



INTERNATIONAL TELECOMMUNICATION UNION

**ITU-T**

**H.235  
Implementors'  
Guide**

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

(5 August 2005)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS  
Systems aspects

---

**Implementors Guide for H.235 V3: “Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals”**

---

## **Summary**

This document is a compilation of reported defects identified in Version 3 of ITU-T Recommendation H.235, which comprises: H.235 (2003-08), H.235 Corrigendum 1 (2005-01), H.235 Amendment 1 (2004-04) and H.235 Amendment 2 (2005-01). It must be read in conjunction with the Recommendations to serve as an additional authoritative source of information for implementers.

It should be noted that H.235 V3 has been superseded by H.235 V4, and this Implementors' Guide is provided solely as assistance to implementors of H.235 V3. The changes, clarifications and corrections defined herein have been included in H.235 V4.

In particular, this Implementors' Guide addresses errors found in H.235 (2003) Annex D, in H.235 (2004) Amendment 1 Annex H and in Annex I.

This Implementors' Guide contains all updates submitted upto and including those at Study Group 16 meeting, July/August 2005, in Geneva (TD 147/PLEN), and was approved on 5 August 2005.

## Contact Information

---

ITU-T Study Group 16 / Rapporteur Question 25/16	Martin Euchner Siemens AG Hofmannstr 51 81359 Munich, Germany	Tel: +49 89 722 5 57 90 Fax: +49 89 722 6 23 66 E-mail: <a href="mailto:martin.euchner@siemens.com">martin.euchner@siemens.com</a>
Editor ITU-T Rec. H.235	Martin Euchner Siemens AG Hofmannstr 51 81359 Munich, Germany	Tel: +49 89 722 5 57 90 Fax: +49 89 722 6 23 66 E-mail: <a href="mailto:martin.euchner@siemens.com">martin.euchner@siemens.com</a>

---

## Table of Contents

<b>1</b>	<b>INTRODUCTION</b> .....	<b>1</b>
<b>2</b>	<b>SCOPE</b> .....	<b>1</b>
<b>3</b>	<b>REFERENCES</b> .....	<b>1</b>
<b>4</b>	<b>NOMENCLATURE</b> .....	<b>2</b>
	<b>DESCRIPTION</b> .....	<b>2</b>
<b>5</b>	<b>TECHNICAL AND EDITORIAL CORRECTIONS TO H.323 SERIES RECOMMENDATIONS</b> .....	<b>2</b>
5.1	CORRECTIONS TO H.235 (2003) ANNEX D “BASELINE SECURITY PROFILE” .....	2
5.2	CORRECTIONS TO H.235 (2003) ANNEX H “FRAMEWORK FOR SECURE AUTHENTICATION IN RAS USING WEAK SHARED SECRETS” .....	3
5.3	CORRECTIONS TO H.235 (2003) ANNEX I “SUPPORT OF DIRECT-ROUTED CALLS” .....	3

# **IMPLEMENTORS' GUIDE FOR ITU-T H.235: "SECURITY AND ENCRYPTION FOR H-SERIES (H.323 AND OTHER H.245-BASED) MULTIMEDIA TERMINALS"**

## **1 Introduction**

This document is a compilation of reported defects identified in Version 3 of ITU-T Recommendation H.235 (2003-08) and its Corrigendum 1 (2005-01) and Amendments 1 (2004-04) and 2 (2005-01). It should be noted that H.235 V3 has been superseded by H.235 V4, and this Implementors' Guide is provided solely as assistance to implementors of H.235 V3. It must be read in conjunction with the Recommendations to serve as an additional authoritative source of information for implementers. The changes, clarifications and corrections defined herein have been included in H.235 V4.

Upon discovering technical defects with any components of H.235 Version 3, please provide a written description directly to the editor of the Recommendation, with copy to the Rapporteur of Q.25/16. The template for a defect report is located at the end of the Guide. Contact information for these parties is included at the front of the document. Return contact information should also be supplied so a dialogue can be established to resolve the matter and an appropriate reply to the defect report can be conveyed. This defect resolution process is open to any interested party. Formal membership in the ITU is not required to participate in this process.

## **2 Scope**

This guide resolves defects in the following categories:

- editorial errors
- technical errors, such as omissions and inconsistencies
- ambiguities

In addition, the Implementors' Guide may include explanatory text found necessary as a result of interpretation difficulties apparent from the defect reports.

This Guide will not address proposed additions, deletions, or modifications to the Recommendations that are not strictly related to implementation difficulties in the above categories. Proposals for new features should be made in through contributions to the ITU-T.

## **3 References**

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation

- ITU-T Recommendation H.235 (2003-08), Security and encryption for H Series (H.323 and other H.245 based) multimedia terminals
- ITU-T Recommendation H.235 (2003) Amendment 1 (2004-04)

- ITU-T Recommendation H.235 (2003) Amendment 2 (2005-01) “Annex G: Usage of the MIKEY key management protocol for the secure real time transport protocol (SRTP) within H.235”
- ITU-T Recommendation H.235 (2003) Corrigendum 1 (01/05)

#### 4 Nomenclature

In addition to traditional revision marks, the following marks and symbols are used to indicate to the reader how changes to the text of a Recommendation should be applied:

<b>Symbol</b>	<b>Description</b>
<u>[Begin Correction]</u>	Identifies the start of revision marked text based on extractions from the published Recommendations affected by the correction being described.
<u>[End Correction]</u>	Identifies the end of revision marked text based on extractions from the published Recommendations affected by the correction being described.
...	Indicates that the portion of the Recommendation between the text appearing before and after this symbol has remained unaffected by the correction being described and has been omitted for brevity.
--- SPECIAL INSTRUCTIONS --- {instructions}	Indicates a set of special editing instructions to be followed.

#### 5 Technical and Editorial Corrections to H.323 Series Recommendations

##### 5.1 Corrections to H.235 (2003) Annex D “Baseline security profile”

<b>Description:</b>	The current text describing the detection of the use of Procedure I supplied in Note 7 is incorrect. The text below supplies the correction.
---------------------	--

[Begin Correction]

...

##### D.6.3.2 Symmetric-key-based signalling message authentication details (procedure I)

...

NOTE 7 – The recipient is able to detect usage of procedure I by evaluating the **tokenOID** within the hashed **EncodedGeneralToken** (detecting presence of "A").

Deleted: B

...

[End Correction]

**5.2 Corrections to H.235 (2003) Annex H “Framework for secure authentication in RAS using weak shared secrets”**

**Description:** The size of initialization vector used in the Symmetric Encryption algorithm for SP1 specified in Annex H.7/H.235 Amendment 1 is incorrect. The text below supplies the correction.

*[Begin Correction]*

...

**H.7 A Specific Security Profile (SP1)**

...

- Master key,  $K_m$ , negotiation: Diffie-Hellman key exchange using the OAKLEY well-known group 2 [RFC 2412], followed by the SHA1 hash reduction of the Diffie-Hellman secret:  $K_m = \text{SHA1}(\text{Diffie-Hellman shared secret})$ .
- Symmetric encryption algorithm: shall be AES-128 in segmented counter mode with a 2-octet party discriminator,  $D$ , a 12-octet initialization vector,  $IV$ , and a 2-octet counter field,  $C$ , such that  $\text{counter} = D \parallel IV \parallel C$ , and  $C = 0$  initially. See [NIST 800-38A] for a description of CTR mode. The party discriminator,  $D$ , is set to 0x3636 when the  $IV$  is generated by the party which issued the GRQ/RRQ, or LRQ, and is set to 0x5c5c when the  $IV$  is generated by the party which responded with GCF/RCF, or LCF. Each party must insure that each  $IV$  it generates is unique; it may use its own method to insure this uniqueness.
- Diffie-Hellman key encryption: shall use the AES-128 segmented counter mode to encrypt the Diffie-Hellman public key (represented as an octet string in network byte order); the initialization vector shall be carried in **ClearToken.initVect**, and the 16-octet key,  $K_p$ , shall be constructed as the high-order 128 bits of the SHA1 hash of the user password:  $K_p = \text{Trunc}(\text{SHA1}(\text{user password}), 16)$ , where  $\text{Trunc}(x,y)$  truncates octet string  $x$  to  $y$  octets. Note that this is typically considered a weak key.

...

*[End Correction]*

**5.3 Corrections to H.235 (2003) Annex I “Support of direct-routed calls”**

**Description:** The text below provides various corrections to the Procedure DRC specified in Annex I/H.235 Amendment 1 and Annex I/H.235 Corrigendum 1.

*[Begin Correction]*

...

**I.9 Procedure DRC**

...

Deleted: 4

Gatekeeper H shall generate a random Challenge-B, encryption key material  $EK_{BH}$  and salting key material  $KS_{BH}$  from the shared secret  $K_{BH}$  using the PRF-based key derivation procedure as defined in I.10 where Challenge-B is substituted as **challenge** and

$CT_{HG} \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow keyDerivationOID$  shall hold "AnnexI-HMAC-SHA1-PRF"; see I.12.

Deleted: V3KeySyncMaterial →

$EK_{GH}$  denotes the encryption key and  $KS_{GH}$  denotes the salting key that are shared between gatekeeper G and gatekeeper H. Gatekeeper H shall generate one random Challenge-G. Gatekeeper H shall generate encryption key material  $EK_{GH}$  and salting key material  $KS_{GH}$  from the shared secret  $K_{GH}$  using the PRF-based key derivation procedure as defined in clause 11 where Challenge-G is substituted for **challenge**.  $CT_{HG} \rightarrow challenge$  shall hold challenge-G, the endpoint ID of the endpoint B shall be set in  $CT_{HG} \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow generalID$ .

Deleted: →V3KeySyncMaterial

Gatekeeper H shall transmit the encrypted  $EK_{BH}$  and the encrypted  $KS_{BH}$  to gatekeeper G. The enhanced OFB (EOFB) encryption mode (see B.2.5) shall be used with the secret, endpoint-specific salting key  $KS_{GH}$ . Applicable encryption algorithms are (see D.11):

...

For the EOFB encryption mode, gatekeeper H shall generate a random initial value IV. For OID "X1", OID "Y1" and OID "Z1" the IV has 64 bits and shall be conveyed within

$CT_{HG} \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow params \rightarrow iv8$ ; whereas the IV has 128 bits for OID "Z2" and shall be conveyed within  $CT_{HG} \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow params \rightarrow iv16$ .

Deleted: →V3KeySyncMaterial

Deleted: →V3KeySyncMaterial

Gatekeeper H shall include  $ENC_{EK_{GH}, KS_{GH}, IV}(EK_{BH})$  and  $ENC_{EK_{GH}, KS_{GH}, IV}(KS_{BH})$  in ClearToken  $CT_{HG}$  with **tokenOID** set to "I3". The obtained ciphertext  $ENC_{EK_{GH}, KS_{GH}, IV}(EK_{BH})$  shall be conveyed in

$CT_{HG} \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow encryptedSessionKey$ ; the obtained ciphertext  $ENC_{EK_{GH}, KS_{GH}, IV}(KS_{BH})$  shall be conveyed in

Deleted: →V3KeySyncMaterial

$CT_{HG} \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow encryptedSaltingKey$ . The encryption algorithm shall be indicated in  $CT_{HG} \rightarrow h235Key \rightarrow algorithmOID$  ("X1", "Y1", "Z1" or "Z2"). Challenge-B shall be placed within  $CT_{HG} \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow clearSaltingKey$ .

Deleted: V3KeySyncMaterial

Deleted: V3KeySyncMaterial

$CT_{HG} \rightarrow generalID$  shall be set to the gatekeeper identifier G whereas  $CT_{HG} \rightarrow sendersID$  shall be set to the gatekeeper identifier H.

Challenge-B shall be conveyed to endpoint B by inclusion of a **profileInfo** within the ClearToken  $CT_{HG} \rightarrow profileInfo \rightarrow elementID = 0$  that identifies this particular profile element:

$CT_{HG} \rightarrow profileInfo \rightarrow paramS$  left unused and  $CT_{HG} \rightarrow profileInfo \rightarrow element \rightarrow octets$  shall hold Challenge-B.

The LCF response shall hold the ClearToken  $CT_{HG}$ .

...

Two ClearTokens shall be included, one  $CT_A$  for the caller A and another one  $CT_B$  for the callee B. Each **ClearToken** shall contain an OID ("I1" or "I2") within **tokenOID** that indicates whether the token is destined for the caller (OID "I1" for  $CT_A$ ) or for the callee (OID "I2" for  $CT_B$ ).

GK G shall decrypt  $CT_{HG} \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow encryptedSessionKey$  to obtain  $EK_{BH}$  and shall decrypt  $CT_{HG} \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow encryptedSaltingKey$  to obtain  $KS_{BH}$ .

The **ClearToken** as defined in this annex may be used in conjunction with other security profiles such as with Annex D or with Annex F that deploy **ClearTokens** as well.

...

The encryption keys  $EK_{AG}$  and  $EK_{BH}$  for the encrypted end-to-end key  $K_{AB}$  shall be derived from the shared secret between the gatekeeper and the endpoints ( $EK_{AG}$  or  $EK_{BH}$ ) using the PRF-based key derivation procedure as defined in clause I.10 where both

$CT_A \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow keyDerivationOID$  and

$CT_B \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow keyDerivationOID$  shall hold "Amptex-I-HMAC-SHA1-PRF", see clause I.12 and  $CT_A \rightarrow challenge$  shall hold Challenge-A.

Deleted: V3KeySyncMaterial

Deleted: V3KeySyncMaterial

Gatekeeper G shall copy Challenge-B from

$CT_{HG} \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow clearSaltingKey$  into  $CT_B \rightarrow challenge$ .

Deleted: V3KeySyncMaterial

$CT_B \rightarrow profileInfo$  shall hold the profile element that was conveyed in  $CT_{HG} \rightarrow profileInfo$  such that in the end endpoint B obtains Challenge-B.

This session secret  $K_{AB}$  shall be encrypted by  $EK_{AG}$  (for CT destined to endpoint A) or by  $EK_{BH}$  (for the CT destined to endpoint B) using an encryption algorithm.

...

For the EOFB encryption mode, the gatekeeper G shall generate a random initial value IV. For OID "X1", OID "Y1" and OID "Z1" the IV has 64 bits and shall be conveyed within

$CT_A \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow params \rightarrow iv8$  and within

$CT_B \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow params \rightarrow iv8$ ; whereas the IV has 128 bits for OID "Z2" and shall be conveyed within  $CT_A \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow params \rightarrow iv16$  and within

$CT_B \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow params \rightarrow iv16$ .

Deleted: V3KeySyncMaterial

Deleted: V3KeySyncMaterial

Deleted: V3KeySyncMaterial

Deleted: V3KeySyncMaterial

The obtained ciphertext  $ENC_{EK_{AG}, KS_{AG}, IV}(K_{AB})$  shall be conveyed in

$CT_A \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow encryptedSessionKey$  and  $ENC_{EK_{BH}, KS_{BH}, IV}(K_{AB})$  shall

then be conveyed in  $CT_B \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow encryptedSessionKey$ . The

encryption algorithm shall be indicated in  $CT_A \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow algorithmOID$

and in  $CT_B \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow algorithmOID$  ("X1", "Y1", "Z1" or "Z2").

Deleted: V3KeySyncMaterial

Deleted: V3KeySyncMaterial

Deleted: V3KeySyncMaterial

Deleted: V3KeySyncMaterial

For the ClearToken destined to endpoint A, the endpoint identifier of endpoint B ( $EPID_B$ ) shall be placed within  $CT_A \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow generalID$ . Likewise for the ClearToken destined to endpoint B, the endpoint identifier of endpoint A ( $EPID_A$ ) shall be placed within

$CT_B \rightarrow h235Key \rightarrow secureSharedSecret \rightarrow generalID$ .

Deleted: V3KeySyncMaterial

Deleted: V3KeySyncMaterial

...

If the received  $CT_A$  was verified as being fresh, endpoint A shall retrieve the IV and compute  $EK_{AG}$  and  $KS_{AG}$  as described above for the gatekeeper G. Endpoint A shall decrypt the **encryptedSessionKey** information found within  $secureSharedSecret$  of  $CT_A$  to obtain  $K_{AB}$ .

Deleted: V3KeySyncMaterial

...

Endpoint B shall verify that the obtained  $CT_B$  is fresh by checking the **timestamp**. Further security checks shall verify the **sendersID** of the ClearToken and **generalID** within  $secureSharedSecret$ . If the received  $CT_B$  was verified as being fresh, endpoint B shall retrieve Challenge-B from  $CT_{HG} \rightarrow profileInfo \rightarrow element \rightarrow octets$ , and retrieve the IV and compute  $EK_{BHG}$  and  $KS_{BH}$ . Challenge-B substituted as **challenge** in clause I.10 as described above for the gatekeeper. Endpoint B shall decrypt the **encryptedSessionKey** information found within  $secureSharedSecret$  of  $CT_B$  to obtain  $K_{AB}$ .

Deleted: V3KeySyncMaterial

Deleted:

Deleted: V3KeySyncMaterial

In case  $CT_B$  was verified as being fresh, endpoint B is able to proceed the call signalling by replying with CALL-PROCEEDING, ALERTING or CONNECT etc., as appropriate.

...

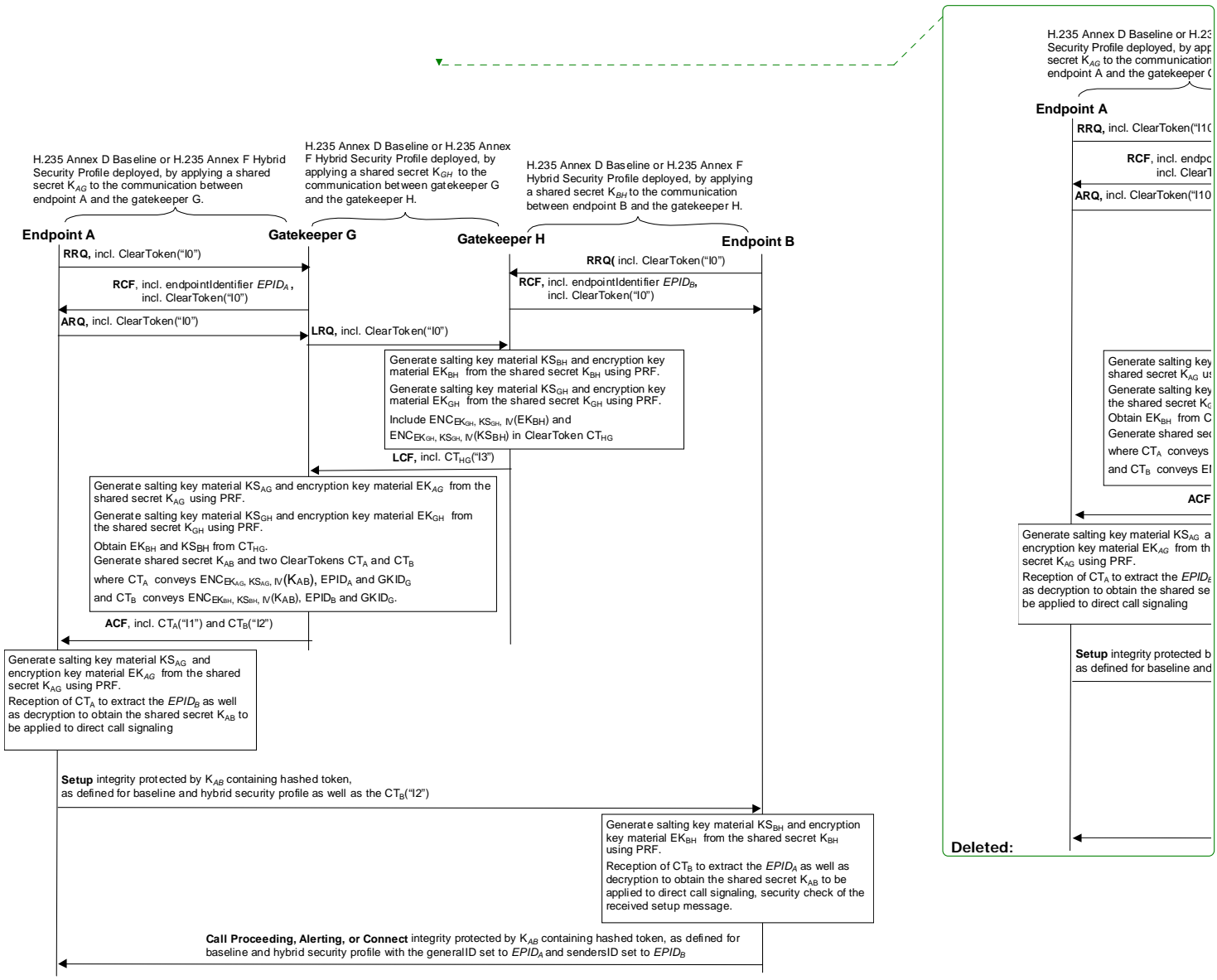


Figure I.2/H.235 – Basic communication flow

[End Correction]

**Annex: ITU-T Rec. H.235 Version 3 Defect Report Form**

<b>DATE:</b>	
<b>CONTACT INFORMATION</b>  <b>NAME:</b> <b>COMPANY:</b> <b>ADDRESS:</b>  <b>TEL:</b> <b>FAX:</b> <b>EMAIL:</b>	
<b>AFFECTED RECOMMENDATIONS:</b>	
<b>DESCRIPTION OF PROBLEM:</b>	
<b>SUGGESTIONS FOR RESOLUTION:</b>	

NOTE - Attach additional pages if more space is required than is provided above.

\_\_\_\_\_