Appendix C

EXAMPLES OF COMMON ABUSES, METHODS AND DETECTION

1	**Eavesdropping and Spying Eavesdropping** For example wiretapping and monitoring of radio frequency emanations. **Spying** Inclusive of criminal acquisition of information by covert observation.	Voice wiretapping methods Observation Tracing sources of equipment used
2	**Scanning** The process of presenting information sequentially to an automated system for the identification of those items that receive a positive response (e.g., until a password is identified)	Printouts from demonstration programmes may be used to incriminate a suspect.
3	**Masquerading** The process of assuming (an intruder) the identity of an authorised user after acquiring the user's ID information	Audit log analysis Password violations Observation Report by person impersonated
4	**Piggyback and Tailgating** Physical piggybacking is a method of accessing to controlled access areas where control is accomplished by electronically or mechanically locked doors. Electronic piggybacking can occur where individuals use terminals in an online computer system and the system automatically verifies identification. Tailgating is the process of connecting a computer user to a computer in the same session as and under the same identifier as another computer user, whose session has been interrupted.	Access observations Interviewed witnesses Examination of journals and logs Out-of-sequence messages Specialized computer programs that analyse characteristics of on line computer user accesses.
5	**False Data Entry** The process of changing data before or during its input to computers (e.g. forging, misrepresenting, or counterfeiting documents; exchanging computer tapes or disks; keyboard entry falsification; failure to enter data; and neutralizing or avoiding controls)	Data comparison Document validation Manual controls Audit log analysis Computer validation Report analysis Computer output comparison Integrity tests (e.g. value limits, logic consistencies, hash totals, cross foot and column totals and forged entry)

6 **Superzapping**

A utility program used as a systems tool to bypass all controls and able to modify or disclose any program or computer-based data. Many program similar to Superzap are available for microcomputers as well. Such powerful utility programs which are used by system programmers and computer operators can be dangerous if it falls into the wrong hands.	Comparison of files with historical copies Discrepancies in output reports, as noted by recipients Examination of computer usage logs

7 **Scavenging**

It is a process to obtain or reuse information that may be left after processing or residual data left in a computer or computer tapes or disks after job execution.	Tracing of discovered proprietary information back to its source Testing of an operating system to reveal residual data after job execution

8 **Trojan Horses**

It is the process of making alteration or covert placement of computer instructions or data in a program so that the computer will perform unauthorized functions. It is the primary method used to insert instructions for other acts of abuse (e.g. logic bombs, salami attacks, and viruses). This is the most commonly used method in computer program-based frauds and sabotage.	Program code comparison Testing of suspected programs Tracing of unexpected events or possible gain from the act to suspected programs and perpetrators Examination of computer audit logs for suspicious programs or pertinent entries

9 **Computer Viruses**

It is a set of computer instructions that can propagate copies of versions of itself into computer programs or data when it is executed within unauthorised programs.	The file size may increase when a virus attaches itself to the program or data in the file. An unexpected change in the time of last update of a program or file may indicate a recent unauthorized modification. If several executable programs have the same date or time in the last update field, they have been updated together, possibly by a virus. A sudden unexpected decrease in free disk space may indicate sabotage by a virus attack. Unexpected disk accesses, especially in the execution of programs that do not use overlays or large data files, may indicate virus activity

10 **Salami Techniques**

It is an automated form of abuse involving Trojan Horses or secret execution of an unauthorised program that causes unnoticed or immaterial debiting of small amounts of assets from a large number of sources or accounts.	Detailed data analysis using a binary search Program comparison Transaction audits Observation of financial activities

11 **Trapdoors**

It is a facility created by programmers to insert code that allows them to compromise the requirements of preventing unintended access to the computer operating systems and unauthorised insertion of modified code, during the debugging phases of program development and later during system maintenance and improvement.	Exhaustive testing Comparison of specification to performance Specific testing based on evidence

12 **Logic Bombs**

It involves a set of instructions in a computer program periodically executed in a computer operating system that determines conditions\ or state of the computer. Such instructions would facilitate the perpetration of an unauthorised or malicious act.	Program code comparisons Testing of suspected programs Tracing of possible gains from the act

13 **Asynchronous Attacks**

These attacks normally force the operating system to perform requested jobs simultaneously, which eventually forces the operating system to use up all the resources available.	System testing of suspected attack methods Repeat execution of a job under normal and secured circumstances

14 **Data Leakage**

This type of computer crime involves the unauthorised removal of data or copies of data from a computer system or computer facility.	Discovery of stolen information Tracing computer storage media back to the computer facility

15 **Software Piracy**

Piracy is the copying and use of computer programs illegally in violation of existing laws. Commercially purchased computer programs are protected by copyright and their use is restricted.	Observation of computer users Search of computer users' facilities and computers Testimony of legitimate computer program purchasers Receivers of copied computer programs

16 **Computer Theft**

Computer theft, burglary, and sale of stolen microcomputers and components are severe problems because the value of the contents of stolen computers often exceeds the value of the hardware taken.	Cross check with ICT asset inventory Identification of equipment Observation Report by owner Audit log

17 **Use of Computer for Criminal Perpetration**

Use of a computer as a tool in a criminal activity such as planning, data communications, or control or even simulating an existing process or modelling a planned method for carrying out a crime, or monitoring a crime (i.e. by the abuser) to guarantee the success of a crime can be carried out easily.	Investigation of possible computer use by suspects Identification of equipment