafting.

Phase III Implementation: Recognizing the need for high-speed data for public safety use, as expressed in the Public Safety Wireless Advisory Committee (PSWAC) final report[3], among others, the P25 standard committee established the P25/34 Committee to address Phase III implementation. Similarly to the P25 approach, the standard committee established the P25/34 user forum to address this issue. Phase III activities are addressing the operation and functionality of a new aeronautical and terrestrial wireless digital wideband/broadband public safety radio standard that could be used to transmit and receive voice, video, and high-speed data in a ubiquitous, wide-area, multiple-agency network. On June 1, 1999, the P25/34 committee released the Statement of Requirements for a wideband aeronautical and terrestrial mobile digital radio technology standard for the wireless transport of rate intensive information.

Due to commonalities, the European Telecommunications Standards Institute (ETSI) and TIA agreed to work collaboratively for the production of mobile broadband specifications for public safety as initiated by ETSI Project TETRA (under the name of DAWS -- Digital Advanced Wireless Services) and by TIA and APCO under APCO's Project 34. During a April 2000 meeting, a draft agreement between ETSI and TIA, proposing the creation of a Public Safety Partnership Project (PSPP), was approved [Later renamed Project MESA (**M**obility for **E**mergency and **S**afety **A**pplications]. On May 25, 2000, ETSI Director General Mr. Karl-Heinz Rosenbrock and TIA Vice President Mr. Dan Bart formally signed the PSPP agreement. The current Partnership Agreement for Project MESA was modified and ratified January 2001 in the City of Mesa, Arizona. Note that Project MESA is further described in another section of this document. The Project was given the name MESA at that time.

Other non-P25 Work Activities (except TR-8.18), including *Wideband Data Standards Project*

- **TIA/EIA/TSB-30, "*Sideband Spectrum Measurement Procedure for Transmitters Not Equipped with Audio Low-Pass Filter*."** This document contains a measurement procedure for use in demonstrating compliance with FCC bandwidth limitation requirements for transmitters that are not equipped with an audio low-pass filter. The term "Transmitter Sideband Spectrum" denotes the level of sideband energy measured in a specified receiver bandwidth over a specified frequency displacement range due to all forms of intended modulation and from sources of unwanted noise within the transmitter.
- **TIA/EIA/TSB-57, "*Sideband Spectrum Measurement Procedure for Transmitters Intended for Use in the 220-222 MHz Band*."** This measurement procedure can be used to demonstrate compliance with FCC bandwidth limitation requirements for transmitters intended for use in the 220-222 MHz band. Transmitters used in this frequency band will operate on 5 kHz channels and a maximum authorized bandwidth of 4 kHz. Assignable frequencies represent the center of the authorized bandwidth.
- **TIA/EIA/TSB-69, "*A System and Standards Definition for a Digital LMR System*."** This enhanced digital access communications system and standards definition describes the functional elements of a Frequency Division Multiple Access (FDMA), digital, trunked, LMR communication system, as well as defining the basic system architecture. This document provides the basic expectations of Enhanced Digital Access Communications Systems (EDACS), and outlines the organization of the family of documents and serves as a foundation for the coherent development of the remaining documents within the family of documents. Additional and more specific information can be referenced in each of the corresponding

[3] http://www.fcc.gov/Bureaus/Wireless/News_Releases/nrwl6043.txt

documents within this family. As a group, the family of documents describes the EDACS, inclusive of the equipment requirements, which allow both compatibility and inoperability between various systems and elements. These systems provide advanced digital LMR services for private organizations, on all levels, including local, state, and national.

The family of documents will be backward compatible and interoperable with existing installed EDACS(TM), per the defined technical definition of Section four. This document describes trunked systems utilizing digital signaling, digital voice, and analog voice for conventional mutual aid operation and is applicable to LMR equipment licensed under NTIA and FCC rules and regulations. They are suitable for 12.5 kHz or 25 kHz channels and designed for Very High Frequency (VHF), Ultra High Frequency (UHF), 800 and 900 MHz frequency bands. The family or specific documents within the family may be applicable in situations other than those noted above.

- **TIA/EIA/TSB-69.1-2, "*Enhanced Digital Access Communications System* (EDACS) *Vocoder and Encryption Definition.*"** This document serves to define the EDACS packet data interface, protocol and procedures.
- **TIA/EIA/TSB-69.3, "*Enhanced Digital Access Communications Systems (EDACS) Digital Air Interface for: Channel Access, Modulation, Messages, and Formats*."** This document defines the digital signaling process to be used for trunking control and voice communications, including channel access, modulation, addressing, working channel formats and messages and error correction. This TSB-69 series document also discusses Radiofrequency (RF) signaling within the EDACS and includes both digital trunking control channel and working channel signaling structures and message formats.
- **TIA/EIA/TSB-69.5 "*Enhanced Digital Access Communications System IMBE* [*Improved Multi-Band Excitation*] *Implementation*."** This document specifies a voice coding method for the EDACS.
- **TIA/EIA/TSB-78, "*Land Mobile Linear Analog Modulation Communications Equipment Measurement and Performance Standards*."** This document aims to standardize parameter titles, definitions, test conditions and the methods of measurement used to ascertain the performance of radio equipment used in the LMR Services that employ linear analog modulation techniques. These include, but are not limited to, tone above band single sideband (TAB), transparent tone in band single sideband (TTIB), and real zero single sideband (RZ™SSB). Harmonizing methods of measurement for base stations, mobiles, and portable/personal equipment is also a goal, and separate standards for these, as an entity, have been included toward this end.
- **TIA/EIA/TSB-92, "*Report on EME Evaluation for RF Cabinet Emissions under FCC MPE Guidelines*."** The purpose of this bulletin is to develop and document methods and procedures of evaluation to establish cabinet emission levels with respect to the FCC-defined electromagnetic exposure (EME) limits. Specifically, the EME characterization is of box-level equipment only (*e.g*., fixed station, vehicular or similar equipment) and is not a substitute for a complete transmitter site environmental assessment by means of computation or site measurement. A limited case analysis, based on the FCC Part 90 type acceptance spurious emissions regulation limits, will be conducted herein to show that type accepted equipment at the box level is within the FCC maximum permissible exposure (MPE) limits.
- **TIA-329-B, "*Minimum Standards for Communication Antennas, Part 1: Base Station Antennas*."** This TIA document defines terms and conditions of measurement used to ascertain the performance of antennas within the scope of this standard and to make possible a comparison of the results of measurements made by different observers on different equipment. TIA-329-B deals only with linearly polarized antennas for use in frequency range 25 MHz to 1 GHz.
- **TIA-329-B-1, "*Minimum Standards for Communication Antennas, Part II: Vehicular Antennas*."** This document supplements TIA-329-B by covering vehicular antennas to the 30-1000 MHz frequency range.
- **TIA/EIA/IS-804, "*Terrestrial LMR - Antenna Systems - Standard Format for Digitized Antenna Patterns*."** This document is intended to standardize the presentation of digitized antenna patterns for antenna systems in the Terrestrial LMR Services.

- **TIA/EIA/TSB-902-A, "*Digital Radio Technical Standards - Public Safety Wideband Data Standards Project – Wideband System and Standards Definition*."** This document enables interoperability in a wideband (**900-series documents**) radio system using high-speed packet data over wideband data channels in the 700 MHz public safety band plan.
- **TIA-902.BAAB, "*Wideband Air Interface (WAI) Scalable Adaptive Modulations (SAM) Physical Layer Specifications*."** The scope of this document is to define the physical layer, or layer 1, of the SAM and associated WAI.
- **TIA-902.BAAC, "*WAI Media Access Control/Radio Link Adaptation (MAC/RLA) Layer Specification.*"** This TIA standard defines the media access control/radio link adaptation layer (*i.e*., MAC/RLA) of the WAI and involves such aspects as frequency configuration, synchronization, channel access, radio channel encryption and scrambling and other MAC layer services, procedures and Protocol Description Unit (PDU) definitions. The WAI, or Uw, is the interface between the Fixed Network Equipment (FNE) and the wireless subscriber units, or directly between subscriber units in a wideband system. Note that a Vehicular Repeater (VR) could additionally act as a relay between a fixed station and mobile radio when coverage limitations require the use of this local coverage area extension.
- **TIA-902.BAAE, "WAI-Logical Link Layer (LLC) Specification."** This document defines the LLC layer of the WAI, whose function is to define the procedures and message formats that permit virtually error free (optional) transmission of LLC frames over the point-to-point or point-to-multipoint mobile routing and control (MRC) to FNE, or MRC to MRC radio frequency link.
- **PN-4869, "*Wideband Data Standards for 700 MHz Public Safety Interoperability Channels*."** This document, proposed as **TIA/EIA-902. XXX (Number not yet identified)**, is in development and will define a wideband data standard for interoperability of public safety agencies using the 700 MHz spectrum band and was initiated at the request of the National Coordination Committee (NCC), a Federal Advisory Committee Act (FACA) advisory committee of the FCC. The data standard will be scalable for 50/100/150 kHz channels.
- **PN-3-0048, "*WAI Isotropic Orthogonal Transform Algorithm (IOTA) Physical Layer*"** (Expected publication 2003): When published, this proposed standard, **TIA-902.BBAB**, will define the physical layer of the IOTA/Orthogonal Frequency Division Multiplexing (OFDM)IOTA/OFDM modulation WAI.
- **PN-3-4912, "*LMR - Security Services Overview*."** This document will provide an overview of the security services available in LMR systems, providing the context to understand why security services are required and gives a general high-level description of how they are provided (including the neutralization of such security threats). The security services defined, in this document, apply to all aspects of LMR systems, including trunking and conventional systems (including voice and data systems), and involve encryption, confidentiality, authentication and integrity and key management aspects.

<u>TR-8.18, *Wireless Systems Compatibility*</u>

One of the functions of this Subcommittee is emergency telecommunications frequency coordination and the prevention of interference during stressful conditions. TR-8.18 is quite active in setting guidelines and methods to proactively identify potential interference.

- **TIA/EIA/TSB-88-A, "*Performance in Noise and Interference-Limited Situations - Recommended Methods for Technology-Independent Modeling, Simulation, and Verification*."** This TSB gives guidance on the following areas: establishment of standardized methodology for modeling and simulating narrowband/bandwidth efficient technologies operating in a post "re-farming" environment; establishment of a standardized methodology for empirically confirming the performance of narrowband/bandwidth efficient systems operating in a post "re-farming" environment; and aggregating the modeling, simulation and empirical performance verification reports into a unified "spectrum management tool kit," which may be employed by frequency coordinators, systems engineers and system operators.

This document defines and advances a scientifically sound standardized methodology for addressing technology compatibility and provides a formal structure and quantitative technical parameters from which automated design and spectrum management tools can be developed based on proposed configurations that may temporarily exist during a migration process or for longer-term solutions for systems that have different technologies.

- **TIA/EIA/TSB-88-A-1, "*Performance in Noise and Interference-Limited Situations - Recommended Methods for Technology-Independent Modeling, Simulation, and Verification - Addendum 1*."** This addendum is intended to expand on the material in TIA/EIA-TSB-88-A, by adding the following information: A well-defined method of calculating height above average terrain (HAAT); a well-defined method of coverage and interference contour calculation; additional bibliographic information for use in association with the other added material; and corrections to material contained in TIA/EIA-TSB-88-A.

2. Work Activities of TIA TR-30.5 Engineering Committee, *Facsimile Terminal Equipment and Systems*

This Engineering Committee is responsible for standards and recommendations relating to facsimile terminal equipment and systems, and to the interfaces between facsimile terminal equipment and systems and; communication equipment, other facsimile terminal equipment; and transmission media. A topic of interest that is presently being explored involves Internet/IP facsimile security. Standards include functional, electrical, and mechanical characteristics and communication protocols that involve point-to-point and multipoint facsimile and audiographic services. Facsimile, as referred to here, include any system that transmits (and receives) still rasterized images, including bi-level, continuous tone and color images.

3. Work Activities of TIA TR-34 Engineering Committee, *Satellite Equipment and Systems*

This TIA Engineering Committee is presently reviewing the issues that would be involved if TIA were to undertake development of a Lawfully Authorized Electronic Surveillance (LAES) standard in support of Communications Assistance for Law Enforcement Act (CALEA), but related to satellite systems. The FBI has requested that TIA consider such a standards activity and the matter is in review.

4. Work Activities of TIA TR-41 Engineering Committee, *User Premises Telecommunications Requirements*

This Engineering Committee is responsible for standards and recommendations relating to telecommunication terminal equipment, user telecommunication systems, private telecommunication networks, private network mobility, unlicensed wireless user premises equipment, and auxiliary equipment and devices, used for voice service and integrated voice-data service. Network interface characteristics are addressed from a terminal equipment perspective. TR-41 is also responsible for standards and recommendations on customer premises for premises wiring necessary for voice and data communications and distribution of multimedia services.

- Standards include service and performance criteria as well as information necessary for proper interworking of equipment, systems and networks with each other, the public networks, and carrier provided private line services. Work also includes regulatory, safety and environmental requirements. Recent security issues that are being worked in TR-41 include IP Telephony, as a new and emerging technology, and involving the marriage of telephony operations on a Local Area Network/Wide Area Network/Metropolitan Area Network (LAN/WAN/MAN) infrastructure. The threats from telephony can be overlayed with the threats native to the IP environment, both passive (*i.e.*, copying information in transit/during storage) and active (modifying information in transit/during storage or disruption of normal operations). In addition to threats against an IP Telephony (IPT) infrastructure (*i.e.,* routers, switches, authentication resources), greater exposure is also being directed towards threats against the IP Telephony application itself, including toll fraud, unauthorized access to resources, unauthorized access to voice mail and other private user information. Other threats involve IPT endpoints (*i.e*., IP phones, gateways, "softphones"), passive and active attacks on the signaling stream (including eavesdropping) and other issues that are of importance.

TR-41.1, *Multiline Terminal Systems*

This subcommittee has published the following documents that specifically address emergency telecommunications issues:

- **ANSI/TIA-464-C-2002, "*Multiline Terminal Systems - Requirements for PBX Switching Equipment.*"** This recently published ANS defines requirements for Private Branch Exchange (PBX) systems and PBX switching equipment. Additionally, this standard addresses E9-1-1 requirements for Centralized Automatic Message Accounting (CAMA) trunks, establishes performance and technical criteria for interfacing and connecting with the various elements of public and private telecommunications networks and helps to assure quality of service. Because of the changing environment in telecommunications and the introduction of new technology, this document will be a living document with periodic revisions.
- **ANSI/TIA/EIA-689-97, "*PBX and KTS Support for Enhanced 9-1-1 Emergency Service Calling.*"** Addresses technical issues associated with multi-line telecommunication system (MLTS) support of enhanced 9-1-1 emergency service calling. It specifically addresses dialing, routing, attendant notification and network interface technical specifications associated with outgoing 9-1-1 calls from MLTS stations.
- **PN-3-3836-RV1, "*PBX and KTS Support of Enhanced 9-1-1 Emergency Calling Service (ECS)*"** (In committee development; Publication estimated 2003): As indicated in title, the proposed **TIA-689-A**, and a proposed ANS revision, will contain requirements for PBX and KTS support of Enhanced 9-1-1 calling. It was developed as a companion document to TIA/EIA-464 and addresses network interface signaling requirements for support of Enhanced 9-1-1, when such a call is dialed. TIA-689-A will also address station-side support features, such as three-digit 9-1-1 dialing and attendant-notification when a 9-1-1 call is dialed.

TR-41.4, *IP Telephony Gateways and Infrastructures*

- **PN-3-0061, "*IP Telephony Security Framework*"** (In committee development): TR-41.4 opened this new project to examine Voice over IP (VoIP) telephone network security, IP network architectural security considerations, authentication, authorization, privacy, governmental requirements and the threat environment within the Customer Premises Equipment (CPE)/Enterprise space. Additionally, this proposed document, **TIA/TSB-139**, will try to develop best practices that address many of the identified threat environments. The subcommittee has identified the need for a security protocol suite tailored for devices with limited resources and conveyed this need to the IETF.
- **PN-3-4726, "*IP Telephony Support for Emergency Calling Services*"** (Expected publication 2003): This proposed document, **TIA/TSB-146**, will describe network architecture elements and their functionality needed for providing E9-1-1 support for IP terminals in an Enterprise Network. Additionally, this TSB will address the problem of locating VoIP terminals as it relates to E9-1-1 services, however, it does not cover terminals connected through gateways.

TR-41.9, *Technical Regulatory Considerations*

- **ANSI/TIA-968-A-2002, Technical Requirements for Connection of Terminal Equipment to the Telephone Network."** This recently published ANS specifies technical criteria for terminal equipment approved in accordance with FCC 47 CFR 68 for direct connection to the public switched telephone network, including private line services provided over wireline facilities owned by providers of wireline telecommunications. These technical criteria are intended to protect the telephone network from the harms defined in 47 CFR 68.3. Conformance to the technical criteria in this standard will not assure compatibility with wireline carrier services. In January 2003, this standard was adopted by the Administrative Council for Terminal Attachments (ACTA). While it doesn't specifically address emergency communications issues, one of its purposes is to help ensure the network's ability to perform under emergency (*e.g.*, high load) conditions. The previous document, **TIA/EIA/IS-968, "*Technical Criteria for Terminal Equipment to prevent Harm to the Telephone Network,*"** will remain valid until July 2004.

5. Work Activities of TIA TR-42 Engineering Committee, *User Premises Telecommunications Infrastructure*

This Engineering Committee is responsible for commercial, industrial and residential cabling standards including telecommunications infrastructure administration, pathways and spaces, and copper and optical fiber systems requirements, including information and requirements necessary for the implementation of telecommunications infrastructure. The following documents can be applicable to cabling issues associated with emergency telecommunications. In particular, the TIA/EIA-569 and 758 standards provide some guidance for alternate routing of cabling into a building to help prevent loss of communications.

- **ANSI/TIA/EIA-568-B.1-2001, "*Commercial Building Telecommunications Cabling Standard - Part 1: General Requirements.*"** This standard specifies a generic telecommunications cabling system for commercial buildings that will support a multi-product, multi-vendor environment.
- **ANSI/TIA/EIA-758-99, "*Customer Owned Outside Plant Telecommunications Cabling Standard.*"** This ANS provides requirements used in the design of the telecommunication pathways and spaces, and the cabling installed between buildings or points in a customer-owned campus environment. Customer-owned campus facilities are typically termed "outside plant" (OSP). For the purpose of this standard, they are termed "customer-owned OSP".

TR-42.2, *Residential Telecommunications Infrastructure*

- **ANSI/TIA/EIA-570-A-99, "*Residential Telecommunications Cabling Standard.*"** This ANS standardizes requirements for residential telecommunications cabling based on the facilities that are necessary for existing and emerging telecommunications services.
- **ANSI/TIA/EIA-570-A-1-2002, "*Residential Telecommunications Cabling Standard - Addendum 1 - Security Cabling for Residences.*"** This ANS addendum provides recommendations and specifications for security cabling systems in residences. It contains references to national and international standards.

TR-42.3, *Pathways and Spaces for Telecommunications Cabling*

- **ANSI/TIA/EIA-569-A-98, "*Commercial Building Standards for Telecommunications Pathways and Spaces.*"** This ANS encompasses telecommunications considerations both within and between buildings. The aspects covered are the pathways into which telecommunications media are placed and the rooms and areas associated with the building used to terminate media and install telecommunications equipment.

TR-42.6, *Telecommunications Infrastructure Administration*

- **TIA/EIA-606-A, "*Administration Standard for Commercial Telecommunications Infrastructure*."** This recently published standard provides guidelines and choices of four classes of administration for maintaining telecommunications infrastructure, based on complexity. In addition, this "living document" is modular and scalable to allow implementation of various portions of the administration system, as desired (supports multi-product and multi-vendor environment). This uniform approach, independent of applications, establishes guidelines for owners, end users, manufacturers, consultants, contractors, designers, installers and facilities administrators involved in the administration of the telecommunications infrastructure.

6. Work Activities of TR-45 Engineering Committee, *Mobile and Personal Communications Systems*

This Engineering Committee is responsible for performance, compatibility, interoperability and service standards for mobile and personal communications systems. These standards pertain to, but are not restricted to, service information, wireless terminal equipment, wireless base station equipment, wireless switching office equipment, ancillary apparatus, auxiliary applications, inter-network and inter-system operations and interfaces.

TR-45 has been involved with the development of security features since the early 1990s (*i.e.*, Authentication, Signaling Message Encryption and Voice Privacy), including Joint Standards Development Work with Committee T1 to address legislated and mandated security services like emergency Services (*e.g.*, E-911 location) and CALEA. Authentication, Signaling Message Encryption, Privacy are supported in TIA/EIA-41 Networks and their radio technologies – Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA) (*i.e.*, cdma2000®), Advanced Mobile Phone System (AMPS)-based systems. In the ongoing interest of security, enhancements to these basic security features have been adopted by TR-45 to support Enhanced Subscriber Authentication (ESA) and Enhanced Subscriber Privacy (ESP) mechanisms for Third Generation (3G) Systems.

TR-45 is also developing standards for Wireless Priority Service (WPS) for CDMA Systems, in parallel with WPS Industry Requirements work, and a Priority Access and Channel Assignment (PACA) technique involving a queued originate mechanism that may be used to support a priority access scheme in the event that either radio or network resources are congested (supported in TIA/EIA-41, TIA/EIA-136-123 and in CDMA-TIA/EIA-95). Note that WPS is a voluntary service based on FCC R&O 00-242 (WT Docket No. 96-86), and is provided to National Security/Emergency Preparedness (NS/EP) Personnel, supporting 5 levels of priority (assigned by National Communications System personnel in U.S.A.). WPS is invoked on a per call basis and is primarily for voice and circuit-switched data calls. WPS requires no modifications to existing handsets; call request is given priority treatment (*e.g.*, queued) when no radio channels are available in the originating or terminating wireless network; calls are completed (based on priority level) when a radio traffic channel becomes available.

TR-45 *Ad Hoc Authentication Group (AHAG)*

This Ad Hoc group addresses cdma2000® packet data security requirements and is responsible for Security Assessment Issues, including IP-related aspects and the selection of cryptographic algorithms to support TR-45 security mechanisms. AHAG also collaborates with the Third Generation Partnership Project 2 (3GPP2) Technical Specification Group (TSG)-S, Working Group (WG) 4.

3rd Generation (3G) cdma2000® Security Features include:

- 128-bit root secret K; 128-bit Entity Authentication [Secure Hash Algorithm (SHA)-1 Algorithm]; 128-bit Message Auth (ENMAC); 128-bit AES Encryption (Rijndael Algorithm); 3GPP Authentication and Key Agreement (AKA) protocol (*for Global Roaming*); Mutual authentication between Mobile and Network; Backwards compatibility; Removable User Identity Module (R-UIM) support; Air interface and Network algorithm negotiation; Mobile IP; Radius/Diameter and Challenge Handshake Authentication Protocol (CHAP) authentication. TR-45 Authentication and Authorization involves the Data Link Layer.

TR-45 Ad Hoc Group, *Lawfully Authorized Electronic Surveillance (LAES)*

Note that the Access and Delivery Functions typically include the ability to protect (*e.g.*, prevent unauthorized access, manipulation, and disclosure) intercept controls, intercepted call content and call-identifying information consistent with Telecommunications Service Provider (TSP) security policies and practices.

Responsibilities include standards development to support the *Communications Assistance for Law Enforcement Act* (CALEA).

- **PN-3-4464, "*Lawfully Authorized Electronic Surveillanc*e"** (In Joint committee ANS ballot process as **SP-4464**; Publication estimated early 2003): Document **SP-4464**, proposed **J-STD-025-A**, was approved for ANSI 60 day default ballot and is expecting a 3/2003 publication time-frame. Correspondence to Committee T1 Chair for a concurrent letter ballot of this revised joint standard document, which includes punch list (*i.e*., additional surveillance capabilities) items, has been requested and is progressing. This project number was on hold pending the FCC 99-230 CC Docket No. 97-213, Third Report and Order before the ANSI publication due to the U.S. Court of Appeals decision of August 15, 2000. The project was revisited following the FCC 02-108, CC Docket No. 97-213, Order on Remand decisions, which was recently released on April 11, 2002. This document defines the interfaces between a telecommunications service provider (TSP) and a law enforcement agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance.
- **PN-4465-RV1, "*Lawfully Authorized Electronic Surveillanc*e"** (In TR-45 LAES Ad Hoc Joint committee development; Publication expected in 2003): This recently initiated joint project (w/ Committee T1) is relative to CALEA compliance and the refinement of J-STD-025-A, "*Lawfully Authorized Electronic Surveillanc*e." This proposed joint standard will be published as **J-STD-025- B** and contain refined requirements for support of packet mode communications surveillance. A new section titled *4.9 Packet Mode Technology* has been added that includes requirements specific to individual packet mode technologies, as well as references to LAES standards from packet mode technologies gathered from liaison input. TR-45 welcomes participation by parties with a material interest in packet mode communications involving a broad range of systems and technologies and their interface to the Collection Function (interface "e" in J-STD-025-A).

TR-45.1, *Analog Technology*

- **TIA/EIA/TSB-119 "*Enhanced System Access Procedures for E911 Calls for Analog Cellular.*"** The FCC has become involved in the resolution of issues concerning public safety in regards to enhanced call completion for E9-1-1 originations. As s result of the FCC 99-096 Second Report and Order (R&O), changes to the ANSI/TIA/EIA-553-A-99, "*Mobile Station - Base Station Compatibility Standard*" are required. In order to comply with this Second R&O, this TSB has been created.
- **TIA/EIA/IS-817, "*A Position Determination Service Standard for Analog Systems.*"** This interim Standard provides, procedures, signaling and messages used in addition to TIA/EIA-553-A as one possible way to support E9-1-1 Position Determination services (there is mention of the FCC E-9-1-1 docket 94-102).
- **TIA/EIA/IS-817-1, "*A Position Determination Service Standard for Analog Systems - Addendum 1.*"** This recently published addendum to TIA/EIA/IS-817 defines the order messages sent by the base station and the order confirmation messages sent by the mobile station, together with mobile station and base station procedures for Position Determination services when operating in analog mode.

TR-45.2, *Wireless Intersystem Technology*

- **ANSI/TIA/EIA-41-D-97, "*Cellular Radio Telecommunications Intersystem Operations.*"** This ANS identifies those cellular services that require intersystem cooperation, to present the general background against which those services are to be provided, and to summarize the principal considerations which have governed and directed the particular approaches taken in the procedural recommendations. Additionally, this document supports Priority Access and Channel Assignment (PACA)[4].

- **TIA/EIA/TSB-114, "*Wireless Network Communication for Emergency Message Broadcast (EMB).*"** This document defines the requirements for broadcasting an announcement of a national, state, or local emergency to the mobile stations (MSs) used for cellular or personal communication services.
- **ANSI/TIA/EIA-664-A-2000, "Wireless *Features Description.*"** This ANS series (ANSI/TIA/EIA-664-000 to 800-A) presents a recommended plan for the implementation of Uniform Features for use in the Cellular Radiotelephone Service. Its intent is to describe services and features so that the manner in which a subscriber may place calls using such features and services may remain reasonably consistent from system to system. Specifically, ANSI/TIA/EIA-664-517-A-2000, "*Wireless Features Description: Priority Access and Channel Assignment*" supports the PACA feature (allowing a subscriber to have "first come, first served"/priority access to voice or traffic channels on call origination.).
- **PN-3-0054, "*TIA/EIA-41 Support for Wireless Priority Service (WPS)*"** (In committee development: scheduled for publication 2003): This proposed standard, **TIA-917**, will supplement GETS (Government Emergency Telecommunications Service) and WPS end-to-end priority capabilities needed by National Security/Emergency Preparedness (NS/EP) personnel during situations of network congestion in cases of localized/national emergencies and natural disasters.

  Industry Requirements (IR) work is being done in parallel with the standards work. WPS Initial Operating Capability (IOC) IRs for CDMA and GSM Systems were developed in February 2002; focusing on originating radio network priority. WPS Final Operating Capability (FOC) IRs focused on priority in the radio network (originating and terminating) and the landline network (GSM completed September 2002; CDMA scheduled for completion in 2003). CDMA WPS IR and standards project **PN-3-0054**, which supports both IOC and FOC, are closely aligned.
- **PN-3-4747, "*Location Services Authentication/Privacy/Security and Enhancements.*"** (In committee development, balloting expected late 2003). This project will provide ANSI/TIA/EIA-41 support for location services architecture, Position Determining Equipment (PDE) and Mobile Positioning Center (MPC) interfaces, as well as areas of uncertainty and accuracy. Additionally, this project will provide ANSI/TIA/EIA-41 support of authentication, privacy and security of location services [previously PN-3-4746]. Expected to be published as **TIA/EIA/IS-881**.

TR-45.2 *Ad Hoc Emergency Services (AHES)* Group

- **J-STD-034, "*Wireless Enhanced Emergency Services.*"** This Joint TIA/Committee T1 document provides a solution for the handling of Wireless Enhanced Emergency Calls. Capabilities include provision of base station, cell site or sector identification information; subscriber identification; callback and reconnect features, as indicated in the FCC R&O (CC Docket No. 94-102) involving Phase I capabilities (callback phone numbers and cell/sector information). Involves Public Safety Answering Point (PSAP) perspective.
- **J-STD-036-A-2002, "*Emergency Services Data Communications.*"** This Joint TIA/Committee T1 document was published in June, 2002 and defines the messaging required to support information transfer to identify and locate wireless emergency service callers (*e.g.*, wireless enhanced emergency calls). This standard incorporates J-STD-036 and 036-1, "*Enhanced Wireless 9-1-1 Phase 2, Addendum 1.*" Note that position reporting privacy restrictions are beyond the scope of this standard. Additionally, note that an

[4] PACA enables an authorized subscriber to originate a queued call when all voice channels are in use. That is, if the subscriber originates a call, but the call cannot be completed because there is currently no free traffic channel to assign to the subscriber, the call is placed into a queue that is maintained by a Base Station, Mobile Switching Center (MSC) and Internetworking Function, typically abbreviated as BMI. When a traffic channel becomes available for use the BMI retrieves a queued call, completes the call, and, while so doing, sends a signal to the subscriber's mobile station or terminal that the previously queued call is being completed.

Addendum 1 for J-STD-036-A, involving position and callback for uninitialized phones, is being balloted within TIA and expects publication in 2003. TR-45.2 has also begun development of a more extensive addendum to J-STD-036-A (probably to be known as J-STD-036-B).

TR-45.3, *Time Division Digital Technology*

- **ANSI/TIA/EIA-136-123-D-2002, "*TMDA Third Generation Wireless - Digital Control Channel Layer 3*."** This ANS describes procedures that support emergency calls, including a provision in the protocols to specifically identify an emergency call. This facility may be used to remove the need for a subscriber to remember the emergency call dialed digits in various jurisdictions. Additionally, this document describes procedures that support an Emergency Information Broadcast, providing for a text message to be displayed to the subscriber, with selectable distinctive alerting. ANSI/TIA/EIA-136-123-A-2000 also describes a queued originate mechanism that may be used to support a priority access scheme (*e.g.*, PAS/WPS PACA) in the event that either radio or network resource is congested.
- **ANSI/TIA/EIA-136-510-B-2000, "*Authentication, Encryption of Signaling Information/User Data, and Privacy*."** This ANS provides information on authentication for the digital control channel, analog voice channel, analog control channel and digital traffic channel. It also provides a description of signaling message encryption, voice privacy and data privacy for TIA/EIA-136 systems.
- **ANSI/TIA/EIA-136-740-2001, "*TDMA 3G Wireless - System Assisted Mobile Positioning through Satellite (SAMPS) Teleservices.*"** This ANS describes enhancements to TIA/EIA-136, including a teleservice that facilitates the exchange of information between a network entity and a mobile station to provide geographic positioning, including protocols that support position reporting to the Public Safety Answering Point (PSAP) or call center, and other aspects related to E9-1-1 mobile caller identification. The SAMPS teleservice defines the procedures and signaling for a handset-based positioning service. SAMPS supports various location-based services and addresses subscriber-positioning requirements in TIA/EIA-136-based networks by utilizing the existing Global Positioning System (GPS) infrastructure and utilizes the data capabilities of TIA/EIA-136 networks to enhance the performance of GPS-equipped MSs by providing "GPS assistance." For information about the network reference model used for SAMPS (when SAMPS is used for emergency calls), see J-STD-036-A. SAMPS Parameter message aspects are also addressed in ANSI/TIA/EIA-136-123-D-2002.
- **ANSI/TIA/EIA-136-741-2002, "*TDMA Third Generation Wireless - System Assisted Mobile Positioning through Satellite (SAMPS) for Analog Systems*."** This ANS was published April 2002 and describes the procedures, signaling, and transport on analog channels (ACC, AVC) that facilitate the exchange of information between a network entity and a mobile station to provide geographic location positioning.

Note: The above ANSI/TIA/EIA-136-XXX documents are included in the ANSI/TIA/EIA-136 Series, Revision D collection.

TR-45.4, *Radio to Switching Technology*

- **TIA/EIA/IS-2000, "CDMA2000® Interoperability Specifications V.40 (IOS V4.0)."** TR-45.4 developed support for Position Determination services on cdma2000® systems.

TR-45.5, *Spread Spectrum Digital Technology*

- **TIA/EIA/IS-2000**, releases involving cdma2000® Spread Spectrum Systems support Emergency Calling.
- **TIA/EIA/IS-2000.4, "*Signaling Link Access Control (LAC) Specification for cdma2000® Spread Spectrum Systems*."** Release 0, A, B, and C support encryption for signaling on dedicated channels. In Release C, support for Authentication and Key Agreement (AKA) authentication protocol was added. This adds message integrity protection.

- **TIA/EIA/IS-2000.5, "*Upper Layer (Layer 3) Signaling Standard for cdma2000*® *Spread Spectrum Systems*."** Position Location Support was added to this Release 0 document. In Release A, the Global Emergency Call parameters and the Access Control based on Call Type (ACCT) feature were added. Origination Messages with the Global Emergency Call Indicator must be encrypted. Note that the latest release is **TIA/EIA/IS-2000.5-C**.

  Additionally, Release 0, A, B, and C support encryption for signaling on dedicated channels. In Release A, support for encryption for voice data and user information on dedicated and common channels was added. Also, in Release A, support for the Rijndael encryption algorithm was added to improve the encryption strength over the previously used encryption algorithm. In Release C, support for Authentication and Key Agreement (AKA) authentication protocol was added. This adds message integrity protection as well as more robust encryption.
- **TIA/EIA/IS-2000.6-A, "*Analog Signaling Standard for cdma2000*® *Spread Spectrum Systems.*"** This part of the cdma2000® family of standards supports and defines PACA service in addition to other more encryption-related aspects. Release B and Release C, published in April and May 2002, respectively, also support PACA and other more encryption/security-related aspects.
- **TIA/EIA/IS-801, "*Position Determination Service Standards for Dual Mode Spread Spectrum Systems*"** and its addendum **TIA/EIA/IS-801-1,** defines a set of signaling messages between the mobile station and base station to provide a position (location) determination service. This document defines the position location feature which provides the capability to locate the mobile station and supports automatic forward link triangulation and GPS position location mechanisms.
- **TIA/EIA/IS-856-1, "*cdma2000*® *High Rate Packet Data Air Interface Specification*."** This part of the cdma2000® family of standards defines a Security Layer that provides the capability to establish an ephemeral session key that is used for authentication of system access attempts by access terminals.
- **TIA-916, "*Recommended Minimum Performance Specification for TIA/EIA/IS-801-1 Spread Spectrum Mobile Stations.*"** This recently published TIA document details definitions, methods of measurement, and minimum performance characteristics for position location capable CDMA Mobile Stations.
- **TIA-925, "*Enhanced Subscriber Privacy for cdma2000*® *High Rate Packet Data*."** This part of the cdma2000® family of standards defines procedures to provide for encryption of bearer traffic and signaling information in the TIA/EIA/IS-856 Security Layer. Specifically, this standard defines the procedures for determining the crypto-sync and other "hook" parameters that are required by the cdma2000® Common Cryptographic Algorithms (CCAs), as well as the interface to the procedures in the CCA to encrypt bearer data and signaling in the TIA/EIA/IS-856 Security Layer.

TR-45.6, *Adjunct Wireless Packet Data Technology*

- **PN-3-0047, "*Lawfully Authorized Electronic Surveillance (LAES) for Packet Data*"** (In committee development; Expected publication in 2003): This proposed TIA standard, **TIA-908**, will involve requirements for supporting packet mode communications surveillance, including collection functions and intercept access point (IAP) aspects.

7. Other Emergency Communications and Communications Network Security Activities Relative to TIA

This section describes other TIA and member activities that involve or relate to Emergency Communications and Communications Network Security.

TIA/ETSI Public Safety Partnership, *Project MESA*

BACKGROUND

The Public Safety Partnership Project (PSPP) or Project MESA (**M**obility for **E**mergency and **S**afety **A**pplications) is the first international communications research and development standardization partnership project whose aim is to develop joint specifications for advanced and future Public Safety/Emergency Response mobile broadband communications technology involving Law Enforcement, Fire Fighting, Homeland Security, National/International Crime and Terror investigations, Emergency and Medical Services and Disaster Response (including mass destruction and bio-terrorism) professionals. The International Telecommunication Union refers to such applications as Public Protection and Disaster Relief (PPDR). The PSPP was given the name "Project MESA" in recognition of the city, where the partnership agreement was finalized (the acronym also serves as an accurate description). The current Partnership Agreement for Project MESA was modified and ratified January 2001 in the City of Mesa, Arizona between the Telecommunications Industry Association (TIA) of the U.S. and the European Telecommunications Standards Institute (ETSI) of Europe.

Due to commonalties between U.S.-centered advanced public safety radio system Project 34 (TIA and APCO) and European-based Digital Advanced Wireless Service (DAWS), TIA and ETSI agreed to collaborate and combine work efforts to provide a forum in which the key players and users can contribute actively to the elaboration of MESA specifications. The project is open to other regions of the world and has observers from Canada and South Korea. Please refer to the www.projectmesa.org Website for further information.

Other organizations/agencies that actively support Project MESA include the Association of Public Safety Communications Officials (APCO), the Project 25 Steering Committee, the Federal Bureau of Investigation (FBI), and the National Institute of Justice (NIJ), the United Nations (UN), the National Telecommunications and Information Administration (NTIA), the Federal Law Enforcement Wireless Users Group (FLEWUG), the Royal Canadian Mounted Police, and the American Red Cross. Regarding standards organization support, a recent international meeting of Global Standards Collaboration-7/RAdio STandardization-10 (GSC-7/RAST-10), recognized Project MESA in a Resolution identifying Public Protection and Disaster Relief as a High Interest Subject.

Project MESA has recently updated and approved the first user-defined Statement of Requirements (SoR), [**Version MESA TS 70.001 V3.1.1a (2002-10)**], which describes and defines future MESA user requirements, specifications, applications and scenarios that involve broadband air interface data rates; allowing Public Safety professionals to communicate over a wide area, using a myriad of technological platforms and applications. Based on the SoR, the MESA Technical Specification Group System (TSG SYS), and its subgroups, are now beginning work on the corresponding technical specifications, which will eventually be submitted to supporting Standards Development Organizations (*i.e.*, TIA, ETSI, etc.) for SDO development and publication.

The end result of this Public Safety/Emergency Response user-oriented activity will be a suite of coordinated specifications and future standards designed for advanced, broadband, interoperable, terrestrial mobility operations, including connectivity to broadband satellite communications (SatCom) services, driven by common scenarios. These requirements can be tailored for specific local and regional implementation scenarios and situations. Such standards and specifications, designed to benefit the Public Safety/Emergency Response community and our nation’s citizens, will be realized in two distinct but highly related areas -- system end-users and system owner/operators.

System End-Users
▪ In-building, portable voice and data coverage.
▪ Real-time support for wireless portable computer applications.
▪ Rapid messaging, including email, free-form text, and file transfers.
▪ Constantly updated personnel and equipment location data.
▪ Arial video for major events, or disaster response coordination.
▪ Transmission and reception of high-resolution digital images.
▪ Satellite connectivity of disaster “hot-spots.”
▪ Real-time incident video and Internet protocol (IP) voice communications overlay.
▪ Full robotics remote control, including audio/video monitoring and transmission.
▪ Remote sensing and aeronautical connectivity (Air-Ground-Air).
▪ Economies of scale for Public Safety/Emergency Response equipment acquisition; also allowing for increased Public Safety/Emergency Response Department access to technology and information.
System Owner/Operators
▪ Local, national, regional and international interoperability.
▪ Frequency neutral technology.
▪ Accommodation of multiple agency networks.
▪ Network authentication and encryption.
▪ Competition in system life cycle procurement.

SECURITY ASPECTS

Project MESA is representative of a vital component of the public safety and public protection platforms of the future. This international specifications and standards effort will ensure future wireless, high-speed data applications, including voice, video, infrared, data, robotics control and many other applications, can be transmitted on a wide-area basis when and if the need exists. The specifications and future standards developed in the Project MESA process will be capable of extremely high levels of security, yet will contain standardized interfaces to public and private networks. It is anticipated that these interfaces will include, but not be limited to, the Public Switched Telephone Network (PSTN), private networks, public and private microwave systems, DS1 and DS3 Common Carrier services, and Integrated Services Digital Networks (ISDN) circuits, as they are applicable. Project MESA is only intended to carry high-speed, digital wireless services, which will supplement other public and private fixed stations, fiber, and hardwire services in place today.

Specifications and standards created in the Project MESA process will ensure future public safety and public protection agencies will have full access to the automated files and tools they need to protect public and private property and reduce morbidity in any major natural or man-created disaster in an efficient and cost-effective manner. Note that just as the existing P25 standards have a definition of “Block Encryption Protocol” which supports a variety of crypto approaches, MESA specifications and standards will need to support a range of encryption options. The draft SoR excerpts related to security are included in **Annex 2**.

<u>STATEMENT OF REQUIREMENTS (SoR) DOCUMENT</u>

The SoR was approved by the Project MESA Steering Committee in 2002. It describes and defines future MESA specifications involving air interface data rates (2 MB/s or greater), including multiple levels of security and encryption to allow public safety/public protection professionals to communicate over a wide area, using a myriad of input/output technological platforms and applications that would include, but not be limited to, secure information, voice, video and infrared video, high-speed data, still photos, enhanced patient and firefighter bio-telemetry information. Specifically, public safety/public protection "users" includes all criminal justice services, emergency management, emergency medical services (EMS), fire, land, natural resource management, military, transportation, wildlife management, and other similar governmental and quasi governmental functions that have a need for aeronautical and terrestrial, high-speed, broadband, digital, mobile wireless communications and telemetry-related services and applications.

Understandably, various Public Safety and Emergency Services may have very different communications needs, which may differ between agencies and countries. Having a common, standardized broadband communications system will help to ensure interoperability of Public Safety/Emergency Response services and applications, within and between agencies and/or countries. Also, to facilitate effective communication and interoperability in emergency situations, it is crucial that both users and various types of terminals can communicate with each other, allowing for information exchange via multiple and divergent facilities, platforms and devices.

The users of professional wireless telecommunications equipment within the Sector of Public Safety/Protection and Disaster Relief (PPDR) have developed the MESA Statement of Requirements document, as they are uniquely aware of, and therefore most qualified to define, qualify and quantify the current and future requirements of Public Safety/Public Protection and other Emergency Response users. The latest version of the SoR describes the services and applications that a future advanced wireless telecommunications system should be able to support, in order to realize the most effective operational environment for the Sector. Emphasis has been placed on those applications that current applied technology cannot carry out to the full, but have been identified by the users and their agencies to be key requirements. This document is unique in the sense that it represents the first transatlantic consolidated view expressed directly by the professional users of advanced wireless telecommunication equipment.

Within Project MESA, this SoR document will be updated at regular intervals and represents the focal source of information for Project MESA's industry members in their work on Research and Development towards the realization of revolutionary new and globally applicable communications specifications and the future standards that evolve from them.

This SoR document is not written specifically to be studied end-to-end, rather it represents a unique source of information with the aim of understanding the often very difficult and dangerous working environments that the public safety/public protection user community is facing, such that industry can provide the most effective and accurate technical solutions.

Finally, it represents the establishment of a clear understanding that the advanced needs of the PPDR Sector should be based on a high mobility broadband wireless network that allows the provision of dynamic bandwidth, offering self-healing characteristics and secure network(s) access. The Project MESA SoR also reflects the vision of a mobile broadband-shared network that can be simultaneously accessed by multiple users, with multiple applications in a specified geographical area that may be fully independent from availability of public networks and supply of electrical power.

- The latest Statement of Requirements document can be viewed at http://www.projectmesa.org/ftp/SSG_SA/Drafts/SoR(latest_version)/.

Global Standards Collaboration (GSC) [Including the Global Radio Standardization Collaboration (GRSC) and the Global Telecommunications Standardization Collaboration (GTSC)][5]

The GSC is comprised of senior representatives of the world's leading radio and telecommunications standards organizations and provides the opportunity for participating telecommunications standards bodies to share

[5] Previously Global Standards Collaboration (GSC) and RAdio STandardization (RAST).

information on their respective work activities, thus fostering cooperation, coordination and the introduction of new telecommunications technologies worldwide. Areas of particular emphasis (*e.g.*, High Interest Subjects) include Next Generation Networks and broadband mobile communication for public safety and emergency services (*i.e.*, PPDR). Such aspects include emergency telecommunications and network security issues. For more information see: http://www.acif.org.au/gsc_rast/.

Other TIA Activities Involving Emergency Communications and Communications Network Security

TIA and its members have been engaged actively with Communications Network Security/Critical Infrastructure [and Asset] Protection (CIP) issues for some time. The newly authorized U.S. Department of Homeland Security (DHS), has been designated the lead agency for physical and cyber protection of the Nation and its Information and Communications (I&C) Sector. Previously the Department of Commerce was the lead agency for the I&C Sector with the Administrator of the National Telecommunications and Information Administration (NTIA) as the Sector Liaison Official (SLO). CIP responsibilities for the I&C Sector include raising I&C Sector awareness of vulnerabilities and risks; assisting the sector to eliminate/mitigate its vulnerabilities; facilitating establishment and operation of I&C Sector information sharing and analysis centers (ISACs); developing cooperative efforts with other countries and international organizations to achieve compatible security policies and strategies; and providing industry with information on results from complementary U.S. Government research and development on critical infrastructure and assets protection. Activities include:

- TIA and TIA member companies have been involved for over 20 years in the President's National Security Telecommunications Advisory Committee (NSTAC), a high-level (Chief Executive) management group of suppliers and operators[6] who counsel the president on national security and emergency preparedness issues. Several years ago NSTAC had proposed the creation of an Information Security Standards Board (ISSB) to determine standards needs for computer systems and manage a conformity assessment program on products and systems to see if they met those standards. For more information on NSTAC, see: http://www.ncs.gov/nstac/nstac.htm.
  - An Information Security Exploratory Committee (ISEC) was formed to evaluate the ISSB proposal. TIA participated on the ISEC and its steering committee. The ISEC strongly recommended increased industry education about potential threats and vulnerabilities, current security products and systems and groups involved in security.
  - TIA has been recently involved, as an industry observer, with the Wireless Task Force (WTF); created under the NSTAC Industry Executive Subcommittee (IES) to address national telecommunications policy issues directly related to wireless services (PCS, cellular, LMR, satellite, unlicensed, WLAN, microwave LOS, etc.) and their national impact on effectiveness and security. The NSTAC WTF will research wireless security issues for NS/EP users, gaining a better understanding of unique NS/EP security requirements and determining where wireless vulnerabilities exist (*e.g.*, customer devices, network interfaces, facilities). The task force will provide policy recommendations to ensure standards bodies and individual companies consider NS/EP requirements when developing wireless connectivity solutions. The task force will also provide policy recommendations to the President addressing how U.S. Government agencies should assess their vulnerabilities, based on wireless technologies being deployed and specific agency requirements. Two recent issues that have been considered:
    - Wireless Priority Access (WPS): Involves WPS on Commercial Mobile Radio Service (CMRS) networks (basically a wireless Government Emergency Telephone Service - GETS). The policy

[6] Includes major communication and network providers, IT, finance and aerospace sectors.

issue being addressed is what is preventing ubiquitous rollout of WPS (carrier liability, vendor liability, etc.). WTF IES Recommendations to be provided to NSTAC committee for consideration of inclusion in NSTAC report to President in 2003.

- Wireless Network Security: The main issue to be addressed involves NS/EP or public safety user access and security with regard to the mirad of network connectivity options. Additionally, TIA's Private Radio Section is considering such aspects as how P25 implements security and how P25 security services might be extended or adopted by other network technologies. The Task Force has recently concluded work and WTF IES Recommendations are to be provided to the NSTAC committee for consideration of inclusion in a future NSTAC report to the President (2003).

- Since its formation, TIA has closely monitored the work of the President's Commission on Critical Infrastructure Protection (PCCIP). The final report of the PCCIP noted that the threat to U.S. infrastructure is real and that the president should take immediate action.
- When President Clinton issued Presidential Decision Direction 63 (PDD 63), TIA staff met with the heads of the Critical Infrastructure Assurance Office (CIAO) and the FBI's National Infrastructure Protection Center (NIPC) to see how TIA could cooperate in these efforts. The NIPC was a FBI and DoJ initiative, to deter, detect and respond to unlawful acts involving computer intrusions and other cyber and physical threats that could adversely impact the critical infrastructures and assets of the U.S.
  - TIA has had representatives of the FBI and NIPC brief TIA members, and TIA was an active participant in the December 1999 partnership kickoff event and in the FBI's Key Asset training program.
  - With PDD-63, the Department of Commerce chose TIA as one of the Sector Coordinators for the Information and Communications Sector.
- As a Sector Coordinator, TIA also holds a Board seat (since March 2001) on the Partnership for Critical Infrastructure Protection (PCIS), a collaborative effort of eight industry sectors deemed by PDD-63 as "critical" infrastructures of this nation's economic and national security. Specifically, PCIS coordinates cross-sector initiatives and interdependency issues, complementing public-private efforts to promote and assure the reliable provision of critical infrastructure services in the face of emerging risks to economic and national security. TIA participates and contributes to cross-sector input for the PCIS.
  - In February 1999, TIA, the United States Telecom Association (USTA) and the Information Technology Association of America (ITAA) were selected to serve as (I&C) Sector coordinators under PDD 63. TIA, USTA, ITAA and the Cellular Telecommunications & Internet Association (CTIA) formed a Critical Infrastructure Protection Consortium and are working with the Department of Commerce and other organizations to increase protection of the nation's communications infrastructure. In May of 2002, the I&C Sector coordinators submitted extensive sector CIP input to the federal government's "*National Strategy to Secure Cyber Space.*" For more information see : http://www.tiaonline.org/media/press_releases/index.cfm?parelease=02-joint%20release%203.
- TIA and its members have participated on the FCC's Network Reliability and Interoperability Council (NRIC), and the previous Network Reliability Council (NRC). The purpose is to assist with analysis of issues that can affect reliability and to determine best practices to recover from natural or man-made outages, including those that might be caused by a computer hacker or terrorist.
  - Relevant NRIC VI Focus Groups (see: http://www.nric.org/charter_vi/index.html):
    - Focus Group 1: Homeland Security
      - Subcommittee 1.A: Physical Security
      - Subcommittee 1.B: Cyber Security
      - Subcommittee 1.C: Public Safety
      - Subcommittee 1.D: Disaster Recovery and Mutual Aid
    - Focus Group 2: Network Reliability
    - Focus Group 3: Network Interoperability

- TIA has represented industry and participated in government CIP activities through the Critical Infrastructure Protection Communications & Information Sector Working Group (CISWG) and its subcommittees that involve Research and Development and International Outreach. For more information see: http://www.ntia.doc.gov/osmhome/cip/ciswg.htm
- For more information on CIP/HS and Cyber Terrorism, see: http://www.tiaonline.org/standards/cip/.

The Board of Directors of the American National Standards Institute (ANSI) approved ANSI to set up a Homeland Security Standards Panel (HSSP), to be a focal point for coordination between the public and private sector on standards needed for Homeland Security. TIA has been active in the planning activities to set up the HSSP which will be open to both ANSI members and non-ANSI members. A Steering Committee meeting of the HSSP is expected in 1Q03.

Annex 1: P25 Service Availability Matrix

SERVICE	CONVENTIONAL	TRUNKED
Telecommunications Services		
Bearer Services		
Circuit-switched unreliable/reliable data	Standard Option	Standard Option
Packet-switched confirmed delivery data	Standard Option	Standard Option
Teleservices		
Broadcast voice call	Not applicable	Mandatory
Unaddressed voice call	Mandatory	Not applicable
Group and individual voice call	Standard Option	Mandatory
Circuit-switched data network access	Standard Option	Standard Option
Packet-switched data network access	Standard Option	Standard Option
Preprogrammed data messaging	Standard Option	Standard Option
Supplementary Service		
Encryption	Standard Option	Standard Option
Priority call and Preemptive priority call	Not applicable	Standard Option
Call interrupt	Standard Option	Standard Option
Voice telephone interconnect	Standard Option	Standard Option
Discreet listening	Standard Option	Standard Option
Silent emergency	Standard Option	Standard Option
Radio unit monitoring	Standard Option	Standard Option
Talking party identification and Call alerting	Standard Option	Standard Option
Subscriber Unit Services		
Intrasystem and Intersystem roaming	Standard Option	Standard Option
Call restriction	Not applicable	Standard Option
Affiliation	Not applicable	Standard Option
Call routing	Not applicable	Standard Option
Encryption update	Standard Option	Standard Option
Network Services		
Registration	Standard Option	Mandatory
Roaming	Mandatory	Mandatory
Authentication and Subscriber terminal disable and enable	Standard Option	Standard Option
Network Management and administration services	Standard Option	Standard Option

Annex 2: Security and Encryption-related Excerpts from MESA Draft Statement of Requirements (S0R), "*Draft DTR/MESA-SA001 V.10 (2002-05-22)*"

Security requirements: Permits effective, efficient, reliable, and, as may be required, secure (authenticated and/or encrypted) intra- and interagency communications (interoperability). The basic security platforms should be capable of being expanded and enhanced to meet each nation's individual requirements without degradation to overall system performance.

Multiple levels of security: All specifications and standards written to comply with the Project MESA SoR should allow for multiple levels and jurisdictionally specific types of security.

Compliant with the need of the participating nations: Specifications and standards written to comply with the Project MESA SoR will also be written to comply with the specific baseline requirement of the national governments that are active within the Project MESA process. Those requirements will be articulated within the body of the SoR or any of its subordinate annexes or related documents and may, as appropriate, be identified as a specific need of a specific nation, government, governmental agency or organization.

Blocking unauthorized access: The specifications and standards written to comply with the Project MESA SoR should include the ability to block access by unauthorized users.

Encryption: Specifications and standards that are compliant with the Project MESA SoR will include a high level of security that will fulfill public safety future needs and requirements. Those needs and requirements will include the extensive use of wireless data and voice systems. These systems should be capable of being encrypted for the extremely secure transmission of all voice and data traffic.

- The specifications and standards written to comply with the Project MESA SoR should include the optional capabilities for robust MESA user device and network security as outlined elsewhere in the present document.
- The specifications and standards that are written to comply with the Project MESA SoR should include the option of having fully encrypted systems and networks. Fully encrypted systems and networks would include all associated control channels and the use of password access codes if applicable.
- The countries that are participating in the Project MESA SoR process believe that future information technology requirements mandate a high level of security for a majority of their governmental and public safety functions. Specifications and standards that are written to comply with the present document should include the capability to provide wireless, multimedia data systems using multiple types of encryption. In order to maximize the effectiveness of agents and officers in the field, a mobile office environment utilizing cryptographically protected wireless voice and data communications should be developed. (The term data includes all forms of data including video and telemetry.)
- The specifications and standards written to comply with the Project MESA SoR should support transparent, secure (authenticated and encrypted) access to national governmental files.
- Both network and application encryption shall be compliant with regional legislation covering lawful interception/CALEA.

General encryption requirements: In order to maximize the effectiveness of agents and officers in the field, a mobile office environment using cryptographically protected wireless data communications should be developed.

Specific and/or unique requirements of the U.S. Government: MESA specifications should accommodate Type I, Type II, Type III, Triple DES and other encryption algorithms used by the U.S. government, other national governments, and local government (if standardized and widely available). They should also accommodate Type IV cryptographic algorithms with OTAR, consistent with P25 Phase I standards used in the U.S.