(12/31/1995)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 02/23/1998

To: Albuquerque **Attn:** Las Cruces RA
Roswell RA
NSD/CID **Attn:** CITAC/Room 11887
SSA [redacted]

From: Albuquerque
Squad 8
Contact: SA [redacted] b6 b7C

Approved By: [redacted] 2/23/98

Drafted By: [redacted] :cmh

Case ID #: (U) ~~(S)~~ 288-HQ-1242560-158 (Pending)

Title: (U) ~~(S)~~ SOLAR SUNRISE;
CITA MATTERS;
OO: HQ;

Synopsis: (U) To set leads at Las Cruces RA and Roswell RA.

(U) ~~(S)~~ ~~**Derived From : Single Source Document**~~
~~**See Classification Authority Reference Section.**~~
~~**Declassify** On: 02/12/2008~~

(U) ~~**Classification Authority Reference:** (S) See Reference Section;~~
~~Classified By: 4511, CITAC/D5; Reason: 1.5(c); Declassify On: 02/12/2008~~

Reference: (U) ~~(S)~~ 288-HQ-1242560 Serial 52

Details: (U) ~~(S)~~ On 02/01/1998, the Department of Defense (DOD) began detecting computer intrusions into its unclassified computer systems at various facilities in the United States. These intrusions are ongoing. At least 11 DOD systems are known to have been compromised and recovery procedures have been initiated. The intruder appears to have targeted domain name servers and obtained root status via exploitation of the "statd" vulnerability in the Solaris 2.4 operating system. Hacker tools imported from a University of Maryland site were used to gain entry. The intruder installed a sniffer program and then closed the vulnerability by transferring a patch from the University of North Carolina. A "backdoor" was created to allow the intruder reentry to the system.

~~SECRET~~

To: Albuquerque From: Albuquerque
Re: (U) ~~(S)~~ 288-HQ-1242560, 02/23/1998

(U) ~~(S)~~ Intrusions, or intrusion attempts, were detected at Andrews Air Force Base (AFB), Columbus AFB, Kirkland AFB, Maxwell AFB (Gunter Annex), Kelly AFB, Lackland AFB, Shaw AFB, MacDill AFB, Naval Station Pearl Harbor, and an Okinawa Marine Corps Base.

(U) ~~(S)~~ Numerous university computer sites in the U.S. appear to have been exploited in a similar fashion. Internet service providers near those universities also appear to have been exploited to access, or attempt to access, DOD computer networks.

(U) ~~(S)~~ In the referenced communication, FBIHQ requested all field offices expeditiously contact all logical sources for any information pertaining to intrusions into Air Force domain name servers using the "statd" exploit on Solaris 2.4 operating systems.

To: Albuquerque From: Albuquerque
Re: (U) (~~S~~) 288-HQ-1242560, 02/23/1998

LEAD (s):

Set Lead 1:

LAS CRUCES RA

AT ALAMOGORDO, NM

(U) (~~S~~) Expeditiously contact the Office of Special Investigations (OSI) at Holloman AFB, ALAMOGORDO, New Mexico, telephone number [redacted] or [redacted] Determine if they have any information pertaining to intrusions into Air Force domain name servers using the "statd" exploit on Solaris 2.4 operating systems. Respond expeditiously with positive results to SSA [redacted] or SSA [redacted] FBIHQ, NSD/CID, CITAC, telephone number [redacted] b6 b7C

Set Lead 2:

ROSWELL RA

AT CLOVIS, NM

(U) (~~S~~) Expeditiously contact the Office of Special Investigations (OSI) at Cannon AFB, Clovis, New Mexico, telephone number [redacted] or [redacted] Determine if they have any information pertaining to intrusions into Air Force domain name servers using the "statd" exploit on Solaris 2.4 operating systems. Respond expeditiously with positive results to SSA [redacted] or SSA [redacted] FBIHQ, NSD/CID, CITAC, telephone number [redacted] b6 b7C

♦♦