

Contents

Special Report Notice Of Disclaimer	iii
List of Figures	viii
Foreword	ix
1. Overview	1-1
1.1 Purpose and Scope	1-2
1.2 Definition of Terms	1-3
1.3 History of Lawfully Authorized Electronic Surveillance	1-5
1.4 Structure and Organization	1-6
2. The Communications Assistance for Law Enforcement Act (CALEA)	2-1
2.1 What is CALEA?	2-1
2.2 Important Dates for CALEA Compliance	2-2
2.2.1 Dates for Core Assistance Capability Requirements	2-2
2.2.2 Date for Additional Assistance Capability Requirements	2-2
2.2.3 Date for Interim Packet Requirements	2-2
2.3 Impacted Entities	2-3
2.3.1 Telecommunications Service Providers (TSPs)	2-3
2.3.2 Telecommunications Equipment Manufacturers and Providers of Telecommunications Support Services	2-3
2.3.3 U.S. Attorney General	2-3
2.3.4 Federal Communications Commission (FCC)	2-4
2.3.5 Telecommunications Industry Association (TIA)	2-5
2.4 CALEA Implementation Guidelines	2-5
2.5 Reference List of CALEA Legislation	2-7
3. Lawfully Authorized Electronic Surveillance in a Circuit-Mode Environment	3-1
3.1 Lawful Access Capabilities	3-3
3.1.1 Core Assistance Capabilities	3-3
3.1.2 Additional Punch List Capabilities	3-4
3.2 CALEA Functional Model	3-5
3.2.1 TSP's Access Function	3-6
3.2.2 TSP's Delivery Function	3-6
3.2.3 TSP's Administration Function	3-7
3.2.4 LEA's Collection Function	3-7
3.2.5 LEA's Administration Function	3-7
3.3 Circuit-Mode Network Architectures to Support Lawful Surveillance	3-8
3.3.1 Integrated Network Architecture	3-8
3.3.1.1 Interfaces in the Integrated Architecture	3-10
3.3.1.1.1 Interface between TSP's IAP Switch and LEA's Collection System	3-10
3.3.1.1.2 Interface between TSP's IAP Switch and TSP's Surveillance Administration System (SAS)	3-13
3.3.1.1.3 Interface between LEA's Administration System and LEA's Collection System	3-13

3.3.1.2 Operations Issues	3-14
3.3.1.2.1 Security of Surveillances	3-14
3.3.1.2.2 Maintenance of Systems	3-14
3.3.1.2.3 Performance of the IAP Switch	3-15
3.3.1.3 Surveillance Administration System (SAS)	3-16
3.3.1.3.1 Configuration Management	3-17
3.3.1.3.2 Record Management	3-17
3.3.1.3.3 Security Management	3-17
3.3.1.3.4 Performance Management	3-18
3.3.1.3.5 Fault Management	3-19
3.3.2 Distributed Architecture	3-19
3.3.2.1 Distributed Architecture Interfaces	3-20
3.3.2.1.1 Interface between TSP's Platform Extension and TSP's Subject Switch	3-20
3.3.2.1.2 Interface between TSP's Platform Extension and LEA's Collection System	3-21
3.3.2.1.3 Interface between TSP's Platform Extension and TSP's SAS	3-21
3.3.3 Service Flow Examples	3-21
3.3.3.1 Basic Call Originating from a Subject	3-22
3.3.3.1.1 Call-Identifying Information Only, Punch List Items Included	3-22
3.3.3.1.2 Call-Identifying Information and Call Content, Punch List Items Not Included	3-23
3.3.3.2 Basic Call Terminating to a Subject, Call-Identifying Information Only, Punch List Item Included	3-24
3.3.3.3 Call Terminating to a Subject, Forwarded By Subject's Service to a Non- Subject, Call-Identifying Information Only, Punch List Items Not Included	3-25
4. Lawfully Authorized Electronic Surveillance in a Packet-Mode Environment	4-1
4.1 Usefulness of IP Header Information	4-2
4.1.1 IP Header Information - Background	4-2
4.1.2 Variability of IP Addresses	4-4
4.1.2.1 Dynamic Address Assignment	4-4
4.1.2.2 Network Address Translation (NAT)	4-5
4.1.2.3 Tunneling	4-6
4.1.2.4 Address Spoofing	4-8
4.1.3 Complexities that a Layered Protocol Introduces	4-8
4.2 Call Management Server (CMS) Architectures	4-10
4.2.1 VoIP Network Architecture with a CMS	4-10
4.2.2 Consideration for a Surveillance Solution	4-12
4.2.3 Variation in CMS Architectures	4-14
4.3 Non-CMS Architectures	4-15
4.3.1 Background	4-15
4.3.2 Potential Surveillance Solutions	4-17
4.3.2.1 Delivery of the Entire Packet Stream	4-17
4.3.2.2 Delivery of IP Header Information	4-18

4.3.2.3 Extraction of Information within the Packet	4-19
4.4 Other Challenges and Issues	4-20
4.4.1 Identification of the Subject	4-20
4.4.2 Types of Court Orders	4-20
4.4.3 Identifying the TSP	4-21
5. Summary	5-1
Appendix A: Bibliography and References	A-1
Appendix B: Glossary	B-1

List of Figures

Figure 1-1	Lawfully Authorized Electronic Surveillance Flow	1-2
Figure 1-2	Network-Based Intercepts	1-3
Figure 3-1	CALEA Functional Model	3-5
Figure 3-2	CALEA Integrated Architecture	3-9
Figure 3-3	SAS Support of CALEA IAP Switches	3-16
Figure 3-4	CALEA Distributed Architecture	3-19
Figure 3-5	Basic Subject-Originated Call (Call-Identifying Information Only); Punch List Items Italicized	3-22
Figure 3-6	Basic Subject-Originated Call (Call-Identifying Information and Call Content)	3-23
Figure 3-7	Basic Terminating Call to a Subject (Call-Identifying Information Only); Punch List item italicized	3-24
Figure 3-8	Terminating Call to a Subject (Call-Identifying Information Only), Call Forwarded by Subject's Service to Non-Subject	3-25
Figure 4-1	Packet Switching	4-3
Figure 4-2	Address Information in an IP Datagram	4-3
Figure 4-3	Dynamic Address Assignment	4-4
Figure 4-4	Example of Network Address Translation (NAT)	4-5
Figure 4-5	Example of Port Address Translation (PAT)	4-6
Figure 4-6	Example of Tunneling	4-7
Figure 4-7	Layers of IP Protocol Stack	4-8
Figure 4-8	IP versus Email Addresses	4-9
Figure 4-9	VoIP Network Architecture with a CMS	4-10
Figure 4-10	Connection-Oriented Protocol Session Establishment	4-15
Figure 4-11	Connectionless Protocol Routing	4-16
Figure 4-12	Identifying the Appropriate TSP	4-21