

DIRECTOR OF CENTRAL INTELLIGENCE
SECURITY COMMITTEE
COMPUTER SECURITY SUBCOMMITTEE

24 September 1981
DCISEC-CSS-M139

STAT 1. The One Hundred and Thirty-Ninth meeting of the Computer Security Subcommittee was held on 15 September 1981 at [redacted] McLean, VA. The meeting was convened at 0930, and attending were:

STAT SIAI [redacted] Chairman
[redacted], Executive Secretary
CIA

STAT Mr. James Studer, Army
Mr. Lynn McNulty, Dept. of State
[redacted] NSA
Mr. Robert Graytock, Dept. of Justice
Mr. Robert Wingfield, Dept. of Energy
Mr. Ronald Lancing, Navy

STAT [redacted] SECOM
Mr. Robert Storck, FBI
Mr. Edward Springer, Los Alamos Nat'l Labs (DoE)
Mr. David Bailey, Los Alamos Nat'l Labs (DoE)

2. The minutes of the previous meeting were reviewed. There were no comments, and thus they were approved as written.

3. Mr. Wingfield (DoE) introduced Messrs. Bailey and Springer from the Los Alamos National Laboratories, where DoE has recently established a centralized computer security group for the Department.

a. Mr. Springer started with a general overview of DoE responsibilities and capabilities, showing how the Los Alamos Labs fit into the overall DoE structure. He then discussed the establishment of the Computer Security Technical Center for DoE at the Los Alamos Labs, which is specifically geared toward addressing the Department's computer security problems. He went on to discuss some of the specific techniques being applied presently, such as DES-type devices for the protection of "unclassified-but-sensitive" traffic, and for file encryption functions. In response to a question on the relative amount of SI processing required by DoE, it became clear that there was very little such processing, and the requirement that does presently exist can be satisfied via periods processing.

b. Mr. Bailey then spoke of several specific programs which were being pursued at the laboratories. He stated that the bulk of their work related to "secure operating systems" was being performed in close cooperation with NSA. It was generally agreed that, since such a small percentage of the DoE processing is SI, they should continue to maintain their primary contact with the DoD community, mainly through the recently formed DoD Computer Security Center at NSA.

c. The basic thrust of the presentation was to apprise the CSS of the existence and capabilities of the DoE Computer Security Center, and offer to participate in, and support, community technical programs (R&D, studies, etc) which are aimed at computer security problems of mutual interest. Consequently, the Los Alamos Labs would like to be considered as a qualified candidate on appropriate technical tasks that the CSS wishes to fund.

4. The CSS next discussed the various proposals which had been submitted for spending the money (\$250K) which has been provided by the SECOM. Each of the proposals which had been submitted were reviewed and discussed. One of the proposals involved the evaluation of the TEMPEST threat to ADP systems. This was rejected by the chairman as being outside the "jurisdiction" of the CSS, falling more properly to the SCOCE (Special Committee On Compromising Emanations). There was some discussion on this point, with some of the membership expressing their concern with TEMPEST as a valid ADP system problem. The chairman offered to draft a letter to the SECOM expressing the membership's concern with TEMPEST problems exhibited by ADP systems.

5. The chairman asked the members to review each of the proposals and express their preference for the tasks to be funded. The most popular proposal was that the develop a technology forecast, to predict/evaluate technological trends which would have an effect on computer security technology, and thus help the community decide the proper directions for R&D. Other proposals chosen as reasonable candidates for CSS funding were those relating to a survey of word processing systems and their security-related capabilities (it was also recommended that the newly-created DoD Computer Security Center be tasked for this project), and a threat study.

may get the results in 10 days

6. The chairman asked that final votes and any further suggestions be phoned to him by the 2nd week of October 1981. Copies of the proposals which have been submitted to date are Enclosed. Questions on any of the proposals should be directed to the originating organization.

7. The next meeting was set for Tuesday, 20 October 1981, at 0930, at [redacted]. The primary item of discussion will be the policy statement for the revision to DCID 1/16.

[redacted signature box]

Executive Secretary

7 Encls:

- 1. Proposal, Subj: Proposals for Funds Submitted by Computer Security Subcommittee Members, dtd 1 Sep 81
- 2. Proposed Contract, Subj: Computer Network Security \$100K, undtd
- 3. Proposed Contract \$50K, undtd
- 4. Proposed Contract R&D Magnetic Media Control Using Technical Means \$75K, undtd

STAT
STAT

5. Dept of Army Ltr, DAMI-AM,
Subj: Recommendations for
Employment of SECOM Funds
Allocated to CSS, dtd 8 Sep 81
6. Proposed Contract, Subj:
Computer Network Security,
\$100K, undtd
7. Dept of Energy Ltr, dtd
17 Sep 81, and Encls thereto

~~SECRET~~

1 SEP 1981

SUBJECT: Proposals for Funds Submitted by Computer Security Subcommittee Members

TO: Chairman, DCI Security Committee

Following are proposals for funds as submitted by membership:

CIA

1. Compile a listing of essential ingredients of the current/ongoing network studies in computer security.
COST: \$45K
2. Identify the security elements that are required in a total (multi-level) network.
COST: \$90-100K

NSA

1. Baseline Computer Security Technology Forecast. Where the technology is and where it is going; trends; what should we pursue?
COST: \$50K
2. Subcommittee participation at selected Computer Security Conferences/Workshops.
COST: \$50K

DIA

1. Individual Identification/Authentication

Prepare a technical evaluation of individual identification capabilities.

Reliable, efficient, and cost effective individual identification is required for access control for physical areas, local and remote host computers, and automated networks. Industry is providing a number of capabilities most of which have identifiable deficiencies; a number of government efforts are under way to develop access control capabilities. A technical study is needed to report/evaluate the current state of the technology.

COST: \$80K

REGRADED UNCLAS WHEN SEPARATED FROM ENCLOSURE(S).

~~SECRET~~

~~SECRET~~

2. Data Classification and Control Markings

Develop a marking system with the capability to identify data classification and restrictive handling controls for intelligence information stored, processed, or extracted by automated systems and networks.

Definitive access control and dissemination labeling capabilities are necessary with development of:

- Common Data Bases
- Delegated Production
- Integrated Data Base
- Automated Networks

COST: \$200K

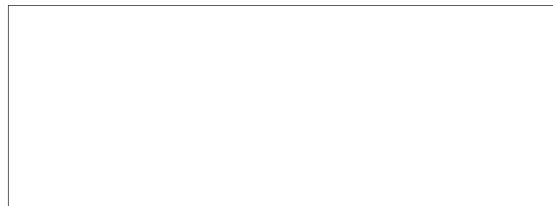
3. Penetration Exercise

Assemble audio surveillance hardware and develop/execute a penetration/collection scenario.

COST: \$150K

If any of the above proposals are determined to have merit, the subcommittee will provide additional details.

Attached as enclosures are additional proposals for your consideration as submitted by the FBI and DOE.



REGRADED UNCLAS WHEN SEPARATED
FROM ENCLOSURE(S).

~~SECRET~~

25X1

Proposed Contract

COMPUTER NETWORK SECURITY

\$100K

I. Introduction

Of all the issues involving ADP security, network security is the most complex. This is because network security spans all facets of security. For example, physical security, personnel security, communications security, TEMPEST security, and computer software security are all important considerations of network security. The distributed nature of networks further complicates issues involving physical and communication security. All the problems and technical issues involved with the security of a single computer is present in a network and is essentially multiplied by the number of computers (i.e., network nodes) in the network. In particular, the issue of multilevel security is greatly complicated in a network.

The combination of the distributed nature of networks and packet switching technology (i.e., the multi-path distribution of packet composition/decomposition) makes total multilevel security a very difficult goal to achieve.

Computer network security issues can be divided up into two areas of concern:

- a. communications security
- b. nodal security

II. Proposed Contract

Amount - \$100K

- "Think piece," original study on security requirements for Network Architecture which would examine:
 - nodes
 - communication lines (Bus, fibre optics, etc.)
- This study should not be directly based on existing developments or biased by past efforts. However, contractors should be aware of past efforts in this area.

Questions to be addressed

- a. Centralized vs decentralized security?
- b. Type of security technology which would be most applicable in centralized systems or decentralized systems?

Should address

1. What capabilities should the networked system have to be secure from standard modes of security compromise, e.g., tapping, penetration, etc.? If encryption is broken what steps need be taken as envisioned by the contractor to eliminate or minimize damage to network?
2. How will the contractor ensure compartmentation of data when nodes are connected to a network which has different levels of classified data?

Givens

- Must conform to security requirements of multicompartmented mode (DCID 1/16 and OMB A-71)
 - multi-CPU's
 - hundred of users
 - multi-geographic locations
 - encryption systems
 - something that is practicable and doable now

Products

- Deliverables
 1. Security requirements (system, physical, procedural) for NODES.
 2. Security requirements for front-end processor (if centralized).
 3. Security requirements for communication links (Bus, fibre optics, etc.).

ISSG/OS/CIA

Proposed Contract

\$50K

I. Objective

Survey existing technical literature, in and out of Intelligence Community, on computer network security architecture and detail specific findings. These findings will be used as a platform to launch a comprehensive study in developing needed system security mechanisms for networked systems now being developed within the Intelligence Community.

Contractor will be asked to detail any gaps in existing network architecture to date which may call for additional studies.

II. Products

- Paper summarizing methodology to date in handling security in "networked systems" processing multilevel classified data for the Intelligence Community. The existing methodology in private industry which might be feasible?
- Gaps which still need to be addressed?

III. Potential Contractors

- SDC
- MITRE
- Network Analysis Corporation
- Van Dyke Associates

ISSG/OS/CIA

Proposed Contract

R&D

Magnetic Media Control Using Technical Means

\$75K

Introduction:

A method is needed for detecting and preventing the unauthorized removal of all portable magnetic storage media from Intelligence Community facilities. The approach should be towards the development of a special type of magnetic media which has something in its composition which can be detected by sensors strategically placed at building exits. The detectable substance would not be removable, transparent to users and not impair the normal utilization of magnetic media. An alternate but less desirable solution would be the development of a device which can be attached to or recorded/written into magnetic media which can be detected by a sensor. The types of portable magnetic media include computer tapes, floppy disks, and cassettes. (U)

This is a current problem presently being addressed through management and administrative procedures neither of which properly addresses the problem. Increasing use of floppy disks in word processing systems and the new family of computer terminals will make the problem worse in the future. (U)

There are presently no known technical means of detecting the surreptitious removal of magnetic media from a controlled area. It appears that the solution to this problem requires new research efforts. (U)

Benefits:

In a sense, the prevention of unauthorized removal of magnetic media is more acute than the hardcopy document control problem. Many documents can be recorded onto a single floppy disk, cassette or magnetic tape. It is highly desirable from the Intelligence Community viewpoint to be able to prevent unauthorized removal of magnetic media. (U)



DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE
WASHINGTON, D.C. 20310

DAMI-AM

8 SEP 1981

SUBJECT: Recommendations for Employment of SECOM Funds Allocated to
CSS

Mr. Len Busic
Chairman,
Computer Security Subcommittee
SECOM, NFIB

1. The purpose of this letter is to comply with your request for a list of recommended projects to be funded by the Computer Security Subcommittee (CSS). It is our firm belief that CSS funds should be allocated only to those projects which will produce an identifiable, tangible product which will have broad Intelligence Community use. Further, applications supported by DIA and the military services should have universal value in military intelligence functions.
2. The most critical requirement facing the entire Intelligence Community (IC) today is the need to Redefine and Restructure the Security and Protection Attributes Which Support the Automated Handling and Communication of Intelligence Information. The multitude of classifications, codewords, caveats, control and dissemination restrictions present in the IC today have introduced great complexity into the processing and transmission of vital intelligence. The proliferation of intelligence systems and current planning for their future interface demands careful, judicious study of this problem and development of a workable, practical, hierarchic structure of standard security and protection attributes which can be implemented in the automated information handling world. I am currently working on the first draft of a much more detailed paper on this subject and will provide it to you when completed. In the meantime, I feel very strongly that the subcommittee should identify and support this project. Because there is already some interest in solution of this problem in the Data Standards Panel of the Intelligence Information Handling Committee, NFIB, it could be made a joint project with that group.
3. Next in priority is the need for a broad, definitive study of The Threats Against Intelligence Automation. Such a study might well be an outgrowth of the compilation activity which DIA RSE-4 now has underway

8 SEP 1981

DAMI-AM

SUBJECT: Recommendations for Employment of SECOM Funds Allocated to CSS

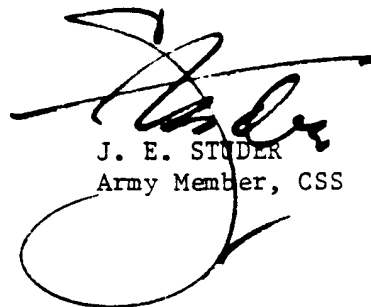
with the Military Intelligence Reserve unit in Texas. If content dictates, this product should be produced in two versions; one hopefully at the SECRET collateral level for broad, general dissemination, and a second at the TOP SECRET SCI level for more restricted IC dissemination. Command- and management-level attention and interest must be gained and maintained through provision of well-written expositions on the serious threats against automated systems.

4. As an ancillary to The Threats Against Intelligence Automation there should be produced, as a separate document if necessary, a serious, lay-man language Compromising Emanation Threat Study. Decision-authorities in Army and the other services are confronted on a daily basis with the requirement to approve or disapprove the design of automated systems at both the tactical and strategic levels which must incorporate protection against compromising emanations. The credibility of this EMSEC requirement is not now well established, except in the electronic engineer-oriented language of NACSEM 5100. There is a demand for a definitive, detailed, explanatory threat and countermeasure document which can be read, understood and applied by managerial personnel without the need for engineer interpretation. Production of this study should be a joint effort with the Subcommittee on Compromising Emanations (SCOCE).

5. There is also a strong requirement for an authoritative Automation Security Dictionary defining all the terms and criteria to be applied in clear, precise language. A precedent exists in United States Communications Security Board (USCSB 2-17) "Glossary of Communications Security and Emanations Security Terms," October 1974.

6. Lastly, a requirement exists for the development and promulgation of an IC guidance document on the application of Risk Analysis Criteria, Procedures, and Techniques for Automation and Communication Systems in the Intelligence Community.

7. I will be happy to elaborate on any of the above recommendations at your request.



J. E. STUDER
Army Member, CSS

Proposed Contract

COMPUTER NETWORK SECURITY

\$100K

I. Introduction

Of all the issues involving ADP security, network security is the most complex. This is because network security spans all facets of security. For example, physical security, personnel security, communications security, TEMPEST security, and computer software security are all important considerations of network security. The distributed nature of networks further complicates issues involving physical and communication security. All the problems and technical issues involved with the security of a single computer is present in a network and is essentially multiplied by the number of computers (i.e., network nodes) in the network. In particular, the issue of multilevel security is greatly complicated in a network.

The combination of the distributed nature of networks and packet switching technology (i.e., the multi-path distribution of packet composition/decomposition) makes total multilevel security a very difficult goal to achieve.

Computer network security issues can be divided up into two areas of concern:

- a. communications security
- b. nodal security

II. Proposed Contract

Amount - \$100K

- "Think piece," original study on security requirements for Network Architecture which would examine:
 - nodes
 - communication lines (Bus, fibre optics, etc.)
- This study should not be directly based on existing developments or biased by past efforts. However, contractors should be aware of past efforts in this area.

Questions to be addressed

- a. Centralized vs decentralized security?
- b. Type of security technology which would be most applicable in centralized systems or decentralized systems?

Should address

1. What capabilities should the networked system have to be secure from standard modes of security compromise, e.g., tapping, penetration, etc.? If encryption is broken what steps need be taken as envisioned by the contractor to eliminate or minimize damage to network?
2. How will the contractor ensure compartmentation of data when nodes are connected to a network which has different levels of classified data?

Givens

- Must conform to security requirements of multicompartemented mode (DCID 1/16 and OMB A-71)
 - multi-CPU's
 - hundred of users
 - multi-geographic locations
 - encryption systems
 - something that is practicable and doable now

Products

- Deliverables
 1. Security requirements (system, physical, procedural) for NODES.
 2. Security requirements for front-end processor (if centralized).
 3. Security requirements for communication links (Bus, fibre optics, etc.).

ISSG/OS/CIA



Department of Energy
Washington, D.C. 20545

Mr. Len T. Basic
Defense Intelligence Agency
Attn: RSE-4
Washington, DC 20301

SEP 17 1981

Dear Mr. Basic:

Enclosed for your review are three computer security projects proposed for funding by the Computer Security Subcommittee. These projects were selected following the discussion at the subcommittee meeting on September 15.

Additionally, I am enclosing a copy of the briefing material as you requested.

Please accept my appreciation for the courtesy and attention shown to Dave Bailey and Ed Springer of the Department of Energy Computer Security Technical Center. Bob Wingfield of my staff indicated that the session was of benefit to the Department of Energy and I trust it was of value to you and the subcommittee members as well.

Sincerely,

A handwritten signature in black ink, appearing to read "R.A.O'Brien", written over a large, stylized flourish.

Robert A. O'Brien
Chief, Operations Security Branch
Division of Security
Office of Safeguards and Security
Defense Programs

4 Enclosures

cc w/Proposed Projects:
Computer Security Subcommittee
Members

Computer Security Subcommittee
Proposed Project

Computer Security Technology Forecast

75 K

Objective: To prepare a baseline technological assessment of the protection of information in computer systems and computer networks. The assessment of the current state of the technology will be accompanied by a forecast outlining problems and possible solutions which will be encountered during the next 5 years. The assessment will be useful to security officers in selecting security controls for systems under their control. The assessment will also be useful in guiding the selection of research and development tasks to fill the gaps in current protection capabilities and in solving the new problems which arise. The assessment and forecast should be updated approximately once every 2 years.

Product: A report containing an assessment of the current state of protection technology and a forecast covering the next 5 years.

Computer Security Subcommittee
Proposed Project

Secure Operating Systems

100 K

Objective: Evaluate the Honeywell Secure Communications Processor (SCOMP) and demonstrate its utility as a secure network front end processor in a data base management application. A SCOMP system will be installed at Los Alamos for system evaluation and software development and will then be reinstated at another location such as Oak Ridge for prototype use as a data base front end for users with differing levels of clearance and need-to-know. The Department of Energy software would be adapted to an SCI application specified by the subcommittee and installed on an existing SCOMP system as directed by the subcommittee.

Product: An installed SCOMP demonstration system.

Computer Security Subcommittee
Proposed Project

Secure Office Workstation

125 K

Objective: Build a prototype workstation capable of providing need-to-know protection for information in the environment in which the information is normally handled. The workstation should not require extensive sanitization before it can be left unattended. TEMPEST will be considered in the system design, but will not be included in the prototype workstation.

Product: Implementation of a prototype workstation demonstrating the needed protection techniques.