MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Compromises of SIGINT Information.

1. At the request of the Director, National Security Agency, the enclosed memorandum from GCHQ on the above subject is forwarded for information.

2. Comments by the Director, NSA, on the enclosed list of recommendations adopted by LSIB to improve the handling of certain UK crypto-systems are briefly summarized below:

   "a. We are also concerned over the danger of transmitting plain-text when various on-line crypto-systems, including 5 UCO, are used and are investigating ways to prevent it.

   "b. We already are printing Encipher and Decipher pads, OTP, in different colors.

   "c. The recommendations regarding ROCKEX and ROLLICK are expected to result in improved security. These equipments are not being used by the U.S."

Enclosure

Copy of DGC/4217 dtd 26 Mar 1954.
DGC/4217

26th March, 1954.

Director,
National Security Agency.

CONTROLS OF SIGINT INFORMATION

As a result of the proposal, referred to in DGC/3555 of 16th July 1953, that L.S.I.B. should review the whole problem of the compromise of Sigint information by misuse of Sigint communications a number of recommendations, designed to bring about a diminution in the number of such compromises, have been adopted.

2. I am glad to be able to tell you that during the period 27th July 1953 to 23rd December 1953 only three further compromises by U.K. authorities have been reported.

3. I am taking the opportunity, while sending you, at Appendix, a copy of the details of these three lapses, to enclose a copy of recommendations adopted by the U.K. concerning specific U.K. cryptosystems which are additional to the Regulations approved and adopted by L.S.I.B. which will be forwarded to U.S.C.I.B. shortly.

Deputy Director.
RECOMMENDATIONS ADOPTED BY L.S.I.B. TO IMPROVE
THE HANDLING OF CERTAIN U.K. CYPHER SYSTEMS.

5 UCO  (a) Highest priority should be given to the investigation
of further improvement of the alarm system bearing in
mind that the machine is normally handled by average
personnel rather than by experts as in the field trials.

(b) The arrangement of the jack field should be modified
(and any other appropriate alterations made) to obviate
errors arising from wrong connections resulting in the
transmission of plain language tape.

O.T.P.  In future the "IN" copy of all one-time-pads used
for Sigint communication should have the bottom right-
hand corner dipped in red dye.

ROOKEX  Apart from strict attention being paid to training
and supervision no further recommendations are made
since the introduction of the mechanical modifications
should effect the necessary improvement in security.

ROLLICK  A set of operating instructions with security sections
suitably highlighted should be issued.
<table>
<thead>
<tr>
<th>Date of Compromise</th>
<th>Circumstances</th>
<th>Classification</th>
<th>Subject Matter</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>27.7.53</td>
<td>Message transmitted by radio in clear over 5000 by 2 Wireless Regiment, Panama. Operator's error leading to transmission of P/L tape being used to test circuit</td>
<td>SECRET codeword</td>
<td></td>
<td>EO 3.3(h)(2) PL 86-36/50 USC 3605</td>
</tr>
<tr>
<td>22.12.53</td>
<td>Check and repeat of two words for corruptions (of no significance out of context) but including codeword</td>
<td>TOP SECRET FROM</td>
<td>Possibility of interception cannot be discounted although the ROLLICK is a VIP point to point system, the codeword must therefore be considered compromised</td>
<td></td>
</tr>
<tr>
<td>23.12.53</td>
<td></td>
<td>CONFIDENTIAL</td>
<td></td>
<td>None, as the cause was due to the Assistant Circuit Controller failing to check on the mechanism after changing the key tape.</td>
</tr>
</tbody>
</table>