17 February 1984

ASSUMPTIONS ABOUT AN INTER-AGENCY DATA SHARING POLICY

1. The Information Systems Board tasked the Computer Security Working Group with monitoring the development of RECON GUARD and with recommending a policy on inter-agency data sharing.

2. The question of a data sharing policy is not normally associated with computer security in that data sharing itself need not (and frequently does not) involve computers at all. A data sharing policy probably involves more political and management issues than it does technical issues. Therefore, the CSWG has not restricted itself to just computer-related aspects in its discussions.

3. Data sharing is fraught with conflicting perceptions and concerns. Originators of data are concerned with the access, use, and storage of their data by sharing agencies. While this has been true for many years, the computer and electronic transmission of data among users has provided much more rapid and wider access to data than has ever existed. The speed and scope of electronic means of data sharing have appreciably heightened originator concerns. Users of shared

data, on the other hand, must digest an increasingly varied volume of raw intelligence. Electronic systems designed to help users react rapidly to changing assignments and intelligence targets press against the customary guidelines (e.g. "need to know") of traditional intelligence.

4. Any data sharing policy will be significantly affected by the interpretation (by both originators and recipients of shared data) of DCID 1/7 (attached). Originators probably would prefer a strict interpretation of DCID 1/7 while users in recipient organizations, due to the pressures of real time analysis, would probably prefer a more flexible interpretation. The constant shared by both originators and recipients of shared data is the responsibility of line management to monitor and ensure responsible protection of the data. Line management may not, however, be well prepared to deal with the complexities of electronic systems.

5. The following assumptions are presented to the ISB to stimulate discussion and therefore guide the CSWG in its pursuit of a recommendation on an inter-agency data sharing policy. No such recommendation can be devised by the group without some policy-level decisions about these assumptions. Each assumption is followed by a series of remarks collectively grouped for discussion. Some are statements, others are questions. The CSWG does not pretend that any are authoritative nor are they a complete outline of all relevant points.

6. Finally, the issue of data sharing has so many facets that the CSWG has tried to limit the number of assumptions for simplicity. Other assumptions or points will certainly arise before a complete data sharing policy can be drafted. This, however, is the first step.

ASSUMPTION 1: The CIA wishes to establish a consistent policy concerning classified amd sensitive inter-agency data sharing.

DISCUSSION:

--the CIA must speak with one voice in dealings with other Intelligence Community components.

--The policy should address data being shared initially, data already shared and accessible from a recipient agency's data base, and data already shared and accessible through a Community network.

--The policy should cover technical, scientific, tactical, numeric and full text, and bibliographic citation sharing.

--The policy should ensure that electronic data sharing equals or surpasses hard copy data sharing in security and administrative control.

--The policy must note the impact of the third agency rule on shared data, especially in data bases accessed by multiple agencies.

ASSUMPTION 2: Adoption of any data sharing policy will depend at least on the physical, technical, and procedural security of both the data transmission link and the storage/access/use of the data within the recipient organization.

DISCUSSION:

--Once data is passed to another agency, it leaves our physical control--whether it be hard copy or electrical data.

--Will the Agency accept minimum safeguards for protection of critical systems that process intelligence information, currently being developed by the DDCI COMPUSEC SAFEGUARDS WORKING GROUP, as a minimum standard?

--All sharing components must certify periodically that the shared data is stored/accessed/used in accordance with the COMPUSEC minimum standard (cited above).

--All users of shared data at recipient organizations must be cleared for the highest level of data to which they might conceivably have or gain access.

--Agency components will accept reasonable assurances from sharing components that the minimum standards are being met.

--Discussion of Agency certainty that minimum standards are not being applied to the satisfaction of the data owners will be covered under ASSUMPTION 5.

ASSUMPTION 3: In addition to minimum security standards, the CIA must have satisfactory assurances that the principle of "need to know" (as defined in DCID 1/7), compartmentation, and protection of sources and methods, are enforced by recipient components and networks.

DISCUSSION:

--DCID 1/7 is specific about the principle of "need to know." Real-time intelligence analysis, and the computer as a tool, both tend to press against the boundaries of a strict construction of the "need to know" principle.

--For initial dissemination hard copy data sharing, human review occurs at the sharing component level and shared data is released to agencies or to specifically named individuals with a need to know.

--For electrically disseminated shared data, the process for authorizing user access must be validated and approved by originator and recipiert organizations to ensure need to know. Changes to such access must also be validated and approved.

--Line management of recipient organizations must also enforce "need to know," compartmentation, and protection of sources and methods.

--For retrospective access and use by recipient organizations--whether hard copy or electrical, scientific, technical, tactical, full text, or bibliographic citation

type systems--must recipient organizations guarantee that "need to know", compartmentation, and protection of sources and methods probably cannot be violated by any individual, or need they guarantee that they monitor those factors to ensure
compliance, e.g. audit trails of queries? It may be possible to track electronically the routing of electronic documents more efficiently than hard copy, but usually in an ex post facto manner.

ASSUMPTION 4: Not all CIA data should be shared, nor should shared data necessarily be made available to all NFIB members.

DISCUSSION:

--CIA originators will be able to choose to share or not share data with specific recipient organizations or named individuals, subject CIA senior management review.

--CIA originators will be able to recall shared data from both specific recipients and all recipients, if necessary.

--CIA originators will be able to specify which individuals, agencies or components can and cannot see shared data. These specifications will be adhered to by recipient organizations and Community networks.

--CIA originators cannot dictate specific internal handling methods by recipient organizations but can expect that shared data will be fully protected according to minimum security standards mentioned above, that compartmentation, "need to know," and protection of sources and methods will be enforced, and that shared data will be handled in accordance with DCID 1/7.

ASSUMPTION 5: If a CIA originator has reason to believe that its shared data is not being properly protected, stored, or accessed in a recipient organization, the originator must request that D/OS investigate. If the deficiency is confirmed, the originator will then halt the sharing of data with that organization until the deficiency is resolved.

DISCUSSION:

--It is not intended that CIA originators will police the operations of sharing agencies. Discovery that protection is not up to minimum standard will probably occur after a flap or compromise.

--This is a drastic, although necessary, weapon that should not be lightly used.

--No CIA originator can unilaterally and permanently cut off a recipient organization without approval of DCI.

ASSUMPTION 6: Decisions to share data should be in accordance with DCID 1/7 and be preceded by written agreements covering the security and administrative arrangements for the protection of the data, additional training required by involved employees and managers to successfully protect the data, and review procedures to satisfy both originators and recipients that the data sharing is beneficial and secure.

DISCUSSION:

--Originators are not always adequately aware of the use/access/storage procedures of recipient organizations.

--Recipients are not always adequately briefed on methods necessary to protect the shared data.

--Data that is shared is not always useful especially over a period of time. Needless sharing of data unacceptably raises the risk inherent in data sharing.

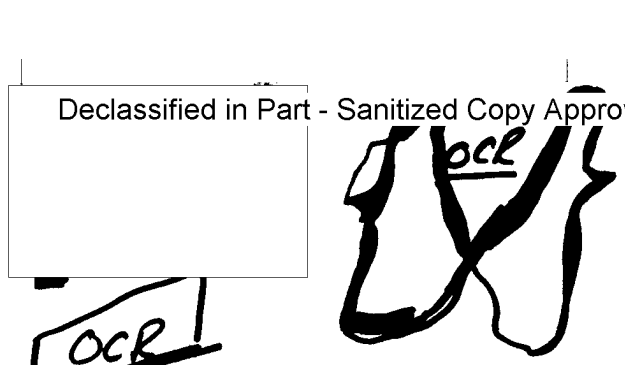
ASSUMPTION 7: If data is shared via an electronic information system, the CIA configuration will ensure as much as possible that no data is released due to technical malfunction, unauthorized tampering, or penetration.

DISCUSSION:

--This is the task of RECON GUARD.

--If CIA is a node in a Community network, should that node point and its data bases be electrically isolated from other CIA systems to prevent unauthorized penetration?

 STAT



OCR

- defer to ISSG on security or simulated approach
- uncomfortable with connection
- today "strange queries" by Knowledge Base threw RECON into a guard tizzy
  - 2000 test works fine but greater number
- ~~Eyeon~~ imply
- Simulation validity in question !!! Not confident
- withdrew RECON
  - pay as you go
  - if it works ~~Recon~~ then Recon
  -
  - ~~Do~~

* participants have to buy *

- DIA, NSA, STATE can get ORCON they were originally on DISSEM & pandora's box but index on all originally on dissemination

- SAFE
  - central index file (Son of Recon) by Sept know how this will differ from RECON

- to offer RECON up to Guard premature.