REPUBLIKA NG PILIPINAS
REPUBLIC OF THE PHILIPPINES
KAGAWARAN NG EDUKASYON
DEPARTMENT OF EDUCATION
DepEd Complex, Meralco Avenue, Pasig City, Philippines

Tanggapan ng Kalihim
Office of the Secretary

Trunkline: 632-1361 to 70
E-Mail: osec@deped.gov.ph
Website: http://www.deped.gov.ph

AUG 0 4 2003

DepEd MEMORANDUM
No. 260, s. 2003

DISSEMINATION OF NATIONAL COMPUTER CENTER (NCC) ICT ADVISORY RE PREVENTIVE MEASURES TO CONTAIN AND STOP FURTHER SPREADING OF COMPUTER VIRUS

To: Undersecretaries
Assistant Secretaries
Bureau Directors
Regional Directors
Schools Division/City Superintendents
District Supervisors
Heads, Public and Private Elementary and Secondary Schools

1. For the information and guidance of all concerned, enclosed is a copy of National Computer Center (NCC) ICT Advisory No. 2003-03 entitled "Preventive Measures to Contain and Stop Further Spreading of the ***W32/SOBIG Computer Virus***, which is self-explanatory.

2. Immediate dissemination of this Memorandum is desired.

EDILBERTO C. DE JESUS
Secretary

Encl.:
As stated

Reference:
None

Allotment: 1—(D.O. 50-97)

To be indicated in the Perpetual Index
under the following subjects:

BUREAUS & OFFICES
COMPUTER EDUCATION

Madel:c:dissemination of NCC-ICT-Virus
8-1-03

(Enclosure to DepEd Memorandum No. 260, s. 2003)

470-8

"Making ICT Serve the People"
National Computer Center (NCC)
www.ncc.gov.ph

ICT ADVISORY No. 2003-03

To: ALL HEADS OF THE NATIONAL GOVERNMENT DEPARTMENTS/AGENCIES/BUREAUS, GOVERNMENT-OWNED AND CONTROLLED CORPORATIONS, GOVERNMENT FINANCIAL INSTITUTIONS, STATE COLLEGES AND UNIVERSITIES, LOCAL GOVERNMENT UNITS, CONSTITUTIONAL OFFICES, HOUSE OF REPRESENTATIVES, THE SENATE AND THE JUDICIARY

Subject: PREVENTIVE MEASURES TO CONTAIN AND STOP FURTHER SPREADING OF THE W32/SOBIG COMPUTER VIRUS

1. This ICT Advisory is being issued in response to the need to contain and stop further spreading of the W32/SOBIG computer virus (Virus Type: Worm) that first appeared sometime in January 2003 and have made a mutated comeback last June 2003.

2. The said computer virus affects MS-Windows Operating Systems (95, 98, Me, NT, 2000 and XP). It uses a built-in Simple Mail Transfer Protocol (SMTP) client and local Windows Network shares to spread itself. The virus-infected e-mail message uses different Subject Lines and the Message Body asks the reader to see the attached file. When the attached file is opened, it copies itself into the Windows folder and adds registry values that will enable it to run on Windows startup. It can download files into infected computers and run them.

3. Although the virus was reported to deactivate last 14 July 2003, the repercussion of its covert communication capabilities may give rise to unspecified problems when the government's computer infrastructure and security is intentionally breached by foreign and undesirable entities for unknown intentions.

4. In view of the adverse effects of the said virus, all government agencies are advised to: (a) Protect all computers in their offices with an anti-virus software together with updated virus information file; (b) Turn off and remove all unnecessary/unneeded services in the operating system; (c) Configure the e-mail server to block e-mail with file attachments (with file extensions .vbs, .bat, .exe, .pif and .scr) that are commonly associated in spreading a computer virus; and (d) Educate all government computer users not to automatically open e-mail file attachments unless they are expecting to receive an attached file.

5. All government agencies are, therefore, advised to implement network security and data recovery system to ensure continuity of their computerization projects and security of their network infrastructure.

CERTIFIED TRUE COPY
7/24/03
RECORDS SECTION
NATIONAL COMPUTER CENTER

Date Issued: 22 July 2003

DR. IBARRA M. GONZALEZ
Director General

OFFICE OF THE UNDERSECRETARY
RECEIVED
BY:
DATE: 7/31
DEPARTMENT OF EDUCATION, CULTURE & SPORTS