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

[January, 2005 Revision]

ABSTRACT
This compendium document identifies many standards, other technical documents, and ongoing activity involving or supporting TIA’s role in Public Safety and Homeland Security, Network Security, Critical Infrastructure Protection and Assurance, National Security/Emergency Preparedness, Emergency Communications Services, Emergency Calling and Location Identification Services, and the Needs of First Responders. This compendium is a “snapshot” of TIA activities and is presented for information, coordination, and reference. It is updated from time to time as new work commences or status changes.

INTRODUCTION
This compendium document identifies many standards, other technical documents, and ongoing activity involving or supporting TIA’s role in Public Safety and Homeland Security, Network Security, Critical Infrastructure Protection and Assurance, National Security/Emergency Preparedness, Emergency Communications Services, Emergency Calling and Location Identification Services, and the Needs of First Responders. In addition, this document encapsulates areas of activity which do not fall under a specific Formulating Group or Engineering Committee. This compendium is a “snapshot” of TIA activities and presented for information, coordination and reference. It is updated from time to time as new work commences or status changes. For the purpose of this document, terms relating to Public Safety and Disaster Response can be considered synonymous (and interchangeable) with terms relating to Public Protection and Disaster Relief.

TIA is accredited by the American National Standards Institute (ANSI), progresses work into the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC), and is recognized under the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) Recommendations A.5 and A.6, respectfully involving the referencing of other organizations1 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). The ITU-Radiocommunication Standardization Sector (ITU-R) also communicates with TIA and references appropriate TIA work in its Recommendations.

Currently, technical work relating to this compendium’s subject matter is mainly being developed under six Engineering Committees (i.e., TRs). See below for a brief overview:

- **TR-8 Committee (Mobile and Personal Private Radio Standards).** Activities include public safety/emergency and commercial land mobile radio communications involving voice and narrowband, wideband and broadband data; stressing interoperability, compatibility, security and efficient analog to digital migration. Work includes the Project 25 family of standards, the Wideband Data Standards Project and Project 34 (related to Project MESA involving broadband data capabilities).

- **TR-30 Committee (Multi-Media Access and Related Protocols and Interfaces).** Activities include technical work related to such devices as modems, standard and IP facsimile and textphones. Related to this compendium, activities presently being explored involve such topics as Internet/IP facsimile security and emergency accessibility service capabilities for textphones over IP and Public Switched Telephone Networks (PSTN),

---

1 Including TIA technical documents, published documents, or work currently being developed under various TIA Engineering Committees.
The work done in this committee has emergency telecommunications service implications and aspects, including enhanced priority treatment, network security, international connectivity, service for the disabled and quality of service.

**TR-34 Committee (Satellite Equipment and Systems).** Future activities may include coordination and new work initiation for applicable security and emergency service/accessibility related satellite communications standards, if deemed appropriate by members. Emergency users may also find interest in capabilities of IP over Satellite (IPoS) work.

**TR-41 Committee (User Premises Telecommunications Requirements).** Activities involve service and performance criteria as well as information necessary for proper interworking of wireline-related equipment, systems and networks with each other, the public networks, and carrier provided private line services. Recent security issues that are being worked in the TR-41 committee include IP Telephony and related infrastructure assurance, wireline network security and support for emergency calling service. Infrastructure assurance, network security and enhanced emergency telecommunications service are all aspects addressed within this committee’s work.

**TR-42 Committee (User Premises Telecommunications Infrastructure).** Activities and documents developed involve commercial, industrial and residential physical cabling infrastructure, pathways and system requirements (copper and optical fiber systems). Such work can be applicable to issues associated with infrastructure assurance, security and emergency telecommunications availability, including guidance for alternate routing of cabling into a building to help prevent loss of communications.

**TR-45 Committee (Mobile and Personal Communications Systems).** Activities involve performance, compatibility, interoperability and service standards pertaining to, but 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. Issues and work applicable to the compendium include wireless emergency calling and priority services, location identification, security, Mobile Equipment Identifiers, lawful interception and related capabilities.

In addition to TIA Engineering Committee work, TIA Members and staff continue to be active in matters (including international partnership projects) involving national and international Public Safety, Homeland Security, National Security and Emergency Preparedness (NS/EP), and Critical Infrastructure Protection and Assurance. TIA also co-chairs the ANSI Homeland Security Standards Panel (ANSI HSSP); is designated a Sector Coordinator under Presidential Decision Directive-63 and Homeland Security Presidential Directive (HSPD)-7; is a non-Resident Member of the National Coordinating Center Telecommunications Information Sharing and Analysis Center (NCC Telecom-ISAC); supports, along with TIA Members, the activities of the President’s National Security Telecommunications Advisory Committee (NSTAC) and the National Infrastructure Advisory Council (NIAC); TIA holds a board seat on the Partnership for Critical Infrastructure Security (PCIS); and on the steering committee of the National Cyber Security Partnership (NCSP).

As an ANSI-accredited SDO, TIA develops consensus-based, voluntary industry standards for a wide variety of national and global communications products and systems. TIA standards and their descriptions can be searched and accessed at: [http://www.tiaonline.org/standards/search_n_order.cfm](http://www.tiaonline.org/standards/search_n_order.cfm). The TIA Standards and Technology (S&T) Department Webpage is available at: [http://www.tiaonline.org/standards/](http://www.tiaonline.org/standards/).

---

**Clarification regarding TIA documents:** Most documents included in this compendium involve American (ANSI-approved) National Standards (ANSs), 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…” Note that the term “standard” implies voluntary, consensus-based development (i.e., international SDO term Recommendation), unless legislated or mandated by an Administration’s rules and regulations (i.e., FCC in the USA, for example, to become a “technical regulation” which are also often referred to as “mandatory standards”).
# TABLE OF CONTENTS

TIA Trade Association Activities Involving Emergency Communications, Communications Network Security and Critical Infrastructure Protection and Assurance

TIA Engineering Committee and Related Standards Activities Involving Emergency Communications, Communications Network Security and Critical Infrastructure Protection and Assurance

   - Project 25, *Standards for Public Safety Radio Communications*  
     - Phase I Development and Implementation: 15  
     - Phase II Development and Implementation Documents: 15  
     - Phase III Development: 16  
     - Related National and International Standardization for Broadband 16  
     - The Wideband Data Standards Project (TIA-902 AND 905-Series) 17  
     - Other TR-8 Work Activities and Documents 17

2. TIA/ETSI Public Safety Partnership, *Project MESA* 18


8. Global Standards Collaboration (GSC) [Including the Global Radio Standardization Collaboration (GRSC) and the Global Telecommunications Standardization Collaboration (GTSC)] 22

Annex 1: P25 Service Availability Matrix 24

Annex 2 TR-8 P25 Phase I
   - System and Standards Definition Documents 25  
   - P25 Service Category Standard Documents 25  
   - P25 System Category Description Documents 26  
   - Equipment Category Description Documents 27

Annex 3 TR-8 P25 Phase II 28

Annex 4, TR-8 Wideband Data Project 29

Annex 5, Other TR-8 Projects 30

Annex 6, Project MESA 31
   - MESA Statement of Requirements (SoR) Document 31  
   - SoR Abstract of MESA User Community’s Technological Needs 32  

Annex 7, MESA Security Aspects 40
   - Security and Encryption-related Excerpts from the MESA Statement of Requirements (S0R): 40
### Annex 8, TR-41 Activities
- TR-41.1, Multiline Terminal Systems
- TR-41.4, IP Telephony Gateways and Infrastructures
- TR-41.9, Technical Regulatory Considerations

### Annex 9, TR-42 Activities
- TR-42.2, Residential Telecommunications Infrastructure
- TR-42.3, Pathways and Spaces for Telecommunications Cabling
- TR-42.4, Outside Plant Telecommunications Infrastructure
- TR-42.6, Telecommunications Infrastructure Administration

### Annex 10, TR-45 Activities
- TR-45 Ad Hoc Authentication Group (AHAG)
- TR-45 Joint Ad Hoc Group, Lawfully Authorized Electronic Surveillance (LAES)
- Future TR-45 LAES Work
- TR-45 ESN/UIM/MEID Ad Hoc Group (EUM)
- TR-45.1, Analog Technology
- TR-45.2, Wireless Intersystem Technology
- TR-45.2 Ad Hoc Emergency Services (AHES) Group
- TR-45.3, Time Division Digital Technology
- TR-45.4, Radio to Switching Technology
- TR-45.5, Spread Spectrum Digital Technology
- TR-45.6, Adjunct Wireless Packet Data Technology
TIA Trade Association Activities Involving Emergency Communications, Communications Network Security and Critical Infrastructure Protection and Assurance

TIA and its members have been engaged actively with Communications Network Security/Critical Infrastructure and Asset Protection (CIP) issues for some several decades. Before 2003, the Department of Commerce was the lead agency for the Information and Communications (I&C) Sector with the Administrator of the National Telecommunications and Information Administration (NTIA) as the Sector Liaison Official (SLO). Under Presidential Directive Decision (PDD)-63, the Department of Commerce designated TIA, in 1999, to be one of the Sector Coordinators for the I&C Sector. CIP responsibilities for the I&C Sector included 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.

As of March 2003, the newly authorized U.S. Department of Homeland Security (DHS), has been designated the lead agency for physical and cyber protection of the Nation’s telecommunication Sector and is now the central federal entity for critical infrastructure and assurance issues. With Homeland Security Presidential Directive 7 (HSPD-7) TIA continues in this role as a Telecommunications Sector Coordinator (with CTIA and USTA). The previous I&C Sector is now composed of the Telecom Sector and the Information Technology (IT) Sector under HSPD-7.

TIA activities have included:

- As a Sector Coordinator, the TIA was subsequently accepted as a non-Resident member of the 24x7 National Coordinating Center Telecommunications – Information Sharing and Analysis Center (NCC Telecom ISAC). Activities include weekly NCC Telecom ISAC staff update meetings, cross-ISAC activities, coordination/outreach to non-ISAC industry members, and other activities, as requested by ISAC members. Includes national emergency alerting and member availability to assist NCC T-ISAC efforts as requested. The NCC T-ISAC is the central contact point for telecommunication sector and connectivity/restoration issues associated with natural/man-made disasters and emergencies, special security events, etc. (All-Hazards).
  - TIA is part of the Emergency Notification System (ENS) of DHS Information Assurance Infrastructure Protection Directorate (DHS IAIP).


- As a Sector Coordinator, TIA also holds a Board seat (since March 2001) on the Partnership for Critical Infrastructure Security (PCIS), a recently re-chartered collaborative effort among participating “critical infrastructure” Sector Coordinators established to support cross-sector and interdependency issues among the sectors identified in PDD-63 and HSPD-7. The PCIS supports the information security, protection and assurance interests of the identified national critical infrastructures and key assets that were defined in PDD-63 and recently expanded with recent Executive Orders, the Homeland Security Act of 2002, and the President’s National Strategies for Homeland Security and Cybersecurity. Such critical sectors include, among others, telecommunications, information technology, banking and finance, transportation, continuous energy supply, chemical, water and food supply. The mission of PCIS is to "coordinate cross-sector initiatives and complement government and industry efforts to promote the assurance of reliable provision of critical infrastructure services in the face of emerging risks to economic and national security." In carrying out its mission, the PCIS provides a forum to promote dialog between industry and government and among the sector coordinators and ISACs on reducing vulnerabilities, mitigating risks, identifying strategic objectives and sharing sound information security practices. TIA continues to participate and support this cross-sector collaborative effort. PCIS meets bi-monthly with the DHS and other Sector Specific Agencies (SSAs) and the ISAC Council, and separately the other month.

- 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 and conformity assessment needed for Homeland Security. Specifically, the HSSP, as another cross-sector activity, will be a coordinating body for the development and enhancement of homeland security and emergency preparedness standards and conformity assessment, as developed by ANSI members and non-ANSI members.
  - TIA has been active in the planning activities to set up the HSSP which is open to both ANSI members and non-ANSI members. In March 2003, Dan Bart, senior vice president, standards and special projects for TIA, was named as private sector Co-chair of the new Homeland Security Standards Panel (HSSP), with NIST as public sector Co-Chair. He also Co-chairs its Steering Committee (SC). The ANSI HSSP SC also functions as a U.S. Technical Advisory Group for the US Expert to the ISO Advisory Group on Security (AGS).

- TIA was appointed to the advisory committee of the National Public Safety Telecommunications Council (NPSTC).
- TIA was appointed to the advisory committee for DHS SAFECOM.
- 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 (e.g., major communications and network providers, IT, finance and aerospace sectors) who counsel the president on relevant national security and emergency preparedness issues. TIA attends business meetings of the NSTAC and participates at the subgroup/task force level. For more NSTAC information and reports, visit: http://www.ncs.gov/nstac/nstac.htm.

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. 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. Also advised that there was not a case for ISSB initiatives at that time due to other industry efforts.

TIA has been 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 Line of Sight (LOS), etc.) and their national impact on effectiveness and security. The NSTAC WTF researched 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 provided policy recommendations to ensure standards bodies and individual companies consider NS/EP requirements when developing wireless connectivity solutions. The task force also provided policy recommendations to the President, via the NSTAC, addressing how U.S. Government agencies could assess their vulnerabilities, based on wireless technologies being deployed and specific agency requirements. Two issues that have been considered include:

- **Wireless Priority Service (WPS):** Involves WPS on Commercial Mobile Radio Service (CMRS) networks (basically a wireless Government Emergency Telecommunications Service - GETS). The policy issue addressed was the preventing ubiquitous rollout of WPS (carrier liability, vendor liability, etc.). WTF IES Recommendations were provided to the NSTAC committee and included in their 2003 NSTAC report to President.

- **Wireless Network Security:** The main issue addressed involves NS/EP or public safety user access and security with regard to the myriad of network connectivity options. 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 concluded work and WTF IES Recommendations were provided to the NSTAC committee for inclusion in their 2003 NSTAC report to President.

The most recent NSTAC IES Task Force is focusing on Next Generation Networks (NGN) National Security/Emergency Preparedness (NS/EP) needs. TIA is actively participating in working groups of the task force, including:

- NSTAC IES NGN Task Force, NGN Description Working Group
- NSTAC IES NGN Task Force, NGN Scenarios and User Requirements Working Group
- NSTAC IES NGN Task Force, NGN Near-Term Recommendations Working Group
- Follow-on NSTAC NGN working groups may include Incident Management, End-to-End Services and Threat Modeling.


- TIA and TIA members have been involved in the activities of President Bush’s National Infrastructure Advisory Council (NIAC). Recent activity includes Prioritization of Cyber Vulnerabilities Working Group.

- Since its formation in 1996, TIA has closely monitored the work of the President’s Commission on Critical Infrastructure Protection (PCCIP). The final report of the PCCIP emphasized the importance of threat mitigation to U.S. infrastructures and called for timely action. A PCCIP Commissioner gave presentations at SUPERCOMM ‘97 and other TIA-hosted events.

- When President Clinton issued Presidential Decision Direction 63 (PDD 63), TIA staff met with the heads of the U.S. Department of Commerce 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 an 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.

- TIA and its members have and continue to participate on the FCC's Network Reliability Council (NRC) and Network Reliability and Interoperability Council (NRIC) and its subgroups. The purpose is to assist with analysis of issues that can affect reliability, security and other FCC-specified analysis areas 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, and create Best Practices.

- Relevant NRIC VI Focus Groups involve Homeland Security (prevention, restoration and public safety), Network Reliability, Network Interoperability and Broadband Deployment.

  - March NRIC VII meeting information: [http://www.nric.org/meetings/meeting20040330.html](http://www.nric.org/meetings/meeting20040330.html).

- TIA participates in DoC NTIA’s Economic Security Working Group (EconSec WG) meetings and participates in its subgroups. TIA has and continues to represent industry, monitor and participate in government CIP activities through the EconSec WG, previously called the Critical Infrastructure Protection Communications & Information Sector Working Group (CISWG), and its subcommittees involving such topics as International Outreach, Research and Development and support for bi/multi-lateral meetings. For example, bi-lateral meetings and multi-lateral meetings on CIP; including government/industry delegations...
involve the nations such as Italy, Canada, Australia, India and Japan; including private meetings with other SDOs or multi-national companies as able. For more information see: http://www.ntia.doc.gov/osmhome/cip/ciswg.htm.

- In 2004, TIA accepted an offer to serve on the National Cyber Security Partnership (NCSP) Steering Committee. This private/public partnership effort supports DHS and other government initiatives.

- Other activities that TIA has been recently involved with that addresses needs of First Responders and Law Enforcement, include:
  - Active public policy programs for urging spectrum for Public Safety and Funding for Public Safety Interoperability.
  - Participated at DHS/NIST Public Safety Interoperability Workshop.
  - Meetings with DHS SAFECOM Office.
  - TIA moderated a Panel on Public Safety needs at SUPERCOMM 2003.
  - Briefings on MESA and other Public Safety-oriented programs at ITU (PPDR/TDR) and elsewhere.
  - Briefings on TIA Public Safety-oriented activities like MESA to CDG Board (Dec 03), CIAJ (Jan 04, Jun 04).
  - Moderated Congressional Research Service (CRS) Panel on Public Safety needs (Nov 03).
  - Supported Global Disaster Information Network (GDIN) event (March 2004).
  - TIA is the Lead SDO on Lawfully Authorized Electronic Surveillance (LAES) standardization for CALEA.

- Other TIA connections with Security/CIP include:
  - The Internet Security Alliance (ISA) is a member of the Electronic Industries Alliance (EIA) along with TIA, and the ISA Executive Director is a Special Advisor to ANSI HSSP.
  - TIA was part of ANSI/ESO (European Standards Organizations - CEN/CENELEC/ETSI) meetings in France 2004 and security standards were a topic on that agenda and will be discussed again at the January 2004 ANSI/ESO meeting in Washington, DC..
  - Security and Privacy of Communications and Location information is an emerging topic for ISO TC 204 WG 16 Intelligent Transportation Systems (ITS) and TIA is a voting member of the US TAG to TC 204 and WAG Admin for WG-16.
  - 3GPP2 develops specifications that ensure security within cdma2000® systems.
  - TIA shares information with other SDOs and international groups like the ITU and GSC involving this compendium’s subject matter.

- For more information on CIP and HS, visit: http://www.tiaonline.org/standards/cip/.


The Telecommunications Industry Association (TIA) is a leading trade organization serving the communications and IT industry, with proven strengths in standards development, domestic and international public policy, and trade shows. Through its worldwide activities, TIA facilitates business development opportunities and a competitive market environment. The association provides a forum for its member companies, the manufacturers and suppliers of products and services used in global communications. TIA represents the communications sector of the Electronic Industries Alliance (EIA).
TIA Engineering Committee and Related Standards Activities Involving Emergency Communications, Communications Network Security and Critical Infrastructure Protection and Assurance

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

The Engineering Committee and its Subcommittees develop and maintain standards for private radio communications systems and equipment (e.g., Public Safety services and commercial operations) for both voice and data applications; addressing all technical matters for systems and services, including definitions, interoperability, compatibility and compliance requirements.

Engineering Committee TR-8 has over 60 years of standards formulation history, starting with Private Land Mobile Radio Systems and frequency modulated (FM) analog technology. However, the past decade has seen the development of standards for digital radio systems of various technologies. This transition has increased the sophistication of radio systems and, as a result, has necessitated an increased level of standardization for many of the components of these systems. In addition, as new technologies are deployed, issues of compatibility and interoperability are of prime importance. In communications systems for public safety and emergency services, reliability and interoperability are especially important. The criticalness of these communications also requires the avoidance of unwanted interference. All these requirements have caused Engineering Committee TR-8 to assume a wider scope in the standards being developed. Due to the nature of this committee, most standards and projects are related to this compendium’s subject nature. See below for descriptions of activity under this TIA Engineering Committee.

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 NASTD [now known as the Association for Telecommunications and Technology Professionals Serving State Government], selected North American Federal Agencies, and the National Communications System (NCS) established Project 25 (P25), headed by a steering committee for selecting voluntary common system standards for digital public safety radio communications (voice and data). A Memorandum of Agreement was signed with the TIA in 1991, to utilize the resources of the TIA, as an ITU-recognized and ANSI-accredited Standards Development Organization, to supply the necessary technical support. Such technical support involved the development in TIA TR-8 of the 102 [and related]-series of technical documents that define the equipment and processes (including interworking and interoperability with other systems) necessary for implementation of the P25 Land Mobile Radio (LMR) standards family. The TIA standards for P25 are open standards, intended for multiple vendor availability; defining the various interfaces such as Common Air Interface, Data Interface, Inter sub system interface, Network Management Interface, Telephone Interface, etc. Phase I of the P25 standard’s family, involving digital voice and limited data, was completed and announced at the August 1995 APCO Convention. Phase II commenced shortly thereafter, with the development of standards for 6.25 kHz FDMA (improved spectrum utilization), a TDMA solution, high-speed data, and a number of system enhancements as its key points of focus. Attention is also paid to interoperability with legacy equipment, roaming capacity and spectral efficiency/channel reuse. In addition, Phase II is undertaking activity involving console interfacing, fixed station

2 Overall, 1,200 individuals from nearly 20 countries participate in TIA’s eight product-oriented Engineering Committees (TR/FO), with over 70 subcommittees and working groups. Formulating groups include representatives from academia, manufacturers, service providers, end-users and government officials.

3 Related to Wideband Data Standards Project (TIA 902-Series). Currently preparing for ANS and in addition has been a contribution to the MESA broadband project.
interfacing and intersystem interfacing labeled Inter Sub-System Interface (ISSI), and man-machine interfaces for console operators that would facilitate centralized training, equipment transitions and personnel movement. Project 25 is included in ITU-R Recommendation M.2014.

In light of recent worldwide terrorist activities, interoperability among first responders is a key initiative of many countries. The primary public service function of P25-compliant equipment and systems is emergency voice communications between line officers (i.e., first responders such as police, firefighters, etc.) in the field and their dispatch points. Such communications require instant transmission and instant response, with a common language link or encryption, as required. As the bandwidth allocated by national authorities for this type of traffic can be limited, P25 systems are primarily utilized for narrowband voice communications (operating in 12.5 kHz radio channels or narrower), with some level of data transmission. Standards related to wide and broadband data applications and interoperability are detailed in other sections of this document (e.g., Public Safety Wideband Data Standards Project and Project MESA). The services provided by P25-compliant systems are intended to be utilized 24/7 with ubiquitous coverage, including inside buildings and structures (with most newer systems), within the geographical areas of responsibility for the first responders. However, with interoperable standards-based systems, mutual aid interoperation is facilitated for large-scale incidents.

The P25 suite of LMR standards (including TIA standards and ANSs) and TSBs allow compliant systems a high degree of equipment interoperability and compatibility, involving digital LMR services for local, state and national (federal) public safety organizations, departments, and agencies. The P25 series of standards 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 communications solutions.

P25-compliant systems are being increasingly adopted and deployed. Today there are over 660 operational Project 25 networks in over 54 countries worldwide providing interoperability for public safety and federal agencies in many environments, including major metropolitan and rural areas. 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 of the railroad industry for a high-quality, secure digital radio system, involving rolling stock, personnel, and transportation vehicles. Additionally, as new technologies and public safety needs evolve, the P25 standards will continue to be refined.

P25 system technology enables public safety agencies to gracefully migrate from analogue FM systems to narrow-band and wide-band digital systems offering enhanced voice and data functionality. P25 technology and migration scenarios involve three phases (two main, one complimentary) of overall implementation. Phase 1 of the P25 standard, involving an FDMA system using compatible FM and QPSK modulations in 12.5 kHz, is complete, with many vendors providing compliant equipment to professional users. Phase II has added FDMA at 6.25 kHz bandwidths and is addressing TDMA alternatives to achieve 6.25 kHz equivalency, data, and a number of system enhancements. Note that work involving high speed data were developed under the Wideband Data Standards Project (TIA 902-series documents) for 700 MHz and are currently being prepared as American National Standards. Information also contributed to MESA Broadband Project.

See below for more development and technical information:

- A searchable listing of published TIA 102-Series documents can be viewed and ordered by pointing your browser to: [http://www.tiaonline.org/standards/search_n_order.cfm](http://www.tiaonline.org/standards/search_n_order.cfm) and search with keyword “Project 25”

---

4 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.
The P25 LMR system has the objectives to provide public safety with:

1) a spectrum-efficient solution that satisfies the spectrum regulator’s requirements for narrow-banding,

2) a digital solution that offers the public safety community more services (such as short messages, caller ID, etc.) as well as better system command and control (an administrator can set up talk groups for the police in one jurisdiction, the police captains over the entire metro community, etc.),

3) a backward-compatible solution to FM analog land mobile radios and to legacy systems for interoperability and to allow a migration path from analog to digital technologies, and

4) a solution that allows the public safety agencies to select among multiple vendors offering multiple options and features such that the agencies can select the radio system’s characteristics based upon their needs and funding requirements.

Related to the topic of this compendium, the following general LMR security overview was recently published:

- **TIA-102.AAAB-A, “Project 25 - Digital Land Mobile Radio - Security Services Overview(R2005)”** This document provides an overview of the security services available in Land Mobile Radio systems. It provides the context in which to understand why security services are required and gives a general high level description of how they are provided.

Concerning the two main phases of P25 work and the eight originally envisioned interoperability standards, six have been completed and published. Five of these, which are collectively referenced as Phase 1, are complete and have compatible equipment and systems from multiple vendors in service today. The sixth, the ISSI (Inter Subsystem Interface), continues to be refined as part of Phase 2, which also addresses three additional interfaces.

---

5 PTIG stands for Project 25 Technology Interest Group, and is a non-profit Trade Association and an alliance of public safety communications officials and manufacturers. PTIG provides education about the standard to public safety users, to encourage interoperability across public safety and federal communication agencies.
The following chart (Figure 1) provides an update on the status of the different interfaces and indicates where the previous completion of the interface has enabled manufacturers to bring compliant equipment to market.

**Figure 1: Status of Interfaces**

<table>
<thead>
<tr>
<th>Project 25 Interoperable Interfaces</th>
<th>Standard Published</th>
<th>Hardware Available</th>
<th>Hardware Procured by Public Safety Agencies</th>
<th>Testing completed to verify conformity with P25</th>
<th>Equipment in Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1 Interfaces</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Common Air Interface (CAI)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x (independent)</td>
<td>x</td>
</tr>
<tr>
<td>Telephone Interconnect Interface</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x (supplier/customer)</td>
<td>x</td>
</tr>
<tr>
<td>Subscriber Data Peripheral Interface</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x (supplier/customer)</td>
<td>x</td>
</tr>
<tr>
<td>Data Network Interface</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x (supplier)</td>
<td>x</td>
</tr>
<tr>
<td>Network Management Interface</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x (supplier/customer)</td>
<td>x</td>
</tr>
<tr>
<td>Phase 2 Interfaces</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inter RF Subsystem Interface (ISSI)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Console Interface</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed Station Interface</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TDMA Operation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* ISSI Overview and Messages Definition documents only. Additional documents in development.*
P25 is intended to cover a broad range of system configurations, spanning conventional unit-unit direct communications, and repeater based communications, as well as trunking system configurations covering anything from single site through nationwide networking. A generic system model was adopted depicting the maximum complexity, although systems may embody all elements at one extreme, or just a simple conventional base station at the other extreme. An alternative system model is also described for infrastructure-less unit to unit direct communications. P25 is designed to serve an environment of many different P25 compliant systems operating either independently, or in concert.

Figure 2 shows the components of a P25 land mobile radio system and each of the eight interfaces. The concept of dividing the system at defined interfaces allows manufacturers to develop products that are specific to their talents and allows users to buy products that are specific to their needs. For example, a manufacturer may build fixed radio stations (identified as base station or fixed in Figure 1). The component would have to meet the requirements of two P25 interfaces (both the Fixed Station Interface and the Common Air Interface). This particular manufacturer might offer very specific features such as it operates over very high temperature changes (ideal for radios on mountain top locations in isolated areas) and the feature is very important to a particular user. Or a manufacturer is willing to build a very basic fixed radio for very little cost but still meet all of the interface requirements. Again this may be appealing to users for some applications. Thus, as the users build out their systems, they can choose components that exactly meet their needs.

The primary component in Figure 2 is the RF SubSystem (RFSS). The RFSS must support six of the eight P25 interfaces. The RFSS is the heart of the system providing for processing all of the calls, setting up of all the command and control messages, and routing of all voice and data packets. The one exception of calls not being processed through the RFSS is shown in Figure 2 with two or more portable and mobile subscriber radios communicating directly with one another. This condition is called “talk around” for communicating around the fixed infrastructure. However “talk around” must also adhere to P25 interface protocols, in this case the Common Air Interface standard. Each of the interfaces is described as follows:

- **Common air interface** – this interface defines the wireless access between mobile and portable radios and between the subscriber (portable and mobile) radios and the fixed or base station radios
- **Subscriber data peripheral interface** – this interface characterizes the signalling for data transfer that must take place between the subscriber radios and the data devices that may be connected to the subscriber radio
- **Fixed station interface** – this interface describes the signalling and messages between the RFSS and the fixed station by defining the voice and data packets (that are sent from/to the subscriber(s) over the common air interface) and all of the command and control messages used to administer the fixed station as well as the subscribers that are communicating through the fixed station.
- **Console interface** – this interface is similar to the fixed station interface but it defines all the signalling and messages between the RFSS and the console, the position that a dispatcher or a supervisor would occupy to provide commands and support to the personnel in the field
- **Network management interface** – this interface to the RFSS allows administrators to control and monitor network fault management and network performance management.
- **Data network interface** – this interface describes the RF subsystem’s connections to computers, data networks, external data sources, etc.
- 14 -

- **Telephone interconnect interface** – this interface between the RFSS and the Public Switched Telephone Network (PSTN) allows field personnel to make connections through the public switched telephone network by using their radios rather than using cellular telephones.

- **Inter RF subsystem interface** – this interface permits users in one system to communicate with users in a different system, from one jurisdiction to another, from one agency to another, from one city to another, etc.

P25 systems are operating today in the VHF, UHF, and 800 MHz bands utilized by public safety communications, and have been for a number of years. A key element of the Project 25 technology is its ability to coexist with existing analogue systems, enabling a graceful migration from analogue to digital, while maintaining an emphasis on interoperability and compatibility among conventional and trunked systems implementations. Primary channel characteristics were chosen early in the process in favour of band splitting current 25 kHz operation to 12.5 kHz for Phase I and then to 6.25 kHz equivalency as part of Phase II. These decisions were weighted in consideration of the United States FCC refarming plan. Note that TIA-905 series of standards are related to Project 25 Phase 2, 2 Slot TDMA series, meeting the 6.25 kHz FCC Mandate.

A modulation was selected from the QPSK family because of its unique ability to support graceful migration. A 4-level FM modulation known as C4FM was selected for Phase I operation in 12.5 kHz, which offers interoperability with C-QPSK linear modulation for Phase II FDMA operation at 6.25 kHz. Phase I and Phase II operate with identical channel formats at 9 600 bit/s. Phase II will use the same vocoder and encryption as Phase I, thus assuring compatibility and interoperability. The modulation selection for Phase II TDMA is in process, involving Project 25 Phase 2, 2 Slot TDMA and 2 slot TDMA Voice Coder or Codec differentiator options.

In the year 2000, US FCC spectrum allocation provided public safety in the United States with 24 MHz of spectrum in the 700 MHz band. As part of this spectrum allocation, the FCC specified the Project 25 Phase I Common Air Interface as the interoperability mode for 700 MHz. This band will support 6.25 kHz bandwidth that can be aggregated based upon user requirements to 25 kHz for integrated voice and data. It also supports a bandwidth of 50 kHz that can be aggregated to 100 kHz, and 150 kHz bandwidths for high-speed data applications.

The fundamental key attribute of P25 is its common channel formats for a wide-range of configurations and applications. Formats for conventional operation are common with trunking operation. Formats for data are common with trunking control or conventional control. Encryption mechanisms are applicable to any service format, should they be data, voice, or control. This commonality yield the "integration" desired for the system definition. Another key attribute of Project 25 is in the hierarchical addressing and inter-subsystem organization which will permit multiple Project 25 systems to either coexist, or offer coordinated service at the discretion of the system operators.

The main priority of each of these systems is to satisfy public safety users of conventional, trunking, and data applications. The system allows for the definition of voice communications in a group call, private call, or interconnect call. The system further allows for the definition of circuit data or packet data bearer services. Any voice or data service may be digitally coded although clear, or encrypted. Further, the digital control necessary for coordinating trunking system operation may be digital clear or encrypted. A hierarchical system design provides for the ability to connect RF subsystems together to provide roaming and or wider-area communications.
**Phase I Development and Implementation:**
The Project 25 Phase I documents are complete and define interoperable, digital public safety radio communications in 12.5 kHz (narrowband) channels. A P25 Phase I-compliant system ensures that any manufacturer’s compliant subscriber radios have access to the services described in the TIA 102-series documents, involving other systems, across system boundaries, backward compatibility, etc., regardless of system infrastructure. As such, the P25 system provides an open interface to the Radiofrequency (RF) subsystem to facilitate interlinking of different vendor’s systems. The Phase I family of documents specify the P25 compliant air interface and digital Vocoder requirements for 12.5 kHz bandwidth operation, along with telephone-to-radio user interconnect, data, trunking and highly-secure encryption, including the Advanced Encryption Standard (AES) approved Federal Information Processing Standard (FIPS). Many systems at the local, state, and federal levels have been implemented and are using various Project 25 compliant and virtually compliant P25 technologies. The P25 standard enables migration from existing analog systems (including conventional, trunked, and encryption technologies) to narrowband public safety digital P25 systems. The table in Annex 1 shows the availability of P25 system services.

See Annex 2 for examples of TR-8 Phase I documents discussed. Full listings of published work are available by searching TIA site as indicated under TR-8 overview.

**Phase II Development and 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. As such, Phase II extensions build on the technology and features of Phase 1 and include Phase II requirements involving backward interoperability with Phase 1. In addition, Phase II activity involve 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. The additional elements and focus that are being considered as part of the Phase II P25 standard technology include:

- Additional air interface specifications to provide further narrow banding operation, at 6.25 kHz equivalent bandwidth operation
- Further work on the interface standards including system, Inter RF Subsystem Interface (ISSI), digital console and fixed station
- Other standardization efforts in progress address a variety of additional public safety user requests, including data and over the air programming.

The standards for the Console Interface and the Fixed Station Interface are progressing and will provide for full-functionality and a digital Interface to devices, including digitized voice, encryption, control and data services. At this time, users are able to interface consoles and fixed stations using analog interfaces similar to those currently used in analog systems.

The ISSI (Inter Subsystem Interface) includes the messaging, testing and evaluation of a series of proposed standards for connecting components between networks. The original ISSI overview document was published as a TIA TSB in 1996 and revised in December 2003 as part of Phase II. Work is currently progressing on the corresponding technical documents. This interface will provide standards for the connection of network elements from different manufacturer’s systems, and for proper security between systems. Even with the technical ISSI standards, there will still be a requirement for interagency agreements on issues such as authentication, access control, and user control of systems.

It can also be noted that Phase II is a vehicle for users to bring additional requirements to the standards process. Many elements are anticipated to be completed around the 2005-2006 time-frame. The Phase II extensions, with the exception of the ISSI, console, and fixed base interfaces, will have minimal impact on first responder
interoperability. Rather, they provide another alternative for spectrum efficiency and expanded competition in the marketplace. Phase II capabilities will facilitate improved communication at the P25-compliant network level and communication agencies will continue to require the functionality of Phase 1, with Phase II expanding the capability of P25. Finally, this implementation will provide users in dense-population areas additional standardized options to meet their long-term user needs within the limits of their existing spectrum allocations. Examples of published documents for Phase II are included in Annex 3.

Phase III Development:
Recognizing the need for high-speed data for public safety use, as expressed in the Public Safety Wireless Advisory Committee (PSWAC) final report, among others, the P25 Standards Committee established the P25/34 Committee to address Phase III implementation. Similar to the P25 approach, the standards committee established the P25/34 user forum to address data communications functions that are complimentary to P25 and other voice solutions. Phase III activities are addressing the operation and functionality of new terrestrial and aeronautical wireless digital wideband/broadband public safety radio standards and capabilities that could be used to transmit and receive voice, video, and high-speed data in a ubiquitous, wide-area, multiple-agency and vendor network. Additionally, the U.S. Department of Homeland Security–Project SAFECOM has published (2004) a SoR which impacts P25 and most other U.S. public safety voice communications standards.

Related National and International Standardization for Broadband

Beginnings of Project MESA
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 an 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 (Mobility for Emergency and Safety Applications). 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. The Project was given the name MESA at that time.

International participation and partnership is encouraged for those standards organizations, agencies, users and industries that may have an interest in next-generation broadband capabilities and service offerings involving a myriad of available and future technologies, services and platforms, as required by individual system operators and the environments (including available infrastructure) with which they and users must function. While MESA activities are aimed initially at public safety and emergency response services, more commercial-oriented applications are also envisioned and encouraged, as appropriate. Note that Project MESA is further described in another section of this document. Project MESA Website: http://www.projectmesa.org.

In the U.S., the FCC allocated 50 MHz of spectrum in the 4.9 GHz band for public safety broadband communications. TIA has since established a broadband data standards subcommittee, TR-8.8, which is developing standards for public safety communications in this band.

Broadband standards operate at different frequencies and bandwidths and provide a different set of optimized capabilities for ultra-high speed data transfer. Use of P25 standards in narrower bandwidths (12.5 kHz and narrower) is significantly more cost-effective for voice and short bursty data.

It is estimated that initial broadband standards will take about eighteen months to two years to complete. Ongoing contributions initiated through TIA to the future broadband standards process are expected to continue

6 URL: http://www.fcc.gov/Bureaus/Wireless/News_Releases/nrwl6043.txt
as technology, environment, and public safety needs evolve. Note that similar to the wideband standards, the broadband standards will complement existing P25 standards.

The National Public Safety Telecommunications Council (NPSTC) is also consolidating several industry user requirements and the resulting list is expected to be quite broad, allowing for initial prioritization of the critical uses of broadband for standards development activities, with ongoing phases of backward-compatible features and improvements.

**The Wideband Data Standards Project (TIA-902 Series)**

On June 1, 1999, the P25/34 committee released its Statement of Requirements for a wideband aeronautical and terrestrial mobile digital radio technology standard for the wireless transport of rate intensive information. As requested by NPSTC, standards definition begun in TIA, with the acceptance of NPSTC using the P25 process to create a series of wideband standards.

Recognizing the need for common Public Safety LMR standards that allow for higher data rates than previously available, TIA TR-8 has developed Digital Radio Wideband Data Standards, as indicated below. Both P25 and Wideband Data are open standards, intended for multiple vendor availability. The 902-series standards are currently being prepared for publications as American National Standards (ANS).

In the U.S., regulatory decisions and plans helped to spur development of LMR wideband standards, including the dedication, by the FCC, of spectrum in the 700 MHz frequency band for wideband data. The channels are at 50 kHz, and can be aggregated to 150 kHz, allowing users data rates as high as 700 kbps. The TIA-902 series of standards for this technology are mainly expected to handle data; however voice traffic is also supported. Interoperability at this point primarily involves the over the air interface. The FCC has mandated the use of both the P25 and wideband data standards for interoperability spectrum at 700 MHz.

Wideband 50 kHz-150 kHz standards for high speed public safety data communications (i.e., video, picture ID, and fingerprinting) have been completed and can enable system deployment. Currently, in the U.S., only spectrum in the 700 MHz band has been allocated to implement standard wideband systems, where incumbent broadcast TV stations currently inhibit use, so these systems cannot be deployed until the TV stations vacate from this band. This issue is currently in deliberation; including Congressional activity to expedite transition.

Wideband standards complement existing P25 standards (e.g., voice and low/medium data rates), operating at different frequencies and bandwidths and providing a different set of optimized capabilities for high speed data transfer. Use of P25 standards in narrower bandwidths (12.5 kHz and narrower) is significantly more cost-effective for voice and short bursty data.

Full listings of currently published documents are available by searching TIA Website indicated under TR-8 overview, using keywords “Wideband Data Standards Project.” Published work involves such topics as the Wideband Air Interface (WAI), Media Access Control/Radio Link Adaptation (MAC/RLA) Layer, Scalable Adaptive Modulation (SAM) Channel Coding, and Isotropic Orthogonal Transform Algorithm (IOTA) Radio Channel Coding (CHC). Additionally, see Annex 4 for examples from this project.

**Other TR-8 Work Activities and Documents**

For other work in TR-8 related to needs of first responders, see Annex 5.
2. TIA/ETSI Public Safety Partnership, Project MESA

BACKGROUND
The Public Safety Partnership Project (PSPP), known as Project MESA (Mobility for Emergency and Safety Applications), is the first international communications standardization partnership project whose aim is to develop joint specifications, based on continued user input, for advanced and future Public Safety/Emergency Response mobile broadband communications capabilities 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) and Telecommunication for Disaster Relief (TDR). 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 commonalities between U.S.-centered advanced public safety radio system Project 34 (TIA and APCO) and European-based Digital Advanced Wireless Service (ETSI 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 participation from all regions of the world and currently has participants and observers from North America, Europe (East and Western) and Asia (including Japan and Korea). Please refer to the www.projectmesa.org Website for further information.

Other organizations/agencies that actively support Project MESA include the U.S. Department of Homeland Security (DHS)-National Communications System and SAFECOM Program, the National Telecommunications and Information Administration (NTIA)/DoC, U.S. Department of Justice and the National Institute of Justice–CommTech Program, U.S. Federal Bureau of Investigation, Association of Public Safety Communications Officials (APCO), the Project 25-Project 34 Steering Committee (in coordination with ETSI TETRA-DAWS), agencies of the United Nations (UN), agencies of the North Atlantic Treaty Organization, the Federal Partnership for Interoperable Communications (FPIC), National Public Safety Telecommunications Council (NPSTC), Industry Canada, the Royal Canadian Mounted Police and the American Red Cross. Additionally, international meetings of Global Standards Collaboration recognize Project MESA in various Resolutions identifying Emergency Communications and Public Protection and Disaster Relief as a High Interest Subjects.

Project MESA’s user group will continue, as needed, to update the user-defined Statement of Requirements (SoR), [Publicly available at: http://www.projectmesa.org/ftp/Specifications/], 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. Additionally, MESA may or may not cover a user’s entire geographical area of responsibility since its function, depending on the scenario, could be to provide localized or “hot spot” services or to support an underlying and very important level of broadband system services, even when a specific emergency is not currently underway. Based on the SoR, the MESA Technical Specification Group System (TSG SYS) is now actively working on the corresponding technical specifications, which will be submitted to the supporting Standards Development Organizations (i.e., TIA, ETSI, etc.) for SDO transposition and publication.

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

<table>
<thead>
<tr>
<th><strong>System End-Users</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• In-building, portable voice and data coverage.</td>
</tr>
<tr>
<td>• Real-time support for wireless portable computer applications.</td>
</tr>
<tr>
<td>• Rapid messaging, including email, free-form text, and file transfers.</td>
</tr>
<tr>
<td>• Constantly updated personnel and equipment location data.</td>
</tr>
<tr>
<td>• Aerial video for major events, or disaster response coordination.</td>
</tr>
<tr>
<td>• Transmission and reception of high-resolution digital images.</td>
</tr>
<tr>
<td>• Satellite connectivity of disaster “hot-spots.”</td>
</tr>
<tr>
<td>• Real-time incident video and Internet protocol (IP) voice communications overlay.</td>
</tr>
<tr>
<td>• Full robotics remote control, including audio/video monitoring and transmission.</td>
</tr>
<tr>
<td>• Remote sensing and aeronautical connectivity (Air-Ground-Air).</td>
</tr>
<tr>
<td>• Economies of scale for Public Safety/Emergency Response equipment acquisition; also allowing for increased Public Safety/Emergency Response Department access to technology and information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>System Owner/Operators</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Local, national, regional and international interoperability.</td>
</tr>
<tr>
<td>• Frequency neutral technology.</td>
</tr>
<tr>
<td>• Accommodation of multiple agency networks.</td>
</tr>
<tr>
<td>• Network authentication and encryption.</td>
</tr>
<tr>
<td>• Competition in system life cycle procurement.</td>
</tr>
</tbody>
</table>

Annex 6, contains additional material related to Project MESA, including User requirements and technical elements. The Annex 7, contains additional material related to Project MESA security aspects.

### 3. Work Activities of TIA TR-30 Engineering Committee, Multi-Media Access, Related Protocols and Interfaces

This Engineering Subcommittee is responsible for Data Circuit Terminating Equipment (DCE) and the interfaces between DCEs and Data Terminal Equipment (DTE), together with the transmission media to which they are connected (e.g., the Public Switched Telephone Network). Standards include functional, electrical, and mechanical characteristics; involving such devices as modems, standard and IP facsimile and textphones. Much of this engineering committee’s activities also involve developing contributions for input to ITU-T Study SG 16, Multimedia Services, Systems and Terminals.

Related to this compendium, activities presently being explored involve such topics as Internet/IP facsimile security and emergency accessibility service capabilities for textphones over IP and PSTN networks, involving national and international standards activity. The work done in this committee has emergency telecommunications service implications and aspects, including Enhanced Priority Treatment, Network Security, International Connectivity and Quality of Service.

**TR-30.1, Modems and Facsimile Terminal Equipment and Systems**

This subcommittee develops domestic standards relating to modems, including modem control, maintenance, error control, and line signals and facsimile terminal equipment and systems. Another main function is the development of technical contributions relating to modems and textphones (i.e., TTY, TDD) for presentation in international standards I such as the ITU-T (Study Group 16). For example, TIA TR-30.1 is working with and providing input to ITU-T Study Group 16, Question 11 on an ITU-T Recommendation for Text over IP (ToIP). This may involve Text Telephony Telecommunications Device for the Deaf [TDD] and teletypewriter [TTY]) over VoIP networks.
Facsimile, as referred to here, includes any system that transmits (and receives) still rasterized images, including bi-level, continuous tone and color images. Related to this compendium, activities presently being explored involve such topics as Internet/IP facsimile security and related emergency service capabilities. Standards include functional, electrical, and mechanical characteristics and communication protocols that involve point-to-point and multipoint facsimile and audiographic services. Additionally, TIA TR-30.1 is working to develop technical contributions to enhance ITU-T Recommendation T.38, “Procedures for Real-Time Group 3 Facsimile Communication over IP Networks,” involving enhanced capabilities for Facsimile over IP (involves emergency telecommunications service aspects and implications).

- **PN-3-0098 (to be published as TIA-1001), “Transport of TIA-825-A over IP Networks”** (In TIA ballot): This project is developing a standard for a gateway to provide reliable transport of textphones over IP networks. Consideration is also being given to emergency telecommunications service and capabilities.
- **ANSI/TIA-825-A-2003, “A Frequency Shift Keyed Modem for Use on the Public Switched Telephone Network.”** This (data interchange equipment) document specifies a FSK modem which operates at nominal data signaling rates of 50 or 45.45 symbols per second over the switched telephone network.

### 4. Work Activities of TIA TR-34 Engineering Committee, Satellite Equipment and Systems

TIA TR-34 Engineering Committee is an established, open forum for satellite technology development. This TIA Engineering Committee recently reviewed the issue of Lawfully Authorized Electronic Surveillance (LAES) in support of Communications Assistance for Law Enforcement Act (CALEA) for satellite systems and concluded that TR-34 could be an avenue (coordination, new work initiation) for applicable security and emergency service/accessibility related communications standards activity, if deemed by membership to be appropriate in the future. Additionally, TR-34 recently completed its work on the development of a new Internet Protocol over Satellite (IPoS) standard known as TIA-1008, “IP Over Satellite (IPoS).” The TIA-1008 specification provides an alternative baseline specification for the provision of an interaction channel for GEO satellite interactive networks with fixed return channel satellite terminals (RCST). This solution may enhance public safety capabilities and access means.

### 5. 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. This Engineering Committee contributes input to ITU-T SG 12, as appropriate, in matters related to transmission performance and quality of service. Additionally, TIA TR-41 developed documents are applicable to emergency telecommunications service requirements.

Standards formulated by this committee 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, network security, QoS and applicable accounting and billing aspects. Recent security issues that are being worked in the TR-41 committee include IP Telephony, as an emerging technology involving the amalgamation 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, and “softphones”), passive and active attacks on the signaling stream.
(including eavesdropping) and other issues that are of importance. Infrastructure assurance, network security and enhanced emergency telecommunications service are aspects addressed within this committee’s work.

Annex 7 is a list of current TR-41 activities related to this compendium.

6. 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 activities and documents of TR-42 can be applicable to physical infrastructure issues associated with assurance, security and emergency telecommunications availability. In particular, the ANSI/TIA/EIA-569-A and 758 standards provide some guidance for alternate routing of cabling into a building to help prevent loss of communications. Annex 8 contains a current snapshot of related TR-42 work.

7. 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.

TIA 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. Authentication, Signaling Message Encryption and 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®), and 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.

The engineering committee has also developed standards for Wireless Priority Service (WPS) for CDMA Systems, in parallel with WPS Industry Requirements work. 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 multiple levels of priority (assigned by DHS 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.

Emergency calling service, location identification, lawful interception and surveillance capabilities and are also developed within this engineering committee. Activities include Joint Standards Development Work with Committee T1 (now ATIS) to address legislated and mandated services, including emergency services (e.g., E9-

---

7 cdma2000® is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2 (Note that TIA is an OP of 3GPP2). When applied to goods and services, the cdma2000® mark certifies their compliance with cdma2000® standards. Geographically (and as of the date of publication), cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States.
1-1 location) and CALEA. Note that recently published European emergency call handling requirements (e.g., ETSI SR 002 180) have been made available to TIA TR-45 and are being taken into consideration within the course of its work (i.e., coordination of E9-1-1/E1-1-2 aspects). TIA TR-45 coordination is also being proposed with TIA TR-41.4 and others regarding E1-1-2 requirements for cdma2000® systems operating in impacted areas. In a related note, currently there are no 3GPP2 documents related to Emergency Services as the project considered such aspects regional. For the North American region, emergency service standards are being developed within TIA TR-45 Committee and referenced in 3GPP2 documentation.

An emerging and important area to address will be emergency services for packet data. 3GPP2 (TSG-X) recently decided this work should not be done in 3GPP2. Likely work may be addressed in TR-45.2, Emergency Services Ad-Hoc Group, and may involve potential coordination with TIA TR-45.6 activities responsible for packet data network support. Also note that work to support IP-based location services is a project in 3GPP2 and such work may also impact Emergency Services for packet data networks (and vice versa). The impacts to TR-45.2 Emergency Services existing specifications and future TR-45.2 IP-Based Emergency Services work projects have not been addressed at this time.

The cdma2000® standardized 3G solution currently operates in 450 MHz, 800 MHz, 1.9 GHz and 2.1 GHz bands and can also serve the feature-rich needs of national security, emergency services and the public safety communications community through spectrum (i.e., leverage spectral proximity) and system flexibility, proven deployment, wide broadband coverage (i.e., EV-DO, EV-DV), COTS procurement and potentially low build-out costs, as appropriate. Cdma2000® provides secure network functionality with multimedia services to meet each agency’s needs while providing interoperability with systems employing IP and PSTN interfaces. The cdma2000® based system could involve public (i.e., NS/EP service on commercial system), private, dedicated, shared or leased ownership/operational arrangements as appropriate or required. Public Safety utilization in lower frequency bands is of particularly growing interest due to inherent security, improved propagation characteristics and signal penetration in buildings, among others.

Annex 9 contains a listing of related work and projects for TR-45.

8. Global Standards Collaboration (GSC) [Including the Global Radio Standardization Collaboration (GRSC) and the Global Telecommunications Standardization Collaboration (GTSC)]8

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 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, network security issues, emergency services between citizens and government and broadband mobile communication for public safety and emergency service (i.e., PPDR/TDR) professionals. For more information on the last GSC-9 meetings, see the TIA Press Release at: http://www.tiaonline.org/media/press_releases/index.cfm?parelease=04-78 or visit the official GSC-9 Website at: http://www.tta.or.kr/gsc/index.jsp. High Interest Subjects and related Resolutions adopted involve emergency communications and security, including:

- Emergency Communications Resolution GSC-9/2
- Next Generation Networks Resolution GSC-9/3
- Cybersecurity Resolution GSC-9/4
- Public Protection and Disaster Relief (PPDR) Resolution GSC-9/9

8 Previously Global Standards Collaboration (GSC) and RAdio STandardization (RAST).
### Annex 1: P25 Service Availability Matrix

<table>
<thead>
<tr>
<th>SERVICE</th>
<th>CONVENTIONAL</th>
<th>TRUNKED</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Telecommunications Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Bearer Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Circuit-switched unreliable/reliable data</td>
<td>Standard Option</td>
<td>Standard Option</td>
</tr>
<tr>
<td>Packet-switched confirmed delivery data</td>
<td>Standard Option</td>
<td>Standard Option</td>
</tr>
<tr>
<td><strong>Teleservices</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast voice call</td>
<td>Not applicable</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Unaddressed voice call</td>
<td>Mandatory</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Group and individual voice call</td>
<td>Standard Option</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Circuit-switched data network access</td>
<td>Standard Option</td>
<td>Standard Option</td>
</tr>
<tr>
<td>Packet-switched data network access</td>
<td>Standard Option</td>
<td>Standard Option</td>
</tr>
<tr>
<td>Preprogrammed data messaging</td>
<td>Standard Option</td>
<td>Standard Option</td>
</tr>
<tr>
<td><strong>Supplementary Service</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>Standard Option</td>
<td>Standard Option</td>
</tr>
<tr>
<td>Priority call and Preemptive priority call</td>
<td>Not applicable</td>
<td>Standard Option</td>
</tr>
<tr>
<td>Call interrupt</td>
<td>Standard Option</td>
<td>Standard Option</td>
</tr>
<tr>
<td>Voice telephone interconnect</td>
<td>Standard Option</td>
<td>Standard Option</td>
</tr>
<tr>
<td>Discreet listening</td>
<td>Standard Option</td>
<td>Standard Option</td>
</tr>
<tr>
<td>Silent emergency</td>
<td>Standard Option</td>
<td>Standard Option</td>
</tr>
<tr>
<td>Radio unit monitoring</td>
<td>Standard Option</td>
<td>Standard Option</td>
</tr>
<tr>
<td>Talking party identification and Call alerting</td>
<td>Standard Option</td>
<td>Standard Option</td>
</tr>
<tr>
<td><strong>Subscriber Unit Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrasystem and Intersystem roaming</td>
<td>Standard Option</td>
<td>Standard Option</td>
</tr>
<tr>
<td>Call restriction</td>
<td>Not applicable</td>
<td>Standard Option</td>
</tr>
<tr>
<td>Affiliation</td>
<td>Not applicable</td>
<td>Standard Option</td>
</tr>
<tr>
<td>Call routing</td>
<td>Not applicable</td>
<td>Standard Option</td>
</tr>
<tr>
<td>Encryption update</td>
<td>Standard Option</td>
<td>Standard Option</td>
</tr>
<tr>
<td><strong>Network Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registration</td>
<td>Standard Option</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Roaming</td>
<td>Mandatory</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Authentication and Subscriber terminal disable and enable</td>
<td>Standard Option</td>
<td>Standard Option</td>
</tr>
<tr>
<td>Network Management and administration services</td>
<td>Standard Option</td>
<td>Standard Option</td>
</tr>
</tbody>
</table>
Annex 2 TR-8 P25 Phase I

System and Standards Definition Documents:

- **TIA/EIA/TSB-102-A (1995), “APCO Project 25 – 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.

- **ANSI/TIA/EIA-102.AAAD (2002), “Project 25 – 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 where 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:
Examples of documents that involve features a P25 Phase I compliant system might have:

- **ANSI/TIA/EIA-102.AAAA-A (2001), “Project 25 – 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 a P25 standard system, especially, through the Common Air Interface (CAI) of such a system.

- **ANSI/TIA-102.AAAB-2002, “APCO Project 25 – Security Services Overview – New Technology Standards Project – Digital Radio Technical Standards.”** This 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. Update in 2005.

- **TIA-102.AAAB-A, “Project 25 - Digital Land Mobile Radio - Security Services Overview(R2005)”** This document provides an overview of the security services available in Land Mobile Radio systems. It provides the context in which to understand why security services are required and gives a general high level description of how they are provided.

(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.CABA (2002), “APCO Project 25 – Interoperability Test Procedures – Conventional Voice Equipment.”** The purpose of this 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.

- **TIA-102.CABB (2003), “Project 25 – Interoperability Test Procedures – Over-the-Air Rekeying (OTAR)” (Published August 2003):** This recently published document defines procedures for testing the interoperability of data, specifically, OTAR commands between RF subsystems and mobile radio subscribers of different manufacturers and models (including firmware).

### 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: Common Air Interface (CAI), vocoder, Inter-RF Subsystem Interface (ISSI), telephone interconnect, data, and network management interface. Examples include:


- **ANSI/TIA/EIA-102.BADA-2000, “Telephone Interconnect Requirements and Definitions (Voice Service).”** This ANS defines telephone voice interconnect requirements for LMR systems (applicable to P25 and other systems). Specifically, involving the interface between a RF subsystem and a public or private switched telephone network. 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, “APCO Project 25 Data Overview – New Technology Standards Project.”** 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-102.BAEA-1-2002, “Project 25 – 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.

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).


---

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


- **ANSI/TIA-102.CAAB-A-2002, “Digital C4FM/CQPSK Transceiver Performance Recommendations.”** 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 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).

- **TIA/TSB-102.CAAC-2002, “Project 25 – Mobile Radio Push-to-Talk and Audio Interface Definitions and Methods of Measurement.”** This document defines a physical and electrical interface to P25 mobile radios. The purpose of the interface is to allow standardized interfacing of external devices that require one or more of the functions of push-to-talk, qualified audio presence, transmit audio and receive audio. The TSB also provides definition and methods of measurement for the transmit audio, receive audio and push-to-talk interfaces for radio equipment used in the private (dispatch) land mobile services.
Annex 3 TR-8 P25 Phase II

- **TIA/EIA/TSB-102.BAAB-A (1995), “APCO Project 25 Common Air Interface Conformance Test.”** This document lists a series of conformance tests for the Common Air Interface that are intended to assure the equipment actually conforms to the formats specified in the CAI. The object of the conformance tests is to assure the equipment may be interoperable with other equipment conforming to the standard. These tests are different and distinct from other performance tests in document reference, which measure the actual limits of equipment performance. The performance and conformance test are mutually complementary. These tests are also different and distinct from lock down tests, which are intended to demonstrate interoperability between different radios. These conformance tests are intended to precede lock down tests.


- **ANSI/TIA/EIA-102.BAAA-A-2003, “APCO Project 25 FDMA Common Air Interface – New Technology Standards Project – Digital Radio Technical Standards.”** 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. The document describes all of the parts of a system for public safety land mobile radio 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 and the CAI allows these radios to send/receive digital data over a radio channel.

- **ANSI/TIA/EIA-102.BAAA-1-99 (Superseded by 102.BAAA-A) “P25 FDMA CAI – Addendum 1.”** This document updates the information contained in TIA/EIA-102.BAAA for P25, Phase 2.

- **ANSI/TIA-102.CAAA-A-2002, “Digital C4FM/CQPSK Transceiver Measurement Methods.”** 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-3-0073 (to be published as TIA-905.BAAC), “Two-Slot TDMA Common Air Interface, Media Access Control (MAC) Layer”** (Publication expected): This document will define the MAC layer specifications for Phase 2 TDMA systems.

- **PN-3-0074 (to be published as TIA-905.BAAD), “Two-Slot TDMA Common Air Interface, Logic Link Control (LLC) Layer”** (Publication expected): This document will define the LLC layer specifications for Phase 2 TDMA systems.

- Other documents for TDMA systems are in the stages of drafting.
Annex 4, TR-8 Wideband Data Project


- TSB-902.AAAA, “Wideband Data System Security Services - Overview Public Safety Wideband Data Standards Project” This document will provide an overview of the security services available in wideband data radio 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.

- Other technical documents include the Wideband Air Interface, Media Access Control/Radio Link Adaptation (MAC/RLA) Layer, Wideband Data Equipment, Radio Communications Performance, WAI Packet Data Specification, WAI Mobility Management, Radio Channel Coding and Scalable Adaptive Modulations.

- A searchable listing of published TIA 902-Series documents can be viewed and ordered by pointing your browser to: [http://www.tiaonline.org/standards/search_n_order.cfm](http://www.tiaonline.org/standards/search_n_order.cfm) and search with keyword “902”
OTHER TR-8 WORK ACTIVITIES AND DOCUMENTS

- **TIA/EIA/TSB-69 (1998), “A System and Standards Definition for a Digital Land Mobile Radio 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 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 EDACSI, 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-69.3 (1998), “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-329-C (2003), “Minimum Standards for Communications Antennas, 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 (Superseded by TIA-329-C), “Minimum Standards for Communication Antennas, Part II: Vehicular Antenna.” This document supplements TIA-329-B by covering vehicular antennas to the 30-1000 MHz frequency range.

Annex 6, Project MESA

MESA Statement of Requirements (SoR) Document

- The latest Statement of Requirements document and more information can be viewed at http://www.projectmesa.org/SoR.htm.

The initial Project MESA SoR document was approved by the Project MESA Steering Committee in 2002 and represents the first trans-Atlantic consolidated view expressed directly by the professional users of advanced wireless data communications equipment and systems. The SoR was developed as part of a global effort to identify and develop uniform capabilities, scenarios, specifications, and eventually a suite of open technical standards that can be used for the elaboration of next-generation wireless broadband data communications equipment and systems. These voluntary standards will be used to achieve the objectives of the MESA user communities. Project MESA’s activities support the efforts of the member organizations from many countries in meeting their own PS/PP and public service wireless data telecommunications requirements.

The Project MESA SoR reflects the vision of a mobile broadband network (shared and/or ad hoc) that can be simultaneously accessed by multiple users, using various applications and levels of security, in a specified geographical area, and that may operate potentially independently from the availability of public networks and the supply of commercial electrical power. Specifically, the SoR describes the services and applications (involving air interface data rates up to 2 megabits per second [Mb/s] or greater) that a future advanced wireless telecommunications system should be able to support, in order to realize the most effective operational environment for the users. Emphasis has been placed on those applications and technological platforms that current technology has not yet satisfactorily addressed, but which have been identified by the users and their agencies as key requirements for applications and services.

Consistent with the MESA users’ missions, it is also expected that the Project MESA SoR and the resulting technical specifications will:

- Emphasize transparent and seamless wide-area network applications
- Include multiple levels of security and data encryption schemes
- Offer robust operational management and control systems capabilities
- Reflect the requirements of MESA users to have priority operational services and priority system restoration
- Provide an extremely reliable service model and ubiquitous coverage within a user’s defined service area.

Additionally, the MESA SoR is intended to describe a functional and open standards-based platform that can be installed as either a private system owned by the government or a governmental–commercial partnership that provides authorized service to MESA user agencies and possibly secondary service to other commercial clients. The Project MESA specifications are not intended to specifically identify particular frequency spectrum for use, thereby allowing standardized technology to be used in any authorized and available spectrum consistent with the required channel bandwidth.

Within the SoR document, a general outline of the MESA user community’s technological needs for the transport and distribution of rate-intensive data, digital video, infrared video, and digital voice for both service-specific and general applications is categorized into six distinct sections:

- Technology needs of each type of MESA user discipline
- General technology requirements
- General, functional, and operational requirements
- Technology and applications
- Use of technologies
- Compatibility requirements for the various applications.
Each section details requirements used in different national and international PS/PP programs. Additionally, four annexes are incorporated into the SoR document, providing additional informational materials to further the reader’s understanding of the requirements and how the resulting technology might be applied in “real-world” applications. The annexes include national and international PS/PP programs; standards, specifications, and requirements; known North American federal, state, and county requirements; and two law enforcement scenarios—a courthouse murder and a state and urban police response to an earthquake event.

The SoR document is not written specifically to be studied end-to-end; rather it represents a unique source of information with the aim of providing an understanding of the unique and often very difficult and dangerous working environments that the MESA user community is facing, that industry can use in providing the most innovative, effective, and accurate technical solutions to meet this unique operational environment. It also represents the establishment of the clear understanding that the advanced needs of this user community should be based on a highly mobile, interoperable, broadband wireless network that allows the provision of dynamic bandwidth, self-healing characteristics and secure network access.

Within Project MESA, the SoR document will be updated at regular intervals and represents the focal source of information for Project MESA’s industry members in their work toward the realization of next-generation, globally applicable communications capabilities, specifications, and the future standards that evolve from them.

Based on the SoR, the MESA Technical Specification Group is now mapping existing capabilities and gaps, progressing toward the development of corresponding technical specifications. A “System of Systems” approach is being utilized, leveraging current and evolving communications technology and user requirements. MESA output will be transposed by supporting standards development organizations (i.e., TIA, ETSI, etc.) for regional development and publication. Other technical organizations and entities are encouraged to consider MESA activities and approved specifications, as well as resulting standards that are published.

**SoR Abstract of MESA User Community’s Technological Needs**

*General Mission Statements and Technology Needs of Each Type of MESA User Discipline*

This section of the Project MESA SoR describes the overall requirements of most MESA user agencies in Europe and North America. The Project MESA specifications and requirements created from the document should include, but are not limited to, the following security and PS/PP providers, services, and functions provided throughout the world. Project MESA participants have indicated the need for the providers, services, and functions stated below because the type of wireless communications support is crucial to ensure quality services can be provided to the constituents they serve. The following providers, services, and functions are included, along with their “Mission Statements” relative to the Project MESA SoR:

- **Criminal Justice Providers**—Project MESA should provide the technology and applications platforms necessary to support new telecommunications and automation tools that are aimed at reducing crime and its impact on the health, welfare, and safety of the citizenry.

- **Emergency Management or Disaster Response/Recovery Agencies**—Communications system requirements for emergency management and disaster services are characterized by a very low usage pattern during routine operations and extremely high usage patterns during major disasters or events. Special operations needs include response functions to an event requiring specialized training for safe and effective operations, consisting of hazardous materials leak and/or spill remediation, mountain rescue and associated technical rescue, collapse search and rescue, swift water rescue, blue water rescue, trench and confined space rescue, and heavy rescue.

- **Health Services**—This service encompasses the missions of two areas, including emergency medical services (EMS) and disaster medicine. Doctors, paramedics, medical technicians, nurses, or volunteers can supply health services, including critical invasive and supportive care of sick and injured citizens and the ability to transfer the people in a safe and controlled environment.

- **Fire Services**—With variations from region to region and country to country, the primary areas of responsibility of the fire services include structural fire fighting and wild land fire fighting, fire safety and prevention, life saving through search and rescue, rendering of humanitarian services, management of hazardous materials and protection of the environment, salvage and damage control, safety management, and mass decontamination.
• Coast Guard Services (and related PS/PP functions)—These services include search and rescue (at sea and other waterways), protection of coastal waters, criminal interdiction, illegal immigration, and disaster and humanitarian assistance in areas of operation.

• Airport Security Services (and related PS/PP functions)—Airport security should include the capability to communicate by secure radio or wireless data services with “Airport Management” and “Control Tower” operations. Airport operations must be able to effectively communicate with various PS/PP organizations for routine and disaster incident communications.

• Hazardous Materials (HAZMAT) (and related PS/PP functions)—HAZMAT incidents can be complex and may involve resources of many different PS/PP organizations, including coordination and management, analysis and material classification, handling, and cleanup and rectification.

• Correctional Institutions—The Project MESA SoR should include specifications and proposed standards to ensure the enhanced long-term wireless communications needs of prisons, jails, and other correctional institutions.

• Correctional Enforcement and Probation Officers—Project MESA specifications and standards will provide correctional and parole officers a full range of high-speed, high-data-rate wireless public safety/public protection services and applications to effectively support their mission.

• Special Event Planning Groups—The Project MESA SoR outlines some of the more urgently needed mobile data communications tools that will help PS/PP agencies be prepared and effectively coordinate response with efficient communications tools to predictable large-scale events simultaneously at various locations.

• General Governmental and/or Government Administration—The technological requirements included in the Project MESA SoR will greatly assist general government services providers in their efforts to offer effective and innovative water, sewage, electrical, public parks, schools, pest abatement and control, building code enforcement, planning and zoning and enforcement, and public health services.

• Land and Natural Resource Management—Governmental agencies at all levels are responsible for the oversight of a nation’s environmental, land, forestry and conservation, and agricultural development. These entities fall into this unique but broad-based PS/PP category. The specifications and standards should define technology capable of operating in these sometimes extremely harsh conditions.

• Transportation’s Organizational Mandates and Missions—Organizations at all levels of government are responsible for the planning, construction, management, and maintenance of many forms of transportation systems. To meet this requirement, these agencies must be able to effectively communicate and respond to events such as snowstorms, mudslides, flooding, earthquakes, and hazardous material spills that impact the world’s transportation infrastructures.

• Intelligent Transportation Systems (ITS)—Many PS/PP transportation organizations interact with what is commonly designated as an ITS, which provide a plethora of information about transportation systems, corridors, and transport vehicles traversing these arteries. The services and applications defined in the Project MESA SoR are intended to enhance, not replace, the existing wireline, fiber-optic, or microwave infrastructures used to provide the traveling public with an ITS.

**Introduction and General Technology—Requirements**

The objective of the Project MESA SoR is to establish a suite of specifications and proposed technical standards that are created from the user’s perspective. Some of the primary capabilities of a Project MESA network may include, but are not limited to, the following:

<table>
<thead>
<tr>
<th>Improvements in spectrum efficiencies</th>
<th>Compatible for multiple international standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorporation of frequency neutrality and/or agility</td>
<td>Two-way communication</td>
</tr>
<tr>
<td>Life-cycle procurements</td>
<td>Multiple levels of security</td>
</tr>
<tr>
<td>Security requirements</td>
<td>Multiple levels of availability of service</td>
</tr>
<tr>
<td>Economical and ergonomically friendly design</td>
<td>End-to-end network integrity</td>
</tr>
<tr>
<td>Digital migration in place</td>
<td>High-speed, error-free service</td>
</tr>
<tr>
<td>Consistent with existing standards.</td>
<td>System and network access</td>
</tr>
<tr>
<td></td>
<td>Compliant with the needs of the participating Nations.</td>
</tr>
</tbody>
</table>
General, Functional, and Operational

The Project MESA specifications and technical standards developed in response to the SoR are intended to provide the baseline technology requirements to allow for the identification and development of universal specifications and standards. The specifications and standards will be regionally transposed to accommodate the implementation of local, wide-area, national, and international high-speed PS/PP data networks. The following issues related to requirements are presented and discussed to further the definition of the requirement and the compilation of the technical specifications:

- Requirements of the Project MESA SoR
- Interface requirements
- Transparent interfaces
- End-to-end transmit time
- Interface protocol requirements
- Dynamic partitioning
- High-speed simultaneous network or system access
- Network pre-emption
- First-in, first-out (FIFO)
- Transparent transfer
- Over-the-air-rekeying (OTAR)
- Automated information requirements
- Blocking of unauthorized access.

- MESA network component identification
- Optional site-by-site implementation and management
- Dynamic remote partitioning
- System and/or network transaction audit trail
- Ability to provide statistical reports
- Agency-by-agency and site-by-site reports
- Dynamic transfer rates and bandwidth allocation
- Degradation and redundancy
- Duty cycle requirements
- Pre-testing technology proposals
- Compliance with national and international rules, regulations, and standards
- High-speed access to national databases.

Technology and Applications

The Project MESA specifications and technical standards are being designed to accommodate, but not be limited to, the transfer of information from multiple digital applications, the use of existing protocols and platforms, in-building and portable service, regional and national interoperability, and interoperability between Project MESA user devices applications and Project MESA compliant systems. Some of the primary attributes of a Project MESA network(s) include, but are not limited to, the following:

- Use of standardized technology
- Use of open architectures
- Migration
- Service platform
- Priority services
- Traffic (data) distribution
- Network and data base interconnectivity
- Dynamic network optimization
- Frequency neutral technology
- Adequate interference protection
- Regulatory compliance
- Environmental safety
- Compliance with Project MESA SoR
- Open interfaces
- Related documents, standards, policies or requirements
- Network transmission requirements
- Location determination
- Delayed transmission and remote stops
- Dynamic updating of data fields.

The Use of Technologies and the Compatibility Requirements for the Various Applications

Project MESA’s analysis and development efforts should elicit specifications and proposed standards that comply with the SoR’s basic requirement for immediate, error-free transfer and display of all forms and types of data. These would include, and not be limited to, text, voice, video, infrared video, photographs, and detailed graphical information. Examples of the data and information that may be supported include maps, engineering plans or drawings, fingerprints, text and graphical files, reports, and all other data, information, or representations developed by applications as may otherwise be specified in the present document. The operational needs to address these issues are incorporated in the Project MESA SoR, providing the user’s perspective of the types of applications, services, and technologies that are expected to be needed to continue improvement of both the performance and safety of PS/PP agencies. Some of the systems, applications, and information and data elements to be considered for inclusion are:
To be transported
- Electronic messaging
- Encryption
- Transparent network and system access
- Access, switching and rebroadcast of ITS and other real time video sources to field resources
- Transmission of complex files
- System integration and interoperability
- Transmission of user and patient monitoring telemeter
- Transmission of geographical location data
- Transmission of full-motion video, still photographs, and images.

Informational Material in Annexes A, B, C, and D
The four current annexes serve as informational material to illustrate and educate interested parties with regard to Project MESA capabilities, including scenarios, illustrations of potential benefit to users and citizens alike, other information and regional efforts. As this is a “living document,” these scenarios, and future ones, will continue to be updated.

- **Annex A** describes national and international public service and public safety programs, and existing potentially applicable standards, specifications, and requirements. Topics of discussion include, but are not limited to, the implementation of interoperable technologies, the impact of the U.S. Government’s Public Safety Wireless Advisory Committee’s (PSWAC) general requirements on Project MESA, the impact of recent major events on the Project MESA SoR, the administrative control of transportation and other related public safety telemetry, the use of global location system in Project MESA, EMS video applications, and search and rescue applications of robotics.

- **Annex B** describes known North American federal, state, and country requirements. The informative material includes, but is not limited to, the Federal Bureau of Investigation’s (FBI) National Crime Information Center (NCIC) 2000 System Requirements, the FBI’s Technology Planning Guide, and the Federal Manual on Approaches to Implementing an Incident-Based Reporting System (Volume 3).

- **Annex C** details a possible law enforcement scenario, i.e., a courthouse murder, in which Project MESA requirements can be used to effectively and efficiently control the incident using Project MESA standards, specifications, and requirements set forth in the SoR.

- **Annex D** details a second possible law enforcement scenario involving a state and urban police response to earthquake damage, in which Project MESA SoR requirements can be used to effectively and efficiently control the incident using Project MESA standards, specifications, and requirements set forth in the SoR.

MESA Technical Specification Group – Systems (TSG SYS)
The MESA technical specifications, based on operational requirements documented in the MESA SoR, are being developed by the TSG SYS members. An important aspect of Project MESA is that it is being defined as a “system of systems” that makes use of the existing infrastructure where available. The technical specification documents will define an open-systems architecture for interoperability that will use existing communications technologies, where appropriate, as building blocks. **Figures 1 and 2** depict the way that existing (gray) and emerging (yellow) technologies might satisfy MESA technical requirements.
Conversely, as technical gaps are identified, requirements for new communications capabilities will be specified, as depicted by the blue ellipses in Figure 3.
Figure 3. New MESA Technical Requirements

Once identified, Project MESA will work with the appropriate technical specification development forums to get MESA technical requirements incorporated into their work (Figure 4).

Figure 4. Project MESA as Technology Broker

A key part of the development process is to identify high-level technical requirements that are common to a variety of SoR-defined operational scenarios. Accomplishing this will support the development of a common communications architecture that satisfies a wide range of user-defined operational requirements. The first step in this process has been to categorize SoR scenarios (e.g. fire, chemical spill, etc) into “scenario classes” which are defined by the coverage area, the operational environment, and the type of PPDR situation (Figure 5). Results from this categorization effort are being further analyzed to identify common characteristics.
Figure 5. Project MESA Scenario Classes

Project MESA participants have made the commitment to complete an initial MESA technical specification by the fall of 2004. Figure 6 depicts the intermediate steps that are being taken to achieve this milestone.

Figure 6. Technical Specification Development Plan
The following paragraphs discuss the individual tasks in the specification development plan:

**Filtered Scenarios:** The purpose of this task is to further consolidate the twelve Project MESA scenario classes into groups of classes having similar communications requirements.

**Deployment Strategies:** The purpose of this task is to identify modular approaches to deploying PPDR communications in Project MESA. For example, a key challenge of the Project MESA TSG SYS will be to determine ways of minimizing spectral use. As a result, this task will consider strategies for dealing with increased spectral requirements as PPDR users transition from day-to-day to emergency situations.

**Traffic/Service Profiling:** The purpose of this task is to identify the traffic (e.g. number of circuits, data rates) and service profiles (e.g. types of data) for the PPDR scenarios. Information resulting from this task will be used to support the development of filtered scenarios.

**System Reference Model Architectures:** The purpose of this task is to evaluate the filtered scenarios and develop system reference model architectures.

**Reference Technologies (ongoing):** The purpose of this task is to consolidate information on the characteristics of technologies that might possibly be used to satisfy Project MESA requirements. Information is currently consolidated in two documents that are updated as “living documents” and are available on the Project MESA website: Wireless LANs and Other Technologies. A third document describing Project MESA open technical issues is also supported under this task. These three documents, while provided for use by TGS SYS members as technical references, are not intended to validate any particular technology for Project MESA.

**Derived System Requirements:** The purpose of this task is to define the Project MESA system technical requirements. This task will produce the *de facto* Project MESA draft system specification.

**Technology Roadmap:** The purpose of this task is to identify technologies that can be used to satisfy Project MESA technical requirements and, where technologies are unavailable, recommend specific areas for technical research or technical development.
Annex 7, MESA 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, commercial 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 intended to carry high-speed, digital wireless services, which will support and/or supplement other public and private fixed stations, fiber, and hardwire services in place today that may provide advanced capabilities to users.

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.

Security and Encryption-related Excerpts from the MESA Statement of Requirements (SoR):

**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

---

*Note: The above text is an excerpt from the Annex 7 of the MESA Security Aspects document and is intended to provide a comprehensive overview of the security aspects covered in the MESA Statement of Requirements (SoR).*
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.
Annex 8, TR- 41 Activities

TR-41.1, Multiline Terminal Systems
This subcommittee has published the following documents that specifically address emergency telecommunications issues:

  This document defines requirements for Private Branch Exchange (PBX) systems and PBX switching equipment. Additionally, this standard addresses enhanced or 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-689-A-2003, “Telecommunications – Multiline Terminal Equipment – PBX and KTS Support of Enhanced 9-1-1 Emergency Calling Service.”** The revision of TIA/EIA-689 is a companion to ANSI/TIA/EIA-464-C-2002, the standard for private branch exchange (PBX) equipment. It contains requirements and recommendations for Emergency telecommunications support of enhanced 9-1-1 emergency calling service for PBX and key telephone systems, specifically dialing, routing, network interface technical specifications and local notification. The standard may be used in the design of multiline telecommunication systems (MLTS) that are installed in many businesses, hotels or campus environments. TIA-689-A, when used in conjunction with referenced documents, will provide guidance to manufacturers to build multiline equipment that helps emergency responders to determine the location of 9-1-1 calls placed by telephone stations connected to MLTS, as occurs with fixed single-line telephones that are typically found in a residence.

- **ANSI/TIA/EIA-689-1997 (SUPERCEDED BY 689-A) “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.

TR-41.4, IP Telephony Gateways and Infrastructures
This subcommittee has established liaison with ETSI EMTEL and made them aware of the work discussed below. In return, it has received copies of EMTEL contributions on emergency services. The subcommittee is also tied in to the work of the National Emergency Number Association (NENA) through participation of individuals in both activities.

- **PN-3-0061 (to be published as TSB-139), “IP Telephony Security Framework”** (In committee development): Subcommittee 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 will 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.

- **TIA/TSB-146 (2003), “Telecommunications – IP Telephony Infrastructures – IP Telephony Support for Emergency Calling Service.”** This published technical document describes network architecture elements and their functionality needed for providing E9-1-1 or ECS support over IP terminals in an Enterprise non-enterprise environment Network. Many countries have similar ECS requirements. Portions of this document may be applicable in providing solutions for those requirements. This TSB addresses ECS calls placed from fixed, mobile, remote dial-in or wireless access VoIP terminals, however does not address scenarios for devices connected to VoIP networks through gateways. This TSB is applicable to supporting emergency telecommunications services. TSB-146 also involved TIA TR-45.1 Subcommittee.
- 43 -

- PN-3-4726-RV1 (to be published as TSB-146-A), “Telecommunications – IP Telephony Infrastructures – IP Telephony Support for Emergency Calling Service” (In committee balloting process): This project is being developed as a revision of TIA/TSB-146 mentioned above and applicable to emergency telecommunications services. Note that recently published European emergency call handling requirements (e.g., ETSI SR 002 180) have been made available to this project and are being taken into consideration (i.e., coordination of E9-1-1/E1-1-2 and Public Safety Answering Point aspects). Coordination with TIA TR-45 is also being proposed with regard to E1-1-2 requirements for cdma2000® systems operating in Europe.

- PN-3-0172, “Enterprise Location Information Server Interfaces.” This purpose of this project is to standardize the application protocol interfaces between the Location Information Server (LIS) application functions and other Enterprise emergency call service entities.

- PN-3-0185, “Link Level Discovery Protocol (LLDP) – Media Endpoint Discovery (MED).” A new IEEE standard, 802.1AB™ “Standard for Local and Metropolitan Networks: Station and Media Access Control – Connectivity Discovery” is currently in a final draft state, and is expected to become a fully recognized standard soon. IEEE 802.1AB™, which is commonly referred to as “Link Layer Discovery Protocol (LLDP),” can be utilized for many advanced features in a VoIP network environment. These features include basic configuration, network policy configuration, Emergency Call Service / E911 location support, inventory control, and more. This project provides extensions to the IEEE 802.1AB™ base protocol, to allow for these functions, and also provides behavioural requirements for devices implementing the extensions to enable correct multi-vendor interoperation.

TR-41.9, Technical Regulatory Considerations

- ANSI/TIA-968-A-2002, “Telecommunications – Telephone Terminal Equipment – 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 47 CFR Code of Federal Regulations) Part 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) and, in virtue of the standard, assists emergency communications/Emergency telecommunications service by helping to ensure the network’s ability to perform under emergency (e.g., high-load) conditions. Additionally, this standard also contains requirements for terminal equipment intended to make sure network billing equipment works properly and supporting emergency telecommunications service. The previous document, TIA/EIA/IS-968, “Technical Criteria for Terminal Equipment to prevent Harm to the Telephone Network,” remained valid until July 2004.

- ANSI/TIA-968-A-1-2003, “Telecommunications – Telephone Terminal Equipment – Technical Requirements for Connection of Terminal Equipment to the Telephone Networks – Addendum 1.” This addendum changes the allowable analog signal power limitations established in the original ANSI/TIA-968-A and the criteria may be applied to terminal equipment approved after publication of this addendum by ACTA. The document also clarifies the status of grandfathered non-approved terminal equipment and addresses several editorial references.

- ANSI/TIA-968-A-2-2004, “Telecommunications – Telephone Terminal Equipment – Technical Requirements for Connection of Terminal Equipment to the Telephone Networks – Addendum 2.” This addendum corrects an error concerning the need to separate leads to non-registered equipment from telecommunications leads, clarifies the specification of non-hazardous voltage sources, and adds cross-references concerning the applicability of criteria for connectors.
Annex 9, TR-42 Activities

TR-42.2, Residential Telecommunications Infrastructure

- ANSI/TIA/EIA-570-A-1999, “Residential Telecommunications Cabling Standard.” This ANSI standardizes requirements for residential telecommunications cabling based on the facilities that are necessary for existing and emerging telecommunications services. Related documents include:
  - ANSI/TIA/EIA-570-A-3-2002, “Residential Telecommunications Cabling Standard – Addendum 3 – Whole-Home Audio Cabling for Residences.” This addendum focuses on whole-home audio cabling to support high-quality stereo to various rooms or areas throughout the residence.

- ANSI/TIA-570-B-2004, “Residential Telecommunications Infrastructure Standard.” This recent ANSI builds on 570-A requirements for residential telecommunications cabling, based on the facilities that are necessary for existing and emerging telecommunications services.

TR-42.3, Pathways and Spaces for Telecommunications Cabling

- ANSI/TIA/EIA-569-A-1998, “Commercial Building Standard for Telecommunications Pathways and Spaces.” This ANSI 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. Additionally, this standard and its related addendum provide some guidance for alternate routing of cabling into a building to help prevent loss of conventional and emergency communications and service. Related standard documents include:
  - ANSI/TIA/EIA-569-A-3-2000, “Commercial Building Standard for Telecommunications Pathways and Spaces, Addendum 3.” This addendum provides information on access flooring systems.
  - ANSI/TIA/EIA-569-A-4-2000, “Commercial Building Standard for Telecommunications Pathways and Spaces, Addendum 4.” This addendum provides information on poke-thru device that allows penetration of above-grade concrete floors and steel decks.
  - ANSI/TIA/EIA-569-A-7-2001, “Commercial Building Standard for Telecommunications Pathways and Spaces – Addendum 7 – Cable Trays and Wirelines.” This addendum replaces Subclause 4.5, Cable Trays and Wirelines, it modifies the standard to clarify industry issues with cable fill for cable trays systems.

TR-42.4, Outside Plant Telecommunications Infrastructure

- ANSI/TIA/EIA-758-1999, “Customer-Owned Outside Plant Telecommunications Cabling Standard.” This ANSI 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.” By nature of this standard, it provides guidance for design and routing of cabling that may help prevent loss of communications and thus enable emergency services.

TR-42.6, Telecommunications Infrastructure Administration

- TIA/EIA-606-A (2002), “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. Implementation considerations may include security, emergency service availability and infrastructure assurance. 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.
Annex 10, TR-45 Activities

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 that are supported within TR-45 Engineering Committee security mechanisms. AHAG also collaborates with the Third Generation Partnership Project 2 (3GPP2) Technical Specification Group (TSG)-S, Working Group (WG) 4 (Security).

- **TIA-946 (2003), “Enhanced Cryptographic Algorithms.”** This TIA document describes detailed cryptographic procedures for wireless system applications. These procedures are used to perform the security services of mutual authentication between mobile stations and base stations, subscriber message encryption and key agreement within wireless equipment. This document includes changes resulting from the publication of 3GPP2 document S.S0078-0. 3rd Generation (3G) cdma2000® Security Features include: 128-bit root secret key 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); and Mutual authentication between Mobile and Network elements.

TR-45 Joint Ad Hoc Group, Lawfully Authorized Electronic Surveillance (LAES)
This Ad Hoc group is presently undergoing restructure of activity. 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 prior to restructure include standards development to support lawful interception and surveillance (i.e., Communications Assistance for Law Enforcement Act (CALEA) in U.S.). The following activity relates to U.S. CALEA requirements and appropriate electronic surveillance capabilities, involving voice and data transmissions:

- **ANSI/J-STD-025-2000, “Lawfully Authorized Electronic Surveillance (CALEA).”** 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.

- **ANSI/J-STD-025-A-2003, “Lawfully Authorized Electronic Surveillance (CALEA).”** This recently approved joint TIA/Committee T1 developed ANS 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. Also involves FBI “punch list” (i.e., additional surveillance capabilities) items. This project 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.

- **J-STD-025-B-2003, “Lawfully Authorized Electronic Surveillance”** (An ANS upgrade PN-3-4465-UGR2 Standard 025-B is currently being balloted in TR-45 LAES Ad Hoc Joint committee default ballot process; publication expected in early 2005. This joint project (w/ ATIS) is relative to CALEA compliance and the refinement of J-STD-025-A, “Lawfully Authorized Electronic Surveillance.” This joint standard contains refined requirements for support of packet mode communication 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. This joint activity 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).

- **PN-3-4465-UGRV3 Standard 025-C** presently undergoing restructure related to LAES AHG activity.
Future TR-45 LAES Work

Going forward as of September, 2004—the LAES work, undertaken within TIA, has been reorganized and divided as appropriate among the TR-45 LAES Ad Hoc, the TR-45.2 (LAES for IMS) and the TR-45.6 (LAES for packet data system) subcommittees. Project Numbers and capabilities documentation will be available in the near future.

TR-45 ESN/UIM/MEID Ad Hoc Group (EUM)

This Ad Hoc group supports equipment identifier issues including recommendations on topics such as ESN manufacturer codes, ESN reclamation, ESN re-use, ESN administration, UIM ID manufacturer codes, UIM administration, MEID global hexadecimal administration and MEID guidelines. The Ad Hoc represents TR-45 relative to global number administration and maintains the industry MEID outreach awareness initiatives while assisting the management of the ESN exhaust timeline.

TR-45.1, Analog Technology

- TIA/EIA/TSB-119 (2000), “Enhanced System Access Procedures for E-9-1-1 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 a 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 (2001), “A Position Determination Standard for Analog Systems.” This interim Standard provides for 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 (2001), “A Position Determination 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-41.000-E-2004, “Part 000: Wireless Radiotelecommunications Intersystem Operations – Introduction to TIA/EIA-41.” (supersedes TIA-41-D) This ANS lists all the system implementation parts of TIA-41-E, and includes options which support Priority Access and Channel Assignment (PACA)9 and other related capabilities.
- TIA/EIA/TSB-114 (1999), “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, “Cellular 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 an authorized subscriber to have “first come, first served” priority access to voice or traffic channels on call origination.). Additionally, TIA-664.804, “Wireless Features Description – Enhanced Security Services” provides detailed information regarding enhanced wireless security services. Enhanced security provides enhanced capabilities for

---

9 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 (BS), Mobile Switching Center (MSC) and Internetworking Function (IWF), 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.
wireless networks and mobile stations. The enhanced security capabilities address unauthorized use of service, unauthorized communications to the mobile station and unauthorized monitoring of subscriber traffic. The security capabilities that address these problems are enhanced subscriber authentication (ESA) and enhanced subscriber privacy (ESP). ESA verifies that a subscriber requesting service and the network are authorized. It also provides data integrity protection against unauthorized modification of messages during transmission. ESP protects user data from unauthorized eavesdropping. From the end user perspective, the enhanced security requirements are independent of the air interface. Thus, the enhanced security capabilities are applicable to all digital air interfaces.

- **PN-3-0054 (approved for publication September 2004 as TIA-917), “TIA/EIA-41 Support for Wireless Priority Service (WPS)” (re-ballot completed in September 2004):** This proposed standard will supplement GETS (Government Emergency Telecommunications Service) wireline 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. This standard involves Full Operating Capability for mobile originated/mobile terminated services and allows WPS to be provided via an operator’s HLRs rather than a government-run SCP platform. Methods are also defined for operators to flexibly allot capacity to NS/EP and normal users.

- **TIA-881 (2004), “TIA/EIA-41-D Location Services Enhancements.”** This document was published March 2004 and provides enhanced 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 standard provides ANSI/TIA/EIA-41 support of authentication, privacy and security of location services.

- **TIA-843 (2004), “Wireless Intelligent Network Support for Location Based Services.”** This document was published in August 2004 and presents a recommended plan for the implementation of Wireless Intelligent Network (WIN) capabilities that support these services. As indicated, Fleet and Asset Management (FAM), Location Based Charging (LBC), Location Based Information Service (LBIS) and Enhanced Call Routing (ECR) are WIN-based services that enable the services to be tailored based on the subscriber’s current location (i.e., geographic position).

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

- **J-STD-034 (2002), “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). This document specifically takes the Public Safety Answering Point (PSAP) perspective into account.

- **J-STD-036-A (2002), “Enhanced Wireless 9-1-1, Phase 2.”** 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.

- **J-STD-036-A-1 (2002), “Enhanced Wireless 9-1-1, Phase 2 – Addendum 1.”** This recently published joint TIA/Committee T1 standard addendum defines messaging required to support information transfer to identify and locate wireless emergency services callers. It provides a solution for handling Wireless Enhanced Emergency Calls for the FCC E9-1-1 Phase 2 mandate. Carrier position reporting to emergency services
systems, as mandated by the FCC under docket 94-102 (incl. orders 96-264, 99-96 and 99-245) has been addressed by this Interim Standard without considering position reporting privacy restrictions that may be desirable for other position reporting services. For this reason, this standard does not preclude these other service restrictions. Position reporting privacy restrictions are beyond the scope of this standard, and are not addressed here. Additional joint work is now under review and progressing towards the development of a more extensive revision to J-STD-036-A (to be published as J-STD-036-B) with modifications to incorporate field experience and extending the use of interim position for X-Y routing to GSM and other 3GPP technologies. The joint TIA/ATIS standard J-STD-036-B is scheduled to be published by December 2004, with MEID and Interim Position for GSM.

- In March 2004, an Addendum J-STD-036-A-1 was published including Interim Position and enhancements to Non-dialable Callback Numbers.

**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. The following documents involving position determination are included in the ANSI/TIA/EIA-136 Series, Release D collection:
  - 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-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-136-741-2002, “TDMA Third Generation Wireless – System Assisted Mobile Positioning through Satellite (SAMPS) for Analog Systems.” This ANS 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.

**TR-45.4, Radio to Switching Technology**

- TIA/EIA-1S-2001-A (2001), “Interoperability Specifications (IOS) for cdma2000® Access Network Interfaces, Release A.” This document describes the overall system functions, including services and features required for interfacing a Base Station with the Mobile Switching Center, with other Base Stations, and with the Packet Control Function (PCF) and for interfacing the PCF with the Packet Data Service Node (PDSN).
- TIA-1S-2001-C (2003), “Interoperability Specifications (IOS) for cdma2000® Access Network Interfaces – Release C.” Engineering activities involving this standard include support for PACA service in addition to other more encryption-related aspects on cdma2000® systems.
- TIA-IS-2001-C.1 (2003), “Interoperability Specifications (IOS) for cdma2000® Access Network Interfaces – Release C Addendum” This standard includes support for TIA-2000-C EV-DV (enhanced voice and data) services on cdma2000® systems. The 1xEV-DV standard offers the flexibility to dynamically balance voice and data traffic by allocating bandwidth on demand and allows for the performance of two high-value tasks simultaneously on a single RF section device, creating an attractive cost structure for operators with the combination of flexible network resource allocation and ability to support concurrent voice and data services.

TR-45.5, Spread Spectrum Digital Technology

- TIA-2000.1-D (2004), “Introduction to cdma2000® Spread Spectrum Systems (2004)” The technical requirements contained in cdma2000® form a compatibility standard for CDMA systems. They ensure that a mobile station can obtain service in a system manufactured in accordance with the cdma2000® standards. Supports Emergency Calling and may provide enhanced Public Safety applicability by providing voice services as well as data services up to 3.1 Mbps on the downlink and 1.8 Mbps on the uplink.
  - These standards have been developed for TIA transposition by the 3rd Generation Partnership Project Two.

- TIA/EIA/IS-2000.5 (latest release is TIA/EIA/IS-2000.5-C)“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. 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 AES encryption (the Rijndael encryption algorithm) was added to improve the encryption strength over the previously used encryption algorithm. In Release C, support for the 3GPP 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 (latest release is TIA/EIA/IS-2000.6-C), “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 (1999), “Position Determination Service Standard for Dual Mode Spread Spectrum Systems.” This IS 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-801-1 (1999), “Position Determination Service Standards for Dual Mode Spread Spectrum Systems, Addendum 1” This document defines a set of signaling messages between the mobile station and base station to provide a position determination service.

- TIA-856-A (2004), “cdma2000® High Rate Packet Data Air Interface Specification” Developed as a packet only system with simpler network architecture where the radio access network connects directly to the internet. It has the same data rates as TIA-2000-D. In addition to the base standards of TIA-2000 and TIA-856, there are many companion standards which provide various services, provide performance and testing requirements, and which define the network. Supports enhanced Public Safety applicability by providing Broadband data services.
  - TIA/EIA/IS-856 (2000), “cdma2000® High Rate Packet Data Air Interface Specification” This specification is primarily oriented toward requirements necessary for the design and implementation of access terminals.
    - TIA/EIA/IS-856-1 (2000), “cdma2000® High Rate Packet Data Air Interface Specification – Addendum 1.” 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-925 (2002), “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 “TR45.AHAG Cryptographic Algorithms” 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 (to be published as TIA-908), “Lawfully Authorized Electronic Surveillance (LAES) for Packet Data”** (In “not active” committee status pending related activities): This proposed TIA standard will involve requirements for supporting packet mode communications surveillance, including collection functions and intercept access point (IAP) aspects.