**U.S. Department of Justice**

Federal Bureau of Investigation

In Reply, Please Refer to
File No. 288-CI-68562

550 Main Street, Room 9000
Cincinnati, Ohio 45202
October 6, 1998

DCFL
500 Duncan Avenue, Room 1009
Bolling AFB, DC 20332-6000

SUBJECT: Request for Computer Forensic Media Analysis

1. **COMPLETE SUBJECT TITLE BLOCK INFORMATION:** Wright-Patterson AFB, Ohio, June 1, 1998, Unauthorized access of governmental and civilian computer systems. Violation of Title 18, USC, Section 1030; Fraud and Related Activity in Connection with Computers.

2. **PRIORITY:** This is a Category 1 intrusion on several military systems. This joint investigation is considered one of the highest priority cases within the FBI and AFOSI realms. The analysis of the enclosed tapes is requested immediately by the Department of Justice, Department of Defense, the Federal Bureau of Investigation and AFOSI.

3. **CLASSIFICATION:** This investigation is classified, however the evidence is not.

4. **CO-CASE AGENTS:** SA [redacted], FBI, Cincinnati, Ohio, commercial [redacted] SA [redacted] AFOSI Det 101, WPAFB, Ohio, DSN [redacted] commercial: [redacted] AFOSI Det 101, WPAFB, Ohio, DSN [redacted] commercial: [redacted] b6 b7C

5. **SYNOPSIS OF THE CASE:** On or about June 1, 1998, WPAFB began detecting intrusions at several Air Force Institute of Technology and Air Force Research Laboratory machines. [redacted] b7E The intrusions originally were detected coming through the University of Cincinnati; however, additional intrusions have been detected at several education sites and numerous Internet Service Providers. The unidentified intruder uses authorized accounts and valid passwords to gain access into the victim systems and then FTP's files, telnets to another system or pop roots. To date, investigative agencies have not been able to detect any sniffer, rootkit or trojanized programming.

288-CI-68562-26

Searched
Serialized
Indexed
Filed

1 - Addressee
1 - Cincinnati (288-CI-68562)
BB:bb (2)

280BB01, OTH

6. **ITEMS TO BE ANALYZED:**

1. One 3GB Hard Drive, Western Digital Caviar 33100 (University of Wisconsin). **Remarks:** AFOSI Form 96 will be e-mailed to DCFL. The OS and other pertinent information will be on 96.

2. One 4mm Digital Data Storage cartridge, 120M, labeled NVTST/OX, (Wright State University). **Remarks:** Ditto as above.

3. Two 8mm Helical-Scan, HS-8/112 Maxell Data Cartridges [redacted] b7E

**SUPPORT REQUESTED:**

Extract all system logs, text, document, etc.
Examine file system for modification to operating system software or configuration.
Examine file system for back doors, check for setuid and setgid files.
Examine file system for any sign of a sniffer program.
Extract data from this 4mm/8mm tape and convert to readable format - cut to CD.
Backup hard drives and place backup on a CD, tape or other format.
Analyze for deleted files and restore deleted files, cut findings to CD.
Extract all pertinent text files of a sexual nature.
Extract all trojanized programs or scripts/code programs, cut to CD.
Provide an analysis report and cut all findings to CD.

7. **PERTINENT DATA:** Coordinate with SA [redacted] and HQ AFOSI/XOII with pertinent data. b6 b7C

8. **AUTHORITY:** OSI Form 96 will be sent electronically.

9. **OTHER DOCUMENTS:** The ACISS report is the same as the one sent on the August 26, 1998 request.

10. **INSTRUCTIONS:** Please make five copies and send all copies of the analysis report to HQ AFOSI/XOII. HQ AFOSI/XOII will distribute the analysis accordingly. Please return all evidence to FBI Cincinnati.

11. POC: SA [redacted] AFOSI Detachment 101 at DSN: [redacted] or commercial: [redacted]

Sincerely yours,

Sheri A. Farrar
Special Agent in Charge

b6
b7C

By: [redacted]
Supervisory Special Agent