

~~CONFIDENTIAL~~

DIRECTOR OF CENTRAL INTELLIGENCE

SECURITY COMMITTEE

Computer Security Subcommittee

DCISEC-CSS-M102

20 July 1977

COMPUTER SECURITY SUBCOMMITTEE

OF THE

DIRECTOR CENTRAL INTELLIGENCE

SECURITY COMMITTEE

Minutes of Meeting

Held at CIA [redacted]

McLean, Va.

14 July 1977

25X1

1. The one-hundred and second meeting of the Computer Security Subcommittee of the Director of Central Intelligence Security Committee was held between 0930 and 1300 hours on 14 July 1977 at CIA, [redacted] In attendance were:

25X1

[redacted]

25X1

Mr. Robert Kyanko, Treasury/Secret Service Member

[redacted]

25X1

Capt. Ron Pherigo, Air Force Member

[redacted]

25X1

Mr. George S. Herrmann, State Member

[redacted]

25X1

LCDR Dean H. Beyer, OJCS Observer

[redacted]

25X1

[redacted]

25X1

Classified by DIRMBA/CHCSS (NSA/CSSM 123-2)
Exempt from GDS TO 11022, Cat 2
Declassify Upon Notification by the Originator

~~CONFIDENTIAL~~

2. The security level of the meeting was TOP SECRET SI.

3. The Chairman opened the meeting with a discussion of a DCI request of the Security Committee to formulate a policy for multi-level computer system security. Specifically, the following note was presented to the members:

" 27 June 1977
To: John McMahon (Director IC Staff)
From: Cdr. McMahon

The Director would like the NFIB to study and formulate a policy for Multi-Level Computer System Security for the Intelligence Community.

Very respectfully yours
McMahon "

Discussion ensued on how to respond to the Director's request. The Chairman stated that he would work with [redacted] and [redacted], Executive Secretary Security Committee in preparing a written response. The DIA and Air Force members requested that the response be coordinated with the Subcommittee before presenting it to the DCI.

IHC 25X1
25X1

4. The Chairman solicited comments from the members on the IHC Computer Security Issue paper. The Army and State members prepared their comments in writing. They are attached to these minutes as inclosures 1 (Army) and 2 (State). The Navy and ERDA members had no comments.

The FBI member advocated the appointment of an advisory group to deal with the problems of R&D and Threat. He also believes that NSA could best serve as the organization responsible for centrally advising the community on matters involving computer security.

The CIA member suggested that the Subcommittee serve as a tasking agent for the Community for resolution of specific problems.

The Air Force member recommended that a better definition of multi-level security be written. He advocated a single set of operating modes and a single, but coordinated, R&D effort. He suggested that there be formal tasking from the Intelligence Community on computer security requirements. He felt that one Agency, such as NSA, should not be appointed a central technical authority role.

CONFIDENTIAL


The DIA member advocates that basic policy in computer security should be established. There also should be guidance on how to test and secure networks. The operational modes in net-working must be defined. DIA non-concurs in the suggestion of NSA being named the central technical authority.

The NSA member suggested that the technical issues of computer security should be addressed by the Subcommittee. Also, the Subcommittee should act as the focal point for the DCI in identifying community computer security needs. The Subcommittee would then recommend to the DCI the best Agency to task for meeting the need. She further feels there should be a publication of wide dissemination on computer vulnerabilities. The Subcommittee should discuss ways of making information on the subject available to users and operators.

The Treasury member agrees with the position presented by the State member. The Treasury member feels there is a fundamental communications gap in computer security, particularly the lack of definitions. He opposes the single agency concept for central technical authority and advocates an interagency group. He stated that Treasury lacks funds for R&D and therefore relies on the Intelligence Community for development in this area.

5. The meeting adjourned with the Chairman announcing a request of each agency to present its R&D programs in Computer Security for the next meeting.

25X1


Executive Secretary
Computer Security Subcommittee

CONFIDENTIAL



DAMI-SS

DEPARTMENT OF THE ARMY

OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE

WASHINGTON, D.C. 20310

13 JUL 1977

MEMORANDUM FOR: CHAIRMAN AND MEMBERS OF THE DCI COMPUTER SECURITY SUBCOMMITTEE

SUBJECT: Comments on IHC Issue Paper on Computer Security

1. The IHC Issue Paper is an excellent summarization of the automation security problems confronting the Intelligence Community today. The traditional problems plus the four additional issues enumerated in the paper are common to all the community membership and should be addressed through a unified approach. It must also be understood that these problems are not only common to the task of protecting classified information in an automated environment, but are equally applicable to the protection of the unclassified information areas which we are obliged to protect--privacy, proprietary, assets, and resources (against theft and fraud). The Intelligence Community has traditionally taken the lead in automation security because of its critical need to protect intelligence sources and methods, but the IC is only a subset of the federal government's automation agencies requiring protection.

2. A universal problem in DOD is the shortage of manpower and financial resources which can be dedicated to the automation security mission. We are all cognizant of many aspects of the overall problem which we could address if we had the resources to commit. Unfortunately, the political climate at this time is not favorable to support for any action which appears to benefit the Intelligence Community as a whole or in its parts.

3. The new privacy directive, which we have not had the opportunity to review yet, reportedly contains requirements which demand that personal data not only must be protected, but that accesses to it must be recorded in an audit trail reviewable on demand by the subject of the data. This protection would extend to the data element level within individual automated records. If we equate these privacy protection requirements to classified information protection we find almost an exact parallel. Control of information to the data element level and maintenance of an audit trail on each access has a clear counterpart in applying the "need-to-know" principle in automated intelligence files.

4. Since there is great public (and hence, congressional) support for privacy protection, we propose that the computer security elements of the various Intelligence Community agencies get behind, encourage, and guide their privacy protection counterparts in the actions necessary to achieve protection (security) at the expense of the privacy groundswell now underway.

DAMI-SS

18 JUL 1977

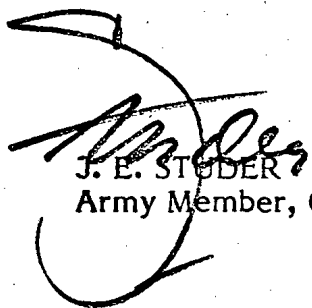
SUBJECT: Comments on IHC Issue Paper on Computer Security

5. The Computer Security Subcommittee (CSS) remains the most suitable vehicle for attack of our common problems. It should continue to be the forum in which general policy for community automation security is aired, argued, and established. The member agencies should then be permitted to convert that general policy to doctrine suitable for application within their jurisdictions.

6. The CSS could be made more effective by providing it with a small permanent support staff (not more than six persons) from IC resources. The support staff could function under policy control of the CSS and provide it with research, editorial, limited technical, and administrative support.

7. We agree with the initial statements of the paragraph titled "Impact on 10-Year Planning," but disagree with the implication of its penultimate sentence. Diversity of membership dictates that autocratic direction of this or any other intelligence effort is undesirable. The Intelligence Community can solve its automation security problems in a "tight," cooperative confederation where each member has an equal voice in policy decisions.

8. New technology applicable to automation security is advancing in quantum leaps. Solution of our problem requires a combination of this new technology with imagination, initiative, existing and developing risk and security management techniques and procedures, dedicated effort, and managerial commitment of money and manpower. Absolute automation security will never be achieved in this dynamic environment, but we can and must provide our agency heads with increasingly sophisticated levels of protection to counter the increasing risks which confront them. Our task, like the testing of the mythical King Tantalus, is an endless challenge.


J. E. STUDER
Army Member, CSS



DEPARTMENT OF STATE

Washington, D.C. 20520

MEMORANDUM

TO: [redacted] Chairman DATE: July 13, 25X1
 Computer Security Subcommittee
 National Security Agency
 Fort George G. Meade, Maryland 20755

THRU: Chief, *A. J. L.* Division of Technical Services
 Office of Security

INFO: INR/DDC: Mr. William E. Berry
 O/ISO: Mr. Wally W. Francis
 SY/PS & I: Mr. William H. Armor
 SY/CC: Miss Concetta Conigliaro

FROM: George S. Herrmann *GSH*
 State Member
 Computer Security Subcommittee

SUBJECT: State Comments on IHC Computer Security Issue Paper

1. Members of the Computer Security Subcommittee have been asked to review an issue paper generated by the DCI Information Handling Committee, a copy of which is attached. Following our review of the paper, we were asked by [redacted] to respo25X1 to several questions. These were:

a. Should NSA be the technical accreditation agency for computer security matters, as it is for COMSEC matters?

b. List the three highest priority computer security problems.

c. Give an estimate of the resources your agency can bring to bear on these problems.

d. After DCID 1/16 is revised and published, what further computer security policy and guidance do we need?

2. I find it rather stimulating to be asked to consider something other than another draft of DCID 1/16, and have read the IHC issue paper with interest. On my initial reading,

CONFIDENTIAL

25X1

CONFIDENTIAL

-2-

the paper did not do much for me: it advances many computer security requirements without suggesting solutions. On re-reading the paper, though, I would suggest that the IHC has done us a service by highlighting prominent holes in our computer security posture. Closing these holes is a proper function of the Computer Security Subcommittee: it doesn't matter who points out our weaknesses, so long as we address them. Accordingly, I find the IHC issue paper a useful departure point for CSS discussion.

3. I propose the following answers to questions:25X1

a. Accreditation Agency:

For my money, NSA should be the U.S. technical accreditation agency for computer security. I have had some experience in complying with NSA-established accreditation procedures for COMSEC installations, and I think they do a first rate job in this area. We need an accrediting agency to establish community-wide standards, and I feel that NSA has the staff, resources and interest to do a thorough job in this area.

b. What are our computer security problems, as a community?

The reconciliation of the operational requirements of the Department of Defense with the computer security requirements of our civilian intelligence-generating agencies is the highest priority computer security problem currently facing the United States Government. We have tried to achieve this reconciliation in subcommittee work to no avail for several years, and work on this issue has quagmired qualified people who would otherwise have addressed problems like those in the IHC issue paper. If decisive action by the DCI can achieve this reconciliation, it should be suggested; if a major R&D effort is required to develop technology that will suit both sides of this issue, such an effort should be initiated.

I suggest that the lack of a community-wide or even agency-wide reporting system for computer security violations is a major problem within the community. If your agency is penetrated, whom do you inform, and what means of reporting do you use? General guidelines of the nature do not presently exist.

CONFIDENTIAL

CONFIDENTIAL

-3-

We cannot wisely develop threat estimates, hardware, firm-ware or software countermeasures to penetration attempts without an effective means of penetration or hazard reporting. I think [redacted] talk at the CSS June meeting was very instructive: a DCI-promulgated procedural guide fore reporting computer security penetrations is a pressing requirement.

25X1

Computer security is a relatively new field, and expertise in this field is not widespread. We need to get this expertise into the hands of intelligence community computer system operators and managers in short order, and we need to do this effectively. I suggest that we need an inter-agency school, provided with instructors from the various member agencies, that will train IC users in the problems of computer security. This school should work closely with private industry to keep its material current.

c. Resource Estimate: The Department of State can provide little in the way of human resources to help solve computer security problems: some financial resources might be made available to support computer security research projects if other agencies were also to contribute funds.

d. Further Guidance: Once DCID 1/16 is published, someone in the IC staff should be charged on a full-time basis with coordinating intelligence community compliance to the directive. This individual or office should work closely with the Computer Security Subcommittee to point out problems and help resolve them. The subcommittee should turn its attention to the development of standards for testing and accreditation.

DISTRIBUTION:

1-Addressee
1-Each info addressee
1-Subject file
1-Reading file

[redacted]

25X1

CONFIDENTIAL