Memorandum

~~SECRET~~

b3
b6
b7C
b7E

To : SAC, WASHINGTON METROPOLITAN FIELD OFFICE Date 9/16/88

From : SA [redacted] CI-7

Subject : UNSUBS;
UNAUTHORIZED USE OF GOVERNMENT COMPUTER SYSTEM IN LAWRENCE BERKELEY LABORATORY, BERKELEY, CALIFORNIA;
[redacted]
OO: WMFO

Pull 196-999*

This communication is classified ~~"Secret"~~ in its entirety.

This matter was originally opened in December, 1986 and has been investigated as a Fraud by Wire matter (196A-999). The case was closed on 2/23/88. Details as to why the case was closed are not included in the file. It is recommended that the investigation be reopened, to be investigated [redacted]

On 9/12/88, SA [redacted] WMFO, prior Case Agent in this matter, provided the writer with a communication he had received from CLIFFORD STOLL, who is very familiar with details of the penetration of the LAWRENCE BERKELEY LABORATORY (LBL) Computer System. The communication includes a letter STOLL received from an unnamed reporter in the Federal Republic of Germany (FRG), setting forth allegations that the suspect in the FBW investigation, [redacted] was assisted in his intrusion into the LBL computer system by another individual in the FRG, known as "Captain Hagbard". The reporter further alleges that "Hagbard" gave details of the entry to unnamed persons from the German Democratic Republic (GDR), for which he was paid 30,000 DM. The reporter states that HAGBARD then reported his GDR contact to the Landesverfassungsschutz in Hannover, FRG.

b3
b6
b7C
b7E

Several concerns remain unaddressed in this matter:

1. During the penetration of the LBL Computer System, operated by the US Department of Energy (DOE), and the related penetrations of other government computer systems, was any classified information stolen?

2. Is there a way to verify that [redacted] was assisted by "Captain Hagbard"? Can it be determined what information, if any, regarding the LBL intrusion that "Hagbard" passed on to the GDR?

3. Are there vulnerabilities in the security of the LBL Computer System that can be exploited by "Hackers"?

9/20/88 FKC

9/22/88

Searched [redacted]
Serialized
Indexed
Filed

b3
b6
b7C
b7E

PI unit 9/20/88
copy 1/17

~~SECRET~~

Memorandum

Charged out 12/6/93

To : SAC, WMFO Date 6/23/93

From : SA [redacted] CI-4

b3
b6
b7C
b7E

Subject: BULKY EVIDENCE PROJECT

Re SSA [redacted] memo dated 5/26/93.

A review has been conducted of [redacted] (converted from 196A-999), to determine whether 196A-999-1B-1 should be retained.

[redacted] was closed on 3/9/89. Prosecution was conducted in the Federal Republic of Germany (FRG). The evidence retained in this investigation consists of computer printouts of two hacking sessions. Per [redacted] LAWRENCE BERKELEY LABORATORY (LBL), where the hacking was monitored, maintained original records on all hacking sessions on floppy diskettes. The printouts in bulky storage were produced from records kept by and at LBL.

As these printouts are duplicate records which were produced for the use of the FBI and as the original records (the diskettes) were retained at LBL, it is recommended that the printouts (196A-999-1B-1) be destroyed

4-WMFO
(1-SSA [redacted]
(1-BULKY PROJECT)
(1- [redacted]
(1- CI-4)

[redacted]

b3
b6
b7C
b7E

[redacted]

Memorandum

~~SECRET~~

b3
b6
b7C
b7E

To : SAC, WMFO [redacted] Date 9/22/88

From SA [redacted] CI-7

Subject : UNSUBS;
UNAUTHORIZED USE OF GOVERNMENT COMPUTER SYSTEM IN LAWRENCE BERKELEY LABORATORY, BERKELEY, CALIFORNIA;
[redacted]
OO: WMFO

This communication is classified ~~"Secret"~~ in its entirety.

[redacted]

The attached communication was provided to the writer on 9/12/88 by SA [redacted] WMFO. The communication had been directed to SA [redacted] by CLIFFORD STOLL, formerly of LAWRENCE BERKELEY LABO LABORATORIES in connection with this investigation.

b6
b7C
b7E

~~SECRET~~
~~Classified by:~~ 8796
~~Declassify on:~~ OADR

[redacted]

[redacted]
SEARCHED [redacted]
SERIALIZED
SEP 2 3 1988
FBI — WASH. FIELD OFFICE
[redacted]

b3
b6
b7C
b7E

~~SECRET~~

** Thank you for choosing GEnie **

The Consumer Information Service
from General Electric
Copyright (C), 1988

b6
b7C

GEnie Logon at: 16:15 EDT on: 880811
Last Access at: 20:28 EDT on: 880807

$ PRIME TIME Rate in Effect ($35/hr) $

* Jonesboro, AR...See "New on GEnie" *

* Visit GEnie at Boston MacWorld *
8/11-8/13. See "New on GEnie".

* Graphics, Scanning and GIF *
"PHOTO" RTC, 7/12, 9PM EDT

* Send a dozen roses just because... *
$39.95 delivered. Type "LDROSES"

You have 1 LETTER WAITING.

GEnie TOP Page 1
GE Information Services

1. About GEnie...	2. New on GEnie
3. GE Mail	4. LiveWire CB
5. Computing	6. Travel
7. Finance	8. Shopping
9. News	10. Games
11. Professional	12. Leisure
13. Reference	14. Logoff

Enter #, or <H>elp?read

Item 3679407 88/08/11 12:41

From: CLIFF-STOLL Cliff Stoll

To: [redacted] [redacted]

b6
b7C

cc: CLIFF-STOLL Cliff Stoll

Sub: letter from reporter in german

Received: from DBSTU1 by Lbl.Bitnet via BITNET ;
Thu, 4 Aug 88 12:33:21 PDT for CLIFF@LBL;
Thu, 4 Aug 88 12:33 PST
Message-Id: <880804123321.29a0015c@Csa2.LBL.Gov>
Date: 4 August 1988, 21:30:38 MEZ
To: CLIFF at LBL
Dear Cliff,
I've got news, so let me start right away.
There is espionage involved in the LBL Hack und there is probably a lead to Pittsburgh.
In 1985 Captain Hagbard and others penetrated a lot of sites which do research in high physics energy, among them Fermilab, Stanford. Vancouver,

Heidelberg Juelich (Germany), CERN and a few others. I wrote a story about it, [redacted] wrote a letter to me. b6
There were also other hackers involved. [redacted] told me of Frimp. Zombie and b7C
Nighthawk. There may also have been Pengo and Fernando from Berlin.
(Both names may become important.)
At the beginning of 1986 (?) Hagbard was contacted by someone who offered him money for successful log-ins. Hagbard said that he later on learned that the money came fron East Germany via a few top-programmers in Berlin who don't know yet that their identities will be revealed soon. So this is top secret information at the moment.
All in all Hagbard got 30000 DM in 1986. As Hagbard's psyche was not very stable and as he was hacking all night long his new contact offered cocaine which he took in 1986. Thus he was hooked.
As Hagbard also had contact to other hackers, among them Pengo, he was asked whether they also needed money. Pengo also took money. (Pengo has always had good contact to everybody else, the Chaos Computer Club, for example. He has also been running a hobby mailbox.)
At a certain time Hagbard was asked to go to East-Berlin and have a talk with an officer of the East German secret service, the Staatssicherheitsdienst. But Hagbard refused to go there. Instead they got log-ins, among them. all successful log-ins connected to LBL.
Only when you started to have [redacted] prosecuted in Germany you put an end b6
to it. There were no more log-ins to sell after 1986 Hagbard went into a b7C
treatment to get off the cocaine and his psychic inst ability,
In May I told [redacted] where he could find Hagbard. [redacted] has done a lot of investigations himself and is hoping that he can help to set a trap for the programmers in Berlin.
In July, when I was away, Hagbard and Pengo went to the Verfassungschutz in Germany. Pengo to the Landesverfassungsschutz in Hamburg and Hagbard to the Landesverfassungsschutz in Hannover. There they revealed the contact with East-Berlin. They were told not to be prosecuted and be able to make a little of money by informing the press, or writing.
Hagbard is in debts. He goes to school at the moment so that he can get a decent job afterwards. He hopes to earn 10000 DM one way or the other. That will not be very easy. I can probably help him a little bit.
He hopes to earn money this way because he can't go work as long as he is at school. I will contact him on 11 August again in Hannover. I hope we will meet, Pengo has vanished.
Secret Services in Germany: Bundesnachrichtendienst (BND) - works abroad, tries to get information from agents outside the country, Probably very much like the CIA in this field.
Militaerischer Abschirmdienst: deals with spying and sabotage inside Germany Is only concerned with the military.
Verfassungsschutz: should try to defend our constitution against "enemies" inside the country. Is politically orientated, is looking for communists, anarchists and terrorists. In fact is also involved, when there are computer crimes.
In the NASA-Hack the Bundesverfassungsschutz was contacted by Steffen Wernery from the Chaos Computer Club before the Hack was published. He hoped that he could make an arrangement so that he and others would not be searched or prosecuted. (I don't know if they really promised something.) [redacted] Within hours the NASA- b3
Hack-Material went tothe [redacted] via Bundesverfassungsschutz. b6
"Bund.." means "federal", "Land.." means "state". b7C
The Verfassungschutz quite often does not inform [redacted] b7D
for example. b7E
Suggestion: Find out whether a [redacted] log-in fits the [redacted] -log-in in the very same order. [redacted] is hardly a hacker. He would have to follow instructions on paper. Hagbard doesn't know. Hagbard would know him because he (Hagbard) really took part in the hack with [redacted]

~~SECRET~~

I would like to have information on: Zombie and Fernando (Perhaps [redacted] will help if you ask him.) b6 b7C
Who asked whether he could publish your article in Germany? Have you ever been contacted by a [redacted]-reporter named [redacted] The new Hacker Bible will probably be released in September. There will be a Hacker-book on the market by the Chaos Club by the end of August.
So long, [redacted]

=END=

Press <RETURN>?

~~SECRET~~

(I-7

~~SECRET~~

INBOX.10 (#984)

TEXT:

VZCZCSF0001

RR HQ WF

DE SF #0001 2860052

ZNY SSSSS

R 110000Z OCT 88

FM FBI SAN FRANCISCO [redacted](P)(ORA 3)

TO DIRECTOR FBI /ROUTINE/

FBI WMFO [redacted](CI-7)/ROUTINE/

BT

~~S E C R E T~~

CITE: //3790//

SUBJECT: UNSUBS; UNAUTHORIZED USE OF GOVERNMENT COMPUTER SYSTEM IN LAWRENCE BERKELEY LABORATORY, BERKELEY, CALIFORNIA; [redacted]

OO: WMFO

ALL MARKINGS, NOTATIONS AND ITEMS OF INFORMATION CONTAINED IN THIS COMMUNICATION ARE CLASSIFIED "~~SECRET~~" UNLESS OTHERWISE NOTED.

RE: WMFO TELETYPE TO FBIHQ AND SAN FRANCISCO DATED SEPTEMBER 27, 1988.

CONTACT HAS BEEN MADE WITH MR. ROY KERTH, ASSOCIATE

b3
b6
b7C
b7E

b3
b6
b7C
b7E

[redacted]

OCT 11 11 '0 8H '88

[redacted]

LABORATORY DIRECTOR FOR GENERAL SCIENCES, LAWRENCE BERKELEY LABORATORY (LBL), BERKELEY, CALIFORNIA, TELEPHONE (415) 486-6661, IN AN EFFORT TO RETRIEVE ALL ORIGINAL PRINT-OUTS FROM HACKING SESSIONS OF THE LBL INTRUDER. KERTH ADVISED THAT HE WAS THE HEAD OF THE COMPUTING DIVISION AT LBL AT THE TIME OF THE HACKING INCIDENT, WHICH WAS HANDLED WITHIN LBL BY DR. CLIFFORD STOHL. STOHL NO LONGER WORKS FOR LBL AND ALL INFORMATION PERTAINING TO THE LBL HACKER HAS BEEN PLACED IN STORAGE. HE WILL REVIEW THIS INFORMATION BUT BELIEVES THAT ALL ORIGINAL PRINT-OUTS HAVE ALREADY BEEN PROVIDED BY STOHL TO THE FBI. FURTHER, KERTH STATED THAT HE WAS NOT AWARE OF ANY OBVIOUSLY CLASSIFIED INFORMATION THAT THE HACKER GAINED ACCESS TO NOR HAD STOHL GIVEN HIM ANY INFORMATION TO THE CONTRARY. KERTH STATED THAT HE WOULD BE OUT OF TOWN FOR APPROXIMATELY ONE WEEK BUT THAT HE WOULD THEN REVIEW ALL MATERIAL STILL IN THE POSSESSION OF LBL PERTAINING TO CAPTIONED MATTER. SAN FRANCISCO WILL ADVISE WMFO OF THE OUTCOME OF THIS REVIEW.

C (G-3); B (DADR)

BT

#0001

NNNN

b6
b7C

~~SECRET~~

READ INBOX TEXT
INBOX HAS 2 DOCUMENTS
FORMS.TEXT HAS 1 DOCUMENT

INBOX.1 (#2597)

TEXT:

VZCZCSF0019

PP HQ WMFO

DE SF #0019 3512222

ZNY SSSSS

P 162158Z DEC 88

FM SAN FRANCISCO [redacted](P)(ORA-3)

b3
b7E

~~SECRET~~

TO DIRECTOR/PRIORITY/

FBI WMFO [redacted](CI-7)/PRIORITY/

BT

~~S E C R E~~ T

CITE: //3790//

SUBJECT: UNSUBS; UNAUTHORIZED USE OF GOVERNMENT COMPUTER SYSTEM IN LAWRENCE BERKELEY LABORATORY, BERKELEY, CALIFORNIA; [redacted]

b3
b6 per FBI, DOE
b7C
b7E

OO: WMFO

THIS COMMUNICATION IS CLASSIFIED ~~SECRET~~ IN ITS ENTIRETY.

RE WMFO TELETYPE TO FBIHQ AND SAN FRANCISCO DATED 9/27/88 AND SAN FRANCISCO TELETYPE TO FBIHQ DATED 10/11/88.

CONTINUOUS CONTACT WITH MR. ROY KERTH, ASSOCIATE LABORATORY DIRECTOR FOR GENERAL SCIENCES, LAWRENCE BERKELEY LABORATOR (LBL), BERKELEY, CALIFORNIA, TELEPHONE [redacted] HAS

PAGE TWO DE SF 0019 S ~~E C R E T~~

DETERMINED THAT THERE ARE NO PRINTOUTS STILL IN THE POSSESSION OF LBL THAT CONTAINS SUBSTANTIVE INFORMATION THAT HAVE NOT BEEN PREVIOUSLY PROVIDED TO THE FBI. THESE PERTINENT PRINTOUTS HAVE BEEN PREVIOUSLY FORWARDED TO ALEXANDRIA DIVISION (ATTENTION: SA [redacted] KERTH ADVISED THAT THEY STILL DO HAVE ALL OF THE DATA REGARDING THE HACKING SESSIONS OF THE LBL INTRUDER IN COMPUTERIZED FORM BUT THAT THIS DATA CONSISTS OF APPROXIMATELY TWO THOUSAND 360K FLOPPY DISKS. THE TOTAL SIZE OF THE COMPUTERIZED DATA, WHICH HAS BEEN TRANSFERRED TO A DISK PACK, IS APPROXIMATELY 720 MILLION CHARACTERS IF KERTH'S RECOLLECTION OF THE NUMBER OF FLOPPY DISKS IS CORRECT. HE CHARACTERIZED THE DATA AS BEING "GIGANTIC" IN SIZE AND REITERATED THAT DR. CLIFFORD STOHL HAD REVIEWED ALL OF THE HACKER'S ACTIVITIES ON A DAILY BASIS AT THE TIME THEY WERE OCCURRING AND ONLY PRINTED OUT THOSE ACTIVITIES THAT HE FELT WERE SENSITIVE IN NATURE. DUE TO THE EXTREMELY LARGE VOLUME OF DATA, STOHL DID NOT PRINT OUT THE ENTIRE CONTENTS OF THE COMPUTERIZED FILES, AND LBL WAS NOT DESIROUS OF DOING SO AT THIS TIME FOR THE FBI. AS A POSSIBLE ALTERNATIVE, KERTH AGREED TO PUT ALL OF THE 720 MEGABYTES OF DATA ONTO A MAG TAPE TO FACILITATE SENDING IT TO WMFO, PROVIDING THAT

b6
b7C

LBL IS ADVISED OF THE DESIRED FORMAT FOR THE DATA. OF COURSE, THE DATA COULD ONLY BE READ BY A COMPUTER WITH A TAPE DRIVE.

KERTH AGAIN ADVISED THAT NEITHER HE NOR STOHL WERE AWARE OF ANY CLASSIFIED INFORMATION ACCESSED BY THE HACKER DURING THE ENTIRE TIME THAT HE WAS GOING THROUGH THE LBL COMPUTERS AND ACCESSING OTHER SYSTEMS. TO THE CONTRARY, ALL SYSTEMS ACCESSED WERE NOTIFIED BY STOHL OR OTHER AGENCIES AT THE TIME OF THE INTRUSIONS AND THESE SYSTEMS WERE DETERMINED TO BE UNCLASSIFIED. THERE WERE ATTEMPTS TO GAIN ACCESS TO CLASSIFIED SYSTEMS BUT ALL WERE UNSUCCESSFUL. IN VIEW OF THE ABOVE, WHICH SAN FRANCISCO HAS BEEN AWARE OF AND MADE KNOWN TO OTHERS OVER THE LONG TIME THAT THIS MATTER HAS BEEN OF INTEREST TO ALEXANDRIA AND WMFO UNDER VARIOUS CLASSIFICATIONS, SAN FRANCISCO IS AT A LOSS TO SEE THE NEXUS BETWEEN CAPTIONED MATTER AND THE UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION.

LEAD. WMFO. AT WASHINGTON, D.C. WILL ADVISE SAN FRANCISCO IF THE COMPUTERIZED DATA IS DESIRED ON A MAGNETIC TAPE, AND IF SO, THE FORMAT TO BE USED BY LBL IN CREATING THE TAPE.

BT

#0019

NNNN

~~SECRET~~

MEMORANDUM

b3
b6
b7C
b7E

TO: SAC, WMFO [redacted] (P) 1/6/89

FM: SA [redacted] (CI-7)

SUB: UNSUB;
UNAUTHORIZED USE OF GOVERNMENT COMPUTER SYSTEM IN
LAWRENCE BERKELEY LABORATORY, BERKELEY, CALIFORNIA;
[redacted]
OO:WMFO

THIS COMMUNICATION IS CLASSIFIED "~~SECRET~~" IN ITS ENTIRETY.

[redacted] b7E

Instant investigation concerns penetrations of numerous government computer systems through unauthorized use of the government computer system at Lawrence Berkeley Laboratory (LBL), Berkeley, California. The penetrations occurred over an extended period of time and were monitored by LBL officials. They were traced back to resident of the Federal Republic of Germany (FRG) residing in Hannover, FRG, a [redacted]

The objective of instant investigation is to determine whether any classified information was accessed during the penetrations. Secondary issues were determination of what, if any, information was passed on to the GDR and identification of vulnerabilities in the LBL and other government computer systems.

[redacted]

~~CLASSIFIED BY: 8796~~
~~DECLASSIFY ON: OADR~~

b3
b6
b7C
b7E

2-WMFO

[redacted]
(2)

PI EXTENSION DATED _____
TICKLER SET FOR 4/7/89
SECRETARY [redacted]
SUPERVISOR _____

[redacted]
SEARCHED [redacted] INDE
SERIALIZE [redacted] LED
JAN 06 1989
[redacted] FIELD OFFICE

~~SECRET~~

[redacted] b3 b7E

Since this investigation was opened, officials at LBL have been recontacted by the FBI. LBL officials advised that all installations penetrated were notified at the time. All systems accessed were unclassified. Although attempts were made to access classified systems, all attempts were unsuccessful. LBL has offered to provide to WMFO computerized data regarding all hacking sessions (approximately 720 megabytes of data).

Additionally, the writer has contacted Special Agent [redacted] Assistant Chief of the Computer Crime Division, Air Force Office of Special Investigations (OSI), who has worked with the former FBI case agent throughout the course of this investigation. [redacted] stated that he too, was aware of no classified information having been accessed. [redacted] described his concern as "aggregation", explaining that a threat to security would arise in a case such as this from the sheer number of penetrations made. Even though no classified information was obtained, enough non-classified information could be obtained as to be damaging when put together. b6 per AFOSI b7C per AFOSI

[redacted] stated that the methods used by the hacker were basic. Rather than gaining access through sophisticated techniques, he succeeded through sheer persistence. He likened it to walking down a long corridor - if enough doors are tried, eventually one will be found to be unlocked.

[redacted] stated that he has contacted all Air Force installations that were penetrated and had them prepare damage assessments. He recommended that the FBI do this for all other government computer systems accessed through LBL.

Accordingly, the following is recommended. LBL should be requested to provide the aforementioned data which would be maintained at WMFO for evidentiary purposes. Facilities which maintain government computer systems penetrated by the LBL hacker should be requested to prepare a damage assessment, in an effort to identify vulnerabilities the hacker exploited and thus prevent future similar penetrations. Finally, Legat Bonn should be contacted to request that FRG authorities interview [redacted] to determine if any information was passed on to the GDR.

A 90 day extension is hereby requested to accomplish the foregoing. b6 b7C

An extension is being granted to establish factual investigative considerations.

ASAC [redacted]

SAC

Memorandum

To : SAC, WMFO Date 6/23/93

From : SA [redacted] CI-4

Subject: BULKY EVIDENCE PROJECT

Re SSA [redacted] memo dated 5/26/93.

A review has been conducted of [redacted] (converted from 196A-999), to determine whether 196A-999-1B-1 should be retained. b3 b6 b7C b7E

[redacted] was closed on 3/9/89. Prosecution was conducted in the Federal Republic of Germany (FRG). The evidence retained in this investigation consists of computer printouts of two hacking sessions. Per [redacted] LAWRENCE BERKELEY LABORATORY (LBL), where the hacking was monitored, maintained original records on all hacking sessions on floppy diskettes. The printouts in bulky storage were produced from records kept by and at LBL.

As these printouts are duplicate records which were produced for the use of the FBI and as the original records (the diskettes) were retained at LBL, it is recommended that the printouts (196A-999-1B-1) be destroyed

4-WMFO
(1-SSA [redacted]
(1-BULKY PROJECT)
(1- [redacted]
(1- CI-4)

[redacted]

b3 b6 b7C b7E

[redacted]

SERIALIZED

JUN 2 8 1993

FBI — WASH. METRO FIE

[redacted]

The following investigative steps are suggested to address the aforementioned issues:

1. A detailed interview should be conducted of LBL officials to determine specifically how the LBL system was penetrated, and how other US Government computer systems were penetrated through the LBL penetration.

2. All evidence maintained through LBL, including lists of US Government documents accessed, should be obtained.

3. A determination must be made of whether the "hacker" obtained any classified documents.

4. Through Legat, Bonn, the Landesverfassungsschutz in Hannover, FRG, should be contacted in an effort to determine whether "Captain Hagbard" contacted them, as detailed above. If such a contact occurred, details of the contact should be obtained.

5. If it is determined that no classified documents were obtained in the LBL intrusion, FBI investigation in this matter should be closed. Details of the intrusion can then be passed on to another US Government agency [redacted] which is better equipped to investigate intrusions of sensitive US Government computer systems, determine whether vulnerabilities in the systems penetrated still exist and, if so, correct same.

~~Classified by: 8796~~
~~Declassify on: OADR~~

b3
b6
b7C
b7E

1-WMFO
[redacted]