

NATIONAL SCIENCE FOUNDATION

4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

Page 1



OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

Date: September 30, 1999
To: File No. 199050017
From: [REDACTED] Special Agent [REDACTED]
[REDACTED] Computer Specialist [REDACTED]
Via: [REDACTED] Assistant Inspector General for Investigations
Subject: Case Closeout [REDACTED]

Background:

On June 2, 1999 [REDACTED] Assistant Systems Administrator at the [REDACTED] [REDACTED] employee, spoke with NSF/OIG Investigations regarding an incident involving a former [REDACTED] Systems Administrator, [REDACTED] explained that [REDACTED] whose employment had been terminated Friday afternoon May 14, 1999, lied to gain physical entry into the NSF building and [REDACTED] office late the same evening by telling the guards he left his keys and badge home. He then gained access to the [REDACTED] computer though most of the passwords were changed earlier that afternoon. [REDACTED] relayed that [REDACTED] [REDACTED] also came into the office without checking in at the Lobby on Monday afternoon. [REDACTED] hired a consultant team to assess the [REDACTED] computer and allegedly found no evidence indicating the system was compromised.

Investigation:

We met with several NSF/Division of Information Systems (DIS) managers regarding the [REDACTED] incident and the NSF Firewall Network. Our meeting confirmed the [REDACTED] account and three prior incidents of potential computer abuses by [REDACTED] were brought forth: a security scan on NSF servers (possibly [REDACTED]) and creating unauthorized user accounts. As a follow up for more [REDACTED]

[REDACTED] P) Office of the Inspector General is supported by twelve government agencies, one of which is NSF. Since the winter of '96, [REDACTED] has been housed at NSF. NSF provides the Network and office space, thereby putting up a smaller level of support relative to the other agencies. NSF allows [REDACTED] to make use of its Firewall Network.

background on [REDACTED] previous encounters with DIS, DIS provided e-mail accounts and logs for the warez incident.

In addition, we interviewed Division of Administrative Services (DAS), which handle NSF building security, regarding the DAS response and accounts of [REDACTED] physical security breach on May 14/15 and 17, 1999.

On June 29, 1999, we interviewed [REDACTED] immediate supervisor, [REDACTED] Office Manager [REDACTED] regarding the recent and previous [REDACTED] incidents, the relationships between [REDACTED] and [REDACTED] and [REDACTED] and NSF Network, [REDACTED] background, and the results of their post-intrusion analysis.

Findings:

Our initial investigation, based on interviews and evidence, confirmed [REDACTED] account of [REDACTED] unauthorized electronic access of a federal computer (violation of the Computer Fraud and Abuse Act, Title 18 U.S.C., Section 1030 (a)) on the night after his employment was terminated May 14, 1999 at NCO. DIS interviews and evidence gathered, also support that [REDACTED] maintained and created a [REDACTED] on the [REDACTED] server (a violation of No Electronic Theft Act and Criminal Infringement of a Copyright, Title 18 U.S.C., Section 2319). We did not, however, uncover any likely personal gain for [REDACTED] in either violation.

Assistant U.S. Attorney, Eastern District of Virginia, [REDACTED] verbally declined the case for prosecution, since there was no substantial damage (at least \$5,000) or a profit to support a felony conviction for the intrusion and [REDACTED]. The Eastern District of VA generally does not prosecute for misdemeanor intrusions and no personal gain piracy.

DAS and DIS have coordinated their efforts to assess and revamp NSF physical and informational security procedures for handling employees and contractors who are no longer employed at NSF. In the interim, DAS has set up a procedure with the guards for those former employees and contractors who are not allowed in the building.

Given the declination, and that [REDACTED] is a low risk threat to the NSF Network and physical security², no further investigation is warranted at this time. This case is closed.

² [REDACTED] has assured us that all passwords have been altered and their servers have been audited and are secured since [REDACTED]. DAS has assured us that they now keep a running list with the Front Desk of all former employees and contractors who are not allowed in the building.