

30 June 2004

Communications and Information

159th Fighter Wing Classified Message Incident (CMI) and Malicious Logic incident (MLI) Reporting

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

Notice: This publication is available digitally on the Headquarters WWW site at: <http://hq.mil>

OPR: 159CF/SCBS (MSgt Tiffanni L. Beckham)
Supersedes: HQ LA ANGI 33-12, 21 May 04

Certified by: 159CF/SCB (MSgt Mark Barrett)
Pages: 9
Distribution: F

This instruction establishes the guidelines and procedures for reporting Classified Message Incidents (CMI) and Malicious Logic Incidents (MLI). It was created to ensure that all personnel have adequate guidance when reporting a CMI and/or a MLI, and are aware of personnel to be notified and actions to be taken should either be detected on 159th Fighter Wing (FW) Wide Area Network.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

1. Glossary of References and Supporting Information. See Attachment 1.

2. Classified Message Incident Reporting. A CMI is a classified message that has been sent or received over an unclassified network. Reporting the detection of classified information on an unclassified system helps to determine how the classified information was introduced to the system, its overall impact on network operations, the effect of Air Force operational missions, and what can be done to prevent future occurrences. All details of a CMI are classified until the systems involved are sanitized of the offending information. Classify notifications and reports until the systems are sanitized and the information is no longer accessible to unauthorized personnel.

3. Roles and Responsibilities. Accomplish the following within your area of responsibility to report a CMI:

3.1. Unit Personnel.

3.1.1. Personnel discovering an electronic file, e-mail message with attachment, document, presentation, etc. containing classified information on a system that is cleared for unclassified only must cease all operations on the affected system immediately. During home station operations report the CMI to the Unit Workgroup Manager (WGM) in person or via secured phone. Details surrounding a CMI are not to be discussed over unsecured phone lines. If the WGM is unavailable contact the Helpdesk at x8312. During exercise operations (ORI/ORE) FW personnel are to notify the Unit Control Center (UCC) immediately.

3.1.2. Ensure that a copy of the HQ LA ANG Form 29, **159FW Classified Message Incident (CMI)/Malicious Logic Checklist**, is located near their workstation at all times.

3.1.3. Users are to follow the steps located on the HQ LA ANG Form 29.

3.2. Unit Workgroup Manager.

3.2.1. Reports CMI information as quickly as possible to the Helpdesk in person or via secured phone. This information cannot be discussed on an unsecured telephone line.

3.2.2. Ensures that the local area network (LAN) cable is disconnected from the affected system

3.2.3. Ensures the affected system is labeled "DO NOT USE" until Network Control Center (NCC) personnel have arrived.

3.2.4. Ensures the system is not left unattended while awaiting NCC personnel arrival.

3.2.5. Ensures that that monitor of the affected system is turned off to prevent viewing of classified information.

3.2.6. Ensure that the affected users' workstations are not used until directed by NCC personnel.

3.3. Helpdesk (HD).

3.3.1. Provides initial assistance by ensuring that the steps on the HQ LA ANG Form 29 have been thoroughly completed.

3.3.2. Opens a HelpBox ticket assigning the job to the Wing Information Assurance (IA) Office.

3.4. Wing Information Assurance Office.

3.4.1. Notifies Information Systems Branch Chief, Network Administrator, Command Post (CP) and Base Information Security Program Manager (ISPM) of CMI event.

3.4.2. Notifies MAJCOM Network Operations and Security Center (NOSC) immediately via secure phone and implements reporting procedures.

3.4.3. Prepare and send a written classified Final Report to the NOSC within 2 hours of completing resolution.

3.4.4. Sends an informational copy of the report to the Unit WGM and the ISPM.

3.5. Network Control Center.

3.5.1. Verifies local containment of the message (i.e. no one has sent it to another installation) and implements sanitization procedures.

3.5.2. When multiple sites are involved, NCC determines the total extent of the contamination and notifies the servicing NCC at the location where the message originated.

4. Malicious Logic Event Reporting. Malicious logic is a program implemented in hardware, firmware, or software, whose purpose is to perform some unauthorized or harmful action. Examples of malicious logic are logic bombs, Trojan horses, viruses, and worms. Network users must report all suspected or

actual malicious logic activity to their Unit WGM. Reporting includes all virus alerts generated by anti-viral software, whether the user believes them to be valid or invalid. NCC personnel determine if the symptoms indicate a known or potential form of malicious logic.

4.1. Unit Personnel.

4.1.1. Every network user must report any suspected or actual malicious logic event to their unit WGM. This includes reporting all virus alerts generated by anti-viral software, whether the user believes them to be valid or invalid. This is so trained personnel can make a determination. If the WGM is unavailable contact the Helpdesk at x8312. During exercise operations (ORI/ORE) FW personnel are to notify the UCC immediately.

4.1.2. Ensure that a copy of the HQ LA ANG Form 29 is located near their workstation at all times.

4.1.3. Users are to follow the steps located on HQ LA ANG Form 29.

4.2. Unit Workgroup Manager.

4.2.1. Reports malicious logic incident as quickly as possible to the Helpdesk.

4.2.2. Ensures that the LAN cable is disconnected from the affected system

4.2.3. Ensures the affected system is labeled "DO NOT USE" until NCC personnel have arrived.

4.2.4. Ensures the system is not left unattended while awaiting NCC personnel arrival.

4.2.5. Ensure that the affected users' workstations are not used until directed by NCC personnel.

4.3. Helpdesk.

4.3.1. Provides initial assistance by ensuring that the steps on the HQ LA ANG Form 29 have been thoroughly completed.

4.3.2. Opens a HelpBox ticket assigning the job to the Wing IA Office.

4.4. Wing Information Assurance Office.

4.4.1. Notifies Information Systems Branch Chief, Network Administrator and CP of the Malicious Logic event.

4.4.2. For valid infections prepare and send reports to the parent NOSC according to the report format in Attachments 4 and 5.

4.4.3. Prepare and send a final report to the parent NOSC within 5 days of the incident being resolved.

4.4.4. Track and compile statistics for all reported malicious logic incidents. Statistical information is used to determine the best methods to prevent future occurrences and facilities.

4.5. Network Control Center.

4.5.1. Verifies local containment of malicious logic (i.e. no one has sent it to another installation) and implements sanitization procedures.

4.5.2. Contact the servicing NOSC as appropriate for assistance when unable to detect, identify, or eradicate the malicious logic.

5. Form Prescribed. HQ LA ANG Form 29, 159FW Classified Message Incident (CMI)/Malicious Logic Checklist.

BY ORDER OF THE GOVERNOR

BENNETT C. LANDRENEAU
Major General, LAARNG
The Adjutant General

OFFICIAL

//Signed//

JOHN B. SOILEAU, JR., COL, LA ANG
Executive Support Staff Officer

Attachment 1
Glossary of References and Supporting Information

References

AFI 33-119, *Electronic Mail (E-Mail) Management and Use*

AFI 33-202, *Network and Computer Security*

AFI 33-204, *Information Assurance Awareness Program*

AFSSI 5020, *Remanence Security*

AFSSI 5021, *Time Compliance Network Order (TCNO) Management And Vulnerability And Incident Reporting*

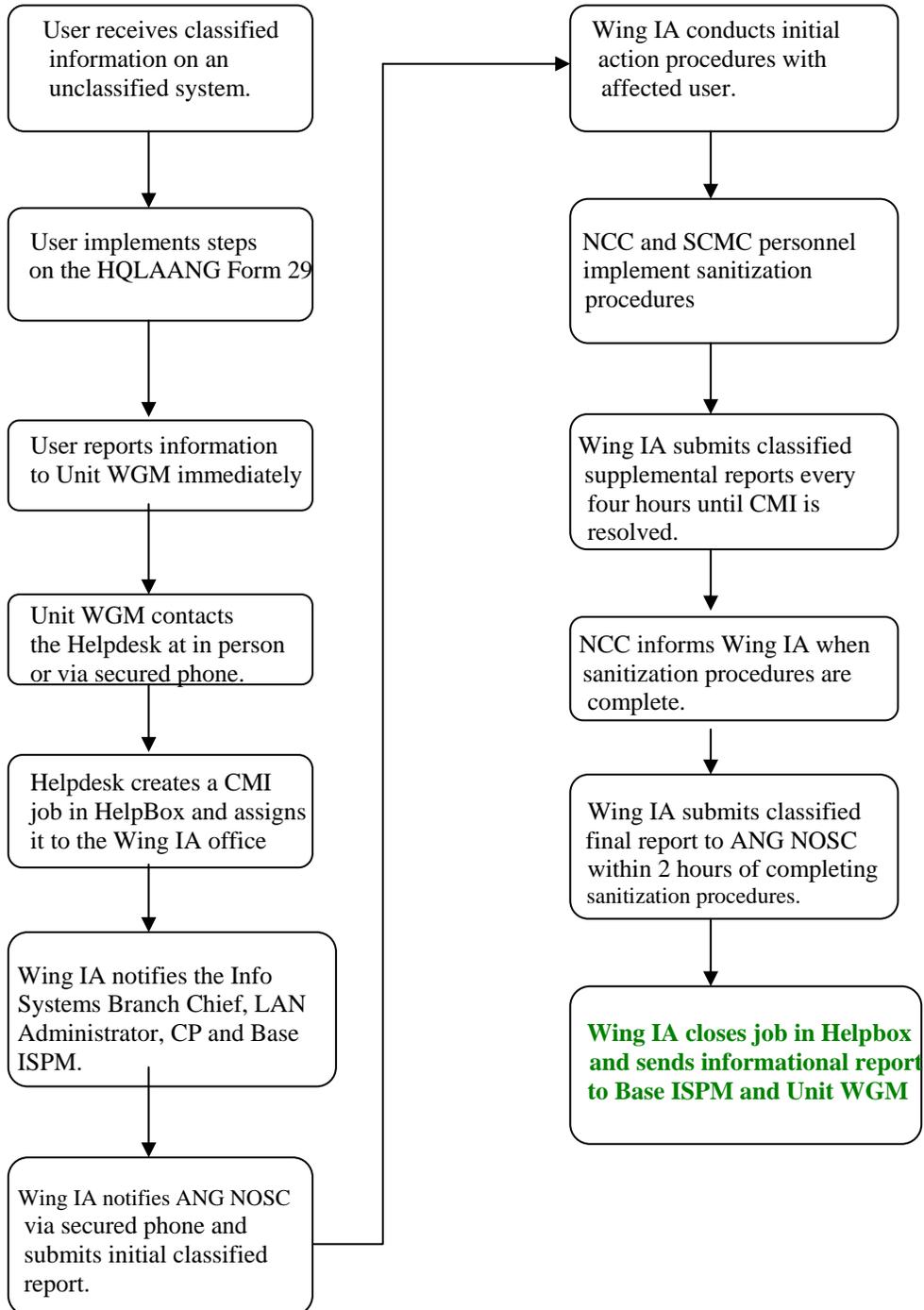
AFSSI 5023, *Viruses and Other Forms of Malicious Logic*

AFSSI 5027, *Network Security Policy*

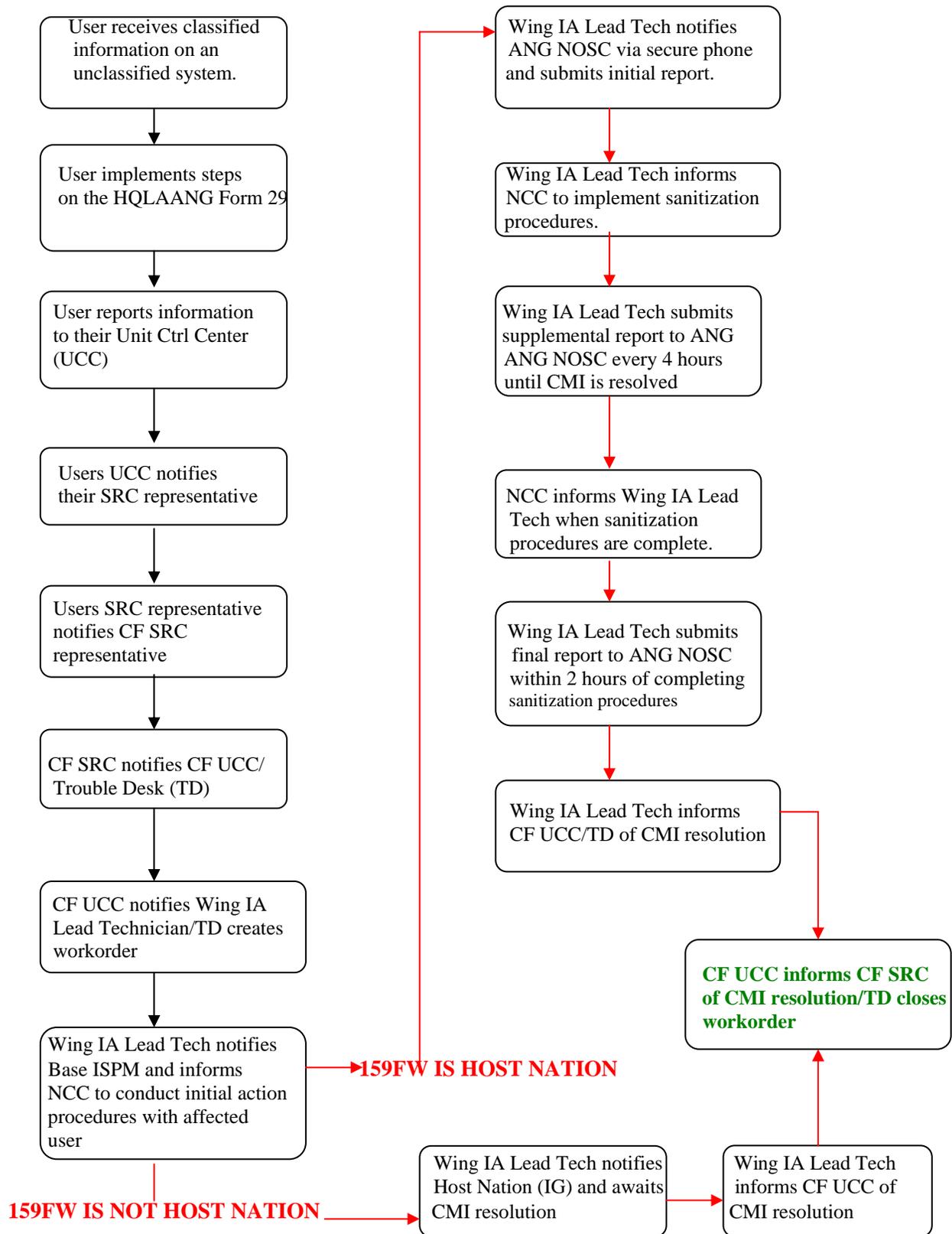
HQ LA ANGI 33-1, *Network Management*

HQ LA ANGI 33-3, *159th Fighter Network Security Policy*

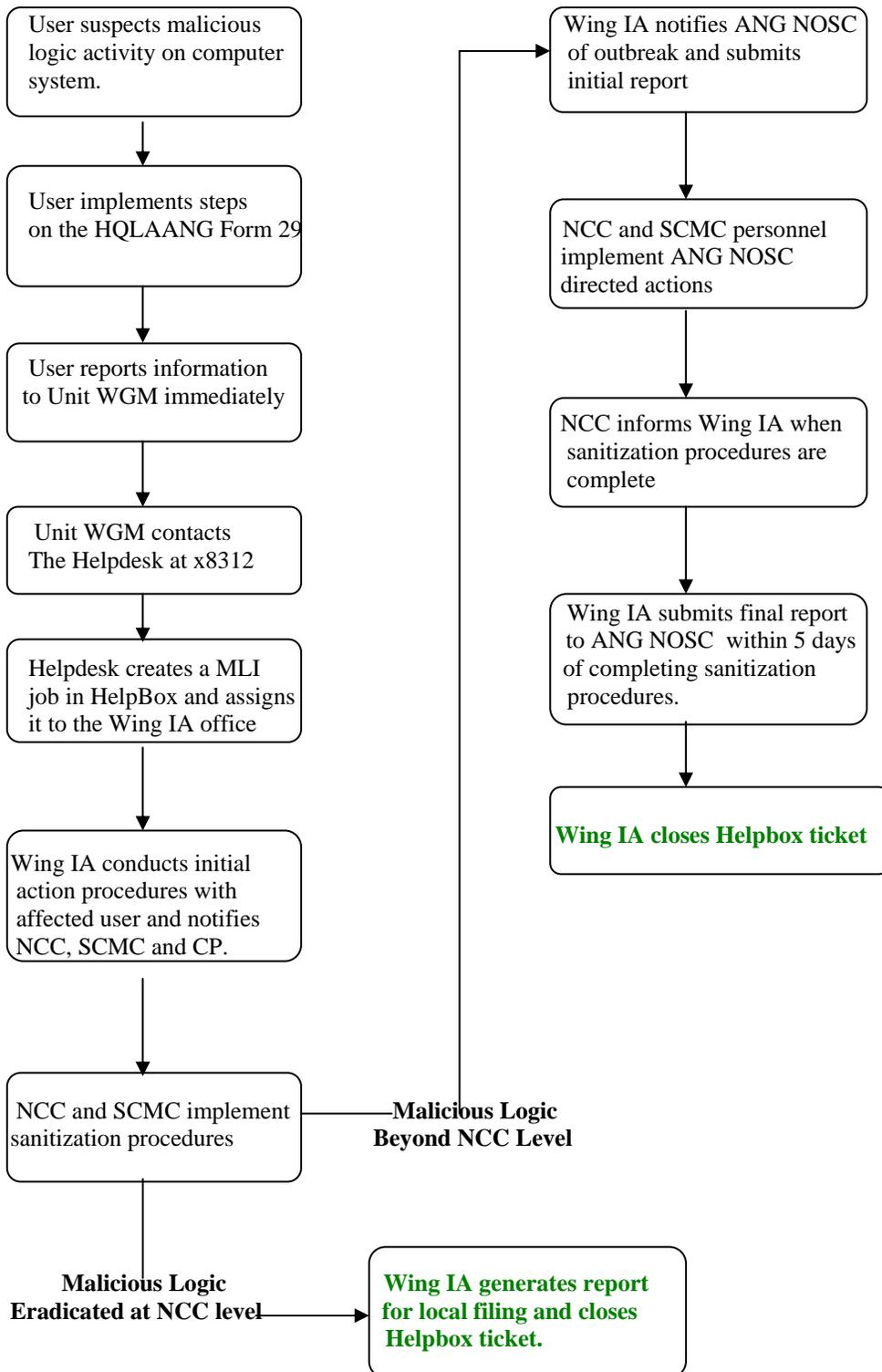
Attachment 2
Classified Message Incident (CMI) Flowchart
 (Home Station Operations)



Attachment 3
Classified Message Incident (CMI) Flowchart
(ORE/ORI Operations)



Attachment 4
Malicious Logic Incident (MLI) Flowchart
 (Home Station Operations)



Attachment 5
Malicious Logic Incident (MLI) Flowchart
(ORE/ORI Operations)

