The Commonwealth of Massachusetts
AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

A. JOSEPH DeNUCCI
AUDITOR

NO. 2004-0002-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION

July 1, 2002 through April 7, 2004

OFFICIAL AUDIT REPORT
JUNE 30, 2004

TABLE OF CONTENTS

INTRODUCTION

The Office of Consumer Affairs and Business Regulation (OCABR) was created under Chapter 24A, Section 1 of the Massachusetts General Laws. The Office, which is headed by a director appointed by the Governor, is located at 10 Park Plaza, Boston, Massachusetts and employs 28 people. The OCABR's mission is to be the state's watchdog charged with educating, informing and protecting consumers. OCABR staffs various consumer hotlines; investigates consumer problems; publishes educational brochures, alerts, and reports; conducts surveys of consumer needs; establishes programs and services to assist consumers in understanding their rights and responsibilities in consumer transactions; recommends and implements consumer protection policies; and monitors the marketplace to promote fair and honest competition. The Office has seven regulatory agencies under its supervision, namely the Department of Telecommunications and Energy, Division of Energy Resources, Division of Banks, Division of Insurance, Division of Professional Licensure, Division of Standards, and the State Racing Commission. During fiscal years 2003 and 2004, appropriations were $1,533,687 and $1,439,583, respectively.

The OCABR and its seven agencies throughout the state are coordinated by the information technology services provided by the Information Technology (IT) Department. The IT Department is staffed by three people headed by the Director of IT. The IT Department's stated mission is to provide and support high quality business solutions and information technology services that improve the lives of citizens, businesses, and employees. The Office operates a number of application systems that include the Consumer Database, which is an access database application that allows staff on the consumer hotline to log calls and record consumer names and issues, and to take requests for educational brochures and other assistance. Also, the Home Improvement Database allows consumers to research a contractor's history of arbitration and guaranty funds claims and records of hearings and other pertinent material. The OCABR uses the Lemon Law Database to record consumer complaints and their resolution.

At the time of our audit, the OCABR's IT systems were connected through the Commonwealth's wide area network to the Administration and Finance's Information Technology Division's (ITD) data center for access to the Massachusetts Management Accounting and Reporting System (MMARS), which is the Commonwealth's centralized accounting information system, and to the Human Resources/Compensation Management System (HR/CMS), which is the Commonwealth's human resources and payroll system.

The IT infrastructure at OCABR consists of 10 networked file servers and 118 desktop computers. The OCABR relies on Microsoft Office Suite products to support its business activities. In addition, OCABR

has implemented Mass Mail, which is an ITD-supported centralized e-mail system utilizing Windows 2000 and Microsoft Outlook.

The Office of the State Auditor's (OSA) examination focused on an evaluation of IT-related controls over OCABR's IT operations and a review of mission-critical applications.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope:

Our audit, which was conducted from September 3, 2003 through April 7, 2004, consisted of an examination of IT-related activities at the Office of Consumer Affairs and Business Regulation (OCABR) for the period of July 1, 2002 through April 7, 2004. Our audit scope included internal controls related to the organization and management of IT activities and operations; an examination of IT policies and standards for IT functions, business continuity and contingency planning, on-site and off-site storage of magnetic media, physical security, system access security, environmental protection, and hardware and software inventory. We also performed a review of selected mission-critical application systems at OCABR.

Audit Objectives:

The primary objective of our audit was to determine whether adequate controls were in place and in effect to provide reasonable assurance that control objectives would be met for selected areas within the IT environment and that application systems were in place to assist the OCABR in meeting its mission. We sought to determine whether IT organizational and management controls were in effect over information technology activities to ensure that such activities are managed effectively and efficiently and that IT policies and procedures are adequately documented.

Regarding system availability, we determined whether controls were in place to provide reasonable assurance, through a business continuity and contingency plan, that required IT processing and access to data files could be regained within an acceptable period of time should IT systems be rendered inoperable or inaccessible. In conjunction with reviewing business continuity and contingency planning, we determined whether adequate on-site and off-site storage of backup copies of magnetic media was in effect to assist recovery efforts.

We sought to determine whether controls over IT resources were in place regarding physical security, system access security, and environmental protection to safeguard computer equipment and data files at the OCABR file server room and offices located at 10 Park Plaza in Boston.

Our objective with respect to the OCABR's hardware and software inventory was to determine whether adequate controls were in place and in effect to provide reasonable assurance that IT-resources were

properly accounted for and safeguarded against unauthorized use, theft, or damage. We reviewed seven application systems installed at OCABR to assess their relative usability, security, and availability.

Audit Methodology

To determine the audit scope and objectives, we performed pre-audit steps, which included obtaining and recording an understanding of relevant operations, including the IT infrastructure and in-house software applications, reviewing documentation and interviewing staff regarding OCABR's mission, operations, and IT organization and management. We interviewed the OCABR's Director of IT, the Systems Analyst, Budget Director and other OCABR staff to obtain an understanding of the OCABR's operations, the IT systems infrastructure, the IT control environment, and the organization of the IT Department. To accomplish a preliminary review of the adequacy of general controls over IT-related functions and assets, we evaluated the degree to which the OCABR had documented, authorized, and approved IT-related control policies and procedures.

To assess the adequacy of general controls regarding IT-related operations, we interviewed OCABR staff, observed operations, and performed selected audit tests. We documented evidence acquired through the course of our review and assessed strengths and weaknesses of the internal control system pertaining to business continuity and contingency planning, physical security, system access security, environmental protection, hardware and software inventory, and selected mission-critical applications.

Regarding our examination of organization and management, we interviewed IT senior management; requested documented IT policies and procedures; reviewed and analyzed the existing IT-related policies, standards, procedures and strategic plans to determine their adequacy; and assessed IT-related management practices. We interviewed IT management and staff to determine whether an IT-related steering committee was in place and operating for the purpose of providing adequate oversight of IT functions and processes. To determine whether the IT-related job descriptions and specifications were up-to-date and reflected current responsibilities and technological knowledge requirements, we obtained a current list of the personnel employed by the IT Department and compared the list to the IT Department organizational chart and the employee's IT-related responsibilities at the time of the examination. We reviewed the adequacy of IT-related operational and management controls through interviews, documentation review, and observation regarding mission, segregation of duties, and extent of management supervision.

To assess the adequacy of controls to provide continued operations, we assessed the degree to which business continuity and continuity plans were required for the OCABR and whether steps had been taken

to implement recovery and contingency plans to regain important operations should IT systems be rendered inoperable or inaccessible. In addition, we interviewed the OCABR's IT staff and business process owners to determine whether a written, tested business continuity and contingency plan was in place, the criticality of application systems had been assessed, and that risks and exposures to computer operations had been evaluated. We also determined whether an alternate processing site had been designated to permit timely restoration of IT capabilities and, if necessary, whether an agreement had been established with the entity providing the alternate site. The alternate processing site would allow OCABR to regain processing should its processing site be damaged or become inaccessible. Further, through interviews with the OCABR's IT staff and an inspection of the on-site and off-site facilities, we reviewed OCABR's backup procedures and assessed the degree to which copies of backup media were stored in secure on-site and off-site locations.

To determine whether IT-related assets were adequately safeguarded from damage or loss, we reviewed physical security over IT resources through observation and interviews with the OCABR IT staff. We determined whether procedures were in place and effect to help prevent unauthorized persons from gaining access to the file server room and whether personnel authorized to access the file server room were specifically instructed in physical security operational standards and procedures. We reviewed potential risk factors regarding physical security through inspection of the file server room and interviews with the management and staff responsible for the file server room. Through observation, we determined whether the door to the file server room was locked at all times and that there was a list maintained of persons authorized to enter the file server room. We interviewed security personnel for the office building within which OCABR resides. To determine whether vendor agreements were in place to cover responding to hardware failures, we interviewed IT staff and reviewed the appropriate list of contracts, and invoices held in the Fiscal Department.

To determine whether system access security controls were in place to provide reasonable assurance that only those personnel authorized to use the Office's network and microcomputer workstations were able to gain access to programs and data files, we evaluated procedures for logon user ID and password administration. Regarding password administration, we reviewed controls to activate and deactivate user IDs and passwords, require appropriate length and composition of passwords, and to ensure that passwords are periodically changed. We determined the frequency with which all staff authorized to access the automated systems were required to change their passwords.

To determine whether user ID and password security was being properly maintained, we interviewed the Director of IT. To determine whether access privileges were provided to only authorized users, we

reviewed procedures for granting system access and compared a system-generated list of OCABR's current users with an HR/CMS employee list for OCABR. We determined whether procedures were in place to provide reasonable assurance that the OCABR's Director of IT was notified in a timely manner of changes in personnel status (e.g., employment terminations, job transfers, or leaves of absence) which would impact access privileges and possibly require deactivation from the system.

To determine whether IT-related assets at the OCABR's office and file server room were adequately safeguarded from damage or loss, we reviewed environmental protection over IT resources through observation and interviews with the OCABR's IT staff. To determine the adequacy of environmental protection, we conducted a walk-though of the file server room and office area, interviewed the Director of IT, and assessed the sufficiency of environmental protection-related policies and procedures for the file server room and the on-site storage area. During the audit, we determined and verified the presence of certain environmental protection controls, such as a dedicated air conditioning system, fire alarms, hand-held and automatic fire suppression measures, and uninterruptible power supplies.

We obtained and reviewed the IT-related asset inventory record to determine whether the OCABR's hardware inventory records were current, accurate, and valid. We compared recorded data related to a selected sample of computer hardware items from the computer hardware inventory listing to the actual computer hardware on hand, and vice versa. We determined whether computer equipment purchased in fiscal year 2003 was properly recorded on the inventory and that the equipment was available for use. We evaluated the adequacy of inventory controls through tests and observations by assessing the integrity of the inventory record, determining whether computer hardware was properly tagged, and that the serial numbers attached to the items were properly recorded on the inventory list. Further, we reviewed the OCABR's IT inventory record to determine whether it contained the appropriate data fields to identify and indicate value, location and condition of the item and whether the OCABR had conducted an annual physical inventory of IT-related assets.

We determined controls in place at OCABR for software inventory. We obtained the policies and procedures for software use and an inventory record of software. We verified that OCABR utilized software tools to monitor the use of authorized software and update software products installed on the agency's network. We obtained documentation of all application systems installed on OCABR's platform, interviewed the application system owners, and obtained a copy of the databases which were deemed mission critical for further analysis. The analysis of the databases involved using MS Access to determine the composition, structure, table layout and report generating features of the respective applications.

Our review was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) and industry auditing practices. The audit criteria used for our control examinations were based on applicable legal requirements, control objectives, and generally accepted IT control practices. In addition to generally accepted control practices, audit criteria were drawn from CobiT for management control practices. CobiT (Control Objectives for Information and Related Technology), is a generally applicable and accepted standard for good information technology security and control practices that provide a reference framework for management, users, and IT audit, control and security practitioners.

AUDIT CONCLUSION

Based on our audit, we found that information technology-related controls at the Office of Consumer Affairs and Business Regulation (OCABR) were in place to provide reasonable assurance that control objectives would be met for IT organization and management, physical security, system access security, and environmental protection. The selected mission-critical applications examined for the audit appeared to be secure, easy to use and able to generate reports that satisfied user needs. While evaluating IT-related hardware, we found that controls were in place to safeguard the hardware, however, the inventory records needed to be strengthened. Although controls in place provided reasonable assurance that IT resources were recorded on the inventory system of record, inventory control and IT configuration management could be strengthened by including additional information regarding value, location and equipment status. Regarding business continuity and contingency planning, we determined that control practices were not in place to provide reasonable assurance that normal business operations could be resumed at the office in a timely manner should the file servers or microcomputer workstations become unavailable for an extended period. In addition, we determined that control practices and procedures for the generation and on-site and off-site storage of backup copies of magnetic media were adequate. We acknowledge that efforts to implement enterprise-based IT management had been initiated by OCABR and should be continued to support IT governance and improved IT management.

We found that the OCABR has a cohesive organizational and management structure within the IT Department. Our review of organization and management confirmed that OCABR's organizational controls included an established chain of command, clearly delineated reporting responsibilities and points of accountability, and documented job descriptions for information technology staff. IT policies and procedures, although thorough, should be strengthened by developing procedures for system development and program change control.

Regarding system access security, our audit disclosed that the OCABR had established adequate system access security controls over its systems to prevent unauthorized access use. We found that appropriate logon procedures were in place to gain access to system resources. In addition, appropriate control practices were in place for password composition, length and frequency of required change, and that passwords would expire upon reaching a pre-set number of days requiring users to enter a new password to continue having system access. Regarding password composition, passwords were case sensitive, required a minimum of eight characters comprising of upper and lowercase alphabetic characters and numeric and/or special characters, and could not include part of the user's name.

Our audit revealed that adequate physical security and environmental protection were being provided for OCABR's IT-related assets. In this regard, we found that areas housing IT resources were appropriately secured, fire detection and suppression measures were in place, processing areas were well maintained, a fire emergency plan was maintained, and drills were executed which included a posted floor plan of the OCABR indicating exits. The audit team discovered that access for a former employee who had left the agency two years prior had not been deactivated. We found that the swipe card list, which enables physical access to the agency's offices, still had the employee listed. We acknowledge that during the audit the former employee's name was removed from the swipe card access list.

With respect to key management, we determined that the OCABR did not hold a physical key list or know who held physical keys to the agency. We determined that employees and contractors of OCABR's landlord, R.M. Bradley, had been assigned keys to the agency. Although OCABR was aware that R.M. Bradley employees had keys, the agency was unaware of the number and specific individuals having key access and R.M. Bradley's employees and contracted employees also held swipe cards to the agency. Although additional physical keys were not held by OCABR, there was a lack of procedures for authorization, distribution or retrieval of physical keys or swipe cards. In addition, there were no procedures requiring that a list be maintained of people who have been provided with physical keys and swipe cards or that a periodic review be conducted of the authorizations granted for physical keys and swipe cards. However, although the OCABR did not have these procedures in place, their landlord did have procedures in place to collect physical keys from former employees and to delete their swipe cards.

Our review of mission-critical applications at OCABR determined that the applications had been designated as mission critical by OCABR and that appropriate system controls had been established to track consumer complaints.

With respect to business continuity and contingency plans, we found that although OCABR had a draft copy in development, the business continuity and contingency plan was not sufficiently comprehensive and had not been tested for timely restoration of business functions should automated systems be rendered inoperable. With regard to the continued availability of computer operations and access to electronic information, we found that the draft version of the business continuity and contingency plan needed to be updated, enhanced and formalized. Without sufficient business continuity planning, a possible long-term loss of OCABR's computer operations could hinder access to processing capabilities and electronic information needed to perform business functions. Although the OCABR generated and stored backup copies of magnetic media at their on and off-site locations, the OCABR did not have a written interagency agreement in place to continue data processing at an alternative site. In addition, although backup copies

of magnetic media were stored in a secure and an environmentally-controlled on-site location, the media was not stored in a fireproof safe. With regard to off-site storage, we found that backup media was stored in a secure location in a fireproof safe.

Our audit of inventory control of IT-related assets revealed that the extent of information on IT resources needed to be enhanced to more adequately support IT configuration management. Improved controls would help ensure that IT resources would be properly recorded and accounted for on OCABR's inventory system of record. Although the OCABR maintained a perpetual inventory of all equipment, the inventory records needed to be strengthened by adding additional data fields. Appropriate data fields should include, at a minimum: location, cost, serial number, description, date placed in service, and tag number to properly track obsolete or inoperable equipment on its inventory record. At the time of our audit, the IT inventory only included the following data fields: location, serial number, description, and tag number.

AUDIT RESULTS

1. Business Continuity and Contingency Planning

We found that although the OCABR IT Department had addressed business continuity planning by developing a recovery strategy and documenting a draft recovery plan, the recovery strategy had not been formally tested. We also found that documentation regarding operational procedures and logistics issues specific to the alternate processing site needed to be further developed. We acknowledge that OCABR had taken steps to ensure that backup copies of magnetic media were stored in on-site and off-site storage locations and were available for recovery efforts. We note, however, if a disaster were to occur, the restoration of automated systems supported by the IT Department may not be attained within a desired period of time.

We found that OCABR's business continuity and contingency plan needed to be updated and enhanced to adequately reflect changes in OCABR's IT operations. At the time of our audit, we found that the "OCA&BR Business Continuity Plan Draft", dated October 6, 2000, including an updated section as of February 5, 2003 on Network Operations, contained outdated and inaccurate information in some sections of the plan. Since the plan had not been fully documented, the level of content varied from section to section.

We found that the structural content of the plan contained many of the important sections of a business continuity plan. The plan did include, however, appropriate topic areas, such as design and overview of the plan, assumptions, maintenance, testing, organization of disaster response and recovery, administrative computing steering committee, business continuity management team, agency support teams, disaster response, disaster detection and determination, disaster notification, team descriptions, initiation of the business continuity plan, damage assessment/salvage, dissemination of public information, and disaster recovery strategy.

Based on interviews and the extent of information in the draft business continuity plan regarding the importance of automated systems, it appeared that OCABR had not formally assessed the relative criticality of their automated systems nor conducted a risk analysis to determine the extent of potential risks and exposures to IT operations. An adequately developed risk analysis and business impact analysis should identify the relevant vulnerabilities and threats that could damage or cause the systems to be inoperable, the likelihood of the threat and frequency of occurrence for each disaster scenario, the cost of recovering the systems, and the impact of a loss of IT services to agency operations.

We acknowledge that the OCABR had initiated efforts to address business continuity and contingency planning to restore automated functions in a timely manner, but needed to test their recovery strategy and the alternate processing site for computer and network operations. Additionally, the documentation of recovery responsibilities and tasks necessary to carry out OCABR's business functions needed to be enhanced to ensure sufficient guidelines to address various disaster scenarios.

The objective of business continuity planning is to provide reasonable assurance that mission-critical and essential functions will continue or be made available should a disaster cause significant disruption to computer or network operations. Generally accepted practices and industry standards for computer operations support the need to have an ongoing business continuity planning process that assesses the relative criticality of information systems in relation to business goals and impact and develops appropriate recovery and contingency plans, as required.

An effective business continuity and contingency plan should provide specific instructions for various courses of action to address different types of disaster scenarios. The plan should identify the ways in which essential services would be provided without full use of the entity's automated systems and, accordingly, the manner and order in which processing resources would be restored or replaced. The plan should identify the policies and procedures to be followed, detailing the logical order for restoring critical and essential data processing functions either at the original site or at an alternate processing site. In addition, the plan should describe the responsibilities and tasks necessary to transfer and safeguard backup copies of data files, program software, and system documentation from off-site storage to the site being used for restoration efforts. Understandably, if off-site storage of backup media were at the same location as the alternate processing site, the plan should include procedures for activating another off-site storage location should use of the alternate processing site be required.

The success of the business continuity planning process requires management commitment and close involvement by system users in the development and testing of the recovery plans. Importantly, efforts must be made to ensure there is a continued clear understanding and documentation of OCABR's information system environment and that appropriate assessments are made of system criticality and associated risks to support IT and user area plans and business impact. Business continuity test plans and scripts should be developed by IT in conjunction with business process owners and that appropriate change management should be in place to maintain business continuity and contingency policies, procedures and related plans.

We determined that procedures regarding the generation and on-site storage of backup copies of magnetic media were adequate. Our audit confirmed that OCABR's IT Department did have a designated location at the Division of Professional Licensure for off-site storage of backup media and that the location used was adequate. While the backup copies will aide in a recovery strategy, a viable alternate processing site is an essential for recovery strategies where the original site is unavailable.

A comprehensive business continuity and contingency plan should document the OCABR's recovery strategies with respect to various disaster scenarios. The recovery plan should contain all pertinent information needed to effectively and efficiently recover critical operations within the needed time frames.

Recommendation

We recommend that OCABR complete its business continuity plan and provide more detailed information regarding the designated alternate processing site. We further recommend that OCABR develop a test strategy in conjunction with business process owners and conduct sufficient review and test steps to confirm the viability of the recovery strategies. The OCABR should implement procedures to provide reasonable assurance that the criticality of systems is evaluated and business continuity requirements are assessed on an annual basis, or upon major changes to user requirements or the IT environment.

As a necessary requirement to successful recovery, the OCABR should ensure through appropriate testing the viability of the alternate processing site(s). Considerations should be made as to the extent of readiness required by the alternate processing site(s). We further recommend that the business continuity and contingency plan once developed and approved be subject to regular testing to ensure its continued viability and that the plan be periodically reviewed and updated as necessary to ensure that it is current, accurate, and complete. The OCABR staff should be trained regarding their responsibilities to be carried out in the event of an emergency or disaster. To the extent possible, personnel should be made aware of manual procedures to be used when automated processing is delayed for an extended period of time. A copy of the business continuity plan should be stored off-site in a secure and accessible location.

The business continuity plan should address the following:

- Emergency procedures to ensure the safety of all affected staff members of the OCABR
- Recovery procedures meant to bring the business back to the state it was in before the incident or disaster

- Communication or notification procedures with employees, the public, equipment suppliers, and public authorities and media.

- Critical information on continuity teams, affected staff, suppliers, public authorities and media.

- Identification of mission-critical and essential application programs, IT resources and required platforms, personnel and supplies, data files and time frames needed for recovery.

- Documentation detailing the responsibilities and activities of the IT Department and its designated staff.

- Definition of several levels of disruption from minor operator or hardware error, to a major destruction or loss of processing capabilities.

- Emergency test procedures and test criteria.

- Up-to-date information regarding the current processing environment for hardware and operating system software, including communications software and network requirements, utilities, and job control language, for all critical production jobs and systems development facilities.

- Copies of agreements for service and/or hardware replacement should be readily available since access to the agreements could become critical during an emergency.

- Procedures for the purchase and or lease replacement of hardware and other specialized equipment should be noted.

- Completion or latest revision date and identification of who prepared and is responsible for each section of the recovery plan and user area plans should be specified.

We further recommend that OCABR ensure that the business continuity framework includes procedures for reassessing the adequacy of the recovery plan and updating the plan accordingly.

Auditee's Response,

> *In regard to the finding that the OCABR business continuity and contingency planning document needs to be updated and enhanced to adequately reflect the change in IT operations at OCABR, we concur and have already begun to update the document to reflect the changes and recommendations put forward in the report. We are also grateful for the acknowledgement that the OCABR business continuity and contingency planning document contains many of the sections deemed important for a business continuity plan and we are including the additional recommended sections identified in the report.*
>
> *We do want to respond to the statement listed in the finding "Based on interviews and the extent of information in the draft business continuity plan regarding the importance of automated systems, it appeared that OCABR had not formally assessed the relative criticality of their automated systems nor conducted a risk analysis to determine the extent of potential risks and exposures to IT operations." While we have not*

created a "formal" assessment and risk analysis document, we have analyzed and understand our risks. As proof of this, OCABR, in conjunction with its agencies, has put in place, based on criticality of systems, a process that ensures that information can be retrieved in the event of a disaster for any of the OCABR agencies. In addition, we have established a remote site and system in Springfield, MA where mission critical files will be stored and can be accessed. It is our expectation that the Springfield site will go "live" with the first OCABR agency in July of this year. A formal assessment and risk analysis section is being added to the business continuity and contingency planning document.

Auditor's Reply

We are pleased that OCABR will continue its efforts to more fully document its recovery and contingency plans. We believe that OCABR has a clear understanding that the retrieval of backup copies of data files and application programs is one of the first steps in a business continuity and contingency plan to be performed in the event of a disaster, and that an alternate processing site with compatible hardware, systems software, and network capabilities is required. We recommend that responsibilities and tasks to be performed by staff at the alternate processing site be documented and encourage OCABR to develop recovery strategies in conjunction with business process owners. We further recommend that OCABR test the recovery plan using the alternate processing site to determine whether the site can accommodate OCABR's business needs.

GLOSSARY

GAGAS	Generally Accepted Government Auditing Standards.
LAN	(Local Area Network) A communications network that serves users within a confined geographical area. It is made up of one or more file servers, a network operating system, a communications link, and workstations.
Operating system	The operating system is a set of programs required for the computer to operate and manage programs and devices, such as printers, terminals and other peripherals. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk.
Workstations	The workstations are the personal computers that are connected to the LAN and perform stand-alone processing and access the network servers as required.
WAN	(Wide Area Network) A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs). Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.