CHECKLIST FOR CLASSIFIED CONTAMINATED SYSTEM

For inadvertent entry of classified information on an unclassified computer system.
Please follow the checklist below.

1. Guard the entire system as if it were classified itself and do not use it further until it is purged by authorized personnel.

2. Turn the monitor off and ensure access to the area is controlled until the computer system has been purged by authorized personnel.

3. Disconnect the LAN cable from the back of the computer and guard any diskettes that were in use at the time the message was received.

4. Protect all details of the contamination at the level of the contamination.

5. Call your unit security manager, your unit computer security officer, the Information Security Office at 5-0755, and the Wing Information Assurance Office at 6-7173 immediately. After normal duty hours contact the Network Control Center at 6-2622.

PRESCRIPTION FOR HANDLING COMPUTER VIRUSES

1. Note the file name and type of virus that is found.

2. Use your anti-virus software to disinfect the computer hard drive or disk. (If you do not have anti-virus software, contact your Unit Computer Security Manager (UCM) or the Wing Information Assurance Office (WIAO) at 6-7173).

3. Check and clean any floppy diskettes used on the system.

4. Contact your UCM and report the virus so a report can be sent to the WIAO.

5. If you know who originated the message or file with the virus, call them and inform them to check their computer system and disks.

6. If you cannot contact your UCM, call the Wing IA Office at 6-7173 or 5-7005 and we will assist you as needed. It is important to report viruses so we can track the effectiveness of the base anti-virus program and assess any needed improvements. However, do not pass along email messages giving virus warnings. Such virus warnings are often hoaxes actually intended to clog the E-mail system.

OPR: 30CS/SCBI **30SWVA33-5, 2 Aug 01**
Supersedes: 30SWVA 33-5, Feb 98 **Distribution: F**

CHECKLIST FOR CLASSIFIED CONTAMINATED SYSTEM

For inadvertent entry of classified information on an unclassified computer system.
Please follow the checklist below.

1. Guard the entire system as if it were classified itself and do not use it further until it is purged by authorized personnel.

2. Turn the monitor off and ensure access to the area is controlled until the computer system has been purged by authorized personnel.

3. Disconnect the LAN cable from the back of the computer and guard any diskettes that were in use at the time the message was received.

4. Protect all details of the contamination at the level of the contamination.

5. Call your unit security manager, your unit computer security officer, the Information Security Office at 5-0755, and the Wing Information Assurance Office at 6-7173 immediately. After normal duty hours contact the Network Control Center at 6-2622.

PRESCRIPTION FOR HANDLING COMPUTER VIRUSES

1. Note the file name and type of virus that is found.

2. Use your anti-virus software to disinfect the computer hard drive or disk. (If you do not have anti-virus software, contact your Unit Computer Security Manager (UCM) or the Wing Information Assurance Office (WIAO) at 6-7173).

3. Check and clean any floppy diskettes used on the system.

4. Contact your UCM and report the virus so a report can be sent to the WIAO.

5. If you know who originated the message or file with the virus, call them and inform them to check their computer system and disks.

6. If you cannot contact your UCM, call the Wing IA Office at 6-7173 or 5-7005 and we will assist you as needed. It is important to report viruses so we can track the effectiveness of the base anti-virus program and assess any needed improvements. However, do not pass along email messages giving virus warnings. Such virus warnings are often hoaxes actually intended to clog the E-mail system.

OPR: 30CS/SCBI **30SWVA33-5, 2 Aug 01**
Supersedes: 30SWVA 33-5, Feb 98 **Distribution: F**