NSA FORM N2288 REV SEP 65
(Supersedes N2288 REV AUG 65 to be used until depleted)

~~TOP SECRET~~
SECURITY CLASSIFICATION

ACTION PRECEDENCE	INFO PRECEDENCE	SPECIAL HANDLING
IMMEDIATE	IMMEDIATE	~~NOFORN~~

DISTRIBUTION
LIM DIS
DIR
ADC
ADN
D32
M5
ADNSG

FROM: DIRNSA

DATE: 24 JAN 68

TO: SSODIA (ATTN: DIAPL-4)

INFO: CHAIRMAN, JCS
JCS/JRC

~~T O P S E C R E T/LIMITED DISTRIBUTION/NOFORN~~

DIR/22

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

SUBJ: NSA ASSESSMENT OF USS PUEBLO LOSS (COMMUNICATIONS SECURITY)

REF: DIADR 00749 JAN 68 (NOTAL)

1. COMSEC IMPACT STATEMENT:

A. IN SUMMATION, THE PROBABLE COMPROMISE OF FOUR MAJOR U. S. COMSEC EQUIPMENTS, INCLUDING THREE OF OUR MODERN ELECTRONIC CRYPTO-EQUIPMENTS, IS A MAJOR INTELLIGENCE COUP WITHOUT PARALLEL IN MODERN HISTORY. UNFORTUNATELY, WE EXPECT THAT THE EXAMINATION OF THESE EQUIPMENTS OR THE MAINTENANCE MANUALS WILL BE A MAJOR HELP TO THE SOVIET BLOC [redacted] WHILE THE DETAILED INFORMATION IS NOT AVAILABLE TO PERMIT AN ACCURATE ASSESSMENT OF WHETHER SOME OF THIS KEYING MATERIAL, MANUALS, OR EQUIPMENT MIGHT HAVE BEEN DESTROYED PRIOR TO CAPTURE, WE ARE TAKING THE PRECAUTIONARY ACTION IN SUPERSEDING THE SUSPECT SYSTEMS AND REDIRECTING COMMUNICATIONS TO ALTERNATE CRYPTOSYSTEMS. THUS, THE PURE COMSEC LOSS IN THE TERMS OF SPECIFIC MESSAGES HAS BEEN MINIMIZED, BUT THE TECHNOLOGY LOSS MAY WELL BE MAJOR, WITH LONG-TERM EFFECTS.

DRAFTER: L. R. SCHULZ, RADM, USN ADN

RELEASING OFFICER: LTG MARSHALL S. CARTER, USA

DOCUMENT MARKING ~~NOT RELEASABLE TO FOREIGN NATIONALS.~~ DIRECTOR ~~GROUP-1-Excluded from automatic downgrading and declassification.~~

RELEASED AT (ZULU)

PAGE 1 OF 3 PAGES

REFERS TO MESSAGE

SECURITY CLASSIFICATION

AGO

AGI

DTG

SUSPENSE

~~TOP SECRET~~

AGI NR.

AGO NR. 01202/24

DTG 241742Z

B. NONE OF THE THREE MACHINE SYSTEMS (KL-47, KW-7, AND KWR-37/KG-14) IS EXPLOITABLE UNLESS THE SPECIFIC ASSOCIATED KEYING MATERIALS (THE KAY KEY CARDS AND THE KAK KEY LISTS) WERE ALSO LOST. ALL KEY ABOARD WAS CAPABLE OF BEING DESTROYED IN FIFTEEN MINUTES OR LESS. EMERGENCY DESTRUCTION WAS INSTITUTED AT LEAST ONE HOUR PRIOR TO FINAL CONTACT AND KEYING MATERIAL IS FIRST PRIORITY. THEREFORE, WITH POSSIBLE EXCEPTION OF THE KEY HELD FOR THE LAST COMMUNICATIONS, IT APPEARS POSSIBLE THAT MOST OF THE KEYING MATERIAL WAS DESTROYED AND NO TRAFFIC IN THE SYSTEMS WAS COMPROMISED. NONETHELESS, AS A PRECAUTIONARY MEASURE, ALL HOLDERS OF THE KEYS HAVE BEEN DIRECTED TO USE ALTERNATIVE SYSTEMS AND TO HOLD ALL PRIOR TRAFFIC PASSED IN THESE KEYS FOR POSSIBLE REVIEW. IN GENERAL, THE CRYPTOSYSTEMS HELD WERE SPECIAL INTELLIGENCE SYSTEMS AND WERE NOT GENERAL SERVICE CRYPTOSYSTEMS. (THE GENERAL KW-37 PACIFIC FLEET BROADCAST WAS NOT COMPROMISED, NOR WERE ANY ARMY, AIR FORCE OR FIXED PLANT DCS COMMUNICATIONS AFFECTED.)

C. THE MANUAL SYSTEMS ABOARD CONSISTED OF TWO LOW-LEVEL OPERATIONS CODES (KAC'S) AND ONE AUTHENTICATION SYSTEM (KAA). ALTHOUGH POSSIBLY DESTROYED, AGAIN AS A PRECAUTIONARY MEASURE, ALL HOLDERS HAVE BEEN DIRECTED TO MINIMIZE THEIR USE PENDING ISSUE OF A REPLACEMENT CODE.

DOCID: 4051721

NSA FORM N2288 DEC 62
(Supersedes N2288 REV AUG 61 to be used until depleted)

~~TOP SECRET~~
SECURITY CLASSIFICATION

ACTION PRECEDENCE	INFO PRECEDENCE	SPECIAL HANDLING

DISTRIBUTION

D. FINALLY, ONE SYSTEM INDICATOR ENCRYPTION SYSTEM AND ONE CALLSIGN ENCRYPTION SYSTEM WERE HELD. CONSEQUENCE OF THEIR LOSS WOULD BE MINIMAL SINCE THEY ARE DETERRENTS TO TRAFFIC ANALYSIS AND DO NOT CONTRIBUTE TO MESSAGE SECURITY.

E. BALANCE OF CRYPTOMATERIAL IN INVENTORY CONSISTS OF SECONDARY VARIABLES (E.G. ROTORS FOR KL-47'S), GENERAL SUPPORTING DOCUMENTS, OPERATING INSTRUCTIONS, AND MAINTENANCE MANUAL. ACQUISITION OF ANY OF THESE ITEMS WILL NOT PERMIT EXPLOITATION OF TRAFFIC UNLESS SPECIFIC KEYS ARE ALSO KNOWN.

2. SIGINT IMPACT STATEMENT FOLLOWS BY SEPARATE MESSAGE. GP-1

M/R: COMSEC impact statement prepared by ADC in coordination with ADN and cleared with DIR and D/DIR.

DRAFTER	RELEASING OFFICER	RELEASED AT (ZULU)
DOCUMENT MARKING		PAGE 3 OF 3 PAGES
REFERS TO MESSAGE	SECURITY CLASSIFICATION	AGI NR.
AGO		AGO NR. 202/24
AGI		
DTG		DTG
SUSPENSE	~~TOP SECRET~~	