

DATE March 1, 1993

PROTECTING BUREAU COMPUTERS FROM COMPUTER VIRUSES

1. PURPOSE AND SCOPE. The purpose of this circular is to remind all Bureau employees and contractors of the threat posed by computer viruses, as well as presenting preventive measures which should be taken to protect Bureau computers against computer viruses.

2. POLICY. It is the policy of the Bureau to implement controls and procedures designed to protect information resources from damage and/or destruction by computer viruses and other forms of malicious software.

3. BACKGROUND. Personal computers (PC's), which are used by many Bureau employees and contractors in their daily job functions, are particularly vulnerable to a special kind of threat, namely computer viruses.

A computer virus is an unwanted computer program which attaches itself to (infects) other programs. Once a virus has infected a program, it will continue to spread itself by infecting other programs, both on the computer's hard disk, and on any floppy diskettes used in the computer. One of the most common ways by which viruses spread from computer to computer is through the use of floppy diskettes.

Once a virus has infected a computer, it may perform a wide variety of functions ranging from displaying simple messages on the monitor screen to destroying all of the data and programs on the computer's hard disk, as is the case with the Michelangelo virus. Additionally, once a virus infects a program, it may either begin to perform its functions immediately, or wait for a specific condition to occur (e.g., the Michelangelo virus does not activate until the computer's date is March 6 and the computer is turned on).

Finally, computer viruses, if not properly guarded against, can rapidly spread to large numbers of computers, causing considerable damage and destruction to data and programs. It is therefore, most important that all computer users take seriously the threat of computer viruses. Section 5 of this circular outlines some preventive measures to safeguard against the virus threat. If followed, these guidelines will significantly decrease the risk of valuable information from being damaged or destroyed.

4. REFERENCES. Department of the Treasury Directive TD P 71-10, Chapter 6, Number 5.A, "MALICIOUS SOFTWARE COUNTERMEASURES," dated October 1, 1992.

DATE March 1, 1993

BEP Circular 10-08.12, "MICROCOMPUTER SECURITY POLICY," dated January 25, 1989.

5. PROCEDURES.

A. To protect Bureau computers against viruses, all persons using Bureau computers should:

- (1) Use only Bureau-approved software on Bureau computers.
- (2) Back up data and programs on a regular basis.
- (3) Have anti-viral software installed on the computer on which you are working. If you do not have access to antiviral software, contact the Computer Systems Security Division (CSSD) at 874-3549 or 874-3554.
- (4) Scan computers for viruses on a regular basis.
- (5) Always scan diskettes before using them on any Bureau computer. This includes master and working diskettes containing off-the-shelf software since there have been cases where diskettes received from software manufacturers have been infected with viruses.

B. If you are certain that the computer you are using is infected with a virus, or you suspect that a virus may be present:

- (1) Contact CSSD for assistance.
- (2) Do not use the infected computer in stand-alone mode, or log on to the local area network (LAN) if the computer in question is networked.
- (3) Do not use any diskettes in the infected computer.
- (4) Do not share any diskettes used on the infected computer with co-workers. If a diskette is infected, the virus could be spread to other computers.
- (5) Attach a notice to the front of the computer warning others not to use the computer because it is infected with a virus.

CIRCULAR

No. 10-08.17

DATE March 1, 1993

Your attention to and awareness of these procedures will greatly assist in protecting the Bureau's valuable information resources which you have worked hard to create and maintain. If you have any questions regarding computer viruses or any of the information presented in this circular, contact the Computer Systems Security Division at 874-3554.

6. OFFICE OF PRIMARY RESPONSIBILITY. Office of Management Control.

<SIGNED>

Peter H. Daly
Director

Distribution "E"