OECD

Description of ICT Infrastructure
# Table of Contents

I. INTRODUCTION .................................................................................................................. 3

II. OVERVIEW ..................................................................................................................... 4

III. DETAILED DESCRIPTION ............................................................................................ 6

IV. SECURITY ......................................................................................................................... 10

V. DEVELOPMENT PRIORITIES .......................................................................................... 12

ANNEX I. ON-GOING OPERATIONAL ACTIVITIES .............................................................. 15

ANNEX II. ICT ACTIVITY INDICATORS ............................................................................. 17

ANNEX III. DATA NETWORK .............................................................................................. 19

ANNEX IV. CENTRAL COMPUTING FACILITIES ................................................................. 20

ANNEX V. DESKTOP INVENTORY ....................................................................................... 26

ANNEX VI. PBX NETWORK .................................................................................................. 27

ANNEX VII. OUTSOURCED ICT ACTIVITIES ..................................................................... 32

DIAGRAM 1 - CAMPUS NETWORK TOPOLOGY ................................................................. 33

DIAGRAM 2 - CAMPUS NETWORK ARCHITECTURE ....................................................... 33

DIAGRAM 3 – EXTERNAL ACCESS INFRASTRUCTURE .................................................... 33
I. Introduction

Information processing and communications services are critical to the success and timely conduct of the Organisation’s work programmes. A primary corporate objective is, therefore, the delivery of fast, secure and round-the-clock ICT services for all staff - whether in any of the OECD offices located around the world, on mission, or working at home – and a growing constituency of government delegates and public audiences – namely:

- Approximately two thousand four hundred staff (2400) with offices at the following locations:
  - Organisation headquarters in Paris – a campus of twenty (20) buildings
  - Information Centres in Berlin, Bonn, Tokyo, Mexico City and Washington DC
  - OECD Offices in Trento and Istanbul

- One hundred forty (140) specialised intergovernmental committees comprised of approximately 60,000 senior officials from National Administrations – in member countries (30) and non-member (over 75)

- Six hundred (600) officials of member countries’ permanent Delegations in Paris

- Press services, subscribers to OECD publications and data, and the general public

ITN, the Information Technology and Network Service of the OECD Secretariat, is responsible for the selection, implementation, management and operation of computing and communications equipment and software that comprise the Organisation’s ICT infrastructure.

The purpose of this document is to provide a description of the OECD ICT infrastructure and is structured on four sections and related annexes, as follows:

- Overview
- Detailed Description
  - Data Network
  - Computing Facilities
    - Central Computing
    - Desktop PCs, Portables and Printers
  - PBX Network
- Security
- Development Priorities
- Annexes
II. Overview

The Organisation's computing, telecommunications, network and PBX facilities rely on widely-accepted industry standards. These facilities are available 24 hours a day, 7 days a week.

The centrally-managed facilities are located in physically secure areas, to which access is reserved to a small number of authorised staff. Entry to the main computing and telecommunications sites, and other technical areas is under continuous surveillance and automatically logged. All centrally-managed systems are password protected.

Extensive alarm systems are in place, and monitored round-the-clock, to provide immediate warning of unauthorised intrusion, detection of fire, detection of flooding, etc., and accompanied in some cases by video surveillance. Mechanisms are in place to automatically shut down air conditioning and electrical power, and release fire-retardant gas, should a fire occur. These systems are tested regularly. Sufficient redundancy exists in the environmental facilities (e.g. air conditioning and electrical systems), such that services could continue to be provided, even in the event of failure of a major environmental component.

Equipment, operating system software and related utilities are regularly upgraded, and vendor bug fixes installed, to ensure continuing good performance and security, and continued support from vendors. Operators are present from 7h00 to 20h00 weekdays to monitor alerts within the network, server and PBX environments, and deal with problems as they arise. Overall uptime is well in excess of 99%.

Critical equipment elements have built-in redundancy, so that failure of a single critical component would not result in service interruption, and critical work could continue, although perhaps at reduced service levels for a short period of time. A stock of replacement parts is maintained on-site for servers, network and PBX equipment.
**Backups**
- Incremental backups of information residing on the central computing facilities are taken daily.

- Full backups – including operating systems, utilities and their configuration -- are taken weekly. These full backups involve over six terabytes of data.

- Copies of both incremental and full backups are kept at the central site for on-going operational purposes (i.e., restoring a file or database at user request, to permit rapid resumption of service in case of equipment failure).

- Duplicate copies are held “off site”, to permit resumption of activity elsewhere in the event of major disaster at the central site.

- Multiple copies of backups of system software and utilities, applications software and databases on the data and PBX networks are also taken regularly.

**Change Control**
Formal change control procedures are rigorously observed to help ensure continued availability and stability of all computing and communications, to ensure that operating procedures and documentation are kept up-to-date, and to avoid inadvertent introduction of security vulnerabilities.

**Hardware and Software Contract Management**
ITN manages maintenance and license contracts which ensure vendor support for major problem resolution, timely replacement of failed equipment, on-going software upgrades and bug fixes for operating systems and utilities.

Annex I includes a list of on-going activities related to the ICT infrastructure
Annex II includes ICT “activity indicators”.
III. Detailed Description

III.A Data Network

The Organisation’s internal network connects over two thousand (2300) user workstations and over three hundred fifty (350) laser printers. Network and inter-networking operating system software and utilities are regularly upgraded, and “fixes” installed, to ensure continuing good network performance and security, and timely support from vendors. Network capacity is regularly increased to accommodate the traffic generated by new client/server, imaging-, and multimedia-based applications. Integrated network management systems (OpenView-NNM, CiscoWorks-LMS, Concord-eHealth and PacketShaper-BandwidthManagement) facilitate timely detection and location of network-related problems.

The internal network is based on TCP/IP protocols and Ethernet switching technology, with a Gigabit multi-layer switching backbone, switched 100/1000BaseT for server connections, and switched 100BaseT for client connections:

- Client workstations have a 100 Mbps fully switched connection to access switches
- Access switches have dual Gigabit Ethernet full-duplex connections to switches in the core backbone
- Servers are connected through fault-tolerant 100 Mbps or Gigabit full-duplex links to server switches

ITN manages the physical cabling infrastructure for the data network, as well as for the PBX network. The twenty buildings comprising the Organisation’s Paris Headquarters are linked by underground proprietary fiber optic cabling and, for the more distant building, local loop or LAN to LAN service. Within-building cabling to desktops and laser printers conforms, with few exceptions, to Category 5 specifications.

Two fault-tolerant 20 Mbps dedicated links to the Internet provide OECD staff with access to the Web, and provide a growing external clientele with access to OECD’s Web pages.

The Information Centres (Berlin, Bonn, Washington DC, Tokyo, Mexico City) and other remote OECD locations (Trento and Instanbul) are linked to the Paris Headquarters through high speed aDSL Internet connections using IPSec-based secure virtual private network facilities. Fallback of the aDSL IPSec tunnel is backed up by an ISDN connection. Whilst ITN manages the configuration and monitors the routers at the Centres, the hardware is supplied, installed and maintained by locally-contracted companies.
Remote Access and Teleworking

- OECD staff can access internal ICT resources remotely. Access control is based on two-level authentication and authorisation protocols using hard/soft tokens and one-time passwords.

- Staff on mission have secure access to internal network resources from OECD laptops via external IP dialup services provided by an international communications carrier (SITA) or directly through the Internet from any high speed wired or wireless access point using a secure IPSec VPN service.

- Authorised staff members can telework from their homes in the Paris area via high speed aDSL Internet connections using the OECD secured IPSec VPN service.

- Secured access to the web mail interface of the OECD internal mail system is also provided from Internet kiosk via a SSL VPN gateway.

High-speed Links

A new Internet based SSL VPN facility now provides (via a high speed Internet access) fast and secure access in parallel with the existing SITA IP dialup VPN facility for about 13000 authorised officials in Member countries to the OECD’s OLISnet information and interaction services. A number of Member countries Delegations and Ministries have deployed dedicated high speed LAN to LAN connections to the OECD’s OLISnet service.

High-speed links are also in place giving OECD staff access, where authorised, to commercial information services (Thompson Finance, SAP, etc.).

Life Cycle and Inventory Management

To protect against obsolescence, as well as to respond to new business needs, network equipment is replaced on an on-going basis, with a complete replacement cycle taking 5-6 five years.

Desktop PCs and portables are typically replaced on a rolling basis every 3-4 years, and printers every 5-6 years.

Annex III includes an inventory of data network equipment and software in service at the Paris Headquarters and remote locations.
III.B Computing Facilities

The OECD’s computing facilities include:
- 220 servers
- 2300 desktop PCs
- 450 portables
- 350 laser printers
- 81 high-speed printers with scanning capabilities

Central Computing

Most servers are based on single or multiple Intel processors, and run Windows operating system (NT 4.0, Windows 2000 or Windows Server 2003). A few highly specialised applications run under Unix and some IP management services (DNS, BootP, DHCP, etc.) run under Linux.

The central computing facilities provide clients with:
- Analytical and econometric modelling tools (FAME, LINK, Troll, etc.)
- Statistical and databases management systems (based on Microsoft SQL Server 2000)
- Administrative and financial systems (SAP, PeopleSoft, etc.)
- Mail and fax messaging (Microsoft Exchange Server 2000)
- File and print services
- Internet/Intranet applications (IIS 4.0/5.0/6.0 and Lotus Domino 5.0)

System Supervision Tools

Suites of specialised management software tools are used to detect server-based hardware and applications problems, and generate alerts to systems engineering staff via e-mail and pager. Scripting tools are used to generate automated actions to correct anomalies detected outside of normal working hours.

Annex IV includes:
- Central computing equipment at the Paris headquarters central and remote locations
- Principal application software in use

Desktop PCs, Printers and Portables

The desktop computing environment is standardised on Intel Pentium processors running Microsoft Windows XP SP1. The standard memory configuration is 512 MB. A variety of software tools (e.g., SMS) facilitate the deployment of software to desktop PCs, collecting PC-related inventory information, and remote diagnosis of desktop-related problems. Portable PCs, also standardised on Intel Pentium processors, run Microsoft’s Windows XP operating system.

Most desktops and portables are installed with a centrally-engineered desktop configuration. This Standard Desktop Environment ensures optimal system stability for all staff and greatly facilitates problem solving and automatic software update. The configuration image includes, in addition to MS/XP, the MS Office XP Suite (Word, Excel, Access, PowerPoint), MS Internet Explorer and Network Associates’ VirusScan. For further protection, on most standard desktop installations the “administrator” rights are centrally managed.

Annex V includes:
- Desktop PCs, portables and printers at the Paris Headquarters and remote locations
- Description of software included in image installed on desktop PCs and portables
III.C PBX Network

The OECD telephone system was upgraded during the period June, 2003 through September 2004.

A network of twelve (12) Nortel PBXs and four thousand (4000) handsets provide telephone services including: voice mail, fax, speed dialling, call forwarding, ring-again, caller-ID, automatic call distribution (ACD), etc. All OECD staff members have a full-featured digital telephone handset. Approximately half of the Organisation’s staff has direct long-distance dialling privileges.

Digital trunks link the PBX network to OECD’s national and international telecommunications carriers (France Telecom and CEGETEL). The OECD offices in Tokyo, Bonn, Berlin, Washington D.C, and Mexico City have their own local PBXs, which are linked with Headquarters via the Organisation’s global telecommunications carrier, but not directly integrated with the PBX network.

The twelve (12) remote PBXs at Headquarters in Paris are interconnected to the central PBX via leased and/or private fiber and copper lines. There are additional MIC lines to each remote PBX to enable outgoing calls to be placed in case of failure of the central PBX or the links to it, and to handle any capacity overflow. A number of handsets are linked directly to the France Telecom network to provide additional emergency backup, in case of complete failure of the Organisation’s telephone system.

ITN manages the PBX installations at the Tokyo and Washington Centres. The Berlin, Bonn and Mexico City Centres manage their PBX installations themselves.

Delegations
The Organisation’s PBX network also provides telephone and fax services for the Dutch, Norwegian, and Swedish Delegations. The Japanese Delegation has a connection with the OECD central PBX. The American, Finnish, and Canadian Delegations manage their own local telephone systems.

Electronic Fax Services
An electronic fax system has been implemented and integrated with the PBX network and Exchange for direct reception and transmission of faxes to and from clients’ Outlook/Exchange accounts. Two fax servers handle twelve out-going and four incoming lines.

Paging Service
ITN also provides paging services for approximately 80 users, using equipment linked to the PBX network. In addition to the principal transmitter and antenna served the Chateau campus area, there are three remote transmitters and antennae, which ensure coverage of annex buildings.

As previously noted, ITN manages the physical cabling infrastructure for the PBX network, as well as for the data network.

Annex VI includes an inventory of PBX network and related software at the Paris Headquarters and at the Information Centres.
IV. Security

The Organisation increasingly relies on external networks - both public (e.g., Internet) and private - for exchange of information. As dependence on external networks grows, however, so too do risks to the integrity and confidentiality of information flows, and to the reliability of information systems. These risks, including computer viruses, unauthorised (“hacker”) intrusion, and “denial of service” attack, can be highly disruptive to the work of the Organisation, and lead to irretrievable loss of information. Security is therefore an important factor in the design and operation of the Organisation’s ICT infrastructure.

Firewalls

Firewalls, combining both packet filtering devices and proxy services, separate resources accessible by the Internet from those accessible only on the OECD’s internal network.

- Public Web servers and other resources available to the Internet are located on specific network partitions protected by firewall (the Internet DMZ). The firewall filters incoming Internet accesses and allows only selected Internet traffic into the DMZ. This traffic is not allowed into the internal network.

- OLISnet servers and other resources available via both external private network and secure Internet SSL VPN are also located on specific network partitions and are protected by a firewall (the Extranet DMZ).

- The firewall filters incoming traffic and allows only selected traffic into the DMZ. This traffic is not allowed into the internal network. The firewalls tightly control any traffic into the internal network, allowing only specific authorized services, such as electronic mail, to pass – and then only through application gateways.

- For outgoing access, all user traffic (mail, HTTP, FTP, etc.) are relayed through application proxy firewalls or through a “stateful” firewall (The term stateful firewall is an industry-wide standard referring to the use of an adaptive security algorithm (ASA) and log tables containing information about all connections made via the firewall.)

- No internal servers are directly exposed to the Internet

- Modems or routers connected directly to desktops are not allowed on the internal network.

Anti-Virus Security

Considerable effort is given to ensuring protection against computer viruses. This includes making sure that staff know how to recognise computer viruses and are aware of their potentially destructive effects. Anti-virus software is installed on desktop PCs, portables, file servers, messaging servers and other servers potentially at risk. Anti-virus signature files on desktop PCs and servers are updated weekly, with interim updates as necessary to deal with specific new computer virus threats. Windows Scripting Host, used by many virulent computer viruses, has been disabled on desktops.

All incoming and outgoing Internet messages are filtered for computer viruses, passing through a dedicated server on which virus signature are automatically updated every hour. Incoming mail with a script or an executable file attachment is held in a quarantine area for two days. A number of automated procedures have been prepared to help deal with severely destructive computer viruses, including quickly switching access to all shared disk drives to read-only mode.

A newly identified threat at the OECD is "spyware", which presents itself through very different forms. Testing is currently underway on various anti-spyware systems.
Intrusion Detection
Three forms of intrusion detection are in use.

1. First, intrusion detection systems have been installed at three points on the external network: at the ISP link, and the Internet and Extranet DMZs. These systems detect traffic patterns typically associated with preliminary attempts from a concerted “hacker” or denial-of-service attack. Alerts are automatically sent to network administrators via email and pager, who then take appropriate action.

2. Second, a vulnerability scanner is used to detect potential security holes on servers on the external DMZ networks. This service, which is regularly updated, looks for known security vulnerabilities, and simulates denial-of-service attacks against these servers. When vulnerability is discovered, the operating system and related applications are updated or re-configured accordingly.

3. Finally, installation and configuration procedures for new computing and network equipment are well documented and carefully followed, to ensure that security vulnerabilities are not inadvertently created. Vendor service packs and, where appropriate, “hot fixes” are regularly applied to implement the latest security features.

External specialists are engaged at least once a year to conduct tests of the intrusion detection security in place at the operating system and application level.

Email Security
Considerable effort has also put in keeping the email flow clean of external spamming pollution, and content inspection (filtering out virus, script, executable, etc.) Incoming email must pass through three levels of inspections before delivery to the user’s mailbox.

In the first and outermost level and at the SMTP protocol level, inspections of the message sender’s identity are performed. Email passes through multi-category filters that inspect its header as well as additional information from the sender. The list of servers relayed by the incoming email is checked against blacklists. Blocks are also in place to prevent OECD mail servers from being used as third party relays. These blocks also prevent abuse or hijacking by external attackers, as well as minimise the impact on the system when mail is received. OECD conforms to industry-standard best practices and participates in fighting unsolicited email by implementing new SPF-policy features to verify email sender identification.
V. Development Priorities

Site renovation / temporary offices in Tour Europe
The OECD headquarters site renovation project will last for several years, involving all staff members during several office and meeting room transitions. During this period, in addition to being affected by the same office transitions, ITN is called upon to address four main challenges:

1. Reorganisation of ICT infrastructure of temporary and new offices and meeting areas
   - In 2003, the reorganisation involved ICT and network installations for 1,000 staff in the Tour Europe office building in La Défense. In 2004, similar restructuring has taken place in the NB, Franqueville and Pascal buildings, parallel to the “closing” of the networks in the Château and the upper floors of NB.

2. Move of staff and associated desktop and network control facilities
   - In 2003-2004, this project involved the move of approximately one thousand staff to Tour Europe, the evacuation of the Château to NB and Pascal, and many other moves across annexes.

3. Rebuild new computing and communications central rooms and networks
   - In 2005/2006, all ICT services, network, servers and telephony will be transferred from the New Building (NB) into a new computer centre located in the La Muette Château. The design phase for the new centre has just finished, involving a special team from ITN. This team is now preparing for the required move of ICT services to the new location. The first step, scheduled for the first quarter of 2005, is to gradually transfer all external operator lines into a new location while minimizing disruption of services.

4. Redesign of network and cabling infrastructure
   - Assist site planning team in the redesign of the entire network and cabling infrastructure for the renovated site.
Hierarchical Storage Management
The volume of information on the Organisation's central computing facilities grows by 40% per year (i.e., doubles every two years). Much of this growth is for legitimate business purposes, though there is a continuing accumulation of files that are inactive and, possibly, no longer needed. The growth of voluminous image, music and video files downloaded from the Internet or contained in e-mail attachments, is of particular concern. Limited policies exist for the governance of these special files, but are not simple to monitor and rely primarily on staff conduct.

Sudden surges in their storage requirements could disrupt critical ICT services for the entire House by saturating available disk space. Furthermore, the cost of disk space and backup equipment required to meet burgeoning storage requirements is diverting limited resources from other important activities.

To help address this situation, a Hierarchical Storage Management (HSM) system will be implemented to alleviate pressures on on-line storage and backup systems. The HSM will separate active from inactive files. Active files will remain on on-line media, and continue to be backed up in accordance with the backup cycles described previously. Inactive files will be automatically migrated to near-line storage. They will be transparently accessible to users, and automatically moved back to on-line media if opened for modification. As files on near-line media will not modifiable, they will need to be backed up only once, and will no longer be part of the weekly full backup cycle.

An HSM system will not, of course, resolve the problem of continued accumulation of inactive, and possibly no longer needed files on near-line and off-line media. An Organisation-wide Storage Management Policy will therefore be developed and introduced in conjunction with implementation of the HSM system. This Policy will include guidelines for appropriate use of the Organisation's storage facilities. It may also entail introduction of some form of storage quotas, for which management would be decentralised to directorates/services, and possibly some form of chargeback.

Computer-Telephony Integration
Computer-Telephony Integration (CTI) is an “enabling” infrastructure technology, which will make possible the deployment of applications providing a new generation of advanced communications services (e.g., voice over IP, unified messaging, etc.). Relative to traditional PBX-based telephony, CTI-based communications technologies offer opportunities for increased productivity, more effective communications, wider reach of communications services, and lower infrastructure and operational costs. The Organisation is therefore evaluating the features and “enterprise readiness” of CTI infrastructure technology, and the new generation of communications services it would make possible.

A move to CTI-based facilities would eliminate the central PBX as a single point of failure for the Organisation’s telephone and fax services.

CTI will also enhance the Client Service area, enabling support staff to identify the caller immediately and to have the client’s history displayed automatically.
**Business Continuity (“Disaster Recovery”)**
A previous external audit of the Organisation’s ICT security drew renewed attention to the need for the Organisation to be able ensure availability of critical computer and communications services to its staff (at headquarters and Centres) and to external clients (officials in Delegations and capitals, Internet clients, etc.) in the event of a major environmental or other disaster putting the main site out of service.

A long-standing goal has been to install equipment in a secondary site which would carry a portion of the normal computing and communications workload, and when necessary take the entire load, albeit in degraded mode. Due to budgetary constraints, however, it has not yet been possible to proceed.
Annex I. On-going Operational Activities

On-going activities related to the operation of the Organisation’s ICT infrastructure include:

**MONITORING of PRODUCTION SYSTEMS**
- Monitoring central computing, network, telecommunications, interphone and pager facilities, and taking prompt remedial action should problems occur; adapting capacity to evolving business needs
- Monitoring security systems (firewall, intrusion detection, mail content inspection, server event logs, network event logs, remote access logs, etc.), and taking prompt remedial action should problems occur
- Monitoring environmental systems (electricity, air conditioning, fire / flooding detection and prevention, access control, alarms), and taking prompt remedial action should problems occur

**MAINTENANCE of PRODUCTION SYSTEMS**
- Installing, configuring, re-locating, removing central computing, network and telecommunications equipment
- Installing new operating system and utility releases, service packs, hot fixes, BIOS upgrades, IOS, CATIOS
- Maintaining the Organisation's cabling / connector infrastructure in good repair; cabling database up-to-date, graphical network documentation up-to-date
- Maintaining anti-virus engine, software and signature files on desktops, servers and the firewall up-to-date
- Maintaining intrusion detection software and signature files for servers on the external network up-to-date
- Managing license renewals, maintenance and support service contracts for central computing, network and telecommunications facilities

**SYSTEM ADMINISTRATION**
- Managing client accounts (XP, Active Directory, Intranet, remote access, etc.), private and shared directory creation/access, storage allocation, archiving of non-active accounts; managing site access
- Managing the central information store and médiathèque; carrying out backup / restore operations
- Managing the stock of replacement server, network, PBX spare parts, and "hot spare" equipment
- Maintaining client databases for hardware, software, central PBX, Voice Mail and Pager system up-to-date
REPORTING and DOCUMENTATION

• Summary reporting for analysis of production down events, resource utilisation, capacity planning; taking pre-emptive remedial action where anomalies are found

• Maintaining documentation on central computing, network and telecommunications architecture, configuration, operating procedures and recovery procedures (and offsite copies) up-to-date

• Maintaining Contact Lists (ITN staff, equipment vendors, software vendors, outsource support, access control) up-to-date; system passwords in front office safe up-to-date

• Maintaining site-related documentation (equipment location, cabling installations, electrical installations, etc.)

• Maintaining knowledge base and client documentation
• Maintaining hardware and software inventory databases

CLIENT SERVICES

• Providing on-going support for resolving desktop, printer, telephony and other reported problems

• Training staff on new systems and features

• Managing support of central ICT services for special events (e.g., Council Ministerial and other high-level meetings; annual maintenance of electrical systems in the New Building and Pascal building, Chateau and Franqueville, and annex buildings; year-end closure; other exceptional events requiring support of central ICT services outside normal working hours)

• Providing specialist technical assistance to ITN staff and Delegations

• Managing change control

SPECIAL PROJECTS

• Testing full recovery procedures for critical applications
• Managing ITN’s participation in EXD projects involving office moves, renovation and security of the Organisation’s physical plant
• Site renovation and move of computer room
• Replacement of electronic fax system
• Replacement of voicemail system
• Installation of unified messaging system
• Installation of IP-Telephony
• Implementation of ITIL methodology
Annex II. ICT Activity Indicators

A. Office Facilities
- 2,300 PCs
- Remote access: 450 laptops and 100 home installations
- 350 printers managed by 2 print servers
  - 100,000 pages printed/day
- Client Support: over 2,500 calls per month; 80% of which are resolved within a day
- E-mail:
  - 600,000 OECD-internal e-mails/month
  - 800,000 incoming Internet e-mails/month,
  - 250,000 outgoing Internet e-mails/month
  - 500 gigabytes of messages stored in private mailboxes
  - 250 gigabytes of messages stored in public folders
  - 170,000 incoming e-mails blocked containing non-cleanable viruses (since January 2004)
  - 500 incoming e-mails/day held in quarantine - majority contain programs as attachments
- Client file storage of 2.4 terabytes on 3 servers:
- Backups:
  - Full backup every weekend: total 6 terabytes, 48 hours required

B. OECD web site
- 24,000 total online pages
- 400,000 visitors to the site/month
- 80,000 pages visited/day
- 11% pages updated/month

C. Network/Communications Facilities
- 2 Fax Servers with 16 lines (12 outgoing and 4 incoming):
- 4000 outgoing faxes/month
- 1200 incoming faxes/month
- Telephone calls: 1,880,000 calls, totalling 6,280,000 minutes, of which:
  - International 1,920,000 minutes
  - Local 3,550,000 minutes
  - National 280,000 minutes
  - Calls to mobiles 300,000 minutes
  - 08/0800 numbers 210,000 minutes
D. OECD Online Information Systems

OLISnet - OECD's Secure Extranet for Government Officials

- Registered OLISnet clients:
  - 13,000 national officials from 2,000 Ministries
  - Over 1,400 clients from 62 International Organisations
  - Nearly 400 clients from 27 non-Member economies

- 200 new account applications per month.
- 15% annual average client growth

- 500 client sessions per day
- 700 client hours - average total daily connect time
- 200,000 client hours per year accessing OECD Committee information
  - documents
  - discussion groups
  - event information
  - publications & statistics

- 50% client access via secure Internet to OLISnet (available since June, 2004)
  - 100% client access via secure Internet expected by early 2005.

OECD Internet Access

- Most Frequent downloads:
  - Current Economic Indicators (Weekly Hot File)
  - Main Economic Indicators
  - Foreign Trade Partner Countries, Monthly
  - Economic Outlook

Summary of ICT Indicators

<table>
<thead>
<tr>
<th>Indicator</th>
<th>2002</th>
<th>2003*</th>
</tr>
</thead>
<tbody>
<tr>
<td>OECD committees and interaction with national administrations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>National officials registered in OLISnet (OECD extranet)</td>
<td>9 600</td>
<td>11 600</td>
</tr>
<tr>
<td>Ministries and agencies with LAN-wide access to OLISnet</td>
<td>90</td>
<td>130</td>
</tr>
<tr>
<td>Delegates registered for committee meetings</td>
<td>35 200</td>
<td>44 400</td>
</tr>
<tr>
<td>Delegate and contact database</td>
<td>108 600</td>
<td>169 800</td>
</tr>
<tr>
<td>OECD Web site</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visits per day</td>
<td>15 000</td>
<td>32 000</td>
</tr>
<tr>
<td>Pages viewed per day</td>
<td>132 000</td>
<td>375 000</td>
</tr>
<tr>
<td>Secretariat use of ICT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mails per month</td>
<td>1.1 million</td>
<td>1.5 million</td>
</tr>
<tr>
<td>Official documents produced per year</td>
<td>11 600</td>
<td>11,000</td>
</tr>
<tr>
<td>Primary statistical databases</td>
<td>&gt;100</td>
<td>&gt;100</td>
</tr>
<tr>
<td>Central data storage (bytes)</td>
<td>1 300 million</td>
<td>1 900 million</td>
</tr>
<tr>
<td>Telephone calls made (minutes)</td>
<td>5.8 million</td>
<td>5.7 million</td>
</tr>
</tbody>
</table>

* Some data relate to March 2003-March 2004
Annex III. Data Network

A. Data Network at Paris Headquarters

A.1 Equipment inventory (active, not including spare parts)

- Cisco Catalyst switches (core, access and server switches)
  - Cat6000
  - Cat5500
  - Cat5509
  - Cat5505
  - Cat4000
  - Cat3750
  - Cat3550
  - Cat3524
  - Cat2940

- Cisco MFSC_II and RSM routers core backbone routers

- Cisco c7204 VRX routers (Internet & Extranet firewalls and routing)
- Cisco c2650 router (Affiliate interconnections)
- Cisco c3725 router (Liaison to Centres)
- Cisco c3620 routers (Extranet OLISDelNet direct dialup for Delegations)
- Cisco c3640 routers (Remote LAN Access)
- Cisco c1600 routers (Facilities Management System & Sevres annex)
- Cisco ASS200 access routers (Remote LAN Access & Home computing)
- Cisco v3000 VPN concentrators (Remote LAN Access & Home computing)
- Cisco PIX (Stateful firewall for application relays)

- Aventail EX1500 SSLVPN gateways (OLISnet and OWA over Internet)
- Motorola X.25 switch (Remote LAN Access & Outgoing modems)

- Access30 (Multiplexing voice & data to CEMT Affilie)
- High-Speed modems to France Telecom “Lignes Spécialisées”

- SITA customer access routers (OLIS/DelNet)
- Access Equipment of commercial information services (SAP, Thompson Finance)

A.2 System software and utilities

- Cisco router Internetwork Operating System
- Cisco catalyst Operating System
- HP-UX
- RedHat and Mandrake Linux OS.
- OpenView HP-UX (Network node management)
- OpenView WinNT (Network node management)
- Cisco CiscoWork (Cisco router & switch management)
- Cisco Secure/ACS (Remote network access authentication/authorisation)
- Security Dynamic ACE/Server (Remote network access authentication/authorisation)
- NetViz (Graphic documentation of network infrastructure)
- Solsoft Security designer (Firewall Security policy management)
- ISS RealSecure Console - IDS
- ISS RealSecure NetworkSensor - IDS
- ISS InternetScanner - IDS
- SNORT – IDS
- BIND – DNS
- SQUID (Proxy & Web Caching)
- Postfix (E-mail Relay)
- SSh (Secure access to public-DMZ servers)

B. Information Centres Data Networks

B.1 Equipment inventory

- Cisco-C1700 routers
- Concentrators/switches

B.2 System software and utilities

- Cisco router IOS version c1700-y-l.112-19.P1
Annex IV. Central Computing Facilities

A. Central Computing Facilities at Paris Headquarters
A.1 Hardware and Software Inventory

Server hardware:
- 151 IBM xSeries servers with an average age of 3 years.
- The processor speeds range from 450 MHz to 2.8 HHz
- Most servers have at least 1 GB of memory.
- 65 Dell or HP desktop PCs for test and backup purposes - average age=3 years
- 6 HP Unix servers
- 2 H 9000 systems
- 4 Series 700 systems

Specialised hardware:
- Multimedia:
  - IPTV equipment for internal video streaming:
    - 2 Audio Tuners (Denon)
    - 4 Tube pre-amplifiers (Behringer)
    - 8 VisCable devices (channel receivers)
    - 7 TV monitor devices (Sony)
    - Magnetoscope (Philips)
    - Input/Output distribution matrix (Vity)
    - Videomics device for generating video titles
  - Video conferencing equipment (internal and external sources):
    - Polyspan view station
    - Cisco RADMCU for multipoint video conferencing
    - 2 RADVision video gateways for LAN/WAN video streams

Operating systems
- Most servers with Windows 2000 Server service pack 3 or 4
- 23 servers run under Window Server 2003
- 60 servers with Windows NT4 SP6a
- 4 servers with Linux version 6.2
- 1 server with SCO-UNIX
- 6 servers with HP Unix versions 10.20 and 11.0

Operating system in-built utilities
- DHCP: Dynamic Host Configuration Protocol for automatic allocation of workstation TCP/IP addresses
- WINS: Windows Internet Name Services for domain name to TCP/IP address resolution

Other utilities
- Quota Advisor, Disk Advisor and Diskeeper on file servers
- NetIQ AppManager for application and OS monitoring
- IBM Director for hardware monitoring
- Microfocus Cobol compiler V 3.1 on 2 servers
- Applix Client Support tool
**Back-end applications**

- MS Exchange 2000 for e-mail
- MS SQL database server version 7 or 2000
- MS Internet Information Server (MIIS) version 5 for WEB applications and publishing
- Lotus Domino server for document databases and WEB publishing
- Vignette for Web publishing
- WebTrends for WWW related statistics
- Adobe Distiller
- MS SMS 2003 for hardware and software inventory, remote connection and software distribution
- WinFrame for terminal server services
- Outlook Web Access for Internet based access to Exchange mailboxes
- FAX Senior V 3.1 integrated with Exchange for incoming and outgoing fax services
- MS SNA server for IBM mainframe connectivity
- ARCServe V9 for domain wide data backups
- MailSweeper for SMTP mail filtering
- McAfee VirusScan and GroupShield
- Sophos AntiVirus
- ISS security suite
A.2 Applications software

A.2.1 Analytical, Statistical and Authoring Systems

- **Statistical Information System (SIS)**
  The new SIS is a corporate facility to manage the production, centralised storage and dissemination of data and metadata. Component modules of the SIS will eventually encompass all aspects of the statistical information life cycle at OECD, including workflow management. Today it includes notably Statworks and MetaStore for managing production data and metadata, OECD.Stat for central storage of validated data and metadata, and PubStat for managing statistical publications. A new browser interface to OECD.Stat is being developed to complement existing data extraction facilities.

- **FAME (Forecasting, Analysis, and Modelling Environment)**
  Fame is time series management and analysis software, which also has extensive graphics facilities. Two Excel add-ins, the OECDFAME Wizard and the FAME/Populator, provide easy access to FAME databases for Excel users.

- **INTERLINK**
  OECD's principal model for macroeconomic policy analysis and projections over the short- and medium-term. The different modules of INTERLINK include a Fortran-based model for policy analysis, a FAME/Excel based solution for developing short-term projections and a model built using the commercial package Troll for projections over the medium-term.

- **AGLINK**
  Model used in conjunction with producing the Agricultural Outlook, based on Troll.

- **SAS**
  SAS (Statistical Analysis System) is an integrated software system providing data access, management and analysis for large cross-sectional databases.

- **Oracle Express**
  Oracle Express is a multidimensional database management system for analytical processing and data reporting.

- **Foreign Trade System (FTS)**
  FTS is specialised software used for the management of voluminous foreign trade statistics.

- **Authoring Environment (AE)**
  AE is a MS Word-based facility which simplifies production of official documents and publications, including the treatment of tables and graphics.
A.2.2 Administrative and Financial Systems

- PEPS (PEOPLESOFT)
  PEPS is used in conjunction with personnel management. The PEPS database contains information on everyone who works, has worked, or wants to work in OECD.

- OPALE
  Opale, drawing on information in PEPS, is used for creation and management of contracts for salaried consultants, auxiliaries, project staff and trainees.

- PATS
  PATS is a time and attendance system used to manage absences and overtime. Directorates’ timekeepers enter annual, home and uncertified sick leave as well as overtime.

- PAYROLL/PENSIONS
  Intranet
  (a) Several applications based on Web technologies are available through the Organisation’s Intranet including:
  - HR Kiosque (for staff consultation of their personnel records)
  - Performance Management (for use in conjunction with annual performance reviews)
  - DETAXE (for management of diplomatic orders)
  - SAFEGE Mapguide (for diffusion of AutoCAD plans)

- SAP
  SAP software is used for the Organisation's budgeting, financial and Treasury management.

- PRISM
  PRISM is a suite of applications including:
  - Missions System, used for the management of official travel.
  - Conference Participants System, used for management of contracts of non-OECD personnel (i.e. invitees, conference costs, non-permanent consultants, candidate interviewees)
  - Translation Request System, used for management of requests forwarded to the Translation Division.
  - Co-Neaburs, used to track planned expenditure, commitments and actual expenditure, against budgets and official data coming from Budget and Finance via SAP.

- ONYX
  Directorates use ONYX for placing office furnishing orders with an external vendor.

- SGT
  SGT is used for billing costs of telephone use.

- Contact Management System
  User for storing information about contacts (job titles, phone numbers, addresses, e-mail and fax addresses, Internet e-mail addresses, etc.), preparing lists of meeting participants, printing labels for envelopes, sending personalised form letters, e-mail or faxes.

- Event Management System
  The Event Management System is used by Directorates and Delegations for the organisation of official meetings.
A.2.3 Online information systems

- OLIS/OLISNET/DELNET
  OLIS provides fast, reliable and secure information exchange and dialogue between Member countries and the Secretariat. Online information available includes official documents, publications, statistics, e-mail, and committee discussion groups.

A.2.4 Records and facilities management systems

- Records Management System (RMS)
  RMS is used for management of official documents of the Organisation.

- Library Management System (LMS)

- Facilities Management System (FMS)

- MULTILIS
  MULTILIS, an online system used for library catalogues, contains the catalogues of five OECD libraries: Central Library, Development Centre Library, ELS Library, PUMA Library and SIGMA Library.

- RIMS (Records Information Management System)
  RMS is used for classification and archiving of documents of the Organisation.

A.2.5 Other Systems

- Photo-Composition System (Creative Suite by ADOBE)

- Authoring Environment
  Authoring Environment allows users to create official documents and publications with the help of templates that ensure conformity to OECD’s presentation standards.

- APPLIX
  Applix is used for the tracking and management of client incidents reported to the Help Desk.
B. OECD Information Centres - Central Computing Facilities

B.1 Washington

Hardware
- 17 Workstations (Pentium 4)
- 1 server Pentium Pro (HP Netserver)
- 3 network printers (HP and Tektronix)
- FAX machine

Operating system and utilities
- Operating systems: Windows XP on 2 workstations

Application software
- MS-Office Professional (Standard Desktop Environment)

B.2 Tokyo

Hardware
- 17 Workstations (Pentium IV)
- 2 servers Pentium
- 7 network printers (Epson)
- FAX machine

Operating system and utilities
- Operating systems: Windows XP 6 workstations

Application software
- MS-Office Professional (Standard Desktop Environment)
- MS-Office Professional Japanese version

B.3 Bonn-Berlin

Hardware
- 14 Workstations (Pentium IV)
- 1 server Pentium
- 13 network printers (HP, Epson, Brother)
- FAX machine
- Picturetel videoconferencing system
- Plasma screen

Operating system and utilities
- Operating systems: Windows XP

Application software
- MS-Office Professional (Standard Desktop Environment)

B.4 Mexico

Hardware
- 10 Workstations (Pentium IV)
- 1 server Pentium (Digital Prioris)
- 2 network printers (Lexmark and Panasonic)
- FAX machine

Operating system and utilities
- Operating systems: Windows XP on 2 workstations

Application software
- MS-Office Professional (Standard Desktop Environment)
A. Desktop Computing

A.1 Equipment inventory
- Desktop PCs: 2300
- Portable PCs: 450
- Printers: 350
- Network Copiers / Scanners: 81

A.2 Desktop software
Standard desktop image is centrally managed and installed on desktop and portable PCs with the following software:
- Ms Windows XP (SP1) Evolution en SP2 dans les 6 prochains mois
- MS Outlook Version XP (2002)
- MS Office Version XP (2002)
- MS Word Version XP (2002)
- MS Excel Version XP (2002)
- MS Powerpoint Version XP (2002)
- MS Photo Editor
- Ms Internet Explorer 6.0 (SP1) Evolution en SP2 dans les 6 prochains mois
- Acrobat Reader 5.05 Evolution en 6.02 dans les 3 prochains mois
- Winzip
- Capture
- NAI Virusscan 4.51 Evolution en 8.01 P2 dans les 6 prochains mois
- IP TV 2.5
A. PBX Network at Paris Headquarters

A.1 Equipment

<table>
<thead>
<tr>
<th>Nouveau Batiment (Site Central)</th>
<th>Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nortel Option 81</td>
<td>Installation - 1986</td>
</tr>
<tr>
<td></td>
<td>Upgraded in 2003</td>
</tr>
<tr>
<td></td>
<td>PABX central et distribution sur Nbat, Château, Norvège, Suède, Finlande</td>
</tr>
<tr>
<td></td>
<td>1300 tph</td>
</tr>
<tr>
<td></td>
<td>27 liens PRI</td>
</tr>
<tr>
<td>Station d’énergie</td>
<td>1980</td>
</tr>
<tr>
<td>Batteries</td>
<td>2000</td>
</tr>
<tr>
<td>Meridian Mail</td>
<td>1995</td>
</tr>
<tr>
<td>Serveur Cieme-infoserv 1</td>
<td>1999</td>
</tr>
<tr>
<td>Serveur Cieme-infoserv 2</td>
<td>1999</td>
</tr>
<tr>
<td>Modem</td>
<td>1999</td>
</tr>
<tr>
<td>Serveur NT</td>
<td>1997</td>
</tr>
<tr>
<td>Serveur NT</td>
<td>1997</td>
</tr>
<tr>
<td>Modem</td>
<td>1996</td>
</tr>
<tr>
<td>Access30</td>
<td>1990</td>
</tr>
<tr>
<td>Access30</td>
<td>1990</td>
</tr>
<tr>
<td>Modem optique</td>
<td>1996</td>
</tr>
<tr>
<td>Modem optique</td>
<td>1996</td>
</tr>
<tr>
<td>Modem</td>
<td>2003</td>
</tr>
<tr>
<td>ITG Trunk</td>
<td>2003</td>
</tr>
<tr>
<td>ITG Trunk</td>
<td>2003</td>
</tr>
<tr>
<td>Fox Cegeltele</td>
<td>2004</td>
</tr>
<tr>
<td>Tunor Completel</td>
<td>2000</td>
</tr>
<tr>
<td>Serveur Call-Pilot</td>
<td>2003</td>
</tr>
<tr>
<td>Serveur OTM</td>
<td>2003</td>
</tr>
<tr>
<td>Bureau NBAT 2185</td>
<td></td>
</tr>
<tr>
<td>Modem</td>
<td>2001</td>
</tr>
<tr>
<td>Modem</td>
<td>2001</td>
</tr>
<tr>
<td>Modem</td>
<td>2001</td>
</tr>
<tr>
<td>Multpleur de TTY</td>
<td>2001</td>
</tr>
<tr>
<td>Multpleur de TTY</td>
<td>2001</td>
</tr>
<tr>
<td>Serveur</td>
<td>2001</td>
</tr>
<tr>
<td>Serveur</td>
<td>2001</td>
</tr>
<tr>
<td>Modem</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Système de messagerie vocale</td>
</tr>
<tr>
<td>Collection des tickets de taxation téléphonique</td>
</tr>
<tr>
<td>Collection des tickets de taxation téléphonique</td>
</tr>
<tr>
<td>Télémaintenance</td>
</tr>
<tr>
<td>Capture des statistiques ACD</td>
</tr>
<tr>
<td>Capture des Logs</td>
</tr>
<tr>
<td>Acces à distance sur SL1</td>
</tr>
<tr>
<td>Acces aux sites distants depuis Nbat</td>
</tr>
<tr>
<td>Déport console de gestion SL1</td>
</tr>
<tr>
<td>Déport console de gestion SL1</td>
</tr>
<tr>
<td>Déport console de gestion MM11</td>
</tr>
<tr>
<td>Déport console de gestion MM11</td>
</tr>
<tr>
<td>Multiplexage Voix et Données sur lien Ldavid</td>
</tr>
<tr>
<td>Multiplexage Voix et Données sur lien A1E</td>
</tr>
<tr>
<td>Lien axe lourd avec Ofeuillet</td>
</tr>
<tr>
<td>Lien axe lourd avec Monaco</td>
</tr>
<tr>
<td>Lien 1 Télécité avec Tour Europe</td>
</tr>
<tr>
<td>Lien 2 Télécité avec Tour Europe</td>
</tr>
<tr>
<td>Lien 1 Télécité avec Pascal</td>
</tr>
<tr>
<td>Lien 2 Télécité avec Pascal</td>
</tr>
<tr>
<td>Lien 1 IP avec Tour Europe</td>
</tr>
<tr>
<td>Lien 2 IP avec Tour Europe</td>
</tr>
<tr>
<td>4 liens T2 avec Cegeltele</td>
</tr>
<tr>
<td>lien LL vers Boulogne</td>
</tr>
<tr>
<td>Test messagerie unifiée</td>
</tr>
<tr>
<td>Gestion des PBXs</td>
</tr>
<tr>
<td>Déport console de gestion Option 81</td>
</tr>
<tr>
<td>Déport console de gestion Option 81</td>
</tr>
<tr>
<td>Déport console de gestion MM13</td>
</tr>
<tr>
<td>Déport console de gestion MM13</td>
</tr>
<tr>
<td>MAJ automatique des PBXs</td>
</tr>
<tr>
<td>MAJ automatique de Meridian Mail</td>
</tr>
<tr>
<td>Connexion sur sites distants</td>
</tr>
</tbody>
</table>
### Nouveau Batiment Visio

<table>
<thead>
<tr>
<th>Composant</th>
<th>Année</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nortel Option-11 V23.47</td>
<td>2000</td>
<td>Switching liens ISDN pour les Visio-conférences</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 50 tph</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 2 liens PRI</td>
</tr>
<tr>
<td>Station d'énergie</td>
<td></td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Batteries</td>
<td>2000</td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Ecran</td>
<td>2000</td>
<td>Console de gestion</td>
</tr>
<tr>
<td>Modem</td>
<td>2000</td>
<td>Télémaintenance</td>
</tr>
<tr>
<td>Réceptions satellites</td>
<td></td>
<td>Equipements liés aux receptions satellites</td>
</tr>
</tbody>
</table>

### Franqueville

<table>
<thead>
<tr>
<th>Composant</th>
<th>Année</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nortel Option-61 R3</td>
<td>1995</td>
<td>Distribution sur Franqueville-1, 400 tph</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 3 liens PRI</td>
</tr>
<tr>
<td>Station d'énergie</td>
<td></td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Batteries</td>
<td></td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Console de gestion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modem</td>
<td></td>
<td>Télémaintenance</td>
</tr>
<tr>
<td>Modem optique</td>
<td>1996</td>
<td>Lien 1 axe lourd avec Maillot</td>
</tr>
<tr>
<td>Modem optique</td>
<td>2004</td>
<td>Lien 2 axe lourd avec Maillot</td>
</tr>
<tr>
<td>Modem optique</td>
<td>1996</td>
<td>Lien 1 axe lourd avec Ingres</td>
</tr>
<tr>
<td>Modem optique</td>
<td>1996</td>
<td>Lien 2 axe lourd avec Ingres</td>
</tr>
</tbody>
</table>

### Pascal

<table>
<thead>
<tr>
<th>Composant</th>
<th>Année</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nortel Option-11 R3</td>
<td>2004</td>
<td>Distribution sur Pascal (partie de Nbat)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 170 tph</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 2 liens PRI</td>
</tr>
<tr>
<td>Station d'énergie</td>
<td></td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Batteries</td>
<td>2004</td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Modem</td>
<td>2004</td>
<td>Télémaintenance</td>
</tr>
<tr>
<td>Modem optique</td>
<td>2004</td>
<td>Lien 1 interne avec site central</td>
</tr>
<tr>
<td>Modem optique</td>
<td>2004</td>
<td>Lien 2 interne avec site central</td>
</tr>
</tbody>
</table>

### Ingres

<table>
<thead>
<tr>
<th>Composant</th>
<th>Année</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nortel Option-61 V25.40</td>
<td>1993</td>
<td>Distribution sur annexe Ingres</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 290 tph</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 3 liens PRI</td>
</tr>
<tr>
<td>Station d'énergie</td>
<td>1993</td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Batteries</td>
<td>2001</td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Console de gestion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modem</td>
<td></td>
<td>Télémaintenance</td>
</tr>
<tr>
<td>Modem optique</td>
<td>1996</td>
<td>Lien 1 axe lourd avec Site Central</td>
</tr>
<tr>
<td>Modem optique</td>
<td>1996</td>
<td>Lien 2 axe lourd avec Site Central</td>
</tr>
</tbody>
</table>

### Maillot

<table>
<thead>
<tr>
<th>Composant</th>
<th>Année</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- 220 tph</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 2 liens PRI</td>
</tr>
<tr>
<td>Station d'énergie</td>
<td></td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Batteries</td>
<td></td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Console de gestion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modem</td>
<td></td>
<td>Télémaintenance</td>
</tr>
<tr>
<td>Modem</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modem optique</td>
<td>1996</td>
<td>Lien 1 axe lourd avec Site Central</td>
</tr>
<tr>
<td>Modem optique</td>
<td>2004</td>
<td>Lien 2 axe lourd avec Site Central</td>
</tr>
</tbody>
</table>

### Octave Feuillet

<table>
<thead>
<tr>
<th>Composant</th>
<th>Année</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nortel Option-11 R3</td>
<td>1995</td>
<td>Distribution sur annexe Ofeuillet et Délégations Hollande,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 70 tph</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 2 liens PRI</td>
</tr>
<tr>
<td>Station d'énergie</td>
<td>1995</td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>-------------------</td>
<td>------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Batteries</td>
<td>2001</td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Console de gestion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modem</td>
<td></td>
<td>Télémaintenance</td>
</tr>
<tr>
<td>Modem optique</td>
<td>1996</td>
<td>Lien axe lourd avec Site Central</td>
</tr>
</tbody>
</table>

**Monaco**

<table>
<thead>
<tr>
<th>Nortel Option-11 R3</th>
<th>1997</th>
<th>Distribution sur annexe Monaco et Suede</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>150 tph</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 liens PRI</td>
</tr>
<tr>
<td>Station d'énergie</td>
<td>1997</td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Batteries</td>
<td>2001</td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Console de gestion</td>
<td></td>
<td>Télémaintenance</td>
</tr>
<tr>
<td>Modem</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modem optique</td>
<td>1996</td>
<td>Lien axe lourd avec Site Centrale</td>
</tr>
</tbody>
</table>

**Louis David**

<table>
<thead>
<tr>
<th>Nortel Option-11 R3</th>
<th>1995</th>
<th>Distribution sur annexe Ldavid</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>40 tph</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 liens PRI</td>
</tr>
<tr>
<td>Station d'énergie</td>
<td>1995</td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Batteries</td>
<td>2001</td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Console de gestion</td>
<td></td>
<td>Télémaintenance</td>
</tr>
<tr>
<td>Access30</td>
<td>1995</td>
<td>Multiplexage Voix et Données sur lien Ldavid</td>
</tr>
<tr>
<td>Modem</td>
<td></td>
<td>Télémaintenance</td>
</tr>
</tbody>
</table>

**Boulogne**

<table>
<thead>
<tr>
<th>Nortel Option-11 R25.4</th>
<th>1994</th>
<th>Distribution sur annexe Boulogne</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>150 tph</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 liens PRI</td>
</tr>
<tr>
<td>Station d'énergie</td>
<td>1994</td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Batteries</td>
<td>2001</td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Console de gestion</td>
<td></td>
<td>Télémaintenance</td>
</tr>
<tr>
<td>Modem</td>
<td></td>
<td>Télémaintenance</td>
</tr>
<tr>
<td>Tunor Compleetel</td>
<td></td>
<td>Lien LL vers Site Centrale</td>
</tr>
</tbody>
</table>

**Issy Les Moulineaux**

<table>
<thead>
<tr>
<th>Nortel Option-11 R25.4</th>
<th>1994</th>
<th>Distribution sur annexe Issy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>180 tph</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 liens PRI</td>
</tr>
<tr>
<td>Station d'énergie</td>
<td>1994</td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Batteries</td>
<td>2001</td>
<td>Alimentation 48V</td>
</tr>
<tr>
<td>Console de gestion</td>
<td></td>
<td>Télémaintenance</td>
</tr>
<tr>
<td>Modem</td>
<td></td>
<td>Télémaintenance</td>
</tr>
</tbody>
</table>
A.2 Telephone Handsets
- 2500 Nortel Taurus 3904 handsets
- 1500 analog handsets

A.3 Telephony Software
- CIEME / InfoServe
  Progiciel permettant la récupération de données téléphoniques (tickets) concernant les communications traitées par l'autocommutateur NORTEL de l'OCDE.
- Call Pilot Version 3.2
  - Voicemail system to replace Meridian Mail.
  - Unified Messaging System integrated with Outlook.
  - Testing underway
- Optivity Manager
  - Administration of ADDS / MOVES / CHANGES for telephone system
  - Testing underway

A.3. Paging Facilities (linked to PBX network)
- 1 central system:
  - ASCOM-NIRA Teletracer 2600
  - Transmitter and antenna installed in New Building in 1993
  - Updated and extended to Tour Europe in 2004
- 9 remote transmitters and antennas in annex buildings
- 80 individual paging units: ASCOM-NIRA
### B. PBXs at the Information Centres

<table>
<thead>
<tr>
<th>Installation</th>
<th>Washington</th>
<th>Tokyo</th>
<th>Mexico</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nortel Option-11 V23.47</strong></td>
<td>1999</td>
<td>Distribution sur agence de Washington</td>
<td>Distribution sur agence de Tokyo</td>
</tr>
<tr>
<td></td>
<td></td>
<td>20 tph</td>
<td>10 tph</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Messagerie intégrée</td>
<td>Messagerie intégrée</td>
</tr>
<tr>
<td></td>
<td></td>
<td>liens analogiques</td>
<td>liens analogiques</td>
</tr>
<tr>
<td><strong>Station d’énergie</strong></td>
<td>Alimentation 48V</td>
<td>Alimentation 48V</td>
<td></td>
</tr>
<tr>
<td><strong>Batteries</strong></td>
<td>Alimentation 48V</td>
<td>Alimentation 48V</td>
<td></td>
</tr>
<tr>
<td><strong>Console de gestion</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Modem</strong></td>
<td>Téléaintenance</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Nortel Option-11</strong></td>
<td>1994</td>
<td>Distribution sur agence de Tokyo</td>
<td>Nortel Option-11 (managed locally by Center staff)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 tph</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Messagerie intégrée</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>liens analogiques</td>
<td></td>
</tr>
</tbody>
</table>

- **Bonn**
  - Siemens (managed locally by Center staff)

- **Berlin**
  - Siemens (managed locally by Center staff)
Annex VII. Outsourced ICT activities

MAINTENANCE
- Installation and maintenance of copper and fibre optic cabling for data and telephone networks
- PCs, printers and office equipment
- Network equipment and software: maintenance and support
- Servers, operating system software and utilities: maintenance and support
- Telephony PBX, handsets and network: maintenance, support and operation
- External audits of NT domain and network security
- Design and support of the Organisation's ICT security "firewall"
- Systems engineering support e.g. problem resolution; migration to Windows 2000, to Exchange 2000 and to SQL Server 2000; monitoring utilities, backup/restore hardware and software
- Network Engineering support e.g. problem resolution; secure remote LAN access; Internet traffic prioritisation; intrusion detection; computer virus protection

SOFTWARE DEVELOPMENT & SERVICES
- Administrative/Financial applications development, e.g. Development and implementation of payroll system was substantially outsourced.
- Analytical/Statistical applications development, e.g. development & implementation of applications such as Tariff & Trade Browser, PSPE database application for PUM, SEC statistical application for STD, TROLL prototype for analytical work in ECO
- OECD web site: Application development and ongoing specialist support.
- OLISnet: Application programming and ongoing specialist support.
- Application programming for Event Management and Room Reservation Systems
- Programming for Web-based business applications
- Help Desk and Desktop Equipment Support Services
- Office moves of telephones and desktop equipment

TELECOMMUNICATIONS
- International Data network linking OECD Centres, travelling staff, and member country administrations
- Metropolitan area network (Links to Annexes)
- Link to public Internet (incoming, outgoing and e-mail)
- Business communications services: remote access and security - specialist advice and guidance.
- Voice Services (local, national, international, to GSM)

HARDWARE Installations
- Desktop Equipment (PCs, printers, laptops)
- Network and Communications Equipment (Network, remote access, telephone systems, etc.)
- Server and Video/Multimedia Equipment

SOFTWARE Licenses
- Network and security software: e.g. Network monitoring and traffic prioritisation, backup, etc.

OFFICE MOVES
- Major tasks partially or fully outsourced:
  - Installation of local PBX
  - Cabling for voice/data, data/voice link with La Muette
  - PC moves