



Audio Verification and Notification Procedures

Revision 1.01 (version October 31st, 2007)

Sponsor Central Station Alarm Association (CSAA)

Contents

Foreword.....	iv
Introduction.....	vi
1 Scope.....	6
1.1 General.....	6
1.2 Definitions.....	6
2 Standard Verification Procedures for Burglar Alarm Signals.....	7
2.1 Procedures for Alarm Signals Received from Systems without “UL Certificated” Service.....	7
2.1.1 Initial Verification Session (should this be defined as 2 way or one way in separate sections?).....	8
2.1.2 If No Contact or Wrong Code.....	8
2.1.3 If Audio Communication is Established.....	8
2.2 Procedures for Alarm Signals Received from Systems with “UL Certificated” Service.....	9
3 Enhanced Audio Verification of Burglar Alarm Signals.....	9
3.1 Extended Time.....	9
3.2 Procedure.....	9
3.2.1 Audio Verification Session (Attempt #1).....	9
3.2.2 Attempt (Call) #2 Other Than Premises.....	9
3.3 Answering Machines.....	9
3.4 Scheduled Events.....	9
3.5 Verified False.....	9
3.6 Call Lists and Priority.....	10
3.7 Compliance with Enhanced Call Verification.....	10
4 Hold-Up.....	10
4.1 Commercial Hold-Up Alarm.....	10
4.2 Residential Panic/Duress/Emergency Alarm.....	10
A.6.1 Surreptitious recording.....	11

Foreword

This standards document is published by the Central Station Alarm Association (CSAA) and was developed and adopted by a consensus of industry volunteers in accordance with CSAA's standards development policies and procedures.

CSAA assumes no responsibility for the use, application or misapplication of this document. Industry members using this document, particularly those having participated in its development and adoption, are considered by CSAA to have waived any right they might otherwise have had to assert claims against CSAA regarding the development process of this standard.

CSAA reserves the right to revise this document at any time. Because CSAA policy requires that every standard be reviewed periodically and be revised, reaffirmed, or withdrawn, users of this document are cautioned to obtain and use the most recent edition of this standard. Current information regarding the revision level or status of this or any other CSAA standard may be obtained by contacting CSAA.

Requests to modify this document are welcome at any time from any party, regardless of membership affiliation with CSAA. Such requests, which must be in writing and sent to the address set forth below, must clearly identify the document and text subject to the proposed modification and should include a draft of proposed changes with supporting comments. Such requests will be considered in accordance with CSAA's standards development policies and procedures.

Written requests for interpretations of a CSAA standard will be considered in accordance with CSAA's standards development policies and procedures. While it is the practice of CSAA staff to process an interpretation request quickly, immediate responses may not be possible since it is often necessary for the appropriate standards subcommittee to review the request and develop an appropriate interpretation.

Requests to modify a standard, requests for interpretations of a standard, or any other comments are welcome and may be sent to:

Central Station Alarm Association 440 Maple Avenue East, Suite 201, Vienna, VA 22180 Tel: 703/242-4670
email:

This document is owned by the Central Station Alarm Association and may not be reproduced, in whole or part, without the prior written permission from CSAA.

ACKNOWLEDGEMENTS

- CSAA Standards Chairman: Louis T. Fiore, L.T.Fiore, Inc.
- CSAA Committee Chairman: Peter P. Giacalone, Giacalone Associates, LLC
- CSAA Staff Administrator: Stephen P. Doyle, Executive Vice President, CSAA
Celia T. Besore, Director of Marketing and Communications, CSAA

This is a *Work in Progress*.

- ACF Associates Tony Fague
- ADT.....Larry Dischert
- ADT..... Thomas Nakatani
- ADT..... Brooke Smith
- Bay Alarm Co.....Shane M. Clary
- CSAA.....Lou Fiore
- GE Security..... Frank Clark
- SonitrolFrank Minni
- SIAC.....Ron Walters
- SIAC..... John Wurnen
- SIAC..... Bill Moody
- S. Pai Consulting.....Sam Pai
- Vector Security.....John Murphy
- Vector Security.....Pam Petrow
- Vector.....Anita Ostrowski

Introduction

This standard defines methods by which false dispatches can be greatly reduced in systems that are audio enabled to allow the monitoring facility to communicate with the end user in a means other than traditional telephone communications. It has been proven that verifying an alarm signal by a monitoring central station will drastically reduce false dispatches. This standard takes a different approach to verification and elevates it to its next level by defining various methods of attaining audio verification.

Alarm Verification and Notification Procedures

1 Scope

This standard has been prepared under the direction of the Security Industry Standards Council (SISC) members with the participation of Central Station Alarm Association (CSAA) members, Security Industry Association (SIA) members, National Burglar & Fire Alarm Association (NBFAA) members, ASIS members and Canadian Alarm Association (CANASA) members. This standard has been developed to allow a consistent method for processing audio enabled alarms and to achieve increased efficiencies by reducing costs and eliminating wasteful efforts associated with potential false alarms. This standard is to be used by alarm monitoring facilities and by state and local units of government in their development of consistent administration criteria for alarms. New technologies and successful efforts to reduce false alarms have led to this standard. The intent of this standard is

1.1 General

If differences exist between this standard and other written Special Instructions with the monitored premises, the Special Instructions shall take precedence.

1.2 Definitions

1.2.1

Audio Verification

An event activated method that provides live real time audio from the protected premises to the central station that enables the monitoring agency to verify whether activity is occurring that appears to warrant the immediate emergency response of responding agencies..

1.2.2

"UL Certificated" Service

The term "UL Certificated" Service, as used in this document, refers to burglar alarm systems that have a UL certificate in force and therefore follow verification procedures outlined in UL 827, UL 2050, ULC S301 or ULC S304 Standards.

1.2.3 Types of Audio Verification Three broad forms of verification may be employed. These include:

1.2.3.1

Listen-In or Listen Back or One-Way Audio

An audio appliance capable of being activated by the initiation of another security appliance. A one-way audio feed will be available to the central station when a device such as a hold-up button or door contact has come into alarm.

1.2.3.2

Two-Way Audio

An event driven, two-way, hands free communications session at the premise between the central station caused by the activation of an alarm event at the premise for the purpose of verifying the validity of an alarm condition and/or gain additional information regarding the cause of the condition.

Enhanced Verification

Enhanced Verification is the attempt by monitoring facility personnel to verify that no emergency appears to exist, at the monitored premises, by means of more thorough procedures such as two (2) or more verification calls, live audio or video, cross zoning, other means or a combination of these procedures.

Methods of Verification

1.2.3.3.1

Electronic Verification

An electronic signal transmitted to the monitoring facility that indicates to its personnel or to its dispatch computer that no emergency appears to exist.

1.2.3.3.2

Verbal

A personal contact by means of telephone or audio conversation with an authorized pass code holder or other authorized person for the protected premises to verify that no emergency exists.

1.4

Notification Call

The call to the law enforcement authority, such as police, fire emergency or medical emergency rescue.

1.5

Dispatch

Notification of law enforcement agency as defined in 1.3. a guard, guards, a runner, runners, other response entities or predetermined combination of the above to respond to the premises.

1.6

Special Instructions

A specific set of instructions to be followed in the event of an alarm, between the monitored premises and the alarm/monitoring company.

1.7

Audio Appliance

INSERT DEFINITION

1.8

Security Appliance

INSERT DEFINITION

1.9

Alarm Event

INSERT DEFINITION

2 Standard Verification Procedures for Burglar Alarm Signals

2.1 Procedures for Alarm Signals Received from Systems without “UL Certificated” Service

Unless Special Instructions exist, monitoring facility personnel shall communicate via the audio verification system with the protected premises for identification and verification of persons

authorized to be on the customer's premises and/or listen to the sounds that indicate something out of the ordinary is apparently happening. [how does this apply to one way?](#)

Two-Way Audio Verification

To insure all reasonable efforts are expended in attaining a verification of an alarm condition and avoiding the necessity for a dispatch the following best practices must be carried out:

2.1.1 Initial Verification Session [\(should this be defined as 2 way or one way in separate sections?\)](#)

Upon receipt of an alarm condition the central station operator will initiate the audio session according to the manufacturers stated command set (most current manufacturers comply with the SIA Audio Verification Standard command set). Upon initiation the central station operator will challenge the user on the premises for a valid code pursuant to industry stated protocol. Upon acknowledgment of valid code, alarm dispatch will be avoided and the central station operator can continue to communicate with the verified, valid user on premises.

2.1.2 If No Contact or Wrong Code

If there is no response or non-communication with the premises via the two-way audio session, the monitoring facility personnel shall make a Notification Call. The operator will disconnect the two-way audio session via manufacturers stated command set. Upon proper termination the operator will dial the second stated verification number provided by the subscriber.

Upon acknowledgment of valid code, alarm dispatch will be avoided and central station operator can continue to communicate with the verified, valid user on premises.

2.1.3 If Audio Communication is Established

If contact is made via the audio verification system, the monitoring facility personnel shall obtain pass code verification or other electronic identification that the person is authorized to be on the premises. Upon receipt of correct identification, and the authorized person states that no emergency exists, responding entities shall not be notified or shall be recalled, if already notified, and the alarm is considered aborted.

2.1.4 No Code

If no code or authorization is provided, the monitoring facility personnel shall attempt to reach an authorized person off premises to verify the authenticity of the on premises person, and failing that shall make a Notification Call. Further explanatory material on this can be found in Annex A.

2.1.5 Wrong Code

If the person(s) contacted cannot be identified by a valid identification code within a reasonable time after the contact as defined in 2.1.2, the monitoring facility personnel shall make a Notification Call.

Listen-In or Listen Back or One-Way Audio

TBD

2.2 Procedures for Alarm Signals Received from Systems with “UL Certificated” Service

Deleted: **Impact Activated Audio**
(Initiation by Frank and Gary)¶
TBD¶

Signals received from certificated systems shall be handled in accordance with the procedures defined in UL Standard 827, UL 2050, ULC S301 or ULC S304.

3 Enhanced Audio Verification of Burglar Alarm Signals

3.1 Extended Time

The maximum time permitted for enhanced verification of a non-certificated system can be extended beyond the time constraints imposed for certificated systems defined in UL 827, UL 2050, ULC S301 or ULC S304.

3.2 Procedure

For burglary alarm signals received from non-certificated commercial burglary alarm systems or any residential alarm system, the following procedures shall be followed (further explanatory material on this can be found in Annex A):

3.2.1 Audio Verification Session (Attempt #1)

The monitoring facility shall attempt an audio verification with the protected premises after receipt of the alarm signal. The procedure defined in 2.1.2 above shall be followed if audio contact is made with premises. Otherwise proceed to 3.2.2 or 3.2.3, whichever is applicable.

3.2.2 Attempt (Call) #2 Other Than Premises

When monitoring facility personnel can not attain contact or verification during the first attempt to the protected premises, a second attempt via a standard telephone call shall be made to an alternate phone number such as a cellular or work number and if the authorized person states that no emergency exists, responding entities shall not be notified or shall be recalled, if already notified, and the alarm considered aborted.

3.3 Answering Machines

When any call reaches an answering machine a message shall be left, clearly stating that it is the alarm company calling and leaving necessary information for the alarm user to promptly contact the monitoring facility.

3.4 Scheduled Events

If an alarm signal is received in connection with a scheduled opening or closing event, additional telephone numbers (doesn't qualify how many?) shall be called on the call list in order to determine whether the alarm signal is caused by an opening or closing error. If no answer or no determination can be made that a false alarm exists, a Notification Call shall occur.

Comment: This was taken from CS-V-01

3.5 Verified False

If the alarm is verified as being false during the first, second or succeeding calls, monitoring facility personnel shall suspend activities relating to the specific signal being worked.

3.6 Call Lists and Priority

Following the Notification Call, attention shall be placed on contacting the emergency call list, until someone is reached to achieve a cancellation of the notification if it is determined that no emergency exists.

3.7 Compliance with Enhanced Call Verification

The Audio verification procedure defined in 3.2.1 shall be permitted in place of or in addition to the second verification call and shall be considered in compliance with the CSAA's published Enhanced Verification Standard (CS-V-01).

4 Hold-Up

4.1 Commercial Hold-Up Alarm

Unless otherwise noted by Special Instructions, the monitoring facility shall not call the protected premises but shall make a Notification Call.

4.2 Residential Panic/Duress/Emergency Alarm

The monitoring facility shall follow the Standard Verification Procedures as defined in section 2.0.

Annex A (Informative)

A.2.1.2.1

If the monitoring facility personnel reaches the protected premises on the first or second call and the person answering the phone does not have the proper code then, if possible, the personnel may attempt to make a 3-way call with the premises person retained as a party to the call. The monitoring facility personnel may attempt to reach others on the call list to verify the authenticity of the person on the protected premises. If this process fails to resolve the issue then the monitoring facility personnel should proceed to make a Notification Call.

A 3.2

Verification Phone Accessibility Guideline. Care should be taken to verify that the emergency call list phone numbers are to phones without call waiting, or alternately that *70 is programmed in front of the monitoring center phone number in the electronic digital communicator. The verification phones at the monitored premises should be accessible after hours (not locked up in an office), such as in the vicinity of commonly used entrances and not be sent to voice mail after hours so the after hours users and cleaning people can hear and answer the phone.

A 5.1

NFPA #72 states that "This code {Household Warning Equipment} is primary concerned with life safety, not with the protection of property. It presumes that the family has an exit plan."

A.5.2 Coverage

Installation of microphones and/or speakers must be installed to provide adequate coverage of the premise and in compliance with manufacturer's recommendations and instructions.

A.5.3 Testing procedures

A.5.4 Operator Test

A.5.5 Site Test

A.6.1 Surreptitious recording

Of the 50 states, 38, as well as the District of Columbia, allow you to record a conversation to which you are a party without informing the other parties you are doing so. Federal wiretap statutes also permit one-party-consent recording of telephone conversations in most circumstances.¹ twelve states forbid the recording of private conversations without the consent of all parties. Those states are California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania and Washington.²

The federal wiretap law, passed in 1968, permits surreptitious recording of conversations when one party consents, "unless such communication is intercepted for the purpose of committing any criminal or tortuous act in violation of the Constitution or laws of the United States or of any State." Amendments signed into law in 1986 and 1994 expand the prohibitions to unauthorized interception of most forms of electronic communications, including satellite transmissions, cellular phone conversations, computer data transmissions and cordless phone conversations.

Most states have copied the federal law. Some expand on the federal law's language and prohibit all surreptitious recording or filming without the consent of all parties. Some state statutes go even further, prohibiting unauthorized filming, observing and broadcasting in addition to recording and eavesdropping, and prescribing additional penalties for divulging or using unlawfully acquired information, and for trespassing to acquire it. In most states, the laws allow for civil as well as criminal liability.

Many of the state statutes make possession of wiretapping devices a crime even though one-party consent to taping conversations may be allowed.

Most of the state statutes permit the recording of speeches and conversations that take place where the parties may reasonably expect to be recorded. Most also exempt from their coverage law enforcement agencies and public utilities that monitor conversations and phone lines in the course of their businesses.

In general, state statutes apply to conversations that take place within a single state.

When the conversation is between parties in states with conflicting eavesdropping and wiretapping laws, federal law generally applies, although either state also may choose to enforce its laws against a violator.

If a reporter in a state that allows one-party consent taping calls a party in a state that requires two-party consent, and tapes the conversation surreptitiously — which is legal under federal law — a state with tough laws prohibiting unauthorized recording may choose to apply its laws regardless of the location of the caller or the existence of a preemptive federal statute. Unfortunately, it is still unclear whether courts will hold that the federal protection preempts the state law.³ It is important to know your state law and the law in the state into which you call before you record surreptitiously.

The federal law and many state laws make it illegal to possess and particularly to publish the contents of an illegal wiretap. Some states that allow recordings make the distribution or publication of those otherwise legal recordings a crime. The U.S. Supreme Court ruled in *Bartnicki v. Vopper* in May 2001 that the media could not be held liable for damages under the federal statute for publishing or broadcasting information that the media obtained from a source who had conducted an illegal wiretap. The recording related to a local union leader's proposal to conduct violent acts in the area. The Court ruled that any claim of privacy in the recorded information was outweighed by the public's interest in a matter of serious public concern.⁴ The Court did not indicate whether disclosure by the media under different circumstances would be considered legal.

The Federal Communications Commission also has adopted a policy, known as the "Telephone Rule."⁵ It requires a reporter who tapes a telephone conversation that will later be broadcast to inform the other party that the tape is intended for broadcast.

Notes

1. 18 U.S.C. § 2510 et seq. (1999) (*Wire and Electronic Communications Interception and Interception of Oral Communications*).

2. Cal. Penal Code §§ 631, 632; Conn. Gen. Stat. § 52-570d; Fla. Stat. Ann. § 934.03; Ill. Rev. Stat. ch.720, para. 5/14-1 to 5/14-6; Md. Code Ann., Cts. & Jud. Proc. § 10-402; Mass. Ann. Laws ch. 272, § 99; Mich. Comp. Laws § 750.539c; Mont. Code Ann. § 45-8-213; Nev. Rev. Stat. Ann. § 200.620, as interpreted in *Lane v. Allstate Ins. Co.*, 969 P.2d 938 (Nev. 1998) (holding that Nevada wiretap statute requires all-party consent); N.H. Rev. Stat. Ann. § 570-A:2; 18 Pa. Cons. Stat. Ann. §§ 5703, 5704; Wash. Rev. Code § 9.73.030.

3. See, e.g., *Krauss v. Globe Int'l, Inc.*, No. 18008-92 (N.Y. Sup.Ct. Sept. 11, 1995) (holding New York law applies to interstate phone call where injury occurred in New York).

4. *Bartnicki v. Vopper*, 121 S. Ct. 1753 (2001).

5. 47 C.F.R. § 73.1206 (1989).