ANSI/J-STD-025-B-2006
APPROVED: JULY 17, 200
REAFFIRMATION: FEBRUARY 9, 20
REAFFIRMATION: MAY 7, 2019

JOINT STANDARD

Lawfully Authorized Electronic Surveillance

J-STD-025-B July 2006

Jointly developed by Telecommunications Industry Association
and Alliance for Telecommunications Industry Solutions

JOINT STANDARDS

Joint Standards and Publications are adopted in accordance with the American National Standards Institute (ANSI) patent policy. By such action, the Telecommunications Industry Association or the Alliance for Telecommunications Industry Solutions does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Standard or Publication.

This Standard does not purport to address all safety problems associated with its use or all applicable regulatory requirements. It is the responsibility of the user of this Standard to establish appropriate safety and health practices and to determine the applicability of regulatory limitations before its use.

This standard was developed under Project No. SP-3-4465-UGRV2-RF2-A, formulated under the cognizance of the TIA TR-45 Committee on Mobile & Personal Communications Systems and ATIS Wireless Technologies and Systems Committee and ATIS Packet Technologies and Systems Committee.

Published by

©TELECOMMUNICATIONS INDUSTRY ASSOCIATION 2019
Technology and Standards Department
1320 N. Courthouse Road, Suite 200
Arlington, VA 22201 U.S.A

Or

©ALLIANCE FOR TELECOMMUNICATIONS INDUSTRY SOLUTIONS 2019
1200 G Street, NW
Suite 500
Washington, DC 20005
(202) 628-6380

NOTICE FROM THE DEVELOPERS

This document has been approved by the Telecommunications Industry Association (TIA) Engineering Committee and the Alliance for Telecommunications Industry Solutions (ATIS).

Users may submit comments to the Standards Secretariat to TIA at the following address: 1320 N. Courthouse, Suite 200, Arlington, VA 22201-3438; Telephone (703)907-7700; Fax: (703)907-7727 or by email to standards@tiaonline.org.

This document was coordinated between ATIS and TIA.

A Word from TIA:
TIA Engineering Standards and Publications are designed to serve the public interest through eliminating misunderstanding between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for his/her particular need. Existence of such Standards and Publications shall not be in any respect preclude any member or nonmember of TIA from manufacturing or selling products not conforming to such Standards and Publications, nor shall the existence of such Standards and Publications preclude their voluntary use by those other than TIA members, whether the standard is to be used either domestically or internationally.

TIA Documents contain information deemed to be of technical value to the industry, and are published at the request of the originating Committee without necessarily following the rigorous public review and resolution of comments which is a procedural part of the development of a American National Standard (ANS). Further details of the development process are available in the TIA Procedures for American National Standards and TIA Engineering Committee Operating Procedures, located at Standards Procedures and Guidelines

A Word from ATIS:
As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's business priorities. ATIS' member companies are currently working to address emergency services, 5G, robocall mitigation, Smart Cities, artificial intelligence-enabled networks, IoT, distributed ledger/blockchain technology, cybersecurity, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle – from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org. Follow ATIS on Twitter and on LinkedIn.

NOTICE FROM PATENT HOLDERS

The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights.

By publication of this standard, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. The patent holder has, however, filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain a license. Details may be obtained from the Telecommunications Industry Association, Alliance for Telecommunications Industry Solutions or the American National Standards Institute.

NOTICE OF COPYRIGHT

NOTICE OF DISCLAIMER AND LIABILITY

The document to which this Notice is affixed (the "Document") has been prepared by one or more Engineering Committees or Formulating Groups of the Telecommunications Industry Association ("TIA"). In addition, the Document was balloted by ATIS Wireless Technologies and Systems Committee and ATIS Packet Technologies and Systems Committee. TIA is not the author of the Document contents, but publishes and claims copyright to the Document pursuant to licenses and permission granted by the authors of the contents.

TIA Engineering Committees and Formulating Groups are expected to conduct their affairs in accordance with the TIA Procedures for American National Standards and TIA Engineering Committee Operating Procedures, the current and predecessor versions of which are available at Standards Procedures and Guidelines. The ATIS Wireless Technologies and Systems Committee and ATIS Packet Technologies and Systems Committee is expected to conduct its affairs in accordance with the ATIS Operating Procedures which is available at http://www.atis.org/legal/op.asp..

TIA's function is to administer the process, but not the content, of document preparation in accordance with the Manual and, when appropriate, the policies and procedures of the American National Standards Institute ("ANSI"). Likewise, ATIS' function, and on behalf of its Committees and Forums, is to administer the process according to its Operating Procedures, but not develop the content of the document. TIA and ATIS do not evaluate, test, verify or investigate the information, and the accuracy, soundness, or credibility of the contents of the Document. In publishing the Document, TIA and ATIS disclaim any undertaking to perform any duty owed to or for anyone.

If the Document is identified or marked as a project number (PN) document, or as a standards proposal (SP) document, persons or parties reading or in any way interested in the Document are cautioned that: (a) the Document is a proposal; (b) there is no assurance that the Document will be approved by any Committee of TIA or any other body in its present or any other form; (c) the Document may be amended, modified or changed in the standards development or any editing process.

The use or practice of contents of this Document may involve the use of intellectual property rights ("IPR"), including pending or issued patents, or copyrights, owned by one or more parties. Neither TIA nor ATIS makes any search or investigation for IPR. When IPR consisting of patents and published pending patent applications are claimed and called to TIA's attention, a statement from the holder thereof is requested, all in accordance with the Manual. When IPR consisting of patents are claimed and called to ATIS's attention, a statement from the holder thereof is requested, all in accordance with the ATIS's Operating Procedures. Neither TIA nor ATIS takes any position with reference to, and disclaims any obligation to investigate or inquire into, the scope or validity of any claims of IPR. Neither TIA or ATIS will neither be a party to discussions of any licensing terms or conditions, which are instead left to the parties involved, nor will TIA or ATIS opine or judge whether proposed licensing terms or conditions are reasonable or non-discriminatory. TIA does not warrant or represent that procedures or practices suggested or provided in the Manual have been complied with as respects the Document or its contents.

TIA and ATIS do not enforce or monitor compliance with the contents of the Document. TIA and ATIS do not certify, inspect, test or otherwise investigate products, designs or services or any claims of compliance with the contents of the Document.

ALL WARRANTIES, EXPRESS OR IMPLIED, ARE DISCLAIMED, INCLUDING WITHOUT LIMITATION, ANY AND ALL WARRANTIES CONCERNING THE ACCURACY OF THE CONTENTS, ITS FITNESS OR APPROPRIATENESS FOR A PARTICULAR PURPOSE OR USE, ITS MERCHANTABILITY AND ITS NON-INFRINGEMENT OF ANY THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS. TIA AND ATIS EXPRESSLY DISCLAIM ANY AND ALL RESPONSIBILITIES FOR THE ACCURACY OF THE CONTENTS AND MAKE NO REPRESENTATIONS OR WARRANTIES REGARDING THE CONTENT'S COMPLIANCE WITH ANY APPLICABLE STATUTE, RULE OR REGULATION, OR THE SAFETY OR HEALTH EFFECTS OF THE CONTENTS OR ANY PRODUCT OR SERVICE REFERRED TO IN THE DOCUMENT OR PRODUCED OR RENDERED TO COMPLY WITH THE CONTENTS.

NEITHER TIA NOR ATIS SHALL BE LIABLE FOR ANY AND ALL DAMAGES, DIRECT OR INDIRECT, ARISING FROM OR RELATING TO ANY USE OF THE CONTENTS CONTAINED HEREIN, INCLUDING WITHOUT LIMITATION ANY AND ALL INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, LITIGATION, OR THE LIKE), WHETHER BASED UPON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING NEGATION OF DAMAGES IS A FUNDAMENTAL ELEMENT OF THE USE OF THE CONTENTS HEREOF, AND THESE CONTENTS WOULD NOT BE PUBLISHED BY TIA WITHOUT SUCH LIMITATIONS.

Abstract

This Standard defines the interfaces between a telecommunication service provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance. A TSP, manufacturer, or support service provider that is in compliance with this Standard will have a "safe harbor" under Section 107 of the Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414: "a [TSP] shall be found to be in compliance with the assistance capability requirements under [CALEA] Section 103, and a manufacturer of telecommunication transmission or switching equipment or a provider of telecommunication support services shall be found in compliance with [CALEA] Section 106."

J-STD-025-A provides the enhancements necessary to support FCC 99-230, CC Docket No. 97-213, Third Report and Order and FCC 02-168, CC Docket No. 97-213, Order on Remand[1]. J-STD-025-B provides enhancements to further support lawfully authorized electronic surveillance of packet data telecommunication services (e.g., cdma2000®[2] packet data).

1. The FCC Third Report and Order [FCC 99-230, CC Docket No. 97-213] introductory paragraph states the following:

   "Specifically, we require that all capabilities of J-STD-025 (interim standard) and six of nine "punch list" capabilities requested by the Department of Justice (DoJ)/Federal Bureau of Investigation (FBI) be implemented by wireline, cellular, and broadband PCS carriers. While we are requiring that a packet-mode capability be implemented by such carriers, we are not at this time adopting technical requirements for packet-mode communications, but will permit packet-mode data to be delivered to law enforcement under the interim standard, discussed below, pending further study of packet-mode communications by the telecommunications industry."

2. cdma2000 is a registered trademark of the Telecommunications Industry Association (TIA-USA).

Document Revision History

Revision	Date	Remarks
0	November 1997	Initial
A	February 2003	Revised to meet the requirements defined in FCC 99-230, CC Docket No. 97-213 and FCC 02-108, CC Docket No. 97-213.
B	January 2004	Revised to include enhancements for packet based telecommunication technologies. J-STD-025-B is both a T1 Trial Use standard and a TIA standard.
B	June 2004	ANSI upgrade to include enhancements for packet based telecommunication technologies.

Contents

List of Tables

List of Figures

Foreword

This foreword is not part of this Standard.

The specification of interface compatibility requirements between telecommunication service providers (TSPs) and law enforcement agencies (LEAs) was developed as a Joint Standards Project between ANSI-Accredited Telecommunications Industry Association, Engineering Committee TR-45, and ANSI-Accredited Committee T1–Telecommunications.

This Standard defines the interfaces between a telecommunication service provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance. A TSP, manufacturer, or support service provider that is in compliance with this Standard will have a "safe harbor" under Section 107 of the Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414: "a [TSP] shall be found to be in compliance with the assistance capability requirements under [CALEA] Section 103, and a manufacturer of telecommunication transmission or switching equipment or a provider of telecommunication support services shall be found in compliance with [CALEA] Section 106."

There are ~~eight seven~~ annexes ~~in~~ to this Standard. All annexes are informative and are not considered part of this Standard.

J-STD-025-A provides the enhancements necessary to support FCC 99-230, CC Docket No. 97-213, Third Report and Order and FCC 02-108, CC Docket No. 97-213, Order on Remand[1]. J-STD-025-B provides enhancements to further support lawfully authorized electronic surveillance of packet data telecommunication services (e.g., cdma2000® packet data).

The enhancements for J-STD-025-B are identified by underlined text. Strike-through text indicates deleted J-STD-025-A text.

All annexes are informative. Information contained in Annexes A through D, and F ~~and G~~ through H does not reflect additional terms, concepts, requirements, messages or parameters for capabilities added in J-STD-025-A as mandated in FCC 99-230, CC Docket No. 97-213 and FCC 02-108, CC Docket No. 97-213, Order on Remand. Annex E, *Informative Access Scenarios - J-STD-025-A,* is exclusively dedicated to J-STD-025-A scenarios. Annex I contains compilable ASN.1 code.

1.The FCC Third Report and Order [FCC 99-230, CC Docket No. 97-213] introductory paragraph states the following:

> "Specifically, we require that all capabilities of J-STD-025 (interim standard) and six of nine "punch list" capabilities requested by the Department of Justice (DoJ)/Federal Bureau of Investigation (FBI) be implemented by wireline, cellular, and broadband PCS carriers. While we are requiring that a packet-mode capability be implemented by such carriers, we are not at this time adopting technical requirements for packet-mode communications, but will permit packet-mode data to be delivered to law enforcement under the interim standard, discussed below, pending further study of packet-mode communications by the telecommunications industry."

1 Introduction

1.1 General

This Standard defines the interfaces between a telecommunication service provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance. A TSP, manufacturer, or support service provider that is in compliance with this Standard will have a "safe harbor" under Section 107 of the Communications Assistance for Law Enforcement Act (CALEA), Public Law 103-414: "a [TSP] shall be found to be in compliance with the assistance capability requirements under [CALEA] Section 103, and a manufacturer of telecommunication transmission or switching equipment or a provider of telecommunication support services shall be found in compliance with [CALEA] Section 106."

J-STD-025-A provides the enhancements necessary to support FCC 99-230, CC Docket No. 97-213, Third Report and Order and FCC 02-108, CC Docket No. 97-213, Order on Remand[1]. J-STD-025-B provides enhancements to further support lawfully authorized electronic surveillance of packet data telecommunication services (e.g., cdma2000® packet data).

As used in this Standard, electronic surveillance refers to the interception and monitoring of communications (i.e., call content), call-identifying information, or both, for a particular telecommunication subscriber as lawfully authorized. In this Standard intercept subject, or more simply a subject, is a telecommunication service subscriber whose communications, call-identifying information, or both, have been authorized by a court to be intercepted and delivered to an LEA. The identification of the subject is limited to identifiers used to access the particular equipment, facility, or communication service (e.g., network address, terminal identity, subscription identity).

As a precondition for a TSP's assistance with Lawfully Authorized Electronic Surveillance (LAES), an LEA must serve a TSP with the necessary legal authorization identifying the intercept subject, the communications and information to be accessed, and service areas where the communications and information can be accessed. Once this authorization is obtained, the TSP shall perform the access and delivery for transmission to the government's procured equipment, facilities, or services.

LEAs recognize that in many instances the telecommunication services subscribed to by certain intercept subjects may permit a TSP to access and

1.The FCC Third Report and Order [FCC 99-230, CC Docket No. 97-213] introductory paragraph states the following:

> "Specifically, we require that all capabilities of J-STD-025 (interim standard) and six of nine "punch list" capabilities requested by the Department of Justice (DoJ)/Federal Bureau of Investigation (FBI) be implemented by wireline, cellular, and broadband PCS carriers. While we are requiring that a packet-mode capability be implemented by such carriers, we are not at this time adopting technical requirements for packet-mode communications, but will permit packet-mode data to be delivered to law enforcement under the interim standard, discussed below, pending further study of packet-mode communications by the telecommunications industry."

deliver communications and call-identifying information without the TSP having to modify its networks or systems. In these instances, the TSP may be fully compliant with the assistance capability requirements set forth in CALEA. For example, a TSP could effect a central office- or local loop-based interception using conventional methods of access and delivery and fully meet an LEA's electronic surveillance needs.

1.2 Purpose

The purpose of this Standard is to facilitate a TSP's compliance with the assistance capability requirements defined in Section 103 of CALEA. This Standard defines services and features to support LAES and the interfaces to deliver intercepted communications and call-identifying information to an LEA when authorized. This Standard also defines a protocol for delivering specific information elements to LEAs. Compliance with this Standard satisfies the "safe harbor" provisions of Section 107 of CALEA and helps ensure efficient and industry-wide implementation of the assistance capability requirements.

1.3 Scope

The scope of this Standard is to define the services to support LAES and the interface between a TSP and an LEA.

1.4 Organization

Section 2 "References" is a list of references used in the preparation of this Standard.

Section 3 "Definitions and Acronyms" defines words and acronyms that are used in this Standard.

Section 4 "Stage 1 Description: User Perspective" defines the LAES services from the user point of view. The user in this case is the LEA.

Section 5 "Stage 2 Description: Network Perspective" defines the network entities and information flows to implement LAES services from a network point of view.

Section 6 "Stage 3 Description: Implementation Perspective" defines the messages and information elements to implement LAES services from an implementation point of view.