APPENDIX D

SPECIAL PROCEDURES FOR USE IN SYSTEMATIC AND MANDATORY REVIEW OF CRYPTOLOGIC INFORMATION

1. General guideline: Cryptologic information uncovered in systematic or mandatory review for declassification of 25-year old government records is not to be declassified by other than the National Security Agency. The information may concern or reveal the processes, techniques, operations, and scope of signals intelligence (SIGINT), which consists of communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT), or it may concern the components of Information Security (INFOSEC) which consists of communications security (COMSEC) and computer security (COMPUSEC), including the communications portion of cover and deception plans. Much cryptologic information is also considered "Foreign Government Information" as defined in Para. 1. l(d) of the Executive Order 12958.

2. Recognition of cryptologic information may not always be an easy task. There are several broad classes of cryptologic information, as follows: .

a. Those that relate to INFOSEC: In documentary form, they provide COMSEC/COMPUSEC guidance or information. Many COMSEC/COMPUSEC documents and materials are accountable under the Communications Security Material Control System. Examples are items bearing telecommunications security (TSEC) nomenclature and crypto keying material for use in enciphering communications and other COMSEC/COMPUSEC documentation such as the National Telecommunications and Information Systems Security Committee or is predecessor organization, COMSEC/COMPUSEC Resources Program documents, COMSEC Equipment Engineering Bulletins, COMSEC Equipment System Descriptions, and COMSEC Technical Bulletins.

b. Those that relate to SIGINT: These appear as reports in various formats that bear security classifications., frequently followed by five-letter codewords, for example, World War II's ULTRA, and often carry warning caveats such as "This document contains codeword material" and "Utmost secrecy is necessary..." or "Handle Via COMINT Channels Only" or HVCCO' or "CCO." Formats may appear as messages having addresses, "from" and "to" sections, and as summaries with SIGINT content with or without other kinds of intelligence and comment.

c. Research, development, test, life cycle support, planning, and evaluation reports and information that relates to either COMSEC, COMPUSEC, or SIGINT.

3. Some commonly used words that help to identify cryptologic documents and materials are "cipher," "code," "codeword," communications intelligence," or "COMINT," "special

intelligence, “ “communications security,” or “COMSEC,“ “computer security or COMPUSEC,” cryptanalysis,” crypto,” cryptography,” “cryptosystem,” “cipher,” ‘decipher,” “decode,” “decrypt,” “direction finding,“ “electronic intelligence” or “ELINT,” “electronic security,” “encipher,” “encode,” “encrypt,“ “foreign instrumentation signals intelligence” or “FISINT” pr “FIS”,” “telemetry’”information systems security” or ‘TNFOSEC,” “intercept,” :key book,” “one-time-pad, “ “bookbreaking,“ “signals intelligence” or “SIGINT,” “signals security,” “TEMPEST,” and “traffic analysis” or “TA.”

4. Special procedures apply to the review and declassification of classified cryptologic information. The following shall be observed in the review of such information.

a. INFOSEC (COMSEC and COMPUSEC) Documents and Materials.

(1) If records or materials in this category are found in agency or department component files that are not under INFOSEC control, refer them to the senior COMSEC/COMPUSEC authority of the agency or department concerned or return them, by appropriate channels, to the address in item 4.c, below.

(2) If the COMSEC/COMPUSEC information has been incorporated into other documents by the receiving agency, that information must be referred to the National Security Agency/Chief Central Security Service (NSA/CSS) for review before declassification occurs.

b. SIGINT (COMINT, ELINT, and FISINT) Information.

(1) If the SIGINT information is contained in a document or record originated by a U.S. Government cryptologic organization and is in the files of a non-cryptologic agency or department, such material will not be declassified. The material maybe destroyed unless the holding agency’s approved records disposition schedule requires its retention. If the material must be retained, it must be referred to the NSA/CSS for systematic review for declassification when it becomes 25-years old or older.

(2) If the SIGINT information has been incorporated by the receiving agency into documents it produces, referral of the SIGINT information to the NSA/CSS for review is necessary prior to any declassification action.

c. COMSEC/COMPUSEC or SIGINT information which requires declassification by the NSA/CSS should be sent to:

Director, National Security Agency/
Chief, Central Security Service
AlTN: Information Policy Staff (N5P6)
Fort George G. Meade, MD 20755-6000