EXHIBIT I

Whistle-Blower's Evidence, Uncut

02:00 AM May, 22, 2006

Former AT&T technician Mark Klein is the key witness in the Electronic Frontier Foundation's class-action lawsuit against the telecommunications company, which alleges that AT&T cooperated in an illegal National Security Agency domestic surveillance program.

Inside the Secret Room

Courtroom Clash!
A federal judge refuses to give AT&T back its internal documents, but orders the EFF not to give them out.

Whistle-Blower's Precognition
Years before the NSA's warrantless surveillance program made national headlines, then-AT&T technician Mark Klein suspected his company was colluding with the government to spy on Americans.

The Ultimate Net Monitoring Tool
A little-known company called Narus makes the packet-inspection technology said to be the basis of the NSA's internet surveillance. Here's how it works.

Plus:
Daily updates from 27B Stroke 6, the Wired News

In a public statement Klein issued last month, he described the NSA's visit to an AT&T office. In an older, less-public statement recently acquired by Wired News, Klein goes into additional details of his discovery of an alleged surveillance operation in an AT&T building in San Francisco.

Klein supports his claim by attaching excerpts of three internal company documents: a Dec. 10, 2002, manual titled "*Study Group 3, LGX/Splitter Wiring, San Francisco*," a Jan. 13, 2003, document titled "*SIMS, Splitter Cut-In and Test Procedure*" and a second "*Cut-In and Test Procedure*" dated Jan. 24, 2003.

Here we present Klein's statement in its entirety, with inline links to all of the document excerpts where he cited them. You can also download the complete file here (pdf). The full AT&T documents are filed under seal in federal court in San Francisco.

AT&T's Implementation of NSA Spying on American Citizens
31 December 2005

I wrote the following document in 2004 when it became clear to me that AT&T, at the behest of the National Security Agency, had illegally installed secret computer gear designed to spy on internet traffic. At the time I thought this was an outgrowth of the notorious Total Information Awareness program, which was attacked by defenders of civil liberties. But now it's been revealed by *The New York Times* that the spying program is vastly bigger and was directly authorized by President Bush, as he himself has now admitted, in flagrant violation of specific statutes and constitutional protections for civil liberties. I am presenting this information to facilitate the dismantling of this dangerous Orwellian project.

AT&T Deploys Government Spy Gear on WorldNet Network
-- 16 January, 2004

In 2003 AT&T built "secret rooms" hidden deep in the bowels of its central offices in various cities, housing computer gear for a government spy operation which taps into the company's popular WorldNet service and the entire internet. These installations enable the government to look at every individual message on the internet and analyze exactly what people are doing. Documents showing the hardwire installation in San Francisco suggest that there are similar locations being installed in numerous other cities.

The physical arrangement, the timing of its construction, the government-imposed secrecy surrounding it and other factors all strongly suggest that its origins are rooted in the Defense Department's Total Information Awareness (TIA) program which brought forth vigorous protests from defenders of constitutionally protected civil liberties last year:

> "As the director of the effort, Vice Adm. John M. Poindexter, has described the system in Pentagon documents and in speeches, it will provide intelligence analysts and law enforcement officials with instant access to information from internet mail and calling records to credit card and banking transactions and travel

documents, without a search warrant." *The New York Times*, 9 November 2002

To mollify critics, the Defense Advanced Research Projects Agency (Darpa) spokesmen have repeatedly asserted that they are only conducting "research" using "artificial synthetic data" or information from "normal DOD intelligence channels" and hence there are "no U.S. citizen privacy implications" (Department of Defense, Office of the Inspector General report on TIA, December 12, 2003). They also changed the name of the program to "Terrorism Information Awareness" to make it more politically palatable. But feeling the heat, Congress made a big show of allegedly cutting off funding for TIA in late 2003, and the political fallout resulted in Adm. Poindexter's abrupt resignation last August. However, the fine print reveals that Congress eliminated funding only for "the majority of the TIA components," allowing several "components" to continue (DOD, *ibid*). The essential hardware elements of a TIA-type spy program are being surreptitiously slipped into "real world" telecommunications offices.

In San Francisco the "secret room" is Room 641A at 611 Folsom Street, the site of a large SBC phone building, three floors of which are occupied by AT&T. High-speed fiber-optic circuits come in on the 8th floor and run down to the 7th floor where they connect to routers for AT&T's WorldNet service, part of the latter's vital "Common Backbone." In order to snoop on these circuits, a special cabinet was installed and cabled to the "secret room" on the 6th floor to monitor the information going through the circuits. (The location code of the cabinet is 070177.04, which denotes the 7th floor, aisle 177 and bay 04.) The "secret room" itself is roughly 24-by-48 feet, containing perhaps a dozen cabinets including such equipment as Sun servers and two Juniper routers, plus an industrial-size air conditioner.

The normal work force of unionized technicians in the office are forbidden to enter the "secret room," which has a special combination lock on the main door. The telltale sign of an illicit government spy operation is the fact that *only people with security clearance from the National Security Agency can enter this room.* In practice this has meant that only one management-level technician works in there. Ironically, the one who set up the room was laid off in late 2003 in one of the company's endless "downsizings," but he was quickly replaced by another.

Plans for the "secret room" were fully drawn up by December 2002, curiously only four months after Darpa started awarding contracts for TIA. One 60-page document, identified as coming from "AT&T Labs Connectivity & Net Services" and authored by the labs' consultant Mathew F. Casamassima, is titled Study Group 3, LGX/Splitter Wiring, San Francisco and dated 12/10/02. This document addresses the special problem of trying to spy on fiber-optic circuits. Unlike copper wire circuits which emit electromagnetic fields that can be tapped into without disturbing the circuits, fiber-optic circuits do not "leak" their light signals. In order to monitor such communications, one has to physically cut into the fiber somehow and divert a portion of the light signal to see the information.

This problem is solved with "splitters" which literally split off a percentage of the light signal so it can be examined. This is the purpose of the special cabinet referred to above: Circuits are connected into it, the light signal is split into two signals, one of which is diverted to the "secret room." The cabinet is totally unnecessary for the circuit to perform -- in fact it introduces problems since the signal level is reduced by the splitter -- its only purpose is to enable a third party to examine the data flowing between sender and recipient on the internet.

The above-referenced document includes a diagram showing the splitting of the light signal, a portion of which is diverted to "SG3 Secure Room," i.e., the so-called "Study Group" spy room. Another page headlined "Cabinet Naming" lists not only the "splitter" cabinet but also the equipment installed in the "SG3" room, including various Sun devices, and Juniper M40e and M160 "backbone" routers. PDF file 4 shows one of many tables detailing the connections between the "splitter" cabinet on the 7th floor (location 070177.04) and a cabinet in the "secret room" on the 6th floor (location 060903.01). Since the San Francisco "secret room" is numbered 3, the implication is that there are at least several more in other cities (Seattle, San Jose, Los Angeles and San Diego are some of the rumored locations), which likely are spread across the United States.

One of the devices in the "Cabinet Naming" list is particularly revealing as to the purpose of the "secret room": a Narus STA 6400. Narus is a 7-year-old company which, because of its particular niche, appeals not only to businessmen (it is backed by AT&T, JP Morgan and Intel, among others) but

also to police, military and intelligence officials. Last November 13-14, for instance, Narus was the "Lead Sponsor" for a technical conference held in McLean, Virginia, titled "Intelligence Support Systems for Lawful Interception and Internet Surveillance." Police officials, FBI and DEA agents, and major telecommunications companies eager to cash in on the "war on terror" had gathered in the hometown of the CIA to discuss their special problems. Among the attendees were AT&T, BellSouth, MCI, Sprint and Verizon. Narus founder, Dr. Ori Cohen, gave a keynote speech. So what does the Narus STA 6400 do?

"The (Narus) STA Platform consists of standalone traffic analyzers that collect network and customer usage information in real time directly from the message.... These analyzers sit on the message pipe into the ISP (internet service provider) cloud rather than tap into each router or ISP device" (*Telecommunications* magazine, April 2000). A Narus press release (1 Dec., 1999) also boasts that its Semantic Traffic Analysis (STA) technology "captures comprehensive customer usage data ... and transforms it into actionable information.... (It) is the only technology that provides complete visibility for all internet applications."

To implement this scheme, WorldNet's high-speed data circuits already in service had to be rerouted to go through the special "splitter" cabinet. This was addressed in another document of 44 pages from AT&T Labs, titled SIMS, Splitter Cut-In and Test Procedure, dated 01/13/03. "SIMS" is an unexplained reference to the secret room. Part of this reads as follows:

> **"A WMS (work) Ticket will be issued by the AT&T Bridgeton Network Operation Center (NOC) to charge time for performing the work described in this procedure document....**
> "This procedure covers the steps required to insert optical splitters into select live Common Backbone (CBB) OC3, OC12 and OC48 optical circuits."

The NOC referred to is in Bridgeton, Missouri, and controls WorldNet operations. (As a sign that government spying goes hand-in-hand with union-busting, the entire (Communication Workers of America) Local 6377 which had jurisdiction over the Bridgeton NOC was wiped out in early 2002

when AT&T fired the union work force and later rehired them as nonunion "management" employees.) The cut-in work was performed in 2003, and since then new circuits are connected through the "splitter" cabinet.

Another Cut-In and Test Procedure document dated January 24, 2003, provides diagrams of how AT&T Core Network circuits were to be run through the "splitter" cabinet. One page lists the circuit IDs of key Peering Links which were "cut-in" in February 2003, including ConXion, Verio, XO, Genuity, Qwest, PAIX, Allegiance, AboveNet, Global Crossing, C&W, UUNET, Level 3, Sprint, Telia, PSINet and Mae West. By the way, Mae West is one of two key internet nodal points in the United States (the other, Mae East, is in Vienna, Virginia). It's not just WorldNet customers who are being spied on -- it's the entire internet.

The next logical question is, what central command is collecting the data sent by the various "secret rooms"? One can only make educated guesses, but perhaps the answer was inadvertently given in the DOD Inspector General's report (cited above):

> "For testing TIA capabilities, Darpa and the U.S. Army Intelligence and Security Command (INSCOM) created an operational research and development environment that uses real-time feedback. The main node of TIA is located at INSCOM (in Fort Belvoir, Virginia)...."

Among the agencies participating or planning to participate in the INSCOM "testing" are the "National Security Agency, the Defense Intelligence Agency, the Central Intelligence Agency, the DOD Counterintelligence Field Activity, the U.S. Strategic Command, the Special Operations Command, the Joint Forces Command and the Joint Warfare Analysis Center." There are also "discussions" going on to bring in "non-DOD federal agencies" such as the FBI.

This is the infrastructure for an Orwellian police state. It must be shut down!

AT&T's Implementation of NSA Spying on American Citizens

31 December 2005

I wrote the following document in 2004 when it became clear to me that AT&T, at the behest of the National Security Agency, had illegally installed secret computer gear designed to spy on internet traffic. At the time I thought this was an outgrowth of the notorious "Total Information Awareness" program which was attacked by defenders of civil liberties. But now it's been revealed by the *New York Times* that the spying program is vastly bigger and was directly authorized by president Bush, as he himself has now admitted, in flagrant violation of specific statutes and Constitutional protections for civil liberties. I am presenting this information to facilitate the dismantling of this dangerous Orwellian project.

AT&T Deploys Government Spy Gear on WorldNet Network

--16 January, 2004

In 2003 AT&T built "secret rooms" hidden deep in the bowels of its central offices in various cities, housing computer gear for a government spy operation which taps into the company's popular WorldNet service and the entire Internet. These installations enable the government to look at *every individual message* on the Internet and analyze exactly what people are doing. Documents showing the hardwire installation in San Francisco suggest that there are similar locations being installed in numerous other cities.

The physical arrangement, the timing of its construction, the government-imposed secrecy surrounding it, and other factors all strongly suggest that its origins are rooted in the Defense Department's "Total Information Awareness" (TIA) program which brought forth vigorous protests from defenders of Constitutionally-protected civil liberties last year:

> "As the director of the effort, Vice Adm. John M. Poindexter, has described the system in Pentagon documents and in speeches, it will provide intelligence analysts and law enforcement officials with instant access to information from Internet mail and calling records to credit card and banking transactions and travel documents, without a search warrant."
> --*The New York Times*, 9 November 2002

To mollify critics, the Defense Advanced Research Projects Agency (DARPA) spokesmen have repeatedly asserted that they are only conducting "research" using "artificial synthetic data" or information from "normal DoD intelligence channels" and hence there are "no U.S. citizen privacy implications" (Department of Defense, Office of the Inspector General report on TIA, December 12, 2003). They also changed the name of the program to "Terrorism Information Awareness" to make it more politically palatable. But feeling the heat, Congress made a big show of allegedly cutting off funding for TIA in late 2003, and the political fallout resulted in Admiral Poindexter's abrupt resignation last August. However, the fine print reveals that Congress eliminated funding only for "the majority of the TIA components," allowing several "components" to continue (DoD, *ibid*). The essential hardware elements of a TIA-type spy program are being surreptitiously slipped into "real world" telecommunications offices.

In San Francisco the "secret room" is Room 641A at 611 Folsom Street, the site of a large SBC phone building, three floors of which are occupied by AT&T. High speed fiber optic circuits come in on the 8th floor and run down to the 7th floor where they connect to routers for AT&T's WorldNet service, part of the latter's vital "Common Backbone." In order to snoop on these circuits, a special cabinet was installed and cabled to the "secret room" on the 6th floor to monitor the information going through the circuits. (The location code of the cabinet is 070177.04, which denotes the 7th floor, aisle 177 and bay 04.) The "secret room" itself is roughly 24-by-48 feet, containing perhaps a dozen cabinets including such equipment as Sun servers and two Juniper routers, plus an industrial-size air conditioner.

The normal workforce of unionized technicians in the office are forbidden to enter the "secret room," which has a special combination lock on the main door. The telltale sign of an illicit government spy operation is the fact that *only people with security clearance from the National Security Agency can enter this room.* In practice this has meant that only one management-level technician works in there. Ironically, the one who set up the room was laid off in late 2003 in one of the company's endless "downsizings," but he was quickly replaced by another.

Plans for the "secret room" were fully drawn up by December 2002, curiously only four months after DARPA started awarding contracts for TIA. One 60-page document, identified as coming from "AT&T Labs Connectivity & Net Services" and authored by the labs' consultant Mathew F. Casamassima, is titled "Study Group 3, LGX/Splitter Wiring, San Francisco and dated 12/10/02. (See sample pdf 1-4.) This document addresses the special problem of trying to spy on fiber optic circuits. Unlike copper wire circuits which emit electromagnetic fields that can be tapped into without disturbing the circuits, fiber optic circuits do not "leak" their light signals. In order to monitor such communications, one has to physically cut into the fiber somehow and divert a portion of the light signal to see the information.

This problem is solved with "splitters" which literally split off a percentage of the light signal so it can be examined. This is the purpose of the special cabinet referred to above: circuits are connected into it, the light signal is split into two signals, one of which is diverted to the "secret room." The cabinet is totally unnecessary for the circuit to perform-- in fact it introduces problems since the signal level is reduced by the splitter—*its only purpose is to enable a third party to examine the data flowing between sender and recipient on the Internet.*

The above-referenced document includes a diagram (pdf 3) showing the splitting of the light signal, a portion of which is diverted to "SG3 Secure Room," i.e., the so-called "Study Group" spy room. Another page headlined "Cabinet Naming" (pdf 2) lists not only the "splitter" cabinet but also the equipment installed in the "SG3" room, including various Sun devices, and Juniper M40e and M160 "backbone" routers. Pdf file 4 shows shows one of many tables detailing the connections between the "splitter" cabinet on the 7th floor (location 070177.04) and a cabinet in the "secret room" on the 6th floor (location 060903.01). Since the San Francisco "secret room" is numbered 3, the implication is that there are at least several more in other cities (Seattle, San Jose, Los Angeles and San Diego are some of the rumored locations), which likely are spread across the U.S.

One of the devices in the "Cabinet Naming" list is particularly revealing as to the purpose of the "secret room": a Narus STA 6400. Narus is a 7-year-old company which, because of its particular niche, appeals not only to businessmen (it is backed by AT&T, JP Morgan and Intel, among others) but also to police, military and intelligence officials. Last November 13-14, for instance, Narus was the "Lead Sponsor" for a technical conference held in McLean, Virginia, titled "Intelligence Support Systems for Lawful Interception and Internet Surveillance."* Police officials, FBI and DEA agents, and major telecommunications companies eager to cash in on the "war on terror" had gathered in the hometown of the CIA to discuss their special problems. Among the attendees were AT&T, BellSouth, MCI, Sprint and Verizon. Narus founder, Dr. Ori Cohen, gave a keynote speech. So what does the Narus STA 6400 do?

"The [Narus] STA Platform consists of standalone traffic analyzers that collect network and customer usage information in real time directly from the message...These analyzers sit on the message pipe into the ISP [Internet Service Provider] cloud rather than tap into each router or ISP device" (*Telecommunications* magazine, April, 2000),** A Narus press release (1 Dec.,1999) also boasts that its Semantic Traffic Analysis (STA) technology "captures comprehensive customer usage data...and transforms it into actionable information...[it] is the only technology that provides complete visibility for all Internet applications."***

To implement this scheme, WorldNet's highspeed data circuits already in service had to be re-routed to go through the special "splitter" cabinet. This was addressed in another document of 44 pages from AT&T Labs, titled "SIMS, Splitter Cut-In and Test Procedure," dated 01/13/03 (pdf 5-6). "SIMS" is an unexplained reference to the secret room. Part of this reads as follows:

> **"A WMS [work] Ticket will be issued by the AT&T Bridgeton Network Operation Center (NOC) to charge time for performing the work described in this procedure document....**
> "This procedure covers the steps required to insert optical splitters into select live Common Backbone (CBB) OC3, OC12 and OC48 optical circuits."

The NOC referred to is in Bridgeton, Missouri, and controls WorldNet operations. (As a sign that government spying goes hand-in-hand with union-busting, the entire CWA Local 6377 which had jurisdiction over the Bridgeton NOC was wiped out in early 2002 when AT&T fired the union workforce and later re-hired them as non-union "management" employees.) The cut-in work was performed in 2003, and since then new circuits are connected through the "splitter" cabinet.

Another "Cut-In and Test Procedure" document dated January 24, 2003, provides diagrams of how AT&T Core Network circuits were to be run through the "splitter" cabinet (pdf 7). One page lists the circuit IDs of key Peering Links which were "cut-in" in February 2003 (pdf 8), including ConXion, Verio, XO, Genuity, Qwest, PAIX, Allegiance, Abovenet, Global Crossing, C&W, UUNET, Level 3, Sprint, Telia, PSINet, and Mae West. By the way, Mae West is one of two key Internet nodal points in the United States (the other, Mae East, is in Vienna, Virginia). It's not just WorldNet customers who are being spied on—it's the entire Internet.

The next logical question is, what central command is collecting the data sent by the various "secret rooms"? One can only make educated guesses, but perhaps the answer was inadvertently given in the DoD Inspector General's report (cited above):

> "For testing TIA capabilities, DARPA and the U.S. Army Intelligence and Security Command (INSCOM) created an operational research and development environment that uses real time feedback. The main node of TIA is located at INSCOM [in Fort Belvoir, Virginia]..."

Among the agencies participating or planning to participate in the INSCOM "testing" are the "National Security Agency, the Defense Intelligence Agency, the Central

Intelligence Agency, the DoD Counterintelligence Field Activity, the U.S. Strategic Command, the Special Operations Command, the Joint Forces Command and the Joint Warfare Analysis Center." There are also "discussions" going on to bring in "non-DoD Federal agencies" such as the FBI.

This is the infrastructure for an Orwellian police state. It must be shut down!

* TeleStrategies postings, see:
http://www.serviceprovidersclub.com/main/event-detail.cfm?eventId=36&v=agenda
http://telestrategies.com/issworld/sponsors.htm
http://telestrategies.com/iss_2004/index.htm

** see http://www.findarticles.com/cf_dls/m0TLC/4_34/62350496/p1/article.jhtml

*** see http://www.lucent.com/press/1299/991201.nsa.html

Labs Connectivity & Net Services

Study Group 3
LGX/Splitter Wiring
San Francisco

Issue 1, 12/10/02

Author: Mathew F. Casamassima
Email: mcasamassima@att.com
Phone: (732) 420-2033

Study Group 3 LGX/Splitter Wiring, San Francisco
Issue 1, 12/10/02

Mathew F. Casamassima, (732) 420-2033, mcasamassima@att.com

Cabinet Naming:

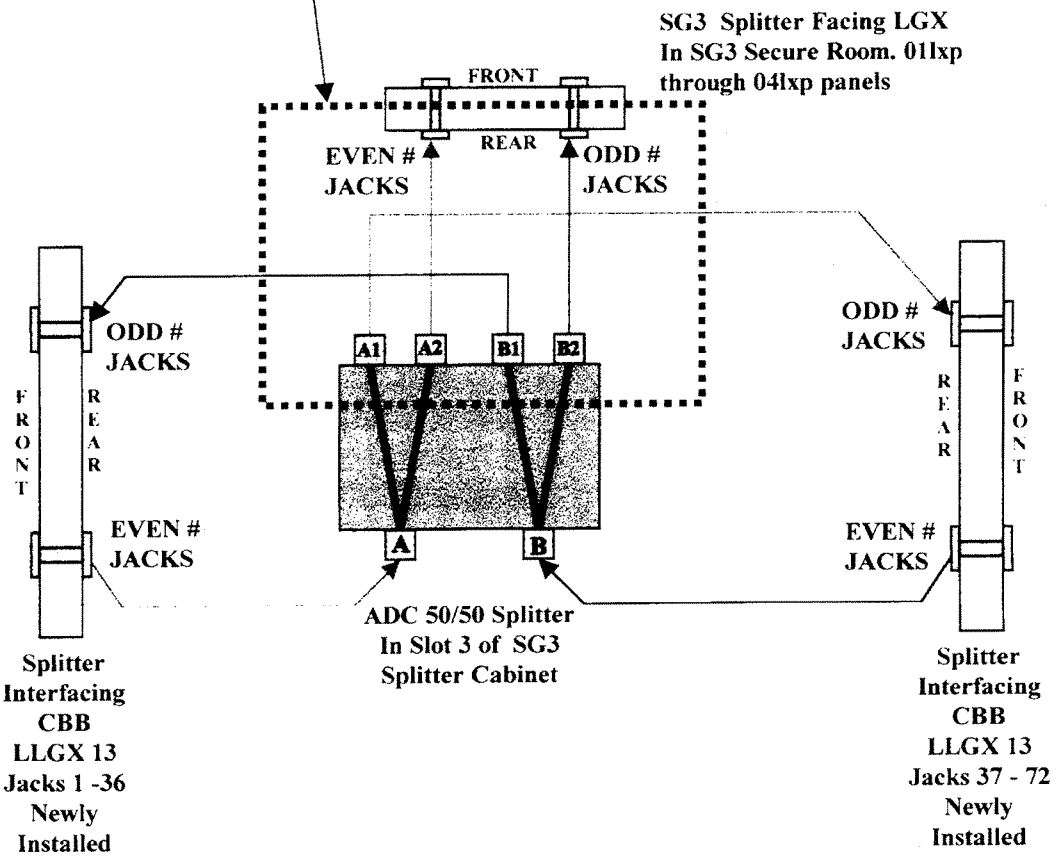
Equipment	Name
Splitter Cabinet	SPC
LGX Cabinet	LXC
Meta Data Cabinet	MDC
Network Management Cabinet	NMC
Data Filter Cabinet	DFC
Juniper M40E Router Cabinet	JC
Sun V880 Cabinet	S8C
Sun 3800 Cabinet	S3C
Sun Storedge Cabinet	SSC
ADC Chassis For LGX	lxp
ADC Chassis For Splitter	spp
ADC Splitter Module	spl
ADC Bulkhead Module (LGX)	bk
Juniper M160	jp
Juniper M40e	j4
Narus STA 6400	nr
Sun Fire V880/Narus Logic Server	s8
Sun Fire 3800	s3
Sun StorEdge T3	st
Sun StorEdge FC switch	sf
Cisco Catalyst 2924M-XL	cz
BayTech DS9	b9
BayTech RPC22	bv
Brocade SilkWorm 2800 Switch	bz
Lucent LGX	LLGX

Study Group 3 LGX/Splitter Wiring, San Francisco
Issue 1, 12/10/02

Mathew F. Casamassima, (732) 420-2033, mcasamassima@att.com

Splitter to SG3 LGX Connectivity

The Tables in this section give the splitter to SG3 LGX connectivity as shown with in the bounds of this box.



Study Group 3 LGX/Splitter Wiring, San Francisco
Issue 1, 12/10/02

Mathew F. Casamassima, (732) 420-2033, mcasamassima@att.com

01lxp SG3 LGX Panel to Splitter Cabinet Connectivity

01lxp SG3 LGX Panel Port (In SG3 Room)	Splitter Cabinet Destination	SG3 LGX Designation Card Text	Splitter End Fiber Label Text
1	01spp/Slot 3/port 14	RR 070177.04 01spp/Slot 3/port 14	FROM: 060903.01 01lxp/JK 1 TO: 01spp/Slot 3/port 14
2	01spp/Slot 3/port 13	RR 070177.04 01spp/Slot 3/port 13	FROM: 060903.01 01lxp/JK 2 TO: 01spp/Slot 3/port 13
3	01spp/Slot 3/port 16	RR 070177.04 01spp/Slot 3/port 16	FROM: 060903.01 01lxp/JK 3 TO: 01spp/Slot 3/port 16
4	01spp/Slot 3/port 15	RR 070177.04 01spp/Slot 3/port 15	FROM: 060903.01 01lxp/JK 4 TO: 01spp/Slot 3/port 15
5	01spp/Slot 3/port 18	RR 070177.04 01spp/Slot 3/port 18	FROM: 060903.01 01lxp/JK 5 TO: 01spp/Slot 3/port 18
6	01spp/Slot 3/port 17	RR 070177.04 01spp/Slot 3/port 17	FROM: 060903.01 01lxp/JK 6 TO: 01spp/Slot 3/port 17
7	01spp/Slot 4/port 20	RR 070177.04 01spp/Slot 4/port 20	FROM: 060903.01 01lxp/JK 7 TO: 01spp/Slot 3/port 20
8	01spp/Slot 4/port 19	RR 070177.04 01spp/Slot 4/port 19	FROM: 060903.01 01lxp/JK 8 TO: 01spp/Slot 3/port 19
9	01spp/Slot 4/port 22	RR 070177.04 01spp/Slot 4/port 22	FROM: 060903.01 01lxp/JK 9 TO: 01spp/Slot 3/port 22
10	01spp/Slot 4/port 21	RR 070177.04 01spp/Slot 4/port 21	FROM: 060903.01 01lxp/JK 10 TO: 01spp/Slot 3/port 21
11	01spp/Slot 4/port 24	RR 070177.04 01spp/Slot 4/port 24	FROM: 060903.01 01lxp/JK 11 TO: 01spp/Slot 3/port 24
12	01spp/Slot 4/port 23	RR 070177.04 01spp/Slot 4/port 23	FROM: 060903.01 01lxp/JK 12 TO: 01spp/Slot 3/port 23
13	01spp/Slot 5/port B2	RR 070177.04 01spp/Slot 5/port B2	FROM: 060903.01 01lxp/JK 13 TO:01spp/Slot 5/port B2
14	01spp/Slot 5/port A2	RR 070177.04 01spp/Slot 5/port A2	FROM: 060903.01 01lxp/JK 14 TO:01spp/Slot 5/port A2
15	01spp/Slot 6/port B2	RR 070177.04 01spp/Slot 6/port B2	FROM: 060903.01 01lxp/JK 15 TO:01spp/Slot 6/port B2
16	01spp/Slot 6/port A2	RR 070177.04 01spp/Slot 6/port A2	FROM: 060903.01 01lxp/JK 16 TO:01spp/Slot 6/port A2

Labs Connectivity & Net Services

SIMS
Splitter Cut-In and Test Procedure

Issue 2, 01/13/03

Author: Mathew F. Casamassima
Email: mcasamassima@att.com
Phone: (732) 420-2033

SIMS - Splitter Test and Cut-In Procedure
Issue 2, 01/13/03

Mathew F. Casamassima, (732) 420-2033, mcasamassima@att.com

1. *Procedure Overview*

A WMS Ticket will be issued by the AT&T Bridgeton Network Operation Center (NOC) to charge time for performing the work described in this procedure document. At some point prior to the splitter cut-in being performed your office will be contacted by the Bridgeton Network Operations Center (NOC) to confirm the WMS Ticket has been received. Bridgeton NOC personnel will again contact OSWF the night of the cut to begin coordination. The work described in the procedure will be supported, on-site, by an IP Field Support Specialist (FSS) from the Day Tech organization.

This procedure covers the steps required to insert optical splitters into select live Common Backbone (CBB) OC3, OC12 and OC48 optical circuits. The splitter insertion will be accomplished by removing existing optical cross-connects and installing new cross-connects all within the CBB LGX complex. The optical splitters will be contained in a standalone cabinet located in the proximity of the CBB LGX complex. The splitters will be pre-cabled by an EF&I vendor to the rear of a dedicated LGX bay (LLGX13) within the CBB LGX complex. A partial installation and test of cross-connects can be done prior to the actual splitter cut-in. This portion of the work can be done outside the CBB maintenance window. An IP FSS member of the Day Tech organization will contact OSWF to schedule the pre-cut portion of the work. Section 2 of this document will describe the pre-cut installation of cross-connects and the pre-cut testing of the new circuit path. The actual cut-in of the splitter will be done during the CBB maintenance window and will be closely coordinated with the Bridge NOC and will be supported, on-site, by an IP FSS member of the Day Tech organization. The actual splitter cut-in is described in Section 3 of this document.

The number of cross-connects required and the final path the circuit will take is dependant on the location of the affected LGX bays within the multiple line-ups of the CBB LGX complex. This procedure will describe all possible splitter cut-in circuit paths. The procedure will also describe the procedures for testing each possible circuit path.

1.1. How to Use this Procedure

This procedure document is quite long. **It is not necessary to read this whole document to do the work.** There are 4 possible LGX arrange that may encounter. By reading section **1.2** below, determine which LGX arrangement applies to the circuit you are working. Then, after reading the introductory paragraphs in Sections 2 and 3, go directly to the subsections within Sections 2 and 3 associated with the LGX arrangement you are dealing with.

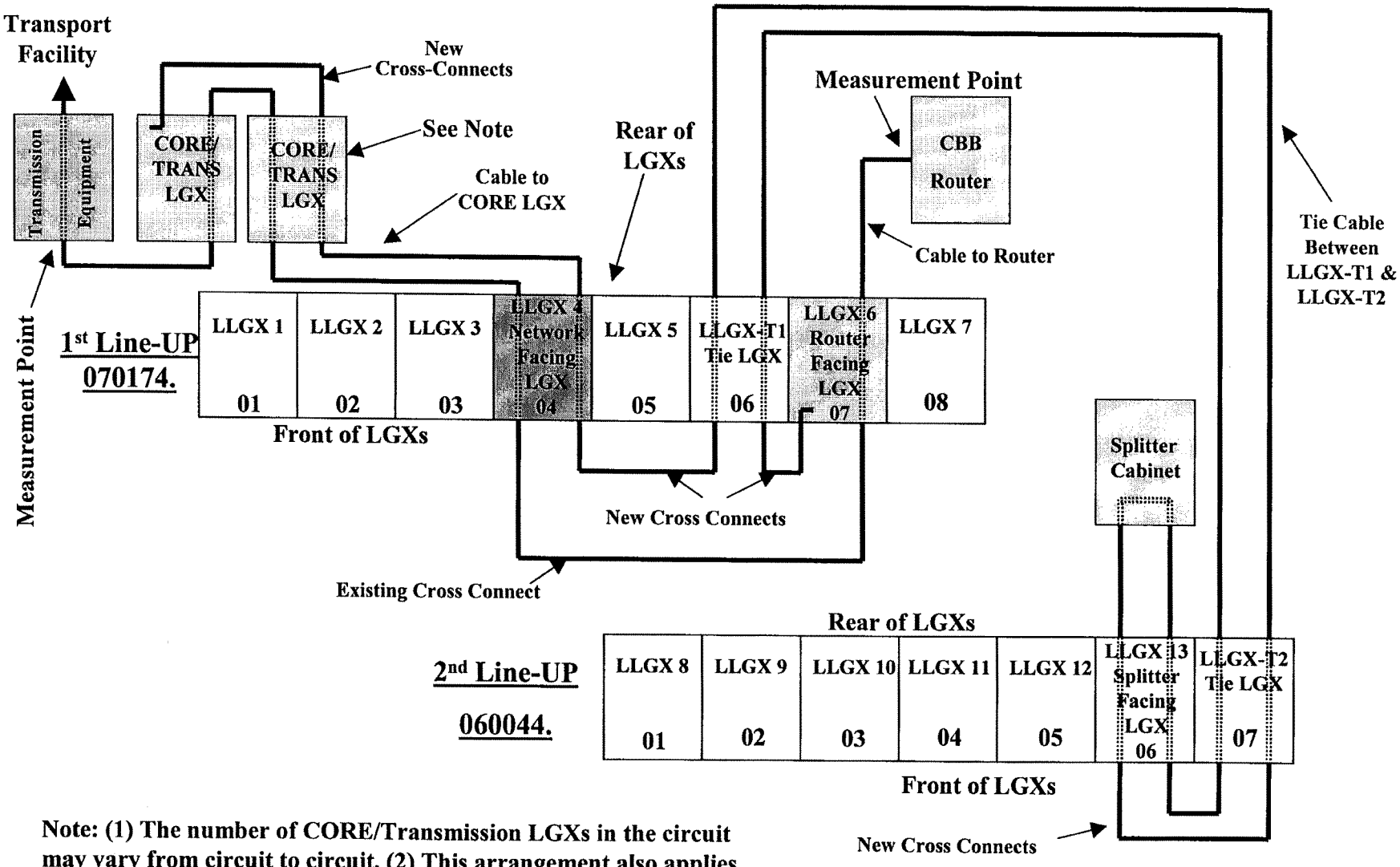
1.2. LGX Definition and LGX-Arrangement:

LGX Definition: There are multiple LGX bays affected by this procedure. Within the CBB LGX complex LGX bays follow a specific naming convention (LLGX 1, LLGX2, LLGX3, LLGX4, ...). This naming convention is uniform across sites. Since this document is designed to cover all sites, this uniform naming convention will be used here. Site-specific engineering will use the LGX FIC code rather than the naming. Prior to the start of the work described here the local IP FSS will label the LGX bays with the naming as presented in this document. The following are generic definitions for the LGX bays affected by this procedure:

Figure 5 - Arrangement 3 - Circuit Connectivity – **Cut Night Measurements**

Network Facing & Router Facing LGX in 1st Line-Up / Splitter Facing LGX in 2nd Line-Up

Overhead View of Bays **(Applies to Circuits AGEC.671212, AGEC.622360, AGEC.622352, IVEC.517519, IVEC.578278, IVEC.502963, IVEC.547506, IVEC.509396, IVEC.597263, IVEC.502961, IVEC.502960 & IWEC.502947)**



Note: (1) The number of CORE/Transmission LGXs in the circuit may vary from circuit to circuit. (2) This arrangement also applies to circuit AGEC.242541 except the Router facing LGX is LLGX 5.

Priority	Peering Link	Ckt Type	ID	AS Number	Circuit Comments	Router	Port	Circuit Engineering Change Order Issue Date	Circuit Engineering Complete Date Requested	Circuit Engineering Complete Date Actual	Splitter Pre-Test Date	Splitter in Circuit Date	Splitter Active Date	Comments
1	ConXion	OC-3	AGEC.622352	4544		sffca01ck	POS 1/3	1/22/2003	1/31/2003	1/22/2003	2/4/2003	2/6/2003		
2	Verio	OC-12	IVEC.517519	2914		sffca01ck	POS 3/1	1/23/2003	1/31/2003	1/23/2003	2/4/2003	2/6/2003		
3	XO	OC-12	IVEC.578278	2828		sffca01ck	POS 3/2	1/23/2003	1/31/2003	1/23/2003	2/4/2003	2/6/2003		
4	Genuity	OC-12	IVEC.502963	1		sffca01ck	POS 3/3	1/23/2003	1/31/2003	1/23/2003	2/4/2003	2/6/2003		
5	Qwest	OC-12	IVEC.547506	209		sffca01ck	POS 5/2	1/30/2003	2/7/2003	1/23/2003	2/11/2003	2/13/2003		
6	PAIX	OC-12	IVEC.509396	nap		sffca01ck	POS 8/1	1/30/2003	2/7/2003	1/23/2003	2/11/2003	2/13/2003		
7	Allegiance	OC-12	IVEC.597263	2548		sffca01ck	POS 8/3	1/30/2003	2/7/2003	1/24/2003	2/11/2003	2/13/2003		
8	Abovenet	OC-12	IVEC.502961	6461		sffca01ck	POS 9/2	1/30/2003	2/7/2003	1/24/2003	2/11/2003	2/13/2003		
9	Global Crossing	OC-12	IVEC.502960	3549		sffca01ck	POS 9/3		2/14/2003		2/18/2003	2/20/2003		
10	C&W	OC-48	IWEC.502947	3561		sffca01ck	POS 2/0		2/14/2003		2/18/2003	2/20/2003		
11	UUNET	OC-48	IWEC.509433	701		sffca02ck4	POS 2/0		2/14/2003		2/18/2003	2/20/2003		
12	Level 3	OC-48	IWEC.509434	3356		sffca02ck4	POS 3/0		2/14/2003		2/18/2003	2/20/2003		
13	Sprint	OC-48	IWEC.509438	1239		sffca02ck4	POS 11/0		2/21/2003		2/25/2003	2/27/2003		
14	Telia	OC-3	AGEC.671212	1299		sffca01ck	POS 0/1		2/21/2003		2/25/2003	2/27/2003		
15	PSINet	OC-3	AGEC.622360	174		sffca01ck	POS 0/2		2/21/2003		2/25/2003	2/27/2003		
16	Mae West	OC-3	AGEC.242541	nap		sffca82ck	POS 2/5		2/21/2003		2/25/2003	2/27/2003		