

**CLASSIFIED INFORMATION SPILLAGE ON INFORMATION SYSTEMS**

**IMMEDIATE ACTION CHECKLIST**

For use of this form, see AR 25-2

**(Completed by the user and IASO)**

1. CLASSIFICATION OF AFFECTED SYSTEM:  UNCLASSIFIED  SECRET  TOP SECRET  OTHER:

2. WAS FILE MARKED WITH CLASSIFICATION MARKINGS?  YES (GO TO 3)  NO (GO TO 4)

3. CLASSIFICATION OF DATA:  UNCLASSIFIED  SECRET  TOP SECRET  OTHER:

- IS TS INFORMATION ON UNCLASSIFIED SYSTEM?

YES - PLAN FOR DESTRUCTION OF ALL AFFECTED MEDIA (GO TO 17)

NO - YOU MAY BE AUTHORIZED TO CLEAR OR PURGE AFFECTED MEDIA (GO TO 4)

4. IS CATEGORY OF INFORMATION?  SPECAT  SAP  SCI  SI  CODEWORD

YES - PLAN FOR DESTRUCTION OF ALL AFFECTED MEDIA (GO TO 17)

NO - THEN YOU MAY BE AUTHORIZED TO CLEAR OR PURGE AFFECTED MEDIA (GO TO 5)

5. DTG OF THE MESSAGE: \_\_\_\_\_ DTG OF IDENTIFICATION: \_\_\_\_\_

- IS DIFFERENCE OF DTG LESS THAN 2 HOURS?

YES - IMPLEMENT TIME-BASED CLEARING ACTIONS.

NO - IMPLEMENT DATA-BASED ACTIONS TO CONTAIN AND PURGE.

6. HOW WAS THE CLASSIFIED INFORMATION DISTRIBUTED/RECEIVED/IDENTIFIED?

EMAIL ATTACHMENT

DESKTOP FILE

FILE SERVER FILE

WEB POSTING

REMOVABLE MEDIA

7. WHO REPORTED/IDENTIFIED THE SPILLAGE?

ARMY

DOD

OTHER GOVERNMENT AGENCY

CONTRACTOR

COMMERCIAL ENTITY

POC'S NAME: \_\_\_\_\_ PHONE NUMBER: \_\_\_\_\_ RANK: \_\_\_\_\_

POSITION: \_\_\_\_\_ E-MAIL ADDRESS: \_\_\_\_\_

UNIT: \_\_\_\_\_

8. WHO DISTRIBUTED THE SPILLAGE? (If not reporting agency)

ARMY

DOD

OTHER GOVERNMENT AGENCY

CONTRACTOR

COMMERCIAL ENTITY

NAME OF SENDER (FROM):

LAST:	FIRST:	E-MAIL:	PHONE:	OFFICE:

NAME OF RECIPIENT(S) (TO): (Continue in Block 24 if additional space is needed)

LAST:	FIRST:	E-MAIL:	PHONE:	OFFICE:

NAME OF RECIPIENT(S) (CC): (Continue in Block 24 if additional space is needed)

LAST:	FIRST:	E-MAIL:	PHONE:	OFFICE:

NAME OF RECIPIENT(S) (BCC): (Continue in Block 24 if additional space is needed)

LAST:	FIRST:	E-MAIL:	PHONE:	OFFICE:

9. ORIGINAL SUBJECT OF MESSAGE: \_\_\_\_\_

10. HAS THE SUBJECT BEEN CHANGED FROM ORIGINAL MESSAGE?  YES  NO

IF YES, WHAT IS THE SUBJECT OF SUBSEQUENT MESSAGE(S): \_\_\_\_\_

11. VIEW, COPY, AND PRINT E-MAIL HEADER INFORMATION:  YES  NO

12. HAS DOCUMENT OR FILE BEEN PRINTED?  YES  NO

13. HAS DOCUMENT OR FILE BEEN SAVED?  YES  NO

WHERE? \_\_\_\_\_

14. HAS THE ORIGINATOR BEEN NOTIFIED?  YES  NO

15. IS THE ORIGINATOR THE LEAD AGENCY FOR THE SPILLAGE?  YES  NO

16. IS THE ORIGINATOR THE ORIGINAL CLASSIFICATION AUTHORITY (OCA)?  YES  NO

17. HAS THE DO OR OCA BEEN CONTACTED?  YES  NO

POC'S NAME: \_\_\_\_\_ PHONE NO (COMM): \_\_\_\_\_ DSN: \_\_\_\_\_

RANK: \_\_\_\_\_ POSITION: \_\_\_\_\_ E-MAIL ADDRESS: \_\_\_\_\_

UNIT: \_\_\_\_\_

18. UNAUTHORIZED SOFTWARE ON SYSTEM THAT SUBSTANTIALLY INCREASED RISK OR THREAT (I.E., IRC, PEER-TO-PEER FILE SHARING APPLICATIONS, ETC.)?  YES  NO

IF YES, CI INVESTIGATORS MUST BE CONTACTED AND ALL CLEARING ACTIONS CEASE.

19. CAN OCA/DO DOWNGRADE INFORMATION?  YES  NO

IF YES, TO WHAT CATEGORY OR CLASSIFICATION? \_\_\_\_\_

IF NO, DESTRUCTION OF ALL AFFECTED MEDIA IS REQUIRED.

20. DOES DOWNGRADED CLASSIFICATION OR CATEGORY AFFECT RESPONSE?  YES  NO

IF YES, GO TO 5.

IF NO, DESTRUCTION OF ALL AFFECTED MEDIA IS REQUIRED.

21. SYSTEM IDENTIFICATION: OS OF THE AFFECTED SYSTEM: \_\_\_\_\_ VERSION: \_\_\_\_\_

22. DID YOU ORIGINATE THE SPILLAGE INCIDENT?  YES  NO

**NOTE:** IF YES, YOUR ORGANIZATION BECOMES THE LEAD AGENCY FOR REPORTING ALL ACTIONS UNLESS DO/OCA TAKES CONTROL OF THE ACCIDENT.

23. LIST WORKSTATIONS AFFECTED (MACHINE NAME AND IP ADDRESS).

24. ADDITIONAL INFORMATION: (LIST ANY ADDITIONAL INFORMATION SUCH AS--WAS AUTO-FORWARDING RULES TURNED ON; WERE THE BCCs SENT; WERE AUTO-REPLIES OR AUTO-ARCHIVES TURNED ON; WERE STORAGE RULES TURNED ON; WAS DATA BACKED UP; WERE DOCUMENTS PRINTED, ETC.)

USER'S NAME:	SIGNATURE:	DATE SIGNED:
--------------	------------	--------------