CONFIDENTIAL

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, DC 20310-1001

REPLY TO
ATTENTION OF

DAMI-CI   2 January 1985

MEMORANDUM FOR SECOM MEMBERS

SUBJECT: DCID 1/16, Security of Computer Operations

1. (U) BACKGROUND:

    a. (U) Current DCID is over 8½ years old; predates revo-
lutionary microcomputer technology.

    b. (C) ADP security techniques lag well behind the
microcomputer revolution.

    c. (U) Explosive, continuing growth in the volume of
Sensitive Compartmented Information (SCI) requires automation
to provide timely dissemination.

    d. (U) ADP terminals and microcomputers are becoming
electronic memos and desks; we cannot afford to build a SCIF
around every such device.

    e. (U) DCID 1/19, Security Policy for SCI Control
Systems, (paragraph 30) sets the precedent for temporary use
and processing of SCI outside a SCIF when operational needs so
require.

2. (U) CONCLUSION. DCID 1/16 must reflect current and
rapidly changing automation technology. The documented threat
to a specific location and not the potential threat must be
stressed.

3. (C) RECOMMENDATION. DCID 1/16 should be revised to
address the microcomputer and community inability to rapidly
devise cost-effective ADP security procedures. Minimum points
to address include:

    a. (U) Stand-alone microcomputer operations without ADP
audit trails.

    b. (U) Microcomputer local area networks (LANs).

CLASSIFIED BY: DCID 1/16
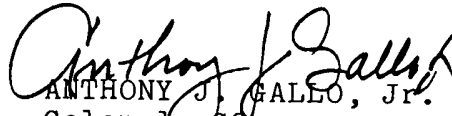DECLASSIFY ON: OADR

CONFIDENTIAL

CONFIDENTIAL

DAMI-CI
SUBJECT: DCID 1/16, Security of Computer Operations

    c. (U) Microcomputer as "dumb" or "smart" terminal linked to a host computer.

    d. (C) State-of-the-art DCID 1/16 standards which permit use of microcomputers and other SCI terminals in a non-SCI facility (SCIF).

ANTHONY J. GALLO, Jr.
Colonel, GS
Army Member

2

CONFIDENTIAL