



**COMPUTER VIRUS**  
**REPORTING PROCEDURES FOR USERS**

<b>STEP 1</b>	<b>STOP! DISCONNECT THE LAN CABLE (see reverse side)</b> <i>Discontinue use of the system.</i>
<b>STEP 2</b>	<b>LEAVE THE SYSTEM POWERED UP.</b> <b>DO NOT</b> click on any prompts, close any windows, or shut down the system.
<b>STEP 3</b>	<b>WRITE IT DOWN!</b> Record notes on reverse side. The CFP or IAO will need the details that occurred during or led to the suspected virus attack. (i.e. Received suspicious e-mail with attachments; Inserted unchecked disk; Downloaded unchecked files; etc.)
<b>STEP 4</b>	If PC starts to behave abnormally or if a related message appears on the monitor of the affected system write it down - in doubt <b>WRITE IT DOWN!</b>
<b>STEP 5</b>	<b>REPORT IT IMMEDIATELY!</b> Contact the Comm Focal Point (CFP) immediately and involve your unit IAO as soon as is reasonable (See contact info on Reverse Side)

NOTE:  
 When reporting a suspected virus to your IAO or the CFP ensure that you record notes as needed on reverse side of this form and provide the technician with Your Name and Number.

**CLASSIFIED MESSAGE INCIDENT (CMI)**  
**REPORTING PROCEDURES FOR USERS**

A *CMI* is defined as a classified message that has been sent and/or received over an unclassified network.

<b>STEP 1</b>	<b>STOP! DISCONNECT LAN CABLE (see rev side)</b> <i>Discontinue use of the system and DO NOT print the classified message unless directed to do so</i>
<b>STEP 2</b>	<b>SECURE</b> affected system(s) / printer(s), area / room and. Limit the exposure of the CMI. <b>DO NOT</b> leave the system unsecured. Ensure all affected equipment remains under positive control of authorized personnel.
<b>STEP 3</b>	<b>TAKE NOTES</b> on reverse side of this form as appropriate. Be aware of possible classified info in your notes
<b>STEP 4</b>	<b>REPORT INCIDENT IMMEDIATELY</b> <b>DO NOT</b> discuss details of the CMI over unsecure lines. Call the CFP (See contact info on Reverse Side), your unit IAO, Supervisor and your Unit Security Manager

**INFOCON LEVELS**

INFOCON presents a structured, coordinated approach to defend against and react to adversarial attacks on DoD computer/telecommunication systems and networks. INFOCON levels are as follows:

INFOCON 5: Routine Net Ops: Normal readiness of information systems and networks that can be sustained indefinitely.

INFOCON 4: Increased Vigilance: In preparation for operations or exercises, with a limited impact to the end user.

INFOCON 3: Enhanced Readiness: Increases the frequency of validation of information networks and its corresponding configuration. Impact to end user is minor.

INFOCON 2: Greater Readiness: Increases the frequency of validation of information networks and its corresponding configuration. Impact to administrators will increase and impact to end user could be significant.

INFOCON 1: Maximum Readiness: Addresses intrusion techniques that cannot be identified or defeated at lower readiness levels. Only implemented in limited cases. Could be significant impact on administrators and end users.

**APR 2012**



**COMPUTER VIRUS**  
**REPORTING PROCEDURES FOR USERS**

<b>STEP 1</b>	<b>STOP! DISCONNECT THE LAN CABLE (see reverse side)</b> <i>Discontinue use of the system.</i>
<b>STEP 2</b>	<b>LEAVE THE SYSTEM POWERED UP.</b> <b>DO NOT</b> click on any prompts, close any windows, or shut down the system.
<b>STEP 3</b>	<b>WRITE IT DOWN!</b> Record notes on reverse side. The CFP or IAO will need the details that occurred during or led to the suspected virus attack. (i.e. Received suspicious e-mail with attachments; Inserted unchecked disk; Downloaded unchecked files; etc.)
<b>STEP 4</b>	If PC starts to behave abnormally or if a related message appears on the monitor of the affected system write it down - in doubt <b>WRITE IT DOWN!</b>
<b>STEP 5</b>	<b>REPORT IT IMMEDIATELY!</b> Contact the Comm Focal Point (CFP) immediately and involve your unit IAO as soon as is reasonable (See contact info on Reverse Side)

NOTE:  
 When reporting a suspected virus to your IAO or the CFP ensure that you record notes as needed on reverse side of this form and provide the technician with Your Name and Number.

**CLASSIFIED MESSAGE INCIDENT (CMI)**  
**REPORTING PROCEDURES FOR USERS**

A *CMI* is defined as a classified message that has been sent and/or received over an unclassified network or network of lower classification.

<b>STEP 1</b>	<b>STOP! DISCONNECT LAN CABLE (see rev side)</b> <i>Discontinue use of the system and DO NOT print the classified message unless directed to do so</i>
<b>STEP 2</b>	<b>SECURE</b> affected system(s) / printer(s), area / room and. Limit the exposure of the CMI. <b>DO NOT</b> leave the system unsecured. Ensure all affected equipment remains under positive control of authorized personnel.
<b>STEP 3</b>	<b>TAKE NOTES</b> on reverse side of this form as appropriate. Be aware of possible classified info in your notes
<b>STEP 4</b>	<b>REPORT INCIDENT IMMEDIATELY</b> <b>DO NOT</b> discuss details of the CMI over unsecure lines. Call the CFP (See contact info on Reverse Side), your unit IAO, Supervisor and your Unit Security Manager

**INFOCON LEVELS**

INFOCON presents a structured, coordinated approach to defend against and react to adversarial attacks on DoD computer/telecommunication systems and networks. INFOCON levels are as follows:

INFOCON 5: Routine Net Ops: Normal readiness of information systems and networks that can be sustained indefinitely.

INFOCON 4: Increased Vigilance: In preparation for operations or exercises, with a limited impact to the end user.

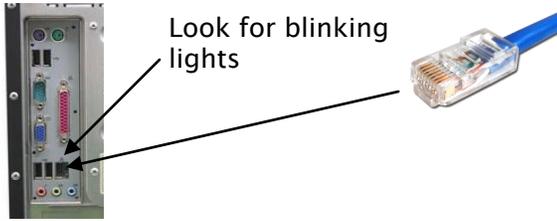
INFOCON 3: Enhanced Readiness: Increases the frequency of validation of information networks and its corresponding configuration. Impact to end user is minor.

INFOCON 2: Greater Readiness: Increases the frequency of validation of information networks and its corresponding configuration. Impact to administrators will increase and impact to end user could be significant.

INFOCON 1: Maximum Readiness: Addresses intrusion techniques that cannot be identified or defeated at lower readiness levels. Only implemented in limited cases. Could be significant impact on administrators and end users.

**APR 2012**

## To disconnect computer from the network



Locate the LAN Jack on rear of computer.  
Depress tab on LAN cable connector and pull gently

**DO NOT Log Off!**  
**DO NOT Power Down!**  
**DO NOT Reboot!**

**Contact the COMM FOCAL POINT (CFP)**

CFP Phone: 722-2666

Your Unit IAO is: \_\_\_\_\_

Unit IAO Phone: \_\_\_\_\_

For additional assistance if needed?  
Wing IA Office: 722-5598

**Do Not Discuss Classified/Sensitive info  
on Unclassified phone. Use STE**

### Notes:

**Use this area to record any known details of incident  
(Protect notes that may be classified or sensitive)**

1. Exact File Name including extension of file contaminated with virus  
or classified info as applicable:

2. Subject of the email containing virus or classified info as applicable:

3. Who sent the file or email:

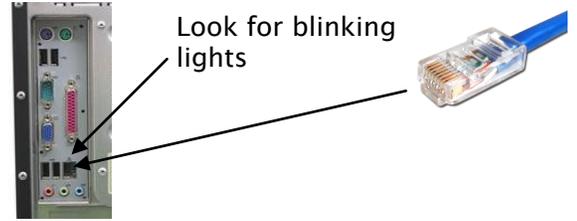
4. List of people who received the file or email as applicable:

5. Was the file or email forwarded beyond original recipients: if so to  
whom?

Additional Information:

**DEPLOY/POST THIS AID NEAR  
COMPUTER WORKSTATIONS**

## To disconnect computer from the network



Locate the LAN Jack on rear of computer.  
Depress tab on LAN cable connector and pull gently

**DO NOT Log Off!**  
**DO NOT Power Down!**  
**DO NOT Reboot!**

**Contact the COMM FOCAL POINT (CFP)**

CFP Phone: 722-2666

Your Unit IAO is: \_\_\_\_\_

Unit IAO Phone: \_\_\_\_\_

For additional assistance if needed?  
Wing IA Office: 722-5598

**Do Not Discuss Classified/Sensitive info  
on Unclassified phone. Use STE**

### Notes:

**Use this area to record any known details of incident  
(Protect notes that may be classified or sensitive)**

1. Exact File Name including extension of file contaminated with virus  
or classified info as applicable:

2. Subject of the email containing virus or classified info as applicable:

3. Who sent the file or email:

4. List of people who received the file or email as applicable:

5. Was the file or email forwarded beyond original recipients: if so to  
whom?

Additional Information:

**DEPLOY/POST THIS AID NEAR  
COMPUTER WORKSTATIONS**