~~SECRET - SECURITY INFORMATION~~

HOW TO DEMONSTRATE COMSEC WEAKNESSES TO NATO COUNTRIES

1. a. It is believed that NATO countries will recognize it to be to the benefit of all for each to improve his own national communications security. Any action that may be taken by the UK and US must not appear to be an infringement of the national sovereignty of any NATO country or a desire to dictate to any of them. Instead of providing for a detailed examination of national practices, therefore, it is preferable to set up minimum security standards. These should be promulgated by NATO for national use. Each country would be asked to evaluate its own practices against these standards and to assure NATO that that country's security is equal to or better than that which these standards would produce.

b. The Security and Evaluation Agency, NATO, which is in the [redacted] would be the agent for such a program. Its action would take three forms:

EO 3.3(h)(2)
PL 86-36/50 USC 3605

(1) Sponsorship of the program thru Standing Group channels and implementation of it if approved.

(2) Provision of assistance and advice, upon request, to individual countries.

(3) Evaluation of the results of the program.

2. Minimum standards can only be worked out in final form after considerable discussion between the [redacted] Such standards must be set forth in extreme detail and must cover all known national

practices of NATO countries in the whole field of communications security. This paper gives only a bare outline of the fields that must be covered. If this approach is agreed upon by the UK and US, the Conference itself should at least produce an agreed list of topics along these lines which will be the basis for later preparation of detailed specifications.

3. In addition to physical security of cryptomaterial, adequate communications security depends on two principles:

[redacted]

b. Cryptographic systems must be adequately secure and properly used.

4. As regards the first of these, it will be necessary to set standards in the following fields:

a. Frequency plans: To include minimum standards for frequency allocation and frequency rotation, with attention paid to the interrelation between frequency changes and call sign changes.

b. Format of cipher text: To include the steps necessary to prevent [redacted] on the basis of such things as length of cryptoparts, discriminants, indicators, group length, etc.

c. Message externals: To include emphasis on eliminating any external elements that would facilitate the identification of traffic, e.g., steps toward attaining uniform heading procedures, etc.

d. Communication procedures: To include measures for general

standardization of communication procedures, for attainment of call sign security, with careful attention to interrelation of call signs and addresses.

e. Plain language transmissions: To include steps toward minimizing transmissions in plain text and procedurally isolating such plain language as must be transmitted.

5. a. The treatment of cryptographic security will include discussion of all systems and equipments known to be in use or available for use by NATO countries other than [redacted] and will state whether or not they are acceptable; if they are acceptable minimum standards will be prescribed for their use. All systems approved for NATO use will be included in the consideration.

b. The fields now contemplated for discussion are as follows:

(1) Hand systems: To include unenciphered and enciphered codes, Slidex or other tactical codes, transpositions, strips, additives on plain text, etc.

(2) Literal, or off-line machines: To include all known Hagelin types, Enigma types, Kryha, etc.

(3) Teleprinter machines: To include Fish types, Olivetti, Hellschreiber, one-time tape systems, etc.

(4) Key-generation and criteria therefor.