CS-1(I)
(8-2-2002)

U.S. DEPARTMENT OF COMMERCE
Economics and Statistics Administration
U.S. CENSUS BUREAU
Acting as Collecting Agent For
BUREAU OF JUSTICE STATISTICS
U.S. DEPARTMENT OF JUSTICE

2001 COMPUTER SECURITY SURVEY INSTRUCTIONS

INTRODUCTION

These instructions are provided to assist you in completing the Computer Security Survey questionnaire. **Part A** provides the general instructions. **Part B** provides question-specific instructions.

PURPOSE OF THE SURVEY

The purpose of this survey is to collect information about the nature and extent of computer security incidents experienced by businesses located in the U.S. The data you report will provide information on the impact of computer crime on businesses. Specifically, data from the Computer Security Survey will provide information on the frequency and types of crime involving computers, the monetary losses sustained as a result of computer crime and the cost of computer security.

LEGAL AUTHORITY AND CONFIDENTIALITY OF DATA

Your participation in this survey is voluntary. We are conducting this survey under the authority of Title 13, United States Code, Section 182. By Section 9 of the same law, your report to the Census Bureau is confidential. It may be seen only by persons sworn to uphold the confidentiality of Census Bureau information and used only for statistical purposes from which no firm may be identified. The law also prohibits the sharing of your data with other agencies, exempts the information you provide from requests made under the Freedom of Information Act and ensures that your responses are immune from legal process, including copies retained in your files.

BURDEN HOUR ESTIMATE

Public reporting burden for this collection of information is estimated to vary from 45 minutes to 3 hours per response, with an average of 1½ hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to: Paperwork Project 0607-0725, U.S. Census Bureau, 4700 Silver Hill Road, Stop 1500, Washington, DC 20233-1500. You may e-mail comments to Paperwork@census.gov; use "Paperwork Project 0607-0725" as the subject.

PLEASE INCLUDE THE FORM NAME AND NUMBER IN ALL CORRESPONDENCE. Respondents are not required to respond to any information collection unless it displays a valid approval number from the Office of Management and Budget. This 8-digit number appears in the top right corner on the front of the Computer Security Survey questionnaire.

PART A – GENERAL INSTRUCTIONS

Survey Scope – This survey collects computer security data for nonfarm companies, organizations and associations operating within the United States. Information for crop and animal production should be excluded. However, companies performing agricultural services are included. **Information for business-related activities of religious organizations, nonprofit organizations and organizations that are government owned but privately operated should be included.**

Reporting Entity – Report computer security data for all **domestic operations** of your company, including all subsidiaries, divisions and locations. A company is a business, service or membership organization consisting of one or more establishments under common ownership or control. It includes all establishments of subsidiary companies, where there is more than 50 percent ownership, as well as establishments of firms which this company has the power to direct or cause the direction of management and policies. **Holding companies should include all subsidiaries under their ownership.** For purposes of this survey, exclude data for Puerto Rico, the Virgin Islands and U.S. Territories. If you are unable to consolidate records for the entire company or have reporting questions, please call **1–800–227–1735.**

Company Changed Operational Status –

a. If this company ceased its operation during 2001, complete the form for the period of time the company was in operation. Also, indicate in Question 23, Operational Status, the company's status and the date the company ceased its operation.

b. If this company was sold during 2001, complete the form for the period of time the company was in operation prior to the acquisition. Indicate in Question 23, Operational Status, the company's status, the date the acquisition became effective and the name and address of the successor company.

Reporting Period – Report data for calendar year 2001. If you cannot provide data on a calendar year basis, fiscal year data are acceptable. If fiscal year data are used and your fiscal period ends in January, February or March, report for the fiscal year ending in 2002. Otherwise, report for the fiscal year ending in 2001. Indicate in Question 22, Reporting Period, the exact dates the data represent if they are not for the calendar year.

PART A – *Continued*

Estimates are acceptable – The data requested on the Computer Security Survey may not correspond to your company's records. If you cannot answer a question from your company records, please provide carefully prepared estimates.

How to Report Dollar Figures – Dollar figures should be **rounded** to thousands of dollars.

For example, if the figure is $1,025,628.79, enter:

Mil.	Thou.	Dol.
$ 1	026	

If the figure is less than $500.00, enter:

Mil.	Thou.	Dol.
$	0	

Additional Forms – Photocopies of this form are acceptable. If you require additional forms, contact us at the toll-free number, e-mail address or business address provided at the bottom of this page. In correspondence, please refer to the 11-digit ID number from the questionnaire's address area.

Filing the Report Form – Return your completed form in the pre-addressed envelope. If you are not using the pre-addressed envelope, return it to the address provided at the bottom of this page or fax it to 1–888–300–5192. Make a copy of the completed questionnaire for your company records.

Filing Extensions – If you cannot complete the survey by the due date shown in the upper left corner on the cover of the form, you may request an extension of time by calling the toll-free number, sending an e-mail or writing to the business address provided below. In all correspondence, please refer to the 11-digit ID number located in the questionnaire's address area.

Direct any **QUESTIONS** regarding this form to:

U.S. Census Bureau
1201 East 10th Street
Jeffersonville, IN 47132-0001
Attn: CS-1

Toll-free Number: 1-800-227-1735
FAX Number: 1-888-300-5192
E-mail: css@census.gov

PART B – INSTRUCTIONS BY QUESTION

SECTION I – COMPUTER SECURITY CONCERNS

Question 1 – What are the top three computer security concerns for this company?

Embezzlement – The unlawful misappropriation of money or other things of value BY THE PERSON TO WHOM IT WAS ENTRUSTED (typically an employee), for his/her own use or purpose.

Fraud – The intentional misrepresentation of information or identity to deceive others, the unlawful use of credit/debit card or ATM or the use of electronic means to transmit deceptive information, in order to obtain money or other things of value. Fraud may be committed by someone inside or outside the company.

Theft of proprietary information – The illegal obtaining of designs, plans, blueprints, codes, computer programs, formulas, recipes, trade secrets, graphics, copyrighted material, data, forms, files, lists, personal or financial information, etc., usually by electronic copying.

Denial of service (to Internet connection or e-mail service) – The disruption or degradation of an Internet connection or e-mail service that results in an interruption of the normal flow of information. Denial of service is usually caused by ping attacks, port scanning probes, excessive amounts of incoming data, etc.

Vandalism or sabotage (electronic) – The deliberate or malicious damage, defacement, destruction or other alteration of electronic files, data, web pages, programs, etc.

Computer virus – A hidden fragment of computer code which propagates by inserting itself into or modifying other programs.

Other intrusion or breach of computer systems – Refers to all other intrusions, breaches and compromises of this company's computer systems (such as hacking or sniffing) regardless of whether or not damage or loss were sustained as a result.

Misuse of computers by employees (Internet, e-mail, etc.) – The improper use of company computer resources by employees, such as using the company's computer resources for personal gain, sending personal or improper e-mail, abusing Internet privileges, loading unlicensed software, etc.

Unlicensed use or copying (piracy) of digital products – software, music, motion pictures, etc. – developed for resale – The unauthorized copying or use of software which the company developed or for which it holds the copyright. Classify unauthorized copying or use of other software by employees under "Misuse of computers by employees (Internet, e-mail, etc.)," above.

SECTION II – COMPUTER INFRASTRUCTURE AND SECURITY

Question 2a – In 2001, what types of computer networks did this company use?

Local area network (LAN) – A computer network that spans a small area such as a single building or group of buildings.

Wide area network (WAN) – A computer network that spans a large geographical area. Usually, a WAN consists of two or more LANs.

Process control network (PCN) – A network with an automated control of a process, such as a manufacturing process or assembly line. It is used extensively in industrial operations, such as oil refining, chemical processing and electrical generation. It uses analog devices to monitor real-world signals and digital computers to do the analysis and controlling. It makes extensive use of analog/digital, digital/analog conversion.

Virtual private network (VPN) – A network that is constructed by using public wires to connect nodes. For example, systems that allow you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network.

Electronic Data Interchange (EDI) – A proprietary electronic system used for exchanging business data over a computer network.

Wireless network (e.g., 802.11) – A type of LAN that uses high-frequency radio waves rather than wires to communicate between nodes. 802.11 refers to a family of specifications for an over-the-air interface between a wireless client and a base station or between two wireless clients.

Internet – Inter-connected networks connecting millions of computers globally. Users can access information and applications from other computers and communicate with other users.

Intranet – An internal network similar to the Internet but surrounded by a firewall to prevent access from users outside the company, organization or facility.

Extranet – A network that uses Internet/Intranet technology to make information available to authorized outsiders. Allows businesses to securely share information with selected suppliers, partners, customers or other businesses.

Stand-alone PCs (not on LAN) – Computers that are not connected to company networks, such as a stand-alone workstation. For the purposes of this survey, a stand-alone computer may have Internet access.

Question 2b – In 2001, how many servers did this company have?

A server is a computer or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files. Users on the network may store files on the server. A print server is a computer that manages one or more printers. A network server is a computer that manages network traffic. A database server is a computer system that processes database queries.

Question 2c – In 2001, how many individual PCs and workstations did this company have?

Include both networked and stand-alone PCs and workstations.

Question 2d – In 2001, which of the following types of access to its networks did this company support?

Remote dial-in access – Refers to using devices and other resources that are not connected directly to a workstation to connect to another computer device. Do not include network access through the Internet.

Wireless access to e-mail, Internet and this company's other networks – Wireless access refers to the use of a device or system that will enable access to a network to which it is not physically connected. For example, a cellular or digital phone, some personal digital assistants (PDAs), some laptop computers, thin client, broadband, etc.

Publicly accessible website WITH e-commerce capabilities – E-commerce capabilities refer to the ability of this company's customers or suppliers to effect transactions via computer networks. Such transactions commit the company and the customer/supplier to an exchange – they do not necessarily include making payment associated with the commitment. For example, if a customer orders products via a website with payment made by check at a later date, this is an e-commerce transaction.

Question 3a – In 2001, what types of computer system security technology did this company use?

Anti-virus software – A utility that looks for viruses, alerts the user and quarantines any that are found.

Biometrics – Methods of generating authentication information for a person by digitizing measurements of a physical characteristic, such as a fingerprint, a hand shape, a retinal pattern, a speech pattern (voice print) or handwriting.

Digital certificates – An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

SECTION II – COMPUTER INFRASTRUCTURE AND SECURITY – Continued

Question 3a – Continued

E-mail logs/filters – E-mail logs keep track of incoming/outgoing messages, including the sender and the recipient. Filters are an automated method of searching the content of e-mail for words, viruses or misuse of computer resources.

System administrative logs – Logs which document details of access to computer systems, such as who logged in, which parts of the system were accessed and when the user logged in and out.

Encryption – The translation of data into a format that requires a code to restore it to the original format. To read an encrypted file, you must have access to a secret key or password that allows you to decrypt it.

Firewall – A physical system or program designed to prevent unauthorized access to or from a private network. Firewalls can be implemented through hardware or software, or a combination of both. Firewalls are used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially Intranets.

Intrusion detection system – An intrusion detection system examines all inbound and outbound network activity and identifies suspicious patterns that may signal a network or system attack from someone attempting to break into or compromise a system.

One-time password generators (smart cards, tokens, keys) – A "one-time password generator" is an authentication device such as a one-time token which randomly changes all or part of the user's password, typically every minute, so that the same password is never used more than once. This technique counters the threat of a replay attack that uses passwords captured by wiretapping or other means of hacking.

Passwords (changed every 30 or 60 days, etc.) – A simple authentication technique in which each password is used repeatedly for a period of time, typically 30, 60 or 90 days, to verify an identity.

Question 4a – In 2001, what types of computer security practices did this company have?

Business continuity program for computer systems – A plan that ensures that an organization can continue to operate after a disaster that would normally prevent it from doing so. For example, a dual system back-up of files in a separate physical location or frequent back-up of files to a separate disk.

Disaster recovery program for computer systems – A plan on how to respond to a computer system emergency. It includes procedures for reporting specific types of problems to designated personnel, repairing or replacing damaged systems, etc. It may include a business continuity program.

Corporate policy on computer security – A defined set of practices and guidelines established by the organization to deal with issues involving computer security. Such practices and guidelines can encompass the responsibilities of both the organization and its employees. Employees have been made aware of this policy.

Regular review of system administrative logs – Reviewing system administrative logs on a regular basis to detect suspicious activity beyond normal daily activity.

Periodic computer security audits – Reviews conducted periodically by the company's security office. For example, the company's strike team might simulate computer security situations and then evaluate how the company performed.

Formal computer security audit standards – An established or authoritative set of criteria used to review computer security systems.

Training employees in computer security practices – Training session(s) designed to educate employees on issues dealing with computer security and the employee's role in following the organization's computer security practices.

Question 4b – If this company had a computer system business continuity or disaster recovery program, was it tested, used in an emergency situation and/or updated in 2001?

Tested – A series of operations, checks or dry runs on the company's business continuity or disaster recovery program to ensure that it worked effectively and remained appropriate to the needs of the organization.

Used in emergency situation – The company's computer system business continuity or disaster recovery program was put to the task in an emergency situation.

Updated – The modification of the business continuity/disaster recovery program to ensure its effectiveness against newly defined security threats.

SECTION III – TYPES OF COMPUTER SECURITY INCIDENTS

Questions 5b, 6b, 7b, 8c, 9c, 10c and 11c – How many of these incidents were reported to law enforcement, FedCIRC, ISAC or CERT?

FedCIRC (Federal Computer Incident Response Center) – The central coordination and analysis facility dealing with computer related issues affecting civilian agencies and departments of the Federal Government.

SECTION III – TYPES OF COMPUTER SECURITY INCIDENTS – Continued

ISAC (Information Sharing and Analysis Center) – An ISAC maintains a secure database, analytic tools and information gathering and distribution facilities designed to allow authorized individuals to submit either anonymous or attributed reports about information security threats, vulnerabilities, incidents and solutions. ISAC members also have access to information and analysis relating to information provided by other members and obtained from other sources, such as the U.S. Government and law enforcement agencies, technology providers and security associations, such as CERT®.

CERT® Coordination Center – An organization that studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats and offer information to help improve computer and network security.

SECTION IV – SPECIFIC INCIDENT INFORMATION

Question 12 – For the incidents reported in this survey, in what month did this company's single most significant computer security incident occur?

Record the two-digit number of the month in which the single most significant computer security incident occured. For example, record "06" for the month of June. See the example below.

06	Month

Question 13a – Which of this company's computer networks were affected in this particular incident?

Local area network (LAN) – A computer network that spans a small area such as a single building or group of buildings.

Wide area network (WAN) – A computer network that spans a large geographical area. Usually, a WAN consists of two or more LANs.

Process control network (PCN) – A network with an automated control of a process, such as a manufacturing process or assembly line. It is used extensively in industrial operations, such as oil refining, chemical processing and electrical generation. It uses analog devices to monitor real-world signals and digital computers to do the analysis and controlling. It makes extensive use of analog/digital, digital/analog conversion.

Virtual private network (VPN) – A network that is constructed by using public wires to connect nodes. For example, systems that allow you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network.

Electronic Data Interchange (EDI) – A proprietary electronic system used for exchanging business data over a computer network.

Wireless network (e.g., 802.11) – A type of LAN that uses high-frequency radio waves rather than wires to communicate between nodes. 802.11 refers to a family of specifications for an over-the-air interface between a wireless client and a base station or between two wireless clients.

E-mail system – The electronic transmission of written messages over communications networks. The messages can be notes entered from the keyboard or electronic files stored on disk.

Internet – Inter-connected networks connecting millions of computers globally. Users can access information and applications from other computers and communicate with other users.

Intranet – An internal network similar to the Internet but surrounded by a firewall to prevent access from users outside the company, organization or facility.

Extranet – A network that uses Internet/Intranet technology to make information available to authorized outsiders. Allows businesses to securely share information with selected suppliers, partners, customers or other businesses.

Stand-alone PC (not on LAN) – A computer that is not connected to company networks, such as a stand-alone workstation. For the purposes of this survey, a stand-alone computer may have Internet access.

Question 13b – Which of the following were used to access this company's networks in this particular incident?

Remote dial-in access – Refers to using devices and other resources that are not connected directly to a workstation to connect to another computer device. Do not include network access through the Internet.

Wireless access to e-mail, Internet and this company's other networks – Wireless access refers to the use of a device or system that will enable access to a network to which it is not physically connected. For example, a cellular or digital phone, some personal digital assistants (PDAs), some laptop computers, thin client, broadband, etc.

Publicly accessible website WITH e-commerce capabilities – E-commerce capabilities refer to the ability of this company's customers or suppliers to effect transactions via computer networks. Such transactions commit the company and the customer/supplier to an exchange – they do not necessarily include making payment associated with the commitment. For example, if a customer can order products via a website with payment made by check at a later date, this is an e-commerce transaction.

SECTION IV – SPECIFIC INCIDENT INFORMATION – Continued

Question 14a – To which of the following organizations was this incident reported?
Mark (X) all that apply.

FedCIRC (Federal Computer Incident Response Center) – The central coordination and analysis facility dealing with computer related issues affecting the civilian agencies and departments of the Federal Government.

ISAC (Information Sharing and Analysis Center) – An ISAC maintains a secure database, analytic tools and information gathering and distribution facilities designed to allow authorized individuals to submit either anonymous or attributed reports about information security threats, vulnerabilities, incidents and solutions. ISAC members also have access to information and analysis relating to information provided by other members and obtained from other sources, such as the U.S. Government and law enforcement agencies, technology providers and security associations, such as CERT®.

CERT® Coordination Center – An organization that studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats and offer information to help improve computer and network security.

Question 15 – What was the relationship between the suspected offender and this company at the time of this particular incident?

Foreign competitor – A company located in another country.

Foreign hacker – A hacker located in another country.

Hacker (no known association with this company) – A hacker in an unknown location or known to be located in the U.S.

Question 17 – In 2001, did this company have a separate insurance policy or rider to cover losses due specifically to computer security breaches?

These policies/riders specifically cover computer system break-in exposures in one form or another. The coverages have descriptive names, such as network security liability insurance, hacker insurance, e-commerce liability and Internet security liability.

Question 18c – What was the estimated revenue lost in 2001 due to this unlicensed use or copying?

The estimated loss may be calculated by taking the difference between the number of software applications installed and the number of licensed software applications sold multiplied by the average selling price of the application for the reporting year.

SECTION VI – COMPANY INFORMATION

Question 19a – In 2001, which of the following Internet services, if any, did this company provide?

Question 19b – In 2001, which of the following Internet services, if any, was the PRIMARY business activity for this company?

Internet Service Provider (ISP) – Companies that provide clients access to the Internet and generally provide related services such as web hosting, web page designing and hardware or software consulting related to Internet connectivity.

Web Search Portal – Companies that operate websites that use a search engine to generate and maintain databases of Internet addresses and content in an easily searchable format. Often they provide additional Internet services, such as e-mail, connections to other websites and news or other limited content.

Internet Publishing – Companies that publish content only on the Internet. They do not provide traditional (non-Internet) versions of the content that they publish.

Internet Broadcasting – Companies that broadcast content only on the Internet. They do not provide traditional (non-Internet) versions of the content that they broadcast.

SECTION VI – COMPANY INFORMATION – Continued

Question 20 – What were the total sales, receipts and operating revenue for this company in 2001?

Report sales, operating receipts and revenue for the year for goods produced and distributed or services provided. Include revenue from investments, rents and royalties only if it is the principal business activity of the company (for example: finance, insurance and real estate companies).

Include all operating receipts from taxable operations, as well as total revenue from tax-exempt activities (contributions, gifts, grants, etc.). Report revenues from customers outside the company including sales of products and services to other companies, individuals, U.S. Government agencies and foreign customers. Include transfers to foreign subsidiaries.

Exclude domestic intra-enterprise transfers, sales by foreign subsidiaries, freight charges and excise taxes.

Question 21 – What was the total number of employees on this company's payroll for the pay period which includes March 12, 2001?

Count EACH part-time employee as one.

Exclude contractors, leased and temporary employees.

Include:

- All full- and part-time employees on the payroll during the pay period including March 12, 2001.
- Salaried officers and executives of a corporation.
- Salaried members of a professional service organization or association (operating under State professional corporation statutes and filing a Federal corporate income tax return).
- Employees on paid sick leave, paid vacations and paid holidays.

Exclude:

- Contractors, purchased or managed services, professional or technical services.
- Proprietors or partners of an unincorporated company.
- Full-and part-time leased employees whose payroll was filed by an employee leasing company.
- Temporary staffing obtained from a staffing service.

Question 22 – Does the information reported in this survey cover the calendar year 2001?

If the data reported are for a period other than calendar year 2001, please enter the beginning and ending dates in the month and year boxes provided. For example, if the beginning date is February 2001 and the ending date is January 2002, complete this question as shown below.

	Month	Year		Month	Year
FROM	02	01	TO	01	02

Question 23 – What was this company's operational status at the end of 2001?

Mark (X) the one category that best indicates the operational status of this company at the end of 2001. If the company has ceased operation or been sold, enter the month and year the action became effective. Also, if the company has been sold, provide the name and address of the successor company.

CONTACT INFORMATION

Provide the name, title, telephone number, fax number and e-mail address of the person to contact if we have questions regarding the information provided.