

~~CONFIDENTIAL~~

SEP 22 1 55 PM '89

18 September 1989

MEMORANDUM FOR: ADP Control Officers

VIA:
Chief, INFOSEC Division

FROM:
Chief, Systems Administration Branch

SUBJECT: Computer Security Advisory

Attached is a notice being circulated in cooperation between OIT and OS/ISG concerning reports about a potentially damaging computer virus. Please note that the notice is a very low-key response to the reported virus possibility and recommends only things that are already sound advice -- namely backing up disk files. OIT and OS do not recommend altering normal operations or otherwise responding with excess efforts.

This advisory is being distributed to you as the ADP Control Officers to allow you to disseminate the information within your components in a fashion under your control and judgement. However, OIT is requesting specifically that you DO NOT simply resend this AIM document to large numbers of people, since such actions can seriously affect AIM performance. Sending a moderate number of documents with limited distribution is preferable.

Thank you for you cooperation.

/ ISD
1107 Ames
F.Y.I.

~~CONFIDENTIAL~~

CONFIDENTIAL

Columbus Day Virus Alert

Recent articles in U. S. computer trade publications and other public media report the existence of a PC DOS or MSDOS based computer virus known as "Datacrime-2" or the "Columbus Day Virus." Classified sources also confirm the existence of the virus in Europe. The virus is designed to spread among IBM compatible PCs by attaching itself to executable files and then acting on 12 or 13 October 1989 to destroy the DOS file system information on disks, making any files on disk inaccessible.

Based upon limited testing, there is no indication that Agency systems are infected. Nonetheless, users of PCs should be aware of this virus and its potential damage. Software obtained for use on Agency systems through sources other than normal acquisition channels are at greatest risk of contamination. The best protection against the damage caused by computer viruses is a regularly scheduled backup of all programs and data. However, it should be noted that if a virus does occur, special precautions are required when restoring files from backups to prevent re-infection.

Please contact the Information Security Technology Assessment Center (ISTAC), Office of Security, on for additional information or assistance.

STAT

CONFIDENTIAL