NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

Date: September 30, 1999
To: File No. I99050016
From: [redacted] Special Agent [redacted]
[redacted] Computer Specialist [redacted]
Via: [redacted] Assistant Inspector Gener[redacted]igations
Subject: [redacted] Closeout [redacted]

Background:

On Monday May 24, 1999 NSF[redacted]lectronically notified our office that on the late afternoon of Friday May 21, 1999, an intruder accessed th[redacted] [redacted] development server. [redacted] and [redacted] exchanged a series of e-mails providing our office a summary and analysis of the[redacted] In the report, DIS summarized the following:

- While monitoring[redacted] the[redacted]gathered intelligence that the[redacted]ragged of their doings in an on-line forum. [redacted] contacte[redacted]Friday May 21, 1999 regarding [redacted]nd[redacted] replacements.
- An intruder gained entry into the development server reserved or[redacted] Accordingly, the intruder used the Front-Page extensions to remotely edit web pages, which is a common NT bug.
- A review of the development server revealed that two home page sites contained nude photos and no other NSF systems were accessed. The [redacted]had no entries after 4/16/99, a date before the incident was discovered.
- The development server was powered off as soon as NSF learned of the intrusion.

Investigation:

On June 4, 1999 several OIG and DIS employees met to discuss several of the recent computer intrusions, including th[redacted] We concluded that the intrusion

[redacted]

breached the Firewall and it was an [redacted] due to the weak security and software bugs inherent in the NT machine development server.

On June 8, 1999 we met with [redacted] to further discuss the recent intrusions and briefly touched on the [redacted]

Findings:

Though [redacted] had determined in their review the method of the intrusion and web page replacement, we lacked any evidence, [redacted]

Because the default home pages had been left on the system and the file system appeared to be intact, no damage resulted. However, the intrusion did breach the NSF Firewall Network and thus, posed a risk to systems within the Firewall Network.

Given the lack of evidence to identify any intruder/s and the lack of damage to the system, we have decided to not go forward in this case. This case is closed.