SS8 Lawful Intercept Briefing

SS8 Networks Overview

- Privately held company with 20+ years of operating history
- 12 years providing Law Intercept solutions
- Headquartered in San Jose, CA
- Market leader in lawful intercept delivery function solution
- 250 worldwide service provider customers
- OEM relationship with some of the largest equipment vendors (Lucent, Nortel, Alcatel)

Agenda

- What is Lawful Intercept (LI)
- How does it work
- Rules, Regulations and Successes

What is Lawful Intercept?

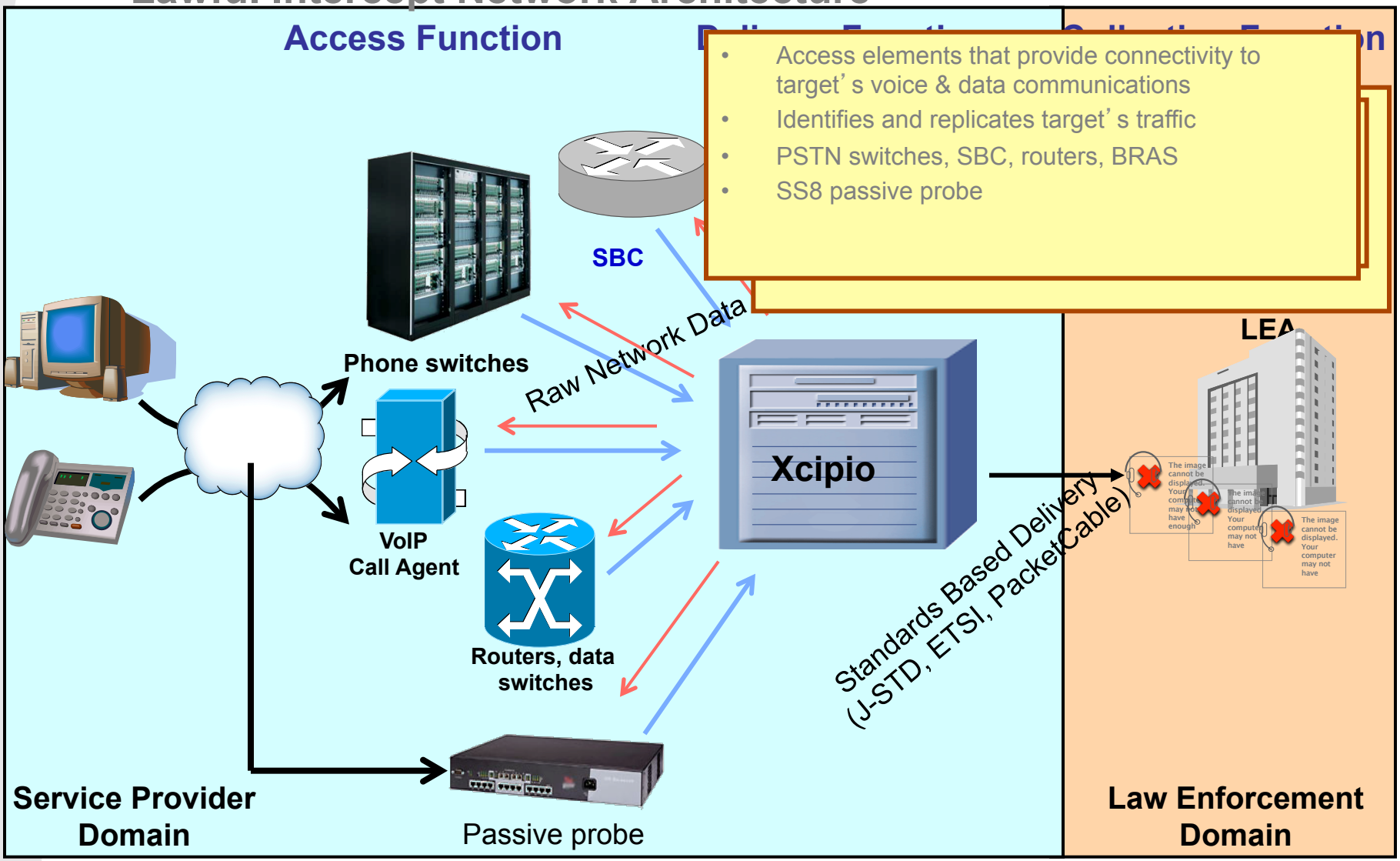
- The targeted intercept of voice and data services, by a service provider on the behalf of Law Enforcement, when authorized by a court

- Uses:
  - Criminal - Investigation and Prosecution of criminal activity
  - Intelligence Gathering - Investigation of individuals for Homeland security, anti-terrorism and other threats

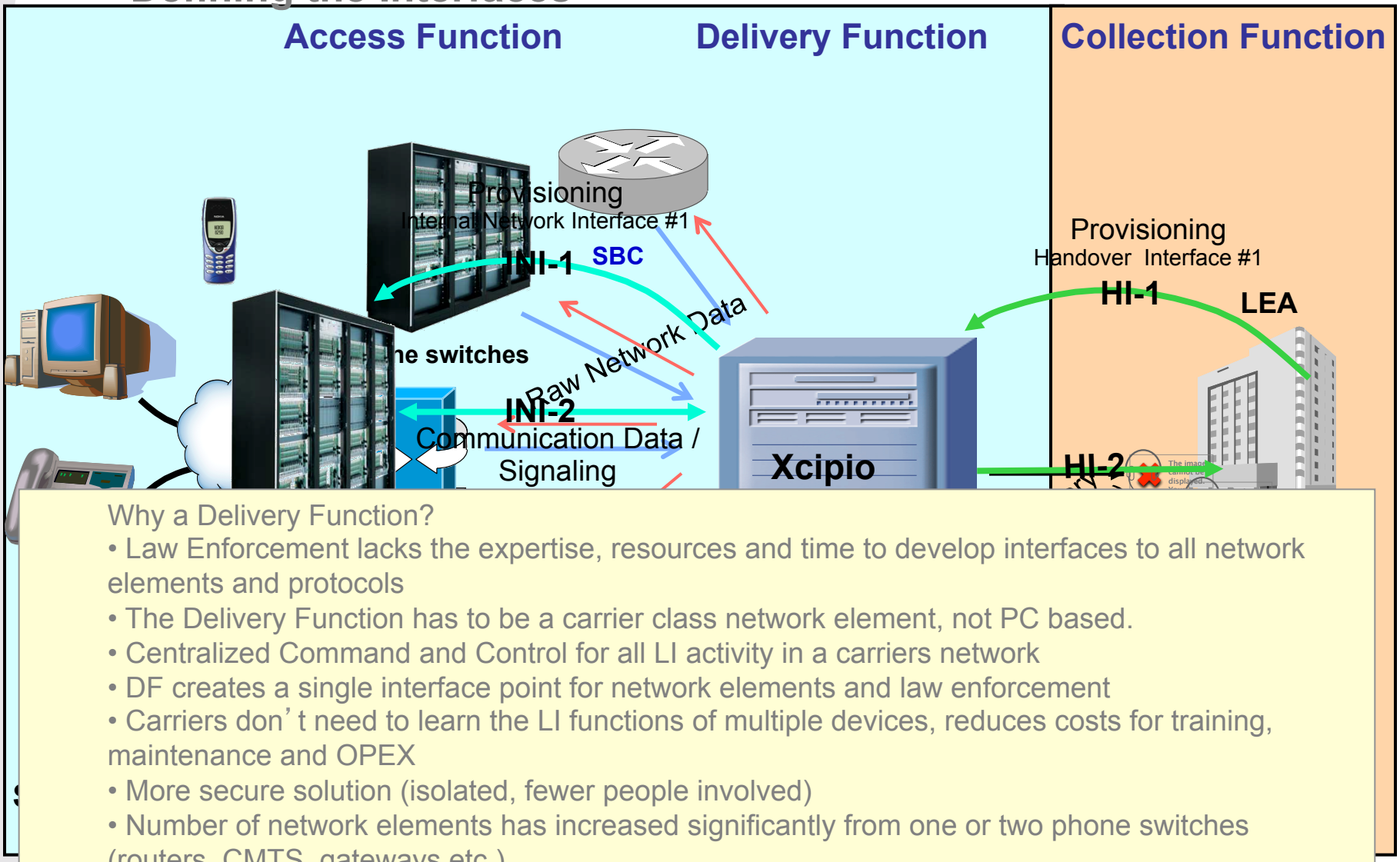
How is Lawful Intercept performed?

- **Identify the user**
  - Determine the target identifier (phone number, email address, IP address etc.)
- **Wait for authentication**
  - When the target utilizes the network they must be authenticated. Watch for that event.
- **Find the edge**
  - When the target authenticates, find the edge device closest to the target (so as not to miss any peer-to-peer transactions) and obtain a copy of the target's communications.

Lawful Intercept Network Architecture



Defining the Interfaces



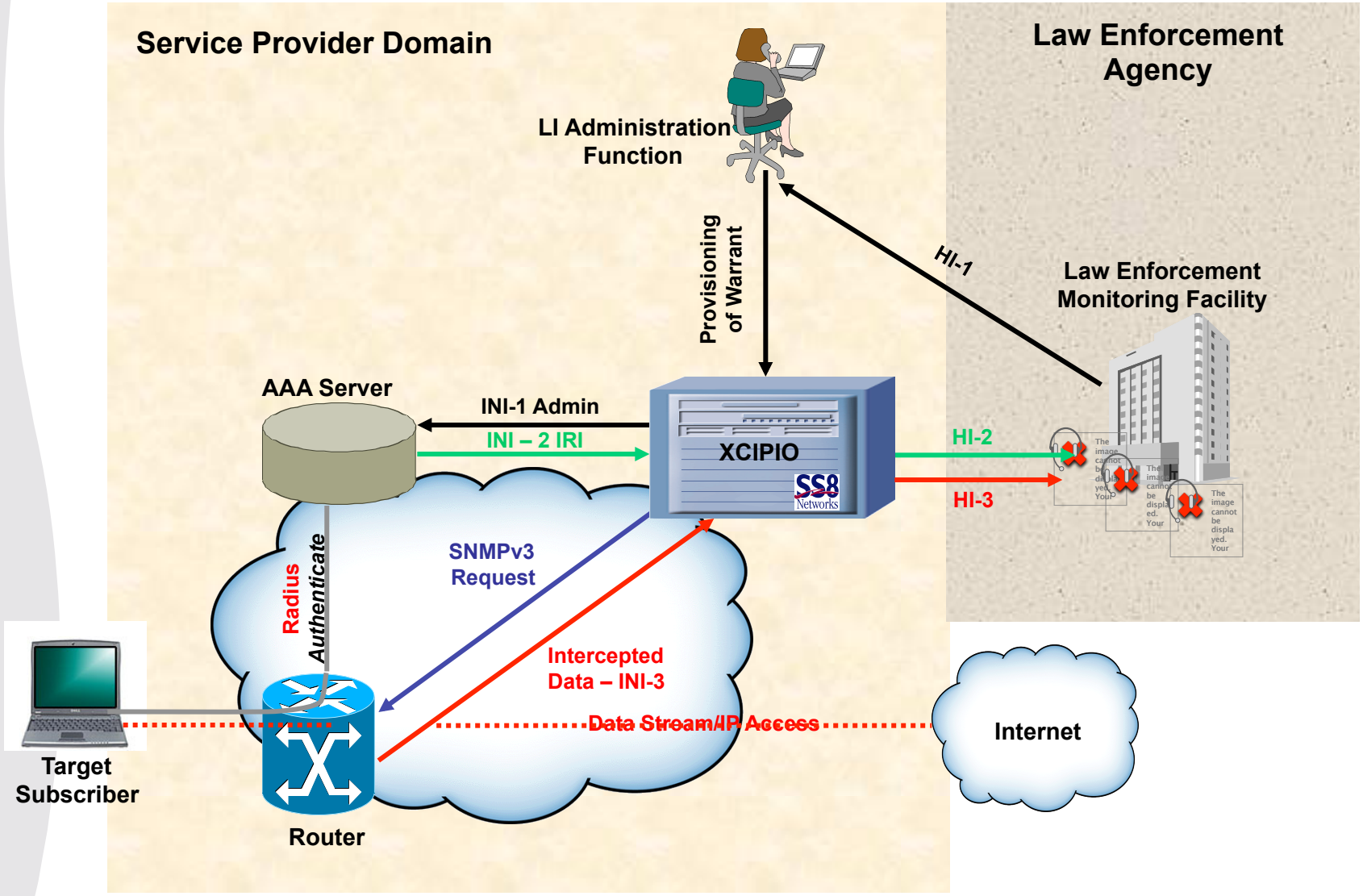
Why a Delivery Function?

- Law Enforcement lacks the expertise, resources and time to develop interfaces to all network elements and protocols
- The Delivery Function has to be a carrier class network element, not PC based.
- Centralized Command and Control for all LI activity in a carriers network
- DF creates a single interface point for network elements and law enforcement
- Carriers don't need to learn the LI functions of multiple devices, reduces costs for training, maintenance and OPEX
- More secure solution (isolated, fewer people involved)
- Number of network elements has increased significantly from one or two phone switches (routers, CMTS, gateways etc.)

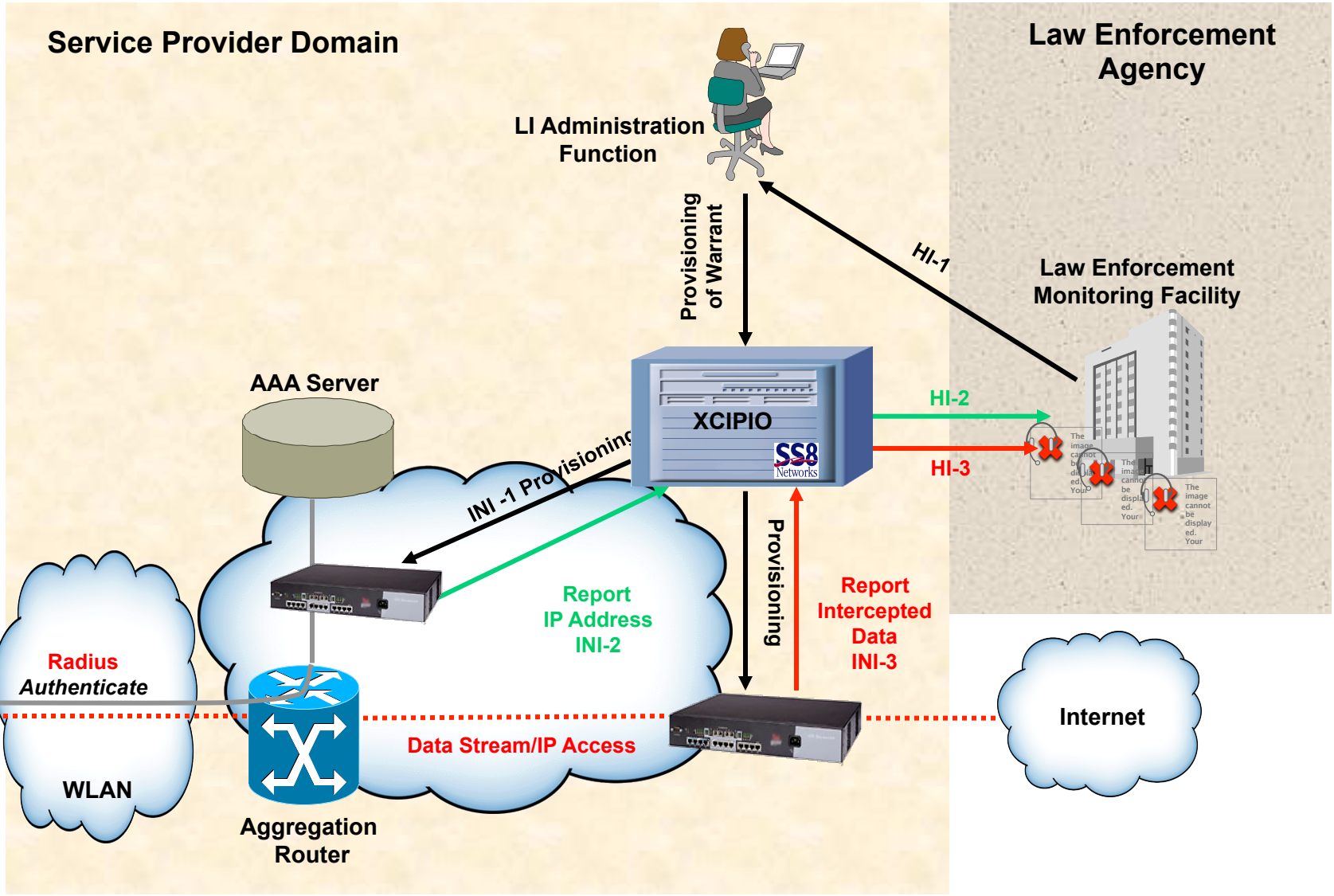
Methods for Lawful Intercept

- **Active Approach**
  - **Work with the** network equipment **manufacturers to develop lawful intercept capability in the network elements.**
  - **Utilize existing network elements for lawful intercept**
  - **Sometimes serious impact to network performance**
  - **No need for additional hardware**
- **Passive Approach**
  - **Use passive** probes or sniffers **as Access Function to monitor the network and filter target's traffic**
  - **Requires expensive additional hardware**
  - **No impact to the network performance**
- **Hybrid – utilizes both**

Active Approach to IP Data Intercept



Passive Approach to IP Data Intercept



Standards

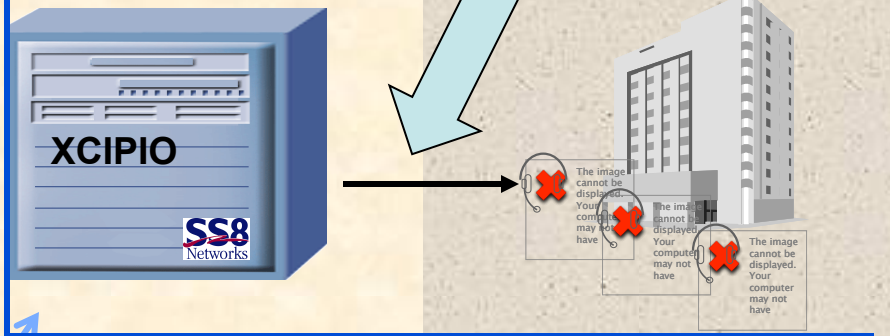
Standards: Impact and Use

Use:

- Mainly used to define how the DF communicates with the CF
- Initiated by US legislation called CALEA – Communications Assistance for Law Enforcement Act. This act required the Telecom industry to come up with standards for accessing and delivering intercepted communications to the LEAs.
- The standard they created is called J-STD-025, it describes how call data and call content is delivered to the CF from the DF.
- Before that custom solutions were developed or bought by Law Enforcement and placed at the service providers premises.
- Since J-STD was adopted several other standards have emerged:
- J-STD-25A – Punchlist
- J-STD-25B – CDMA2000 wireless data
- PacketCable – VoIP for Cable networks
- T1.678 – VoIP for wireline, PTT, PoC
- ETSI 33.108 – GPRS wireless data
- ETSI 102.232 – ISP data intercepts

Delivery Func

One exception is PacketCable. It also defines how the AFs in a cable network communicate with the DF



vironment without any ability to produce off-

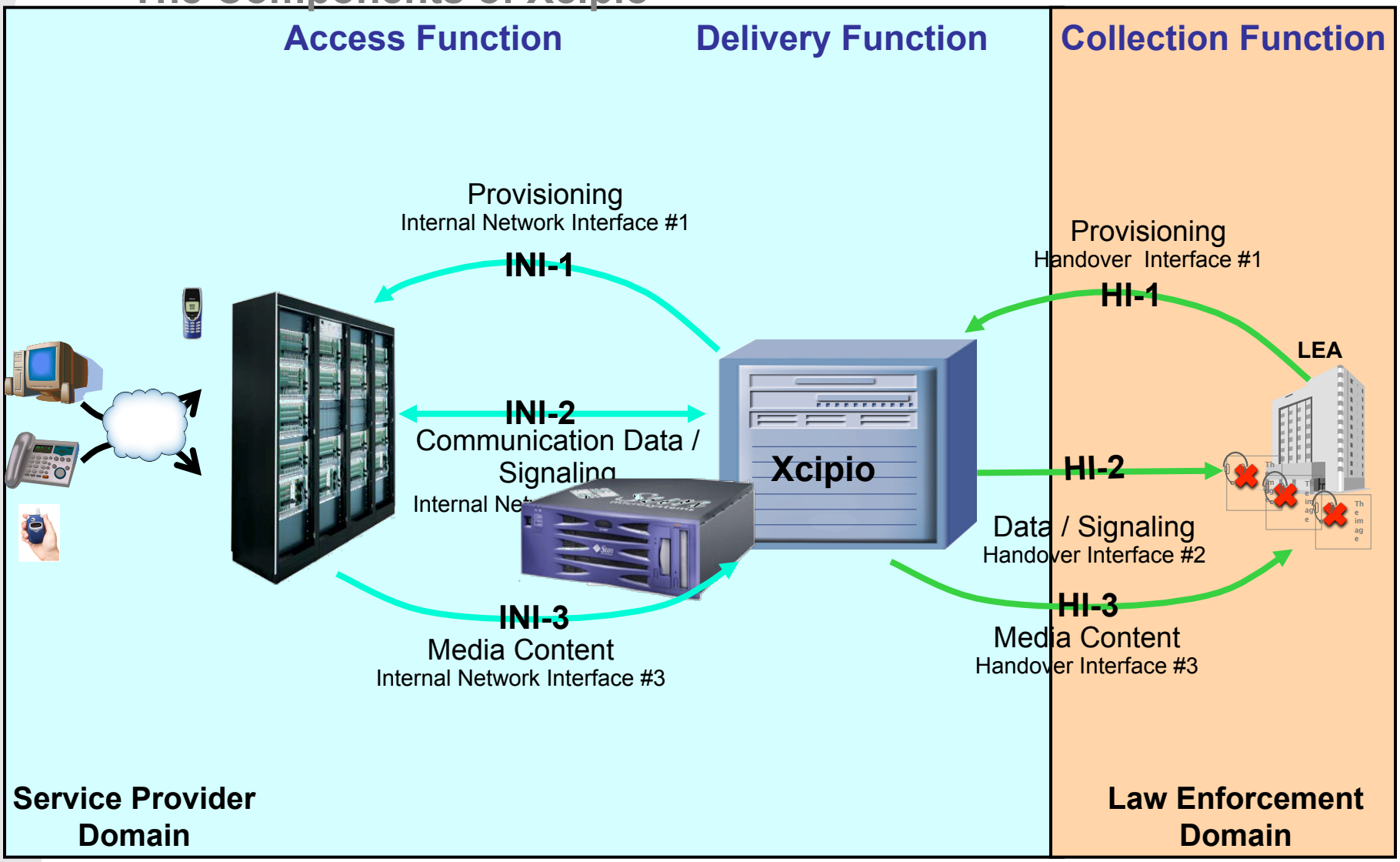
F), Collection Function (CF)

d the need for interfaces

SS8 Networks

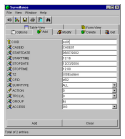
A bit about Xcipio

The Components of Xcipio



The Components of Xcipio

User Interface
Remote or local access to Xcipio



INI-1 Provisioning Element
Database, User Interface

INI-2 Intercept Engine
Call data, call events, signaling

LIS – Lawful Intercept Server
Core Software Application
- real-time processing -

Physical Layer
Sun servers, Ethernet connectivity,
IP packets, switch matrix cards

INI-3 Content Processor
Filters, encapsulates content
(IP, VoIP, TDM, HTTP etc.)

Provisioning Element:
Database, supports User Interface, maintains all warrant information, creates shared memory image of intercept information

HI-1

TCP/IP stacks, error logs, alarms, SNMP, Managed object structure etc.

HI-2

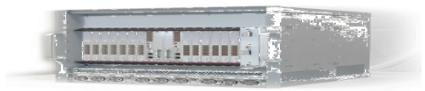
PE-2200
Software module

IE-2100
Software module

LIS
Software release

Primary Server

IP Packet processing



TDM Switch Matrix

Content Processor
processing, routing, replicating, identification, encapsulation, encryption and delivery of content (packet and/or TDM voice) to law enforcement in real-time.

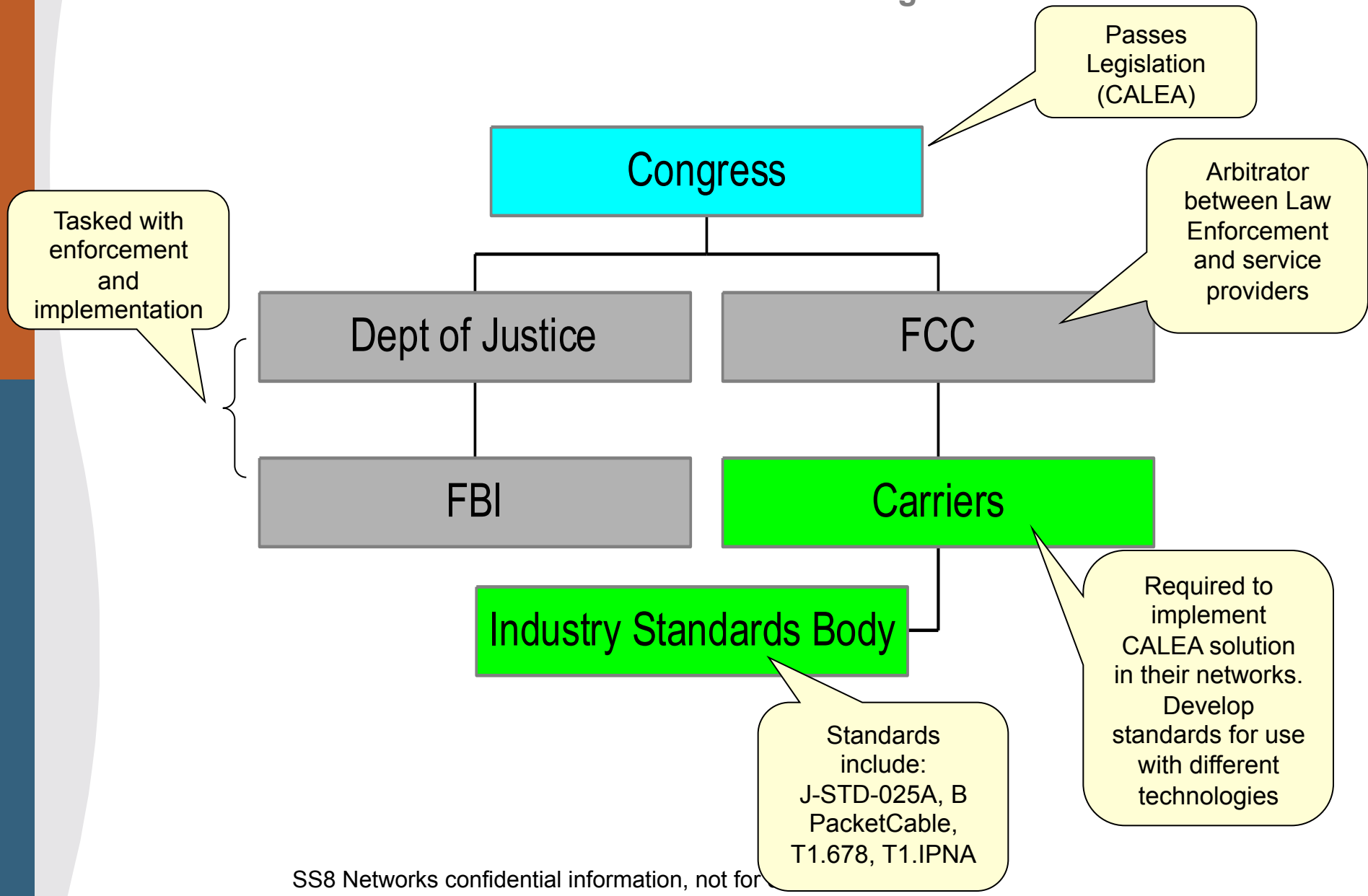
Passive probe

CP-2300
Software module

HI-3

Rules and Regulations

CALEA Decision Making



The Burden on Law Enforcement

- The first tool available to track bad guys is with a **subpoena** for call records. This is done on a regular basis and 10's of thousands of these are done on an annual basis. These are literally copies of relevant phone bills that are sent to the LEA either electronically or as paper copies. Many times they are uploaded into a Collection Function for analysis.
- The next step is to get a warrant for a **Pen Register or Trap and Trace**. These are historical terms used to identify calling activities (off-hook, ringing, answer, disconnect, call forward, hookflash etc.). These events are sent in real time from the delivery function to the collection function for analysis. Far fewer of these are done then the subpoenas for call records
- The last step is to get a **Title III**. This is usually only approved after a true need is demonstrated to the judge. This is also quite expensive for Law Enforcement. US law dictates that the intercept must be monitored live, 24 hours a day, by a Law Enforcement agent and any part of the conversation that isn't relevant to the case must be "minimized". In addition to the live monitoring (requiring multiple teams), there is usually a ground team surveiling the target. So due to the significant burden to justify the grounds for such a warrant and the manpower required to support it, very few (relatively speaking ~1700) are done each year.

CALEA Report Requirements for Congress

Department of Justice - CALEA → Audit Report DOJ Inspector General – April *

Department of Justice - FISA → DOJ Attorney General Report - April

Federal and State LEA → Admin. Office of US Courts – Wiretap Report - April

Congress

* Not covered here

Recent Events

In 2004 the FBI, DOJ and DEA filed a joint petition asking the FCC to clarify the implementation of CALEA for Broadband and VoIP providers.

In August 2005 the FCC issued a "First Report and Order" deeming that "Facilities based and inter-connected VoIP providers" must provide CALEA support. It also required that compliance be achieved within 18 months of the Order.

In May 2006 the FCC issued a "Second Report and Order" confirming that there would be no extensions and that the service providers must come into compliance by the original date stated in the First Report and Order.

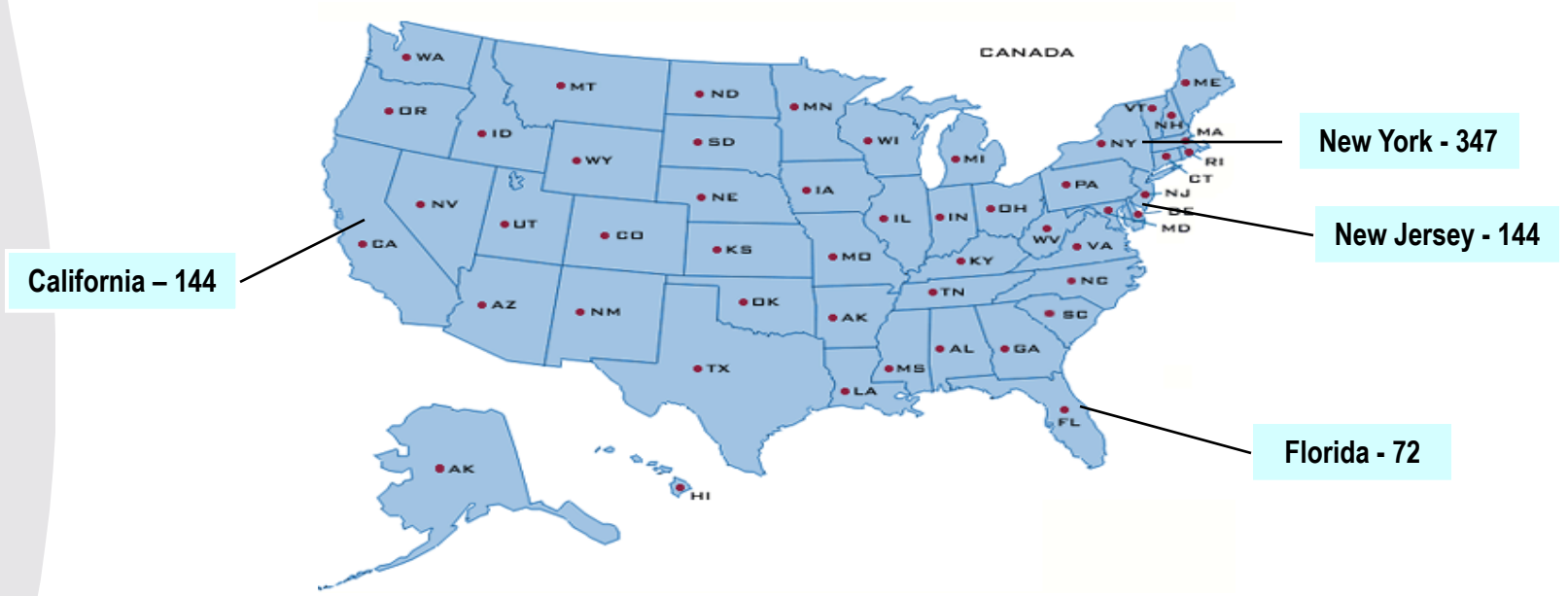
On June 9th, an appeal made on behalf of Service providers seeking to stall or alter the FCC report was denied by the DC Circuit Court and the FCC ruling was upheld.

Service providers now have a true call to action and must come into compliance by May 14th 2007

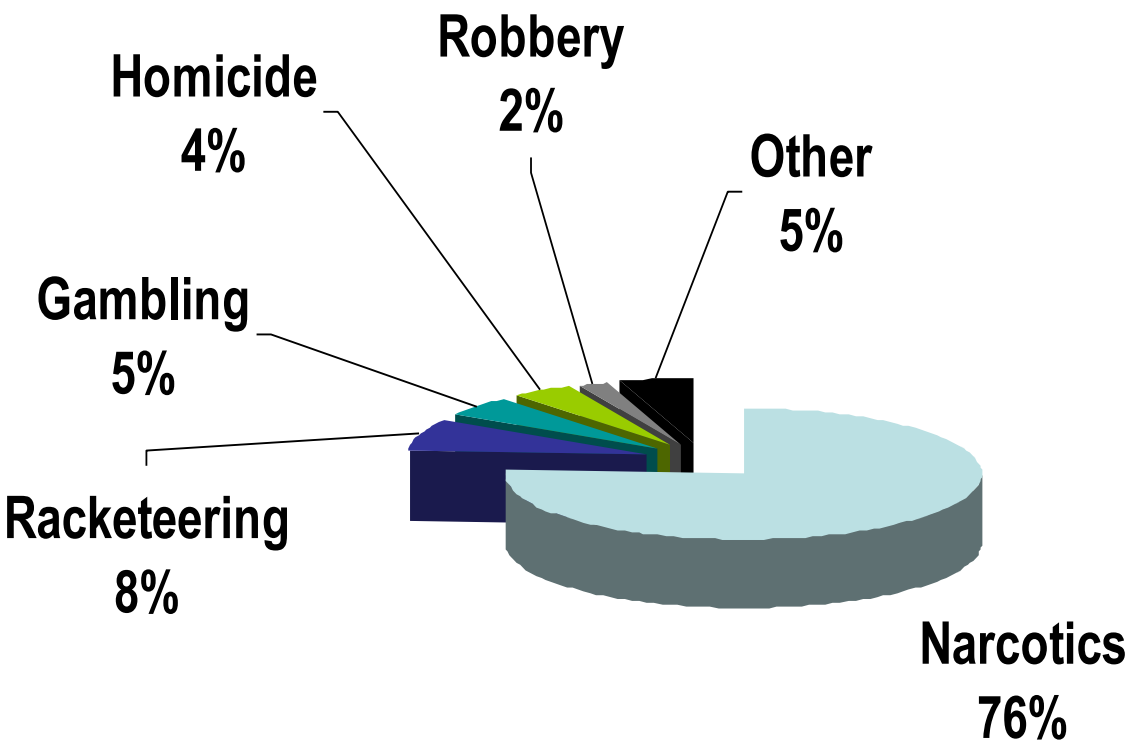
Impact

Number of Intercept Orders

- 2004 Authorized Intercept Orders: 1,710
  - Increase of 19% from prior year
- Federal: 730 State: 980
  - Federal increase of 26%
  - State increase of 13%
- Four states accounted for 76% of intercept orders



Intercept Applications by Offense Type



Duration of Intercept Orders

- Average duration of 43 days
  - Decrease from prior year of 44 days
- Average original duration of 28 days
  - 1,341 extensions averaging 28 days authorized
  - Increase of 17% from prior year
- Longest was 390 days
  - Federal: racketeering (IL)
  - State: narcotics (NY)
- 24 (Federal) and 59 (State) in operation for less than one week

Activity of Intercept Orders

- Average number of persons communications intercepted
  - 126 per order
    - Average number of communications per order was 3,017
  - Increase from prior year of 116 per order
- Average percentage of communications that were incriminating was 21%
  - Decrease of 33% from prior year
- 88% for portable devices (mobile communications)
  - 94% telephonic
- Most active
  - 206,444 computer messages over 30 days (counterfeiting)
  - 107,779 computer messages over 30 days (racketeering)
  - 681 per day for 30 days (narcotics)

Costs of Intercept Orders

- Costs reflect installing intercept devices and monitoring communications
- 2004 cost average of $63,011
  - Overall up 1% from prior year
  - Federal average cost of $75,527, increase of 5%
  - State average cost of $52,490, decrease of 3%

Arrests and Convictions

- Statistics skewed due to length of cases beyond reporting period
  - Leveled by filing of Supplemental Reports
- 4,506 persons arrested based on intercepts
  - Increase of 23%
- 634 persons convicted (14%)
- Federal accounted for 53% of arrests and 23% of convictions
- Supplemental reporting
  - 2,153 arrests and 1,683 convictions based on prior years intercepts

Various Case Highlights

15 arrests with 7 Convictions
Seizure of 50 kilos cocaine; 3 vehicles; 15 weapons; $2.6M

4 arrests
Seizure of 2 tons marijuana; 10 vehicles; 4 weapons; $2.1M

45 arrests
Seizure of 16 pounds methamphetamine; 6 kilos cocaine; 2 indoor marijuana operations; 7 vehicle; 26 weapons; $1.1M

11 day wiretap led to arrest of conspirators planning to murder police officer

One day wiretap led to recovery of kidnapping victim

11 arrests
Seizure of 23 kilos cocaine; 9 vehicles; 20 weapons; $1.7M

Department of Justice - FISA Report

- Foreign Intelligence Surveillance Act
  - Requirement to report to Congress – filed in April
  - Report is only amount of orders
  - FISA applications and orders are governed by Separate Court system
    - *Relatively secret, in fact most Americans do not know of Court's existence*
- 1,754 application and orders approved
  - This is the extent of information provided

Thank You

Scott W. Coleman
Dir. Of Marketing - LI