TRANSMITTAL SLIP	DATE 25 Mar 87	
TO: [redacted] C/MD/M&CG/OIT		
ROOM NO. 2D02	BUILDING Hqs	
REMARKS:		
FROM: [redacted] EXA/DDA		
ROOM NO. 7D24	BUILDING Hqs	EXTENSION

STAT

STAT

STAT

FORM NO. 241 1 FEB 56 REPLACES FORM 36-8 WHICH MAY BE USED. (47)

Administrative - Internal Use Only

EXA /

Deputy Director
for Administration

25 March, 1987

Note To: Chief, Management Division,
M&CG/OIT

Subject: Modems

Rich,

I'm not trying to be a pest (although I frequently succeed anyway), but I need to follow-up on the attached note. After the recent Hannover Hacker case in which telephone connectivity enabled the compromise of more than 200 computer systems, there is a great deal of sensitivity to the danger of modems.

Can you bring me up-to-date on our plans, if any, to solve the modem threat through technical means?

[redacted]

Executive Assistant to the DDA

Administrative - Internal Use Only

12 November 1986

STAT NOTE FOR: [redacted]
Chief, Management Division, OIT

STAT FROM: [redacted]
EXA/DDA

SUBJECT: Modems - What to do about them?

Rich:

STAT 1. During a briefing last month by [redacted] to the DDA, Bill raised the question: What can, should we do about modems? His concern is that someone could easily connect their PC to their black telephone via a modem and thus compromise large volumes of Agency data.

STAT 2. I spoke briefly with [redacted] about this issue. According to my (possibly flawed) notes, Steve said:

- The new PBX has built-in capabilities which could obviate the need for many (but probably not all) modems. There is currently nothing in the NBCPO plan or budget to utilize this facility, however.
- It would be difficult and expensive to program the PBX to detect unauthorized modem usage. One alternative would be to audit any long telephone sessions, which are typical of PC-modem calls.
- A less expensive option might be to establish a tighter policy on modems--perhaps requiring registration, certification, and tagging. Any modem not tagged and registered would result in a security violation.

3. There are probably many creative solutions which would reduce the potential threats from modems. Would you please bounce this concept around informally in OIT to see if there is an inexpensive, verifiable solution? This obviously isn't a top priority item. Perhaps someone in OIT could assemble some ideas over the next several months. Sound feasible?

STAT [redacted]

STAT cc: [redacted] OIT/NBCPO