NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM

FROM: [redacted] Special Agent [redacted]
[redacted] Computer Specialist [redacted]

Via: [redacted] Assistant Inspector General for Investigations

DATE: March 30, 2000

RE: Case Closeout #I99070032

Background

The NSF administers the United States Antarctic Program (USAP) for the entire Federal Government through a contract for support operations to the USAP. Network administration and other IT operations for the USAP are included as part of the contractor's duties.

On July 19, 1999 OIG was notified by [redacted] Manager of Technology Development, Office of Polar Programs (OPP) that intruders had illegally accessed six U.S. Polar Program servers at the South Pole Station, McMurdo Stations, and ASA Headquarters in the June and July 1999 timeframe. The six known compromised systems include oak.spole.gov (199.4.250.1), pamanda1.spole.gov (204.89.132.91), and pamanda2.spole.gov (204.89.132.92) at South Pole Station; terror.mcmurdo.gov (157.132.107.66) and vinson.mcmurdo.gov (157.132.119.50) at McMurdo Station; and www.asa.org (198.59.57.65) at ASA Headquarters.

The calculated financial damages are based on estimated expended labor resources including ASA Headquarters, South Pole, and McMurdo personnel and procured new hardware at Denver. These damages do not include labor and hardware costs for the pamanda1 and pamanda2 servers[1].

[1] The pamanda servers are administered under the control of Antarctic Muon and Neutrino Detector Array (AMANDA) Project scientists, though they share South Pole Network and have a trust relationship with oak.spole.gov (under full ASA control). AMANDA, funded by NSF Physics Division and Polar Programs, is a collaborated project composed of the [redacted]

In addition to financial damages, other likely damages and risks include compromised user accounts and passwords at South Pole and McMurdo Stations and unauthorized access to proprietary scientific data from the AMANDA Project.

Investigation

Analysis of the available log evidence for the South Pole (oak.spole.gov only[2]) and McMurdo intrusions, provided to OIG Agents, indicates the intrusions or attempts to intrude backdated to March through May 1999 timeframe, and originated from multiple international Internet Service Provider (ISP) accounts as a points of unauthorized entry or target reconnaissance. The logs capture only four intruder ISP accounts, which originate from the U.S. (MCI World Com, EarthLink, and US West) and Canada (Rogers@Home). The other intruder IP addresses for the South Pole and McMurdo intrusions originate primarily from Brazil and Chile.

The OIG Agent sent 2703 (f) letters notifying the three U.S. ISPs of a potential 2703 Court Order for all subscriber and transactional data. The Agent contacted the Canadian Royal Mounted Police, Computer Crime Division for investigative assistance regarding the Canadian ISP. We referred the case to the Eastern District of Virginia, U.S. Attorney's Office to request Court Orders and coordination. Subsequently, in December, we established the four ISPs no longer had the requested subscriber and transactional information, as most ISPs commonly do not backup beyond one month.

Findings

As a result of the inability to trace the first point of the intrusions, we were forced to close the case unsolved. We subsequently communicated recommendations to OPP for upgrading station network security and future incident response coordination, due to our assessment that South Pole and McMurdo servers remain likely and easy targets.

[2] The only pamanda1 and pamanda2 logs in our possession are the logs attached to the CERT. It appears that these logs represent activity captured by the intruder's sniffer.