[redacted] b6 b7C

~~SECRET~~/NOFORN

April 15, 1999

Director Freeh:

RE: (U) "MOONLIGHT MAZE"

RECENT DEVELOPMENTS

(U) On 4/2/1999, the Moonlight Maze Coordination Group (MMCG) deployed a team to Moscow, Russia, [redacted] The team consisted of the case agent from FBI Baltimore, a language specialist from FBI San Francisco, a supervisory special agent from FBIHQ, a representative from NASA and two representatives from Air Force Office of Special Investigations,.

(U) The MMCG team discussed the details of the intrusions previously identified by the MMCG [redacted] The MMCG briefed several [redacted] investigators on the details of the case and requested assistance to determine the origin of the intrusions. The team discussed connection data from five computer intrusions involving systems from the Army, Navy, NASA, and a commercial Internet Service Provider (ISP). b6 b7C b7D b7E

[redacted]

(U) [redacted] assigned a team of investigators to each ISP. The MMCG team traveled with [redacted] The two other [redacted] teams determined that [redacted] had gone bankrupt and merged [redacted]

1 [redacted] b6 b7C
1 - Briefing Book

HMH:dhg
(18)

~~Derived From: Multiple Sources~~
~~Declassify On: X1~~

~~SECRET~~/NOFORN

288-4-6856-98 BB

[redacted] b6 b7C

[redacted]

Pls serialize, thks BB

BBW BB

[redacted] b7D

(U) [redacted] provided the team with a memorandum, of which a transcribed copy is attached to this note, which explained that they would present the evidence to the Prosecutor's Office for a decision about opening a criminal case.

(U) The MMCG returned from Moscow on 4/10/1999. On 4/15/1999, ALAT [redacted] contacted [redacted] to obtain an update on their investigation. [redacted] b6 b7C b7D

[redacted] During the week of [redacted] have advised the Legat that they will provide him with the intruder's identity after they brief [redacted] replacement and obtain his approval.

(U) (~~S~~/NF) Deputy Assistant Director [redacted] is scheduled to meet with the NIPC's Interagency Senior Coordinating Group on Monday 4/19/1999, to update them on the MMCG's activities and obtain information from the intelligence community about any recent intelligence collection concerning this matter.

BACKGROUND

(U) "MOONLIGHT MAZE" is the code name for a number of investigations of intrusions into various military, governmental, educational and other computer systems in the United States, United Kingdom, Canada, Brazil and Germany. Field investigations are being conducted by the Albuquerque, Baltimore, Cincinnati, Jackson, New Orleans, and Springfield Divisions as Offices of Origin and the Atlanta, Boston, Charlotte, Detroit, Indianapolis, Jacksonville, Knoxville, Mobile, New York, Pittsburgh, Salt Lake City, San Francisco, and Washington Field Divisions as Lead Offices. The National Infrastructure Protection Center

(NIPC) is coordinating these investigations with investigators from the Air Force Office of Special Investigations, Army, Naval Criminal Investigative Service, Defense Criminal Investigative Service, National Aeronautics Space Administration, Department Of Energy, as well as [redacted] The NIPC is also coordinating internationally [redacted] The NIPC has ensured that Legats London, Moscow and Ottawa are advised of the investigation in their respective territory. b1 b7D

(U) These investigations were initiated when intrusions were discovered at Wright Patterson Air Force Base (WPAFB), Ohio, and the Army Research Laboratory (ARL), Maryland, and other unclassified military systems, as well as various governmental, commercial and educational computer systems in the United States.

(U) The intruder(s) into WPAFB, went through the University of Cincinnati, Cincinnati, Ohio [redacted] A pen register and trap and trace [redacted] b3 b7E

(U) Intrusions into DOE systems include intrusion activity at Los Alamos National Laboratory (LANL), Sandia National Laboratory (SNL), Lawrence Livermore National Laboratory (LLNL), and Brookhaven National Laboratory. DOE's Computer Incident Advisory Capability (CIAC) has been active in this incident. Activity on DOE systems has been confined to unclassified networks.

[redacted] b7D b7E

[redacted]

b3
b6
b7C
b7E

~~(S/NF)~~ On 12/12/1998, the Metropolitan Police in London, England, installed a new

[redacted]

b1
(S)

[redacted] (S) b1

(U) On 1/8/1999, Deputy Assistant Director (DAD) Michael A. Vatis and Section Chief Kenneth M. Geide briefed Dr. Hamre, updating him regarding captioned matter.

[redacted] (S)

(U) As of 1/13/1999, the intruder(s) continued to attempt, and in some instance succeeded, in intruding into Department of Defense (DOD) computer systems. The intruder(s) continues to mainly operate Monday through Friday during European business hours. Notably, the intruder(s) was active on 12/25/1998, a weekday, but was not active on 1/7-8/1999, both weekdays and Orthodox Christmas holidays in Russia.

~~(S/NF)~~ On 1/13/1999, DAD Vatis hosted a meeting with senior representatives from the agencies involved in captioned matter (as victims and/or investigators). The principals who attended the meeting were:

Major General John Campbell, Commander, JTF-CND, DOD
Ms. Sheila Dryden, Principle Director for Security and Information Operations, Office of the Secretary of Defense, DOD

[redacted] (S)

[redacted] (S) b1

Mr. Edward Curran, Director, Office of Counterintelligence, DOE
Ms. Roberta Gross, Inspector General, NASA

~~(S/NF)~~ The purpose of this meeting was to brief the status of captioned matter and to discuss next steps. The attendees were advised:

- that the NIPC is coordinating the investigation and analysis of "MOONLIGHT MAZE" with full participation by DOD, [redacted] DOE, NASA, Department of Justice (S) b1
- that numerous FBI field offices are investigating this matter, collecting evidence (primarily transnational data) from the ever expanding number of victims
- that the NIPC Cyber Emergency Support Team (CEST) is providing technical assistance to victim sites and field offices, and is conducting the technical analysis of the transnational logs obtained from the victim sites

[redacted] (S)

- that the NIPC is working with Army and Navy to determine the feasibility and desirability for setting up an electronic "honeypot" to assist in attributing the intrusions
- that the NIPC was considering making contact [redacted] to request assistance in resolving this investigation b7D

~~(S/NF)~~ DAD Vatis then sought the views of the agencies on the next steps in order to reach a collective decision, where possible, and to determine where any disagreements lie. The attendees responded positively to the status briefing. There was unanimity among the attendees

[redacted] (S) b1

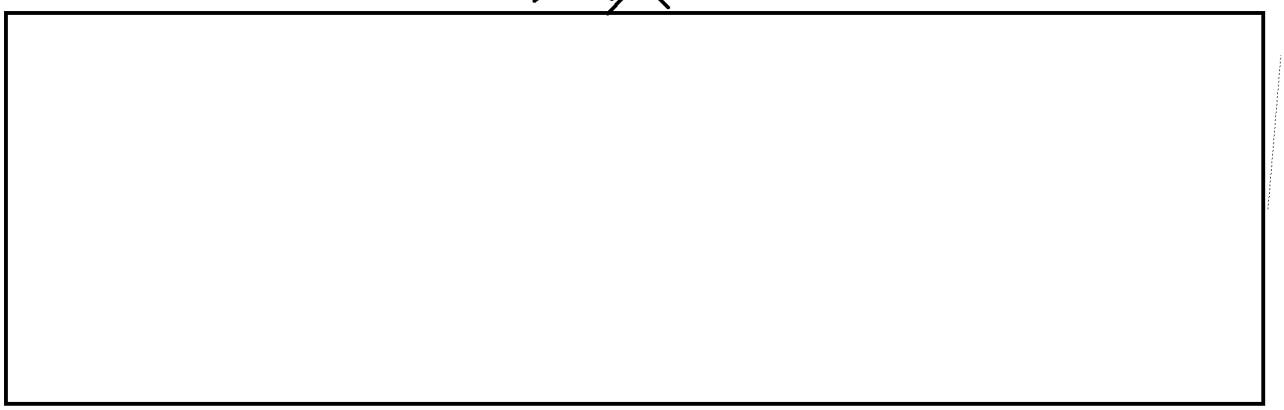
[redacted] The attendees agreed that the FBI should continue to aggressively

pursue the criminal investigation of captioned matter, especially collecting and analyzing computer log information obtained by court order from the numerous victims revealing the intruder's activities, methodologies and targets. The attendees also agreed that the NIPC should coordinate the development of a passive "honeypot(s)" at Army and/or Navy victim sites that may assist in providing identifying information about the intruder (his Internet Protocol address, the operating system running on his machine, etc.). The group discussed the technical feasibility and conditions for creating a second "honeypot(s)" containing a "beacon" file. This technique involves planting computer source code in a file that executes when retrieved by the intruder, performing search activities in the intruder's computer and sending the results of the search to the investigators. The group agreed that more information is required before this investigative step can be taken. The NIPC will coordinate the development and execution of such a step, as appropriate.

(U) On 1/16/1999, investigation determined that an account belonging to [redacted] b6 b7C b7E [redacted] During an interview of [redacted] by his supervisor, on 1/22/1999, he admitted to illicitly downloading files from [redacted] using his wife's account on 1/15/1999 [redacted] stated that he did not know that [redacted] was being monitored when he signed onto the "it" account to obtain a copy of the hacker tools. [redacted] only had the IP address of where the tools were located. Once signed onto the [redacted] system, [redacted] followed the intruder's path, in an effort to locate the tools [redacted] unable to locate the tools in a specific directory, subsequently began searching the intruder's directories for files and downloaded three files to his machine in Ellicott City, Maryland. FBI Baltimore executed a search warrant at [redacted] residence, seizing five computers, two of which were owned by [redacted] employer. The systems are being examined by the Computer Analysis and Response Team (CART), Laboratory Division.

(U) On 1/18/1999, the NIPC was notified from the victimized [redacted] site in London b7E regarding a compromise at the Brookhaven National Laboratory, located in Long Island, New York. Also compromised the same day was an Army network located in Vicksburg, Mississippi. The compromise was of a super computing center containing Cray and IBM supercomputers. The Army CID is determining the damage to the supercomputers.

[redacted] b7D



b1 (S)

(U) On 2/25/1999, the FBI briefed captioned matter to key staff members of the House Permanent Select Committee for Intelligence and the Senate Select Committee for Intelligence. Representatives from [redacted] DOD's Joint Task Force - Computer Network Defense (JTF-CND) also participated in these briefings. b1

(S)

(U) [redacted] requested to be told, "without compromising the investigation, what is going on?" [redacted] asked "Is Weldon exaggerating? How do the recent attacks differ from what has happened so far (Weldon says the 'electronic Pearl Harbor' of which Hamre spoke last year has gone from if to when and the when is today)?" [redacted] would like to speak to somebody at the Pentagon, "on the record about this." b6 b7C

(U) On 2/25/1999, and again on 2/26/1999, [redacted] attempted to telephonically contact Douglas G. Perritt, Deputy Director, NIPC, in an effort to obtain comment regarding comments attributed to Representative Weldon. Perritt has not responded to [redacted] telephone calls.

(U) On 3/1/1999, Defense Week published an article "Hamre to Hill: 'We're in a Cyberwar'," a copy of which is attached, concerning Dr. Hamre's testimony. The article does not mention the Russian connection, but otherwise captures the gist of Dr. Hamre's testimony.

b1 (S)

b1

(S)

(U) On 3/4/1999, ABC Nightly News and the ABCNEWS.com web site aired a story "Target Pentagon: Cyber-Attack Mounted Through Russia." This report apparently stems from the earlier report, on 3/1/1999, by Defense Week, concerning Deputy Secretary of Defense John Hamre's testimony on "MOONLIGHT MAZE" before the House National Security Committee and the Research and Development Sub-Committee. Other related articles which have also been posted on the web are: "US Currently Under Cyber Attack?" posted by AntiOnline on 3/4/1999; "Pentagon and Hackers in 'Cyberwar'," posted by MSNBC on 3/4/1999; "Pentagon hackers traced to Russia," posted by CNNInteractive on 3/5/1999; "Pentagon 'at war' with computer hackers," posted by CNNInteractive on 3/5/1999; and "Electronic Desert Storm," posted by AntiOnline on 3/5/1999. The New York Times and New York Times Online also posted two articles, "Computer Hackers are Stopped," and "Hacker 'Attacks' On Pentagon May Be More Like Espionage," posted 3/5/1999, and 3/8/1999, respectively, regarding this investigation. A copy of these articles are attached to this note. Reports of information attributed to interviews of Representative Curt Weldon, Chairman, House National Security Committee, and Deputy Secretary of Defense Hamre, have also been aired periodically on CNN Headline News since 3/5/1999. The ABC story reported that "the Pentagon's military computer systems are being subjected too ongoing, sophisticated and organized cyber-attacks. And unlike in past attacks by teenage hackers, officials believe the latest series of strikes at defense networks may be a concerted and coordinated effort coming from abroad." Until Friday, the Defense Department had not publicly acknowledged this latest cyber-war. But in an interview with ABCNEWS, Deputy Secretary of Defense Hamre, who oversees all Pentagon computer security matters, confirmed the attacks have occurred over the last several months and called them 'a major concern.' The ABCNEWS article noted that "this is an ongoing law enforcement and intelligence matter. Officials believe some of the most sophisticated attacks are coming from Russia. Federal investigators are detecting probes and attacks on U.S. military research and technology systems -- including the nuclear weapons laboratories run by the Department of Energy."

(U) The 3/8/1999, New York Times article stated that "In recent weeks, Government officials involved with defense have described a new kind of 'cyberwar' being fought on the

Internet, with unknown hackers unleashing relentless assaults on military computers." This article noted that ". . . some computer security experts stress that while the hacker activity that the House heard about is a potential threat, calling it an attack could be an overstatement." This article also noted that "The Pentagon has said that, as is the case with the vast majority of hacking attempts, the recent probes did not result in the penetration of any computers storing sensitive information." Representative Weldon is quoted as stating "We know of banks who've had their fire walls broken and money transferred out, and they're not going to talk about it." Representative Weldon noted that the private sector needs to cooperate more with the government "in this area."

(U) In light of the press coverage, the consensus among the participating agencies was that we had no real choice but to go directly to [redacted] with a request for assistance to investigate selected intrusion activity captured during this investigation. The NIPC, working with the Department of Justice and other Federal Investigative Agencies, [redacted] The MMCG, described below, prepared an operations plan, which was subsequently approved. [redacted] b7D

[redacted] b1 (S)

(U) In spite of the ABC story on 3/4/1999, intrusions continued. On 3/5/1999, between 0228 and 0906 Eastern Standard Time (EST), there were two intrusions into LLNL, one intrusion into Lawrence Berkeley Laboratory (LBL), and one intrusion into Argonne National Laboratory passing through Jefferson County Library [redacted] b7E

[redacted] These intrusions are consistent with other intrusions associated with "MOONLIGHT MAZE." These intrusions are significant in that they occurred well after the national press releases regarding the "MOONLIGHT MAZE." b7E

(U) On 3/1/1999, the MMCG was established to strengthen the focus and assessment of the intrusion activities related to this investigation. The MMCG is composed of forty personnel from the following law enforcement, intelligence and Computer Emergency Response Teams (CERT) organizations: [redacted] DISA, Department of Justice (DOJ), Department of Energy (S) b1
(DOE), National Aeronautical and Space Administration (NASA), Air Force Office of Special Investigations (AFOSI), Naval Criminal Investigative Service (NCIS), Defense Criminal Investigative Service (DCIS), US Army Criminal Investigative Division (USACID), US Army Military Intelligence (USAMI), Defense Intelligence Agency (DIA), [redacted] (S)
[redacted] Air Force Information Warfare Center (AFIWC), Navy CERT, Army CERT, FBI Baltimore, Eurasian Section, National Security Division and the NIPC.

[redacted] b7D

(U) On 4/2/1999, a team from the MMCG deployed to Moscow, Russia to work [redacted] this matter. The team returned to Washington, D.C. on 4/10/1999. Prior to departure, the team received security briefings from FBIHQ security personnel and NSD Russian Program Managers, [redacted] (S) b1
Concurrence regarding the investigative teams travel have been obtained from the FBI International Relations Branch (IRB), Legat Moscow and U.S. Ambassador Collins.

(U) I will keep you apprised of significant developments regarding this matter.

[redacted] b6 b7C

~~NOT APPROPRIATE FOR DISSEMINATION TO THE PUBLIC~~

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu