BY THE ORDER OF THE COMMANDER
NORAD AND USNORTHCOM

NORAD AND USNORTHCOM
INSTRUCTION 33-172

11 JUNE 2010

CURRENT AND ESSENTIAL, 27 OCT 12

Communication and Information

NETWORK CLASSIFIED MATERIAL INCIDENT (NCMI) REPORTING

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the Headquarters NORAD and USNORTHCOM e-publishing website for downloading and ordering at https://operations.noradnorthcom.mil/C1/Library/Web%20Part%20Pages%20%20Functional%20Topics/Command%20Publications%20and%20Forms.aspx

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: N-NC/J653 (Information Assurance)

Certified by: N-NC/CS
(Maj Gen Howard N. Thompson)

Pages: 10

This instruction implements and expands incident reporting and response procedures for NORAD and USNORTHCOM information systems users based on Department of Defense (DOD) 5200.1-R, ***Information Security Program*** and NNCI 31-128, ***NORAD and USNORTHCOM Security Program***. This instruction applies to Headquarters NORAD and USNORTHCOM, NORAD Regions and Sectors, USNORTHCOM Subordinate Commands, and all assigned elements operating on the NORAD and USNORTHCOM enterprise network consisting of the SECRET Internet Protocol Router Network (SIPRNET), Non-Classified Internet Protocol Router Network (NIPRNET), Releasable to Canada Network (RELCAN), and SIPRNET Releasable (SIPR-R/SIPR-REL). This instruction does not apply to Air Force Reserve Command (AFRC) or National Guard (NG) units. Nothing in this policy shall alter or supersede the existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333 and other laws and regulations. Paragraphs 2.3.1, 2.3.2, 2.3.3, 2.3.4, 2.3.5, 2.3.6 and 2.3.8 of this instruction are punitive. Military personnel who violate these provisions may be subject to adverse administrative action or punishment under the *Uniform Code of Military Justice* (UCMJ) or *Canadian Code of Service Discipline*. Civilian employees who violate these provisions are subject to adverse actions in accordance with applicable civilian employee directives. Personnel not subject to the UCMJ, to include contractors, who fail to comply with these requirements are also subject to disciplinary and administrative action by their employer, and prosecutorial actions as authorized by criminal or civil sanctions under various authorities including, but not limited to, the United States Code, contractual support obligations, and the Federal and the state regulations. Send recommendations to change, add, or delete information in this instruction to the Office of Primary Responsibility (OPR) using the AF IMT 847, ***Recommendation for Change of Publication;*** route AF IMT 847s from the field through the appropriate functional's chain of command. This publication may be supplemented at any level, but all direct supplements must be routed to the OPR of this publication for coordination prior to certification and approval. Maintain and dispose of records created as a result of prescribed processes in accordance with the Joint Staff Disposition Schedule CJCSM 5760.01, ***Joint Staff and Combatant Command Records Management Manual: Vol I (Procedures) & Vol II (Disposition Schedule).*** The glossary of references and supporting information are found at **Attachment 1.**

1. Background. NORAD and USNORTHCOM information and information systems are instrumental in our ability to fight our nation's battles and our information infrastructure is vulnerable to many types of network incidents. These incidents include classified information inappropriately transferred to a lower classification network/system. To preserve our information technology advantage over our enemies, every NORAD and USNORTHCOM enterprise network user must become the front line of defense and knowledgeable in the proper reporting procedures in the event of a Network Classified Material Incident (NCMI). All organizations will provide incident details indicated in the NCMI Report checklist **Attachment 2**.

2. Roles and Responsibilities:

2.1. NORAD and USNORTHCOM Command Security Manager (N-NC/CSM) will:

2.1.1. Respond to collateral CONFIDENTIAL, SECRET and TOP SECRET NCMIs reported by Security Managers (SM). Refer SCI to the Special Security Officer (SSO).

2.1.2. Assist SM in validating the suspected NCMI, as required.

2.1.3. Report validated NCMIs to Network Operations and Security Center (NOSC) (719) 556-7059.

2.1.4. Initiate formal investigation IAW DOD 5200.1-R if incident involves possible or actual compromise of classified material resulting from improper handling by NORAD and USNORTHCOM personnel or contactors.

2.1.5. Ensure investigation report determines root cause of NCMI and recommends corrective action to include changes to process, procedures, and/or suggested personnel actions.

2.1.6. Ensure counseling or administrative actions are documented.

2.1.7. Send a Chief of Staff memorandum to the offender's Director. The Director will reply with what corrective actions were taken with regards to individuals involved and preventative measures.

2.1.8. Send copy of final investigation report to the CMI Response Coordinator (CRC).

2.2. Security Managers/Special Security Officer will:

2.2.1. Ensure each network user knows who their Security Manager (SM) and/or SSO are and how to contact them 24/7.

2.2.2. When responding to an NCMI, assist the identifier in validating the information classification using the Classification Guidance, or speaking with the data owners, or the Original Classification Authority (OCA). If classified information was mishandled (spilled):

2.2.2.1. Notify CSM and provide finding details and supporting references from the Classification Guidance via secure means by the end of the first duty day.

2.2.2.2. Notify the chain of command of the individual(s) involved in the incident via secure means.

2.2.2.3. All incidents involving SCI material will be reported to an SCI security official in the responsible SSO's office IAW DOD S-5105.21-M-1 Ch4.

2.2.2.4. Cooperate with investigating officials.

2.3. Network Users will:

2.3.1. (Mandatory) Identify classified material improperly stored or transmitted using NORAD and USNORTHCOM networks/systems.

2.3.1.1. (Mandatory) Cease work on system. **DO NOT POWER OFF EQUIPMENT OR DISCONNECT FROM NETWORK**.

2.3.1.2. (Mandatory) Protect classified material. **DO NOT DELETE OR MODIFY FILE, DOCUMENT, OR EMAIL**.

2.3.1.3. (Mandatory) If the information is collateral classified, notify unit SM immediately, requesting verification of the incident.

2.3.1.4. (Mandatory) If the information is SCI, notify the responsible SSO immediately, requesting verification of the incident.

2.3.1.5. (Mandatory) If unit SM is unavailable, notify Command Security via secure means.

2.3.1.6. If classified information appears in the public media, NORAD and USNORTHCOM personnel must be careful not to make any statement that would confirm the accuracy or verify the classified status of the information. Refer all inquiries to N-NC Public Affairs office.

2.3.1.7. (Mandatory) Cooperate with investigation officials.

2.4. (Mandatory) Supervisors of individual(s) who mishandle classified information will document the remedial actions taken to prevent future spills.

2.5. Network Control Center (NCC) will:

2.5.1. Develop a response checklist.

2.5.2. Collect initial incident data from the NOSC.

2.5.3. Coordinate response actions with the NOSC.

2.5.4. Support enterprise NCCs in performing response and cleaning activities, when requested.

2.5.5. Execute appropriate response and sanitization actions.

2.5.6. Report sanitization actions complete to the NOSC.

2.6. CMI Response Coordinator (CRC) will:

2.6.1. Track incident and supporting investigation.

2.6.2. Analyze incident data for trends. Track hours spent working on cleaning and estimated cost (to include statistics from all involved parties).

2.6.3. Coordinate on investigation close out report.

2.7. Network Operations and Security Center (NOSC is located at Peterson AFB, Building 2, phone (719) 556-7059 or DSN 834-7059) **will:**

2.7.1. If incident involves SCI, ensure coordination with the SSO’s office for instructions on cleaning.

2.7.3. Direct locking of user account, when deemed appropriate.

2.7.4. Notify responsible NCC to initiate sanitization actions (if required).

2.7.5. Notify external NOSC or supporting organizations to initiate sanitization actions (if required).

2.7.6. Coordinate and send Executive Summary (EXSUM) to N-NC/CSM for formal investigation. Include security offices of external organizations involved in the incident on distribution of EXSUM. EXSUM and any other status email/document will be marked IAW EO 12958 as amended using the Information Security Oversight Office (ISOO) Implementing Directive 1, dtd 25 Mar 03, effective 22 Sep 03.

2.7.7. Provide status updates to N-NC/J6 leadership, CSM and/or SSO as cleanup and investigation progresses.

2.7.8. Verify sanitization complete within scope of affected networks.

2.7.9. Send close-out EXSUM to J6 leadership, Command Security, SSO and involved external organizations.

3. Classification Guidance. Protect the transmission, reception, and storage of security incident information and reports at the same level of classification as the information compromised. This guidance applies to all verbal as well as written communications. All details of the security incident are classified until the systems involved are sanitized and the information is no longer accessible to unauthorized personnel.

4. Process Flow. The NCMI handling process follows a four-phased approach: Assessment, Containment, Sanitization, and Investigations/Notification. For more details, see **paragraph 5**.

5. Process Walk-Through:

5.1. Assessment Phase (See **Attachment 2** for process diagram of Assessment Phase)

5.1.1. Assessment of classified information.

5.1.2. Individual initially identifying the information as classified (identifier) immediately notifies SM of allegedly classified information residing on an automated information system exceeding the level of classification for which the device is approved.

5.1.3. The identifier is responsible for providing proof of classification. Proof of classification must be a paragraph reference to the source document, classification guide, or confirmation of original classification authority (OCA). The identifier should contact the SM for assistance in finding proof of the classification.

5.1.4. If the determination is the information is classified, then the SM will notify the CSM.

5.1.5. SM will notify the unit chain of command with all pertinent data including the level of infection/impact.

5.2. Containment Phase (See **Attachment 3** for process diagram of Containment Phase):

5.2.1. Containment of classified information.

5.2.2. NCC will disconnect all affected workstations within their span of control from network (if required).

5.2.3. NCC locks user accounts of all recipients of the NCMI. If the classified information resides on file or web servers, the NCC will isolate these devices from the network.

5.2.4. NCC provides initial NCMI report to the supporting NOSC. Forward, via SIPRNET, a copy of the actual message/file involved in the NCMI (i.e., email message, attachment, copy of information from the web page where classified information was posted, or file) to the supporting NOSC. **Do not forward TOP SECRET or SCI information.**

5.3. Sanitization Phase (See **Attachment 4** for process diagram of Sanitization Phase):

5.3.1. NCC recommends sanitization measures, based on information obtained from initial incident report and possible operational impact.

5.3.2. NOSC, in consultation with N-NC/J63, provides direction to the supporting NCC.

5.3.3. NCC implements sanitization measures, to include measures to sanitize affected workstations.

5.3.4. NCC notifies NOSC when sanitization measures are complete.

5.3.5. NCC re-enables all quarantined systems when sanitization measures are complete.

5.3.6. NCC submits final NCMI report to the NOSC.

5.3.7. NOSC report details to J6 via final EXSUM.

5.4. Investigation and Notification Phase (See **Attachment 5** for process diagram of Investigation and Notification Phase):

5.4.1. CSM contact 21SW to appoint investigation official.

5.4.2. Investigation official interviews staff involved in the NCMI.

5.4.3. Investigation official prepares final report with findings and recommendations.

5.4.4. CSM forward copy of investigation report to the NOSC.

DIANE E. H. WEBBER, RDML, USN
Director, Command Control Systems

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

EO 12958, ***Classified National Security Information***, 17 Apr 95

DOD 5200.1-R, ***Information Security Program,*** 14 Jan 97

CJCSM 5760.01, ***Joint Staff and Combatant Command Records Management,*** 10 Mar 03

NNCI 31-128, ***NORAD and USNORTHCOM Security Program,*** 1 Sep 09

Abbreviations and Acronyms

AFRC—Air Force Reserve Command

CMI—Classified Material Incident

CRC—CMI Response Coordinator

CSM—Command Security Manager

EXSUM—Executive Summary

JCSC—Joint Communications Support Center

N-NC—NORAD-USNORTHCOM

NCC—Network Control Center

NCMI—Network Classified Material Incident

NG—National Guard

NIPRNET—Non-Classified Internet Protocol Router Network

NOSC—Network Operations and Security Center

OCA—Original Classification Authority

RELCAN—Releasable to Canada Network

SCI—Sensitive Compartmented Information

SIPR-REL—Releasable to AGCU

SIPRNET—SECRET Internet Protocol Router Network

SM—Security Manager

SSO—Special Security Officer

TNCC—Theater Network Operations Control Center

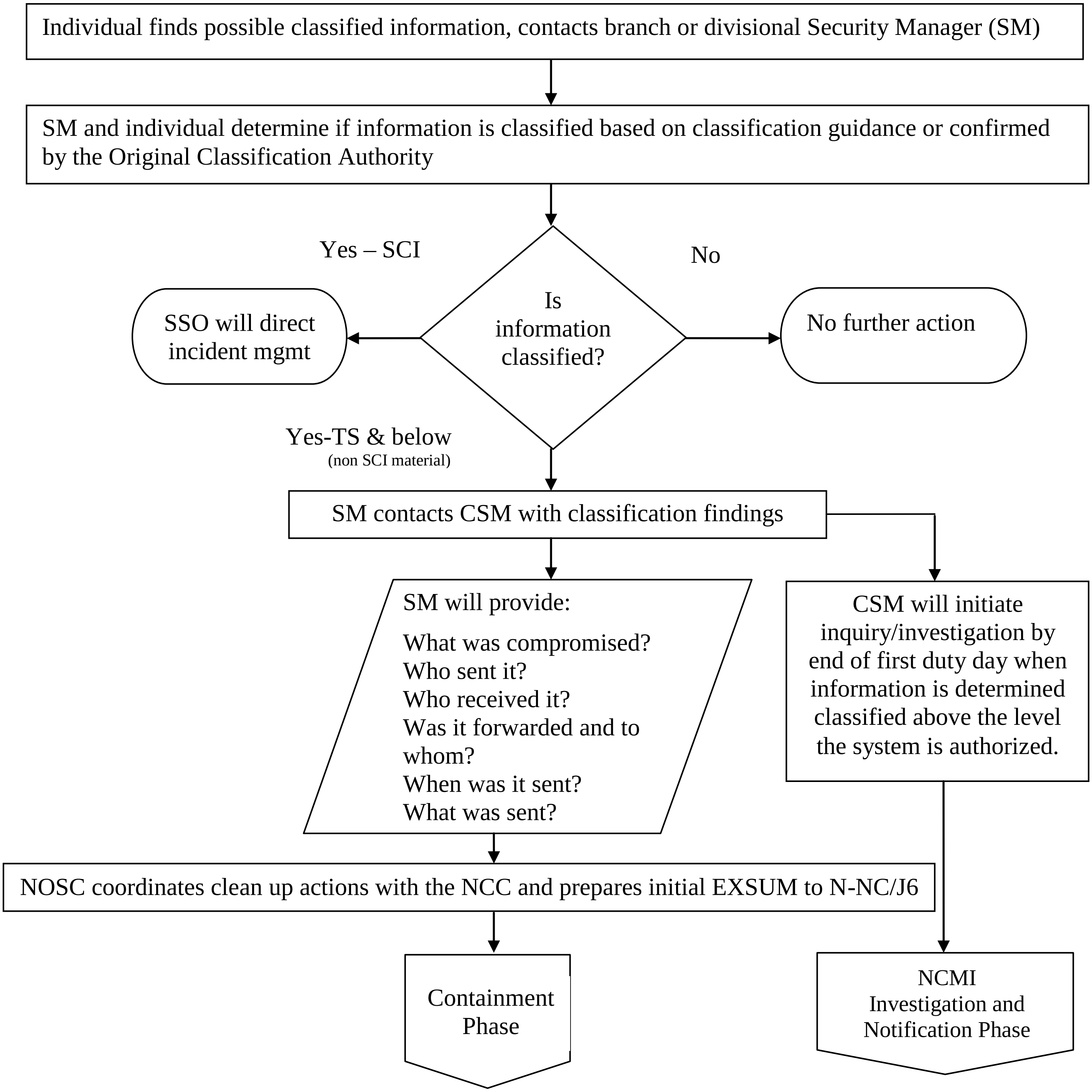
TS—TOP SECRET

Terms

NCC refers to the Operation & Maintenance (O&M) personnel and/or organization at each NORAD and USNORTHCOM location that may have to take action to contain and/or sanitize spills. At the Headquarters, NCC refers to N-NC/J624. At the Subordinate Commands and Regions/Sectors, the NCC will refer to their O&M organizations.

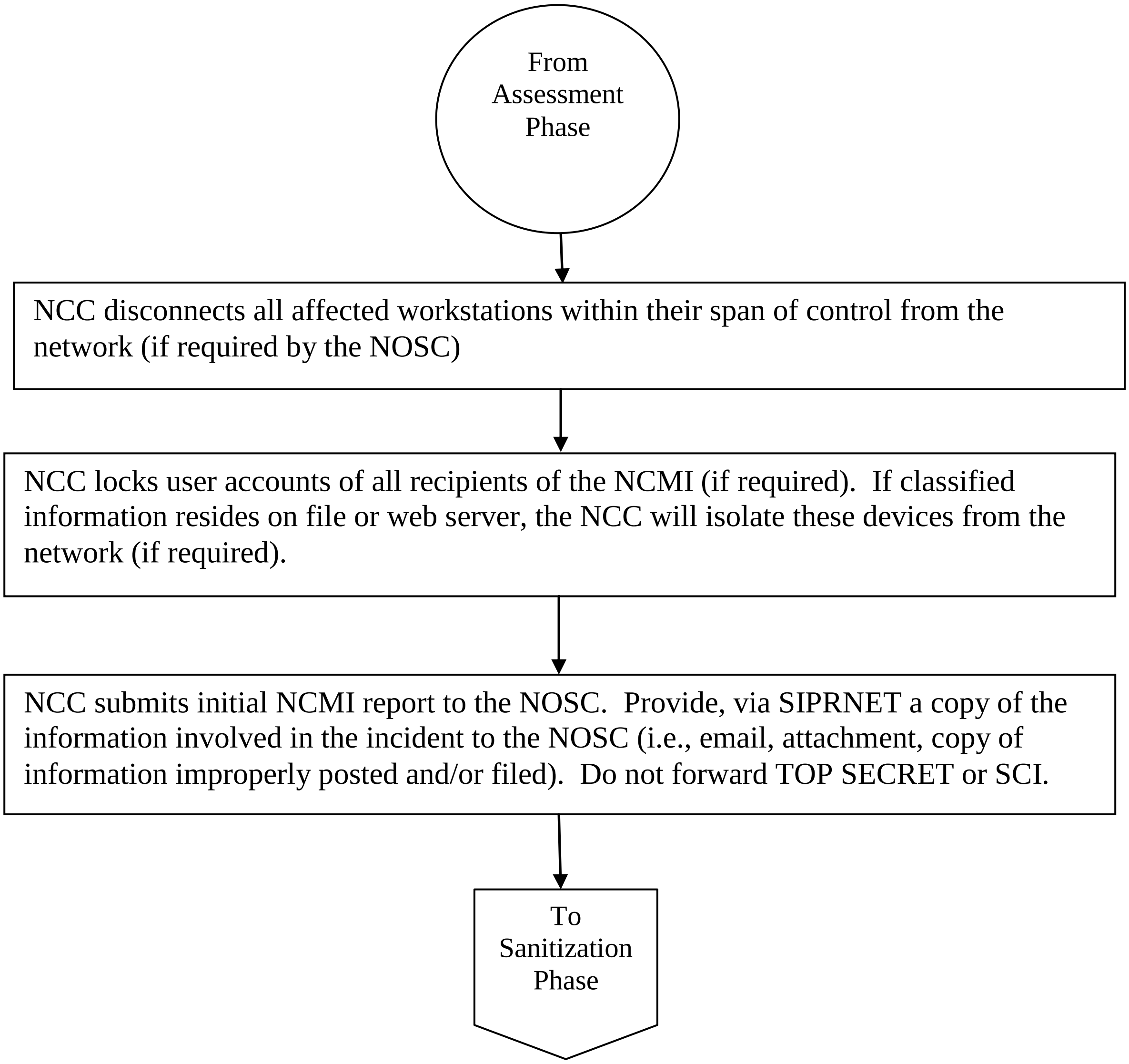
Attachment 2

NETWORK CLASSIFIED MATERIAL INCIDENT (NCMI)–ASSESSMENT PHASE


Individual finds possible classified information, contacts branch or divisional Security Manager (SM)
SM and individual determine if information is classified based on classification guidance or confirmed by the Original Classification Authority
Yes – SCI
No
Is information classified?
SSO will direct incident mgmt
No further action
Yes-TS & below
(non SCI material)
SM contacts CSM with classification findings
SM will provide:
What was compromised?
Who sent it?
Who received it?
Was it forwarded and to whom?
When was it sent?
What was sent?
CSM will initiate inquiry/investigation by end of first duty day when information is determined classified above the level the system is authorized.
NOSC coordinates clean up actions with the NCC and prepares initial EXSUM to N-NC/J6
Containment Phase
NCMI Investigation and Notification Phase

Attachment 3

NETWORK CLASSIFIED MATERIAL INCIDENT (NCMI)–CONTAINMENT PHASE



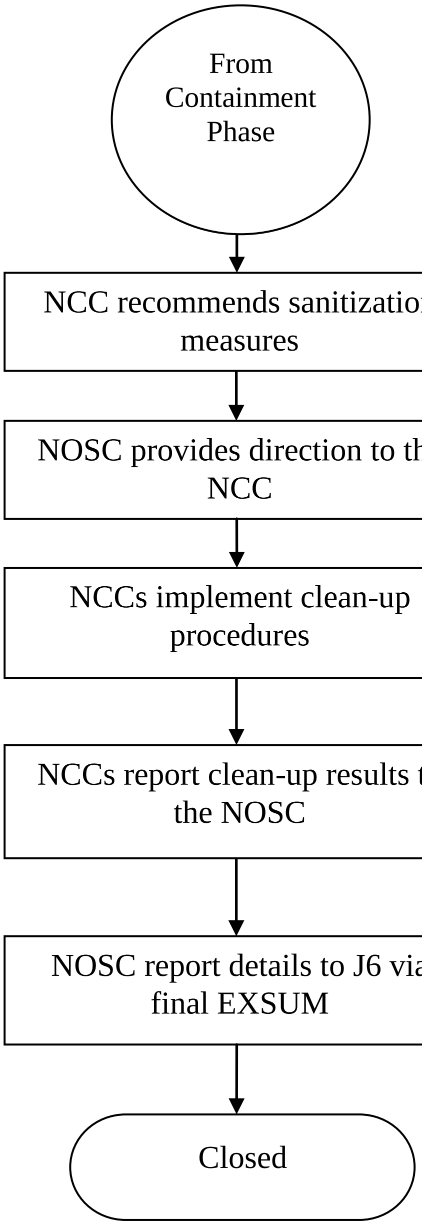
NCC disconnects all affected workstations within their span of control from the network (if required by the NOSC)

NCC locks user accounts of all recipients of the NCMI (if required). If classified information resides on file or web server, the NCC will isolate these devices from the network (if required).

NCC submits initial NCMI report to the NOSC. Provide, via SIPRNET a copy of the information involved in the incident to the NOSC (i.e., email, attachment, copy of information improperly posted and/or filed). Do not forward TOP SECRET or SCI.

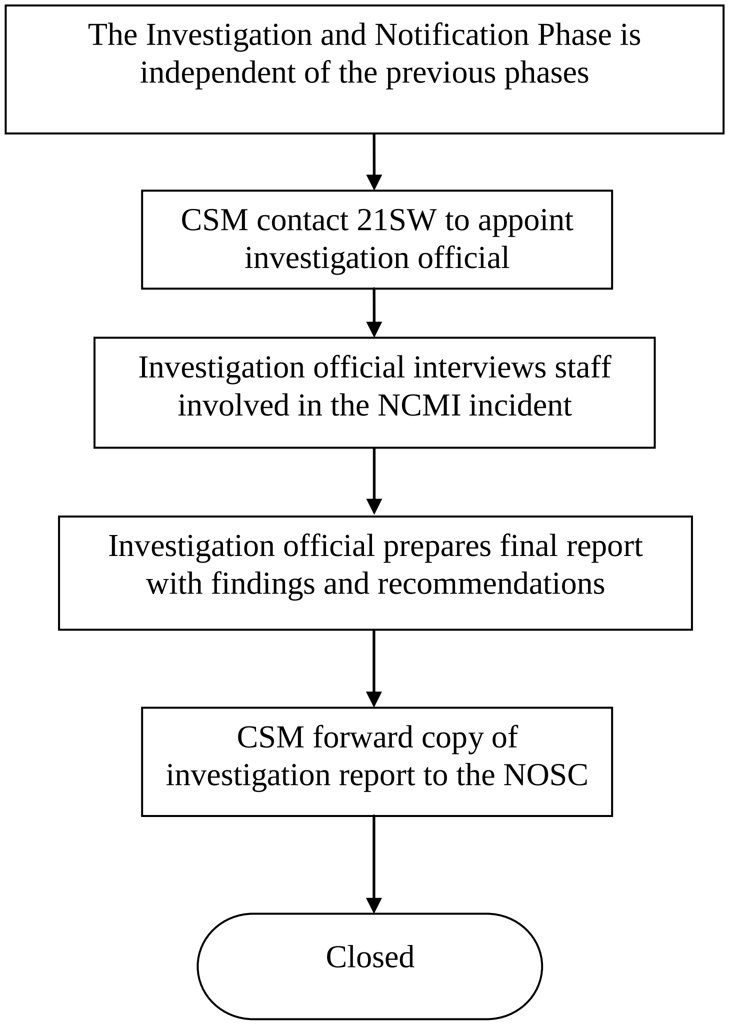
Attachment 4

NETWORK CLASSIFIED MATERIAL INCIDENT (NCMI)–SANITIZATION PHASE


From Containment Phase
NCC recommends sanitization measures
NOSC provides direction to the NCC
NCCs implement clean-up procedures
NCCs report clean-up results to the NOSC
NOSC report details to J6 via final EXSUM
Closed

Attachment 5

NETWORK CLASSIFIED MATERIAL INCIDENT (NCMI)–INVESTIGATION AND NOTIFICATION PHASE


The Investigation and Notification Phase is independent of the previous phases
CSM contact 21SW to appoint investigation official
Investigation official interviews staff involved in the NCMI incident
Investigation official prepares final report with findings and recommendations
CSM forward copy of investigation report to the NOSC
Closed