FROM: DIRNSA
TO: SSO DIA (ATTN: DIPL-4)
INFO: CHAIRMAN JCS
JOCS (JRC)

DATE: 2 FEB 68

SUBJ: ASSESSMENT OF PUEBLO LOSS

MY DIR-21-68 AND DIR-22-68 REFER.

FURTHER NSA ANALYSIS OF POSSIBLE COMPROMISE OF COMSEC AND SIGINT ACTIVITIES IN CONNECTION WITH THE PUEBLO INCIDENT HAS RESULTED IN THE FOLLOWING UPDATED REPORT WHICH WAS PRESENTED TO THE POLICY SUB-COMMITTEE OF THE HOUSE ARMED SERVICES COMMITTEE ON 1 FEBRUARY BY THE DIRECTOR OF NSA.

QUOTE NATIONAL SECURITY AGENCY ACTIVITIES ARE CENTERED ABOUT TWO MAJOR PURPOSES: ONE IS TO MAINTAIN THE SECURITY OF THE UNITED STATES COMMUNICATIONS, AND SECOND IS TO TAKE ADVANTAGE OF THE COMMUNICATIONS OF TARGET NATIONS. THE "BILL OF DESTRUCTION" COVERING THE EQUIPMENT OF THE PUEBLO PROVIDED FOR DESTRUCTION OF
KEY CARDS AND KEY LISTS, THEN OF THE EQUIPMENT, THEN CODES AND AUTHENTICATION MATERIALS, AND FINALLY MAINTENANCE AND OPERATING MANUALS. WHILE IT IS THEORETICALLY POSSIBLE TO HAVE ELECTRONIC AUTOMATIC DETONATION GEAR, THE PUEBLO WAS NOT SO EQUIPPED. THE HAZARDS OF AUTOMATIC DETONATION EQUIPMENT ON BOARD A SHIP ARE WEIGHED AGAINST OTHER METHODS OF DESTRUCTION AND THE POSSIBLE DAMAGE FROM COMPROMISE, AND ARE GENERALLY CONSIDERED UNACCEPTABLE.

FOR THE PAST 30 YEARS IT HAS BEEN THE GENERAL U.S. PRACTICE THAT, WHERE POSSIBLE, SECURITY OF U.S. COMMUNICATIONS WILL NOT DEPEND SOLELY ON PHYSICAL PROTECTION OF THE EQUIPMENT USED TO ENCIPHER AND DECIPHER THE MESSAGES. DURING THE PAST 20 YEARS NO EQUIPMENT HAS BEEN PRODUCED WITHOUT VARIABLES WHICH DEPEND UPON KEYING ELEMENTS, USUALLY KEY LISTS OR KEY CARDS, FOR THEIR PRIMARY SECURITY. IN PARTICULAR, ALL THE COMMUNICATION SECURITY EQUIPMENTS WHICH THE PUEBLO CARRIED DEPENDED UPON EITHER KEY LISTS OR KEY CARDS. LOSS OF A PARTICULAR EQUIPMENT WITH THE KEYING ELEMENT WOULD NOT
The key list enables the user to establish a unique machine set-up for a crypto period which is not longer than 24 hours. The key card is a card punched with a specified pattern and is inserted into the machine by means of a card holder. The key card and holder permit feeler pins to make contact through randomly positioned holes and effectively rewire the cipher machines, again not less often than each 24 hours. The number of combinations resulting from a card system is astronomical and a message which is transmitted through a machine using a particular keying element can only be read at the other end by a machine with an identical keying element.

It is the National Security Agency's judgment that no degradation to the security of other U.S. communications can result from this compromise even if the equipment...
AND THE KEY LISTS WERE CAPTURED INTACT, SINCE STEPS WERE
TAKEN IMMEDIATELY TO SUPERSEDE ALL OF THE KEYING MATERIALS.

IN THE WORST POSSIBLE CASE, THE FEW MESSAGES TO AND FROM
THE PUEBLO COULD BE READ IF ALL MATERIALS AND EQUIPMENT
WERE CAPTURED INTACT.

MESSAGE TRAFFIC FROM THE PUEBLO, AS WELL AS FROM
THE NORTH KOREANS, INDICATED A DESTRUCTION EFFORT ON
BOARD THE VESSEL BY FIRE AS WELL AS JETTISONING. FROM HER
COMMUNICATIONS, IT MAY BE INFERRED THAT THE BULK OF HER
KEY MATERIAL, PERHAPS ALL, AND AS MUCH EQUIPMENT AS
POSSIBLE WAS DESTROYED, BUT THAT SEVERAL PUBLICATIONS WERE
PROBABLY COMPROMISED. WE WILL NOT KNOW WHAT UNTIL THE
CREW IS RELEASED AND DEBRIEFED.

ON THE INTELLIGENCE SIDE, THE PUEBLO CARRIED A
SUFFICIENT AMOUNT OF COLLECTION GEAR TO ENABLE HER TO
MONITOR NORTH KOREAN COMMUNICATIONS AND RADAR FACILITIES
ON THE EAST COAST THIS

EQUIPMENT WAS GENERALLY UNCLASSIFIED (FOUR PIECES
CLASSIFIED CONFIDENTIAL) BUT THE USE TO WHICH THE EQUIPMENT
COULD BE PUT AND THE RESULTS DERIVED THEREFROM ARE CLASSIFIED. IT IS VERY POSSIBLE THAT IF THE EQUIPMENT WAS UNDAMAGED A REASONABLY PRECISE RECONSTRUCTION OF THE PUEBLO'S INTELLIGENCE MISSION COULD BE ACCOMPLISHED.

IN ADDITION TO THE EQUIPMENT REFERRED TO ABOVE, THE PUEBLO CARRIED A SUBSTANTIAL NUMBER OF TECHNICAL PUBLICATIONS AND ANALYTICAL AIDS REQUIRED TO ENABLE HER TO DISCHARGE THE INTELLIGENCE COLLECTION MISSION. IF THESE ITEMS WERE CAPTURED INTACT, THEY WOULD GIVE THE NORTH KOREANS PRECISE INFORMATION ON THE EXTENT OF U.S. KNOWLEDGE OF THEIR COMMUNICATIONS TECHNIQUES, USAGE, AND RADAR EQUIPMENTS. THE PUBLICATIONS ALSO REVEAL A MORE LIMITED U.S. KNOWLEDGE OF THE GENERAL SOVIET COMMUNICATIONS PRACTICES.

THIS INFORMATION, IF COMPROMISED, WOULD STIMULATE EITHER OF THE TWO NATIONS TO CHANGE THEIR COMMUNICATIONS PRACTICES, SUPERSEDE THEIR CALL SIGN SYSTEMS AND/OR MODIFY THEIR OPERATIONAL CODES.

ALTHOUGH THE POSSIBLE LOSS OF THE COMMUNICATIONS
SECURITY EQUIPMENT OR MATERIALS IN NO WAY WILL
COMPROMISE U.S. COMMUNICATIONS, IT NONETHELESS
HAS THIS SERIOUS ASPECT.

THE CAPTURE OF THE MODERN U.S. COMMUNICATIONS SECURITY
EQUIPMENTS OR THE MAINTENANCE AND OPERATIONS MANUALS
COULD STIMULATE ONE OR OTHER OF THESE COUNTRIES (OR
POSSIBLY COMMUNIST CHINA) TO MAKE MAJOR CHANGES IN
THEIR COMMUNICATIONS SECURITY EQUIPMENT AND PRACTICES.
THIS COULD VERY SERIOUSLY HAMPER U.S.
SIGNALS INTELLIGENCE PRODUCTION ON THESE NATIONS IN
THE FUTURE.

THERE WERE THIRTY (TWENTY-NINE ENLISTED AND ONE
OFFICER) NAVY SECURITY PERSONNEL ON BOARD THE SHIP.
MOST OF THESE MEN AND OFFICERS WERE HIGHLY SKILLED
AND REPRESENTED SEVERAL YEARS OF EXPERIENCE IN THE
BUSINESS. SOME OF THEM HAD INTIMATE KNOWLEDGE OF A
NUMBER OF SENSITIVE NAVY COLLECTION AND ANALYTIC
EFFORTS AND A FEW OF THEM HAD SOME KNOWLEDGE OF ONE OR TWO SENSITIVE NATIONAL SECURITY AGENCY PROJECTS. DEPENDING ON THE DURESS TO WHICH THEY MAY BE SUBJECTED AND THE AMOUNT THEY MAY RECALL, SERIOUS COMPROMISE OF SEVERAL HIGHLY CLASSIFIED PROJECTS COULD ENSUE FROM THEIR INVOLUNTARY REVELATION OF THE SCOPE OF THE U.S. SIGNALS INTELLIGENCE EFFORT. THIS COULD RESULT IN DEFENSIVE MEASURES BY THE SOVIETS TO DENY THE U.S. FURTHER INFORMATION.

HOWEVER, NO DAMAGE TO OUR OWN COMMUNICATIONS SECURITY WOULD FOLLOW EVEN FROM THE FORCEFUL EXTRACTION OF INFORMATION FROM CAPTURED PERSONNEL. UNQUOTE.