

**UNITED STATES COMPUTER EMERGENCY
READINESS TEAM
(US-CERT)**



US-CERT OPERATIONS

**Incident & Event Summary
Department of Defense (DOD)**

Tuesday 5/8/2007



soc@us-cert.gov

888-282-0870

http://www.us-cert.gov

Executive Summary

The National Cyber Security Division (NCS) United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security (DHS) and the public and private sectors. Established in 2003 to protect the nation's internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. The organization interacts with federal agencies, state and local governments, industry professionals, and others to improve information sharing and incident response coordination and to reduce cyber threats and vulnerabilities.

This report is intended to provide an overview of the incident and event trends observed by US-CERT impacting Department of Defense (DOD).

The Federal Information Security Management Act (FISMA) of 2002 requires all agencies to report security incidents to the US-CERT. A computer incident within the federal government, as defined by NIST Special Publication 800-61 is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In order to maintain standard reporting nomenclature and meaningful reporting metrics, US-CERT utilizes the incident and event categories defined in Table 1 and Table 2 below.

Table 1: Federal Agency Incident Categories

CATEGORY	NAME	DESCRIPTION
CAT 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.
CAT 2	Denial of Service (DoS)	An attack that <i>successfully</i> prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
CAT 3	Malicious Code	<i>Successful</i> installation of malicious software (i.e., virus, worm, spyware, bots, Trojan horse, or other code-based malicious entity) that infects or affects an operating system or application. Agencies are NOT required to report malicious logic that has been <i>successfully quarantined</i> by antivirus (AV) software.
CAT 4	Improper Usage	A person violates acceptable computing use policies.

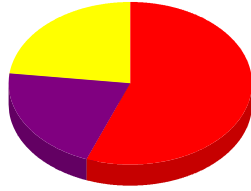
Table 2: Federal Agency Event Categories

CATEGORY	NAME	DESCRIPTION
CAT 5	Scans / Probes / Attempted Access	This category includes an activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
CAT 6	Investigation	<i>Unconfirmed</i> incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

Department of Defense (DOD) Reporting Trends and Metrics

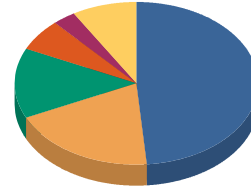
The following trends and data are current as of 05/08/07 and are based on PII incidents and events impacting the Department of Defense (DOD) that were reported to US-CERT during the current federal fiscal year.

Figure 1.1: Incidents and Events by Category



Unauthorized Access	77	55.8%
Improper Usage	29	21.0%
Under Investigation / Other	32	23.2%
Total:	138	100.0%

Figure 1.2: Top Five Incidents & Events vs. All Others



Equipment Theft/Loss	67	48.6%
Policy Violation	27	19.6%
Non Cyber	19	13.8%
Suspicious System Activity	9	6.5%
Privileged Access	4	2.9%
Others	12	8.7%
Total:	138	100.0%

Figure 1.3: Monthly Ticket Volume

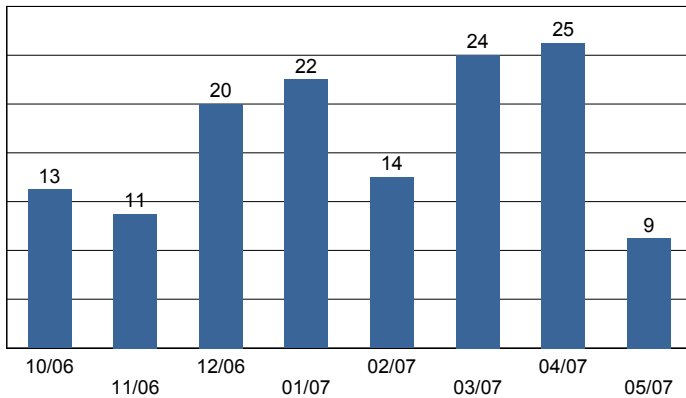


Figure 1.4: Top Incident or Event Reported by Month

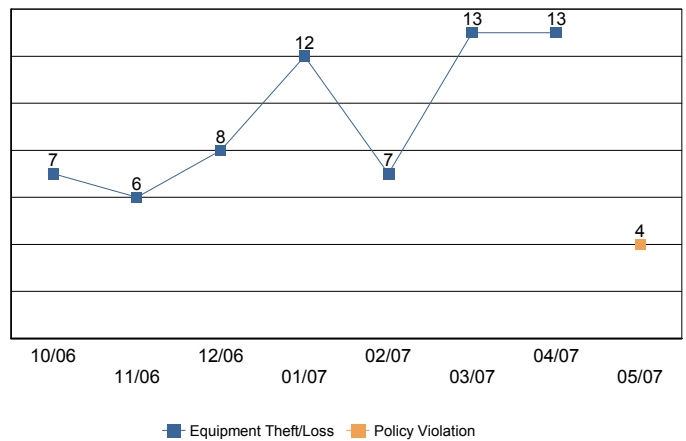
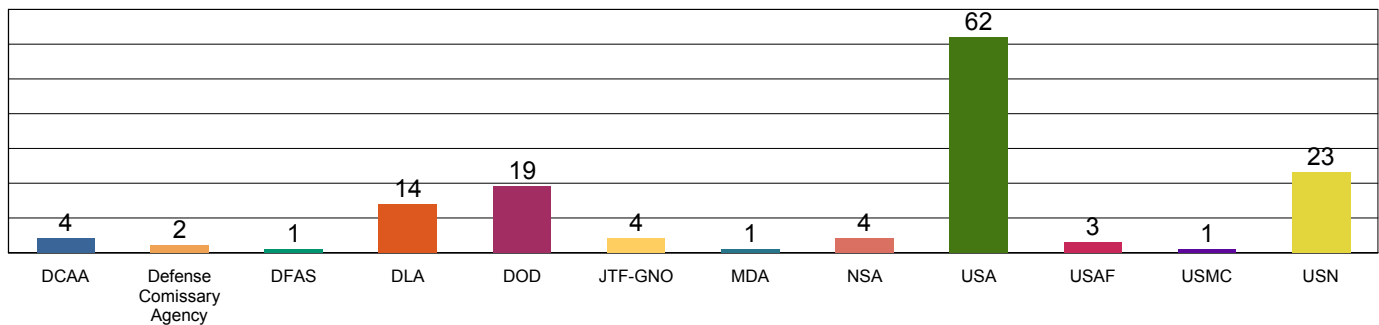


Figure 1.5: Tickets by Sub Organization



US#042024 Created: 1/24/2007 7:26:50PM

Problem Type: 04-Improper Usage

Sub-Type: Policy Violation

PII Involved: Yes

Last Edited: 1/25/2007 2:18:49AM

Report Method: EMail

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: JTF-GNO

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Air Force (USAF)

Occurred: 01/24/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: User

Incident Status: Open

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Not Reported

AV: Not Reported

Agency reports unencrypted emails sent containing PII were sent to wrong recipients. The amount of individuals affected is being investigated.

Ticket Status: CLOSED On 01/24/07 at 7:29:12PM

US#041949 Created: 1/24/2007 9:48:14AM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 2/9/2007 2:47:57AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By:

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Air Force (USAF)

Occurred: 01/24/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Not Reported

Incident Status: Not Reported

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Not Reported

AV: Not Reported

Agency user reports the names and SSN's of individuals were downloaded to a thumb drive. The thumb drive was lost. It is uncertain if the names and social security numbers were compromised. The agency has notified the Privacy Act Manager and is in the process of notifying the 1956 personnel that were listed on the thumb drive that their PII information may have been compromised.

Ticket Status: CLOSED On 02/09/07 at 2:47:34AM

US#040308 Created: 1/9/2007 12:11:34PM

Problem Type: 04-Improper Usage

Sub-Type: Policy Violation

PII Involved: Yes

Last Edited: 2/9/2007 7:20:01AM

Report Method: Email

Reporting Sector: Agency (Department of Homeland Security (DHS))

Reported By: Joshua Silva

Tracking #: 2007-01-018

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Air Force (USAF)

Occurred: 01/04/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Other

Incident Status: Unknown

Impact: Medium

Sites: 1

Systems: 1

Function: Not Reported

OS: Not Reported

AV: Not Reported

An agency reported while searching the web a FOUO Document was posted on Google from NORAD / USNORTHCOM.

Ticket Status: CLOSED On 02/09/07 at 7:19:54AM

US#054497 Created: 5/7/2007 9:33:04PM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 5/8/2007 12:06:30PM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Fred Adams

Tracking #: SIR (07-510)

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 05/07/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Other

Incident Status: Unknown

Impact: Medium

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Not Reported

AV: Not Reported

An agency reports a laptop was stolen from an individual's POV containing encrypted PII data.

Ticket Status: CLOSED On 05/07/07 at 9:52:52PM

US#054356 Created: 5/5/2007 10:25:10PM

Problem Type: 04-Improper Usage

Sub-Type: Policy Violation

PII Involved: Yes

Last Edited: 5/5/2007 10:35:38AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Joy Renfro

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 05/05/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Not Reported

Incident Status: Not Reported

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Not Reported

AV: Not Reported

Agency reports that PII was sent via email that was neither encrypted or sent to the correct group list. The message was recalled, but copies left the email servers as they were forwarded to either a personal account or to a blackberry.

Ticket Status: CLOSED On 05/05/07 at 10:28:04PM

US#053990 Created: 4/30/2007 6:59:17PM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 5/1/2007 8:05:25AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By:

Tracking #: SIR (07-492)

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 04/30/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: 3rd Party

Incident Status: Closed

Impact: Not Reported

Sites: Not Reported

Systems: 1

Function: Laptop

OS: Windows XP

AV: Installed

An agency reports that an employee had a laptop and a government issued credit card stolen. PII was involved. Law enforcement has been notified and the incident is under investigation.

Ticket Status: ASSIGNED

US#053877 Created: 4/30/2007 11:54:17AM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 5/1/2007 2:48:25AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: john metzler

Tracking #: NGOH2007001

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 04/27/07 19:00

Timezone: Eastern Standard Time - EST

Identified By: Not Reported

Incident Status: Closed

Impact: Not Reported

Sites: Not Reported

Systems: 1

Function: Laptop

OS: Not Reported

AV: Not Reported

An agency reports a stolen laptop containing PII. Incident has been reported to local law enforcement.

Ticket Status: CLOSED On 04/30/07 at 11:59:28AM

US#053538 Created: 4/25/2007 7:46:20PM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 4/26/2007 12:44:14PM

Report Method: Web

Reporting Sector: Agency (Department of Defense (DOD))

Reported By:

Tracking #: US-CERT - 2007-USCERT2SC2DC

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 04/25/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: 3rd Party

Incident Status: Not Reported

Impact: Not Reported

Sites: Not Reported

Systems: 1

Function: Laptop

OS: Not Reported

AV: Not Reported

An agency reports an employee's vehicle was broken into and his laptop was stolen. The laptop contained PII. Local law enforcement has been notified.

Ticket Status: CLOSED On 04/25/07 at 7:51:09PM

US#052829 Created: 4/19/2007 12:09:51PM

Problem Type: 04-Improper Usage

Sub-Type: Policy Violation

PII Involved: Yes

Last Edited: 4/25/2007 10:19:35AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Evelyn Taylor

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 04/13/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: 3rd Party

Incident Status: Not Reported

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Windows XP

AV: Installed

An agency reports an employee inadvertently sent an e-mail to 15 individuals with a spreadsheet attachment that contained personal identifiable information (PII) of 1,970 people.

Ticket Status: CLOSED On 04/24/07 at 12:31:58PM

US#052556 Created: 4/17/2007 3:55:39PM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 4/18/2007 3:46:24AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Fredrick Adams

Tracking #: #2007-USCERT3MKCYN

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 04/17/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Other

Incident Status: Unknown

Impact: Medium

Sites: 1

Systems: 1

Function: Laptop

OS: Not Reported

AV: Not Reported

An agency report a stolen laptop. The vehicle was vehicle vandalized and the laptop removed.

Ticket Status: CLOSED On 04/17/07 at 4:01:11PM

US#051970 Created: 4/10/2007 2:13:28PM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 4/11/2007 12:57:12PM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Fred Adams

Tracking #: 2007-USCERT1RUV9S

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 04/10/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Other

Incident Status: Unknown

Impact: Medium

Sites: 1

Systems: 1

Function: Blackberry/PDA/Mobile Agent,Laptop

OS: Not Reported

AV: Not Reported

An agency reports an employee's agency issued laptop was stolen. Access to the laptop requires user name, password and CAC card authentication. Laptop contained PII.

Ticket Status: CLOSED On 04/10/07 at 2:14:58PM

US#051940 Created: 4/10/2007 10:53:40AM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 4/11/2007 2:53:04AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Jack Borders

Tracking #: 2007-0001

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 04/10/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Other

Incident Status: Unknown

Impact: Medium

Sites: 1

Systems: 1

Function: Laptop

OS: Not Reported

AV: Not Reported

An agency reports an employee's privately owned vehicle was vandalized and the agency issued laptop was stolen from the vehicle. The laptop was not encrypted and it contained PII data.

Ticket Status: CLOSED On 04/10/07 at 10:55:00AM

US#051860 Created: 4/9/2007 2:25:48PM
Problem Type: 01-Unauthorized Access
Sub-Type: Equipment
PII Involved: Yes

Last Edited: 4/10/2007 2:43:45AM Assigned To: Incident Handling
Report Method: Email
Reporting Sector: Agency (Department of Defense (DOD))
Reported By: Richard B. Hogle
Tracking #: NOPD Item # D-06305-07

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 04/05/07 0:00 **Impact:** Not Reported **Function:** Blackberry/PDA/Mobile Agent
Timezone: Eastern Standard Time - EST **# Sites:** Not Reported **OS:** Not Reported
Identified By: User **# Systems:** 1 **AV:** Not Reported
Incident Status: Open

An agency reports a stolen Blackberry and CAC (Common Access Card). Local law enforcement is investigating. PII involved.

Ticket Status: CLOSED On 04/09/07 at 2:47:40PM

US#051656 Created: 4/6/2007 7:21:37PM
Problem Type: 01-Unauthorized Access
Sub-Type: Equipment
PII Involved: Yes

Last Edited: 4/7/2007 4:48:38AM Assigned To: Incident Handling
Report Method: Email
Reporting Sector: Agency (Department of Defense (DOD))
Reported By: Fred
Tracking #: SIR 07-437

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 04/05/07 22:37 **Impact:** Not Reported **Function:** Not Reported
Timezone: Eastern Standard Time - EST **# Sites:** Not Reported **OS:** Not Reported
Identified By: Not Reported **# Systems:** Not Reported **AV:** Not Reported
Incident Status: Not Reported

A laptop was stolen from GOV parked at the operator's residence.

Ticket Status: CLOSED On 04/06/07 at 7:27:52PM

US#051505 Created: 4/5/2007 9:25:38PM
Problem Type: 01-Unauthorized Access
Sub-Type: Equipment
PII Involved: Yes

Last Edited: 4/25/2007 11:44:59AM Assigned To: Incident Handling
Report Method: Web
Reporting Sector: Agency (Department of Defense (DOD))
Reported By: Fred Adams
Tracking #: SIR 07-434

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 04/05/07 15:30 **Impact:** Not Reported **Function:** Laptop
Timezone: Eastern Standard Time - EST **# Sites:** 1 **OS:** Not Reported
Identified By: Not Reported **# Systems:** 1 **AV:** Not Reported
Incident Status: Not Reported

An agency reports an employee lost their laptop. PII was involved. It is unknown the type and the amount of PII possibly compromised.

Ticket Status: CLOSED On 04/25/07 at 11:44:33PM

US#050803 Created: 3/29/2007 2:19:25PM
Problem Type: 01-Unauthorized Access
Sub-Type: Equipment
PII Involved: Yes

Last Edited: 3/30/2007 6:05:23AM Assigned To: Analysis
Report Method: Email
Reporting Sector: Agency (Department of Defense (DOD))
Reported By: Ken Foster
Tracking #: CCIR 07-0129

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 03/29/07 0:00 **Impact:** Not Reported **Function:** Workstation
Timezone: Eastern Standard Time - EST **# Sites:** Not Reported **OS:** Windows XP
Identified By: Administrator **# Systems:** Not Reported **AV:** Not Reported
Incident Status: Open

An agency reports a computer was missing the hard drive, memory stick, and video card when it was brought in for maintenance. The hard drive contained PII on 1500 individuals. The CIO and law enforcement were notified.

Ticket Status: CLOSED On 03/29/07 at 3:03:14PM

US#050655 Created: 3/28/2007 12:39:33PM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 3/29/2007 3:04:37AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By:

Tracking #: SIR (07-415)

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 03/28/07 7:40

Timezone: Eastern Standard Time - EST

Identified By: Not Reported

Incident Status: Open

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Laptop

OS: Not Reported

AV: Not Reported

An agency reports a stolen laptop. PII is involved. Local law enforcement was notified.

Ticket Status: CLOSED On 03/28/07 at 12:43:40PM

US#050561 Created: 3/27/2007 10:31:53PM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 4/12/2007 12:09:32PM

Report Method: Web

Reporting Sector: Agency (Department of Defense (DOD))

Reported By:

Tracking #: SIR (07-412)

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 03/27/07 8:00

Timezone: Eastern Standard Time - EST

Identified By: 3rd Party

Incident Status: Open

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Laptop

OS: Not Reported

AV: Not Reported

An agency reports an employee had a laptop stolen. The laptop is user / password protected. 58 cases of PII may be involved.

Ticket Status: CLOSED On 04/12/07 at 12:09:23AM

US#050544 Created: 3/27/2007 5:35:49PM

Problem Type: 06-Investigation

Sub-Type: Non Cyber

PII Involved: Yes

Last Edited: 3/28/2007 5:19:40AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Melissa Robinson

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 03/23/07 22:22

Timezone: Eastern Standard Time - EST

Identified By: Administrator

Incident Status: Open

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Other

OS: Not Reported

AV: Not Reported

An agency reports the unauthorized transmittal and storage of Leave and Earning Statement information. The statements contained PII.

Ticket Status: CLOSED On 03/27/07 at 5:42:09PM

US#049855 Created: 3/22/2007 4:28:15PM

Problem Type: 06-Investigation

Sub-Type: Non Cyber

PII Involved: Yes

Last Edited: 3/23/2007 5:46:10AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Lance Hughey

Tracking #: #2007-USCERT199A50

Assigned To: Law Enforcement/Intel Group

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 03/22/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Other

Incident Status: Unknown

Impact: Medium

Sites: 1

Systems: 1

Function: Not Reported

OS: Not Reported

AV: Not Reported

An agency reports an individual was caught stealing PII. The incident affects 39 individual contractors, federal employees, and members of the public. The incident is still under investigation.

Ticket Status: ASSIGNED

US#049553 Created: 3/20/2007 10:50:35AM

Problem Type: 04-Improper Usage

Sub-Type: Policy Violation

PII Involved: Yes

Last Edited: 3/21/2007 3:53:18AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Linda Ladieu

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 03/18/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Administrator

Incident Status: Closed

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Server

OS: Not Reported

AV: Not Reported

An agency reports a PII compromise. A sensitive file had shared permission's' on the server. The agency immediately ceased access to the folder. The disclosure may affect over 1200 individuals.

Ticket Status: CLOSED On 03/20/07 at 11:07:25AM

US#049032 Created: 3/16/2007 10:24:15AM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 3/16/2007 10:57:58AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Phillip Cozort

Tracking #: 353ENGP70740001

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 03/14/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Other

Incident Status: Unknown

Impact: Medium

Sites: 1

Systems: 1

Function: Not Reported

OS: Not Reported

AV: Not Reported

An agency reported a classified laptop is missing from an office space. The laptop was being used at a workshop to view data.

Ticket Status: CLOSED On 03/16/07 at 10:25:29AM

US#048828 Created: 3/14/2007 6:14:12PM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 3/27/2007 8:43:50AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Jeannette Blumenthal

Tracking #: DOD-Stolen Laptop

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 03/13/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: 3rd Party

Incident Status: Closed

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Not Reported

AV: Installed

An agency reports a laptop computer with case files stolen from the vehicle of an employee. The electronic media was encrypted. An additional unencrypted file containing 16,000 employee's PII was determined to be on the laptop.

Ticket Status: CLOSED On 03/14/07 at 6:16:27PM

US#048823 Created: 3/14/2007 5:49:11PM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 3/15/2007 4:30:19AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Fred Adams

Tracking #: SIR 07-371

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 03/14/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Other

Incident Status: Unknown

Impact: Medium

Sites: 1

Systems: 1

Function: Laptop

OS: Not Reported

AV: Not Reported

An agency reported the agency laptop was stolen from an employee's vehicle. The laptop and the PII data was password protected and encrypted.

Ticket Status: CLOSED On 03/14/07 at 5:50:54PM

US#048577 Created: 3/12/2007 7:55:47PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 3/13/2007 7:04:00AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Louis DiTullio**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA) / Training and Doctrine Command (TRADOC)**Occurred:** 03/11/07 7:24**Timezone:** Eastern Standard Time - EST**Identified By:** Other**Incident Status:** Closed**Impact:** Not Reported**# Sites:** 1**# Systems:** 1**Function:** Laptop**OS:** Not Reported**AV:** Installed

An agency reports that a laptop was lost or stolen and contains personally identifiable information (PII).

Ticket Status: CLOSED On 03/12/07 at 7:59:18PM

US#048107 Created: 3/9/2007 9:01:57PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 3/9/2007 9:08:12AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Ken Foster**Tracking #:** 07-0093

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 03/09/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** User**Incident Status:** Closed**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Blackberry/PDA/Mobile Agent**OS:** Not Reported**AV:** Not Reported

Agency reports that an individual lost his government issued PDA. The PDA had his own personal information and no other.

Ticket Status: ASSIGNED

US#046738 Created: 2/28/2007 2:15:23PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 3/1/2007 3:39:44AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** JOY RENFRO**Tracking #:** # 2007-USCERT339EUC

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 02/28/07 11:07**Timezone:** Eastern Standard Time - EST**Identified By:** Other**Incident Status:** Unknown**Impact:** Medium**# Sites:** 1**# Systems:** 1**Function:** Laptop**OS:** Windows XP**AV:** Installed

An agency reports that a terminated employee failed to turn in an agency issued laptop. PII was on the hard drive of laptop.

Ticket Status: CLOSED On 02/28/07 at 2:19:07PM

US#046629 Created: 2/27/2007 4:15:53PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 2/28/2007 6:18:11AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** John Leach**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 02/20/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** User**Incident Status:** Closed**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** 1**Function:** Laptop**OS:** Not Reported**AV:** Installed

An agency reports a laptop computer missing from an individual's section. The laptop was up to date on all patches.

Ticket Status: CLOSED On 02/27/07 at 4:18:36PM

US#045869 Created: 2/21/2007 6:17:55PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 2/22/2007 7:10:04AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** CHRISTOPHER KRAFT**Tracking #:** 2007-USCERT20X96N

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 01/26/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Other**Incident Status:** Unknown**Impact:** Medium**# Sites:** 1**# Systems:** 3**Function:** Laptop**OS:** Not Reported**AV:** Not Reported

An agency has reported several laptop computers were taken from an individuals home. The Albuquerque Police Department was notified and a report filed.

Ticket Status: CLOSED On 02/22/07 at 3:02:12AM

US#045809 Created: 2/21/2007 10:30:49AM

Problem Type: 06-Investigation**Sub-Type:** Non Cyber**PII Involved:** Yes

Last Edited: 2/22/2007 3:59:51AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Sharon Pitts**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 02/07/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Other**Incident Status:** Closed**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

Agency reports PII was discovered. The PII contained pilot names, full SSNs, addresses, login identifications, passwords, dates of birth, and dates of last promotion.

Ticket Status: CLOSED On 02/21/07 at 10:40:51AM

US#045681 Created: 2/20/2007 3:25:16PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 2/21/2007 6:55:38AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** George Paschetto**Tracking #:** USCERT3CUI3H

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA) / Training and Doctrine Command (TRADOC)**Occurred:** 02/20/07 14:40**Timezone:** Eastern Standard Time - EST**Identified By:** User**Incident Status:** Closed**Impact:** High**# Sites:** 1**# Systems:** 1**Function:** Laptop**OS:** Not Reported**AV:** Not Reported

An agency reports that a laptop containing Personally Identifiable Information (PII) has been lost or stolen.

Ticket Status: CLOSED On 02/20/07 at 4:02:36PM

US#044929 Created: 2/14/2007 3:37:03PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 2/14/2007 3:50:13AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:****Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 02/13/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** User**Incident Status:** Closed**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** 1**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

Agency reports theft of a laptop and USB drive from his home. The USB drive contained PII information for nine individuals.

Ticket Status: CLOSED On 02/14/07 at 3:41:53PM

US#044607 Created: 2/12/2007 11:16:22AM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 2/12/2007 11:27:43AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Fred Adams**Tracking #:** SIR (07-291)

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 02/12/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** User**Incident Status:** Closed**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Laptop**OS:** Not Reported**AV:** Not Reported

An agency is reporting the loss or theft of a laptop from a POV. PII is involved.

Ticket Status: CLOSED On 02/12/07 at 11:20:36AM

US#044121 Created: 2/8/2007 12:26:55PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 2/9/2007 12:46:30PM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Gloris Davis**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 02/08/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** User**Incident Status:** Open**Impact:** Low**# Sites:** 1**# Systems:** 3**Function:** Laptop**OS:** Windows XP**AV:** Installed

An agency is reporting that three laptops have been stolen. PII is involved.

Ticket Status: CLOSED On 02/09/07 at 12:46:02AM

US#043001 Created: 2/1/2007 2:12:15PM

Problem Type: 04-Improper Usage**Sub-Type:** Policy Violation**PII Involved:** Yes

Last Edited: 2/28/2007 12:04:19PM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Eleanor Brings**Tracking #:** 2007-USCERT3FDVYU

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 02/01/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Other**Incident Status:** Unknown**Impact:** Medium**# Sites:** 1**# Systems:** 1**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

An agency reports that personal information was disclosed and publicly accessible on a FTP server. The file was immediately made inaccessible after the discovery.

Ticket Status: CLOSED On 02/28/07 at 12:03:51PM

US#042997 Created: 2/1/2007 1:59:32PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Network**PII Involved:** Yes

Last Edited: 2/1/2007 2:30:31AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:****Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 02/01/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Not Reported**Incident Status:** Not Reported**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

Agency reports the names, grades, title, office, last 4 digits of SSN, and position sensitivity for 32,077 employees could be downloaded by the public as a single spreadsheet. The spreadsheet was removed from the FTP server.

Ticket Status: ASSIGNED

US#042567 Created: 1/29/2007 4:09:41PM

Problem Type: 04-Improper Usage**Sub-Type:** Policy Violation**PII Involved:** Yes

Last Edited: 2/21/2007 8:35:23AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** JTF-GNO**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 01/29/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** User**Incident Status:** Not Reported**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

An agency reports that a employee sent email that was encrypted that contained PII on 5 documents to 23 personnel without a valid need to know. The employee also sent unencrypted email that contained PII to the proper recipients

Ticket Status: CLOSED On 02/08/07 at 12:57:59AM

US#042176 Created: 1/26/2007 10:52:59AM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 1/29/2007 2:35:09AM

Report Method: Web**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Fred Adams**Tracking #:** SIR# 07-254

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 01/26/07 10:50**Timezone:** Eastern Standard Time - EST**Identified By:** 3rd Party**Incident Status:** Open**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Laptop**OS:** Not Reported**AV:** Not Reported

Agency reports laptop and CAC card was stolen. PII involved.

Ticket Status: CLOSED On 01/26/07 at 10:58:33AM

US#042112 Created: 1/25/2007 2:46:26PM

Problem Type: 04-Improper Usage**Sub-Type:** Policy Violation**PII Involved:** Yes

Last Edited: 2/2/2007 10:44:17AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** grant.stoebner**Tracking #:** 2007-USCERTPLAFS

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 01/25/07 11:24**Timezone:** Eastern Standard Time - EST**Identified By:** User**Incident Status:** Open**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

Agency reports employee transferred within agency. Before employee transferred the employee copied a database that contained PII records on approximately 430-450 employees on to their thumb drive.

Ticket Status: CLOSED On 01/25/07 at 2:51:21PM

US#041832 Created: 1/23/2007 11:34:34AM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 1/29/2007 2:31:58AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Fred Adams**Tracking #:** SIR 07-244

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 01/21/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Not Reported**Incident Status:** Open**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

Agency reports a laptop was stolen from a vehicle. It contained PII of 285 people.

Ticket Status: RE-OPENED

US#041439 Created: 1/19/2007 8:47:32PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 1/30/2007 8:51:40AM

Report Method: Web**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Fred Adams**Tracking #:** 07-238

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 01/19/07 11:42**Timezone:** Eastern Standard Time - EST**Identified By:** User**Incident Status:** Open**Impact:** Not Reported**# Sites:** 1**# Systems:** 1**Function:** Laptop**OS:** Not Reported**AV:** Not Reported

Federal agency reports the theft of a government laptop which contained PII

Ticket Status: CLOSED On 01/19/07 at 9:39:10PM

US#041093 Created: 1/16/2007 7:14:22PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 1/29/2007 2:31:37AM

Report Method: Web**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:****Tracking #:** SIR (07-225)

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 01/16/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** User**Incident Status:** Not Reported**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Laptop**OS:** Not Reported**AV:** Not Reported

Agency reports employee's laptop stolen out of vehicle. PII involved.

Ticket Status: CLOSED On 01/16/07 at 7:18:14PM

US#041067 Created: 1/16/2007 4:13:50PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 1/17/2007 4:41:55AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Rachel Brooke**Tracking #:** 006122707-E

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 01/12/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Administrator**Incident Status:** Open**Impact:** Medium**# Sites:** 1**# Systems:** 1**Function:** Laptop**OS:** Windows XP**AV:** Installed

An organization reports a stolen laptop. The laptop carrying case had the individuals PII and a financial document (Military LES) enclosed.

Ticket Status: CLOSED On 01/16/07 at 4:14:16PM

US#040628 Created: 1/12/2007 10:28:51AM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 2/1/2007 11:32:58AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Eleanor Brings**Tracking #:** 2007-USCERH3CJ8

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 08/28/06 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Other**Incident Status:** Unknown**Impact:** Medium**# Sites:** 1**# Systems:** 1**Function:** Laptop**OS:** Not Reported**AV:** Not Reported

An agency has reported a laptop was stolen from an agency in August 2006, and just being reported by the individual. The laptop contained PII data, but the level of the PII is unknown at this time. The laptop belonged to a retired individual of the agency, and being used by an agency advisor.

Ticket Status: CLOSED On 02/01/07 at 11:32:47PM

US#040019 Created: 1/6/2007 1:31:37PM
Problem Type: 01-Unauthorized Access
Sub-Type: Equipment
PII Involved: Yes

Last Edited: 2/2/2007 12:08:57PM Assigned To: Incident Handling
Report Method: Email
Reporting Sector: Agency (Department of Defense (DOD))
Reported By: Frederick Adams
Tracking #: Not Reported

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 01/06/07 0:00 **Impact:** Not Reported **Function:** Not Reported
Timezone: Eastern Standard Time - EST **# Sites:** Not Reported **OS:** Not Reported
Identified By: Not Reported **# Systems:** Not Reported **AV:** Not Reported
Incident Status: Not Reported

Agency reports that a laptop with unknown number of PII was stolen. The laptop was stolen while civilian recruiter was on vacation. Agency is investigating what PII was contained on the laptop by analysing a database.

Ticket Status: CLOSED On 02/02/07 at 12:08:31AM

US#039825 Created: 1/4/2007 10:36:55AM
Problem Type: 01-Unauthorized Access
Sub-Type: Equipment
PII Involved: Yes

Last Edited: 1/5/2007 2:29:08AM Assigned To: Incident Handling
Report Method: Email
Reporting Sector: Agency (Department of Defense (DOD))
Reported By: Fred Adams
Tracking #: 2007-USCERT319QG4

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 12/31/06 0:00 **Impact:** Medium **Function:** Laptop
Timezone: Eastern Standard Time - EST **# Sites:** 1 **OS:** Not Reported
Identified By: Other **# Systems:** 1 **AV:** Not Reported
Incident Status: Unknown

An agency reports a stolen laptop. The laptop contain PII on four individuals. The local police department was notified; letters were sent notifying compromised individuals.

Ticket Status: CLOSED On 01/05/07 at 2:25:07AM

US#039363 Created: 12/28/2006 5:18:01PM
Problem Type: 01-Unauthorized Access
Sub-Type: Equipment
PII Involved: Yes

Last Edited: 12/29/2006 6:39:09AM Assigned To: Incident Handling
Report Method: Email
Reporting Sector: Agency (Department of Defense (DOD))
Reported By: Fred Adams
Tracking #: US-CERT - 2006-USCERT3AW9IN

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 12/18/06 0:00 **Impact:** Not Reported **Function:** Laptop
Timezone: Eastern Standard Time - EST **# Sites:** Not Reported **OS:** Not Reported
Identified By: 3rd Party **# Systems:** 1 **AV:** Not Reported
Incident Status: Closed

Agency reports a member's laptop was stolen from his car. Currently it is unknown if PII was stored on the laptop. Incident is still under investigation.

Ticket Status: CLOSED On 12/28/06 at 5:22:42PM

US#038642 Created: 12/20/2006 7:55:29AM
Problem Type: 01-Unauthorized Access
Sub-Type: Equipment
PII Involved: Yes

Last Edited: 1/29/2007 2:30:30AM Assigned To: Incident Handling
Report Method: Email
Reporting Sector: Agency (Department of Defense (DOD))
Reported By: Fred Adams
Tracking #: 2006-USCERT1M9R4N

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 12/16/06 0:00 **Impact:** Medium **Function:** Not Reported
Timezone: Eastern Standard Time - EST **# Sites:** 1 **OS:** Not Reported
Identified By: Not Reported **# Systems:** 1 **AV:** Not Reported
Incident Status: Unknown

An agency reported a stolen laptop. The laptop was secured in a desk drawer. The laptop requires a CAC card as well as a pin number to gain access. There are 19 individuals' PII stored on the laptop that could be affected.

Ticket Status: CLOSED On 12/21/06 at 4:50:12AM

US#038027 Created: 12/14/2006 3:41:32PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 1/11/2007 2:28:31AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Jeffrey Dolsen**Tracking #:** 2006-USCERT1BMP4T

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 12/07/06 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Other**Incident Status:** Unknown**Impact:** Medium**# Sites:** 1**# Systems:** 1**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

An agency reported a laptop was taken from a locked unmarked police vehicle. The laptop contained no PII. Three officer evaluation reports listing the name and SSN's were saved to the desk top. All of the individuals were advised of the theft, and were advised to be extra vigilant to prevent unauthorized use of there personal information.

Ticket Status: CLOSED On 01/11/07 at 2:28:25PM

US#037642 Created: 12/11/2006 8:53:37PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Privileged Account or System Access**PII Involved:** Yes

Last Edited: 2/8/2007 9:26:32AM

Report Method: Web**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** RCERT-CONUS**Tracking #:** 747182 and 747187

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 11/30/06 13:16**Timezone:** GMT + 06 (UTC + 06)**Identified By:** Not Reported**Incident Status:** Not Reported**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** 2**Function:** Not Reported**OS:** Windows 2003 Server**AV:** Not Reported

An agency reports two file servers containing EPHI/PII were identified with rootkits. One server is windows 2000, the other is windows 2003. The impact is unknown. It has not been determined if the data was compromised.

Ticket Status: CLOSED On 01/24/07 at 10:21:46PM

US#036361 Created: 12/4/2006 12:32:39PM

Problem Type: 04-Improper Usage**Sub-Type:** Policy Violation**PII Involved:** Yes

Last Edited: 12/5/2006 5:15:11AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Daniel Kwon**Tracking #:** 2006-USCERT1KZ2CK

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 12/01/06 16:43**Timezone:** Eastern Standard Time - EST**Identified By:** 3rd Party**Incident Status:** Open**Impact:** High**# Sites:** 1**# Systems:** 1**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

Agency reports employee used PII to conduct fraud involving insurance company. It is suspected that 25 individuals may be affected. CID is involved and will notify all suspected individuals of the investigative process.

Ticket Status: CLOSED On 12/04/06 at 12:44:54PM

US#036313 Created: 12/4/2006 9:59:31AM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 12/5/2006 6:05:43AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Fred Adams**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA) / UNITED STATES ARMY RECRUITING COMMAND**Occurred:** 12/02/06 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** 3rd Party**Incident Status:** Open**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Laptop**OS:** Not Reported**AV:** Installed

Agency reports that a laptop was stolen from individuals POV. The laptop contained PII but needs an access card and PIN to view the information.

Ticket Status: CLOSED On 12/04/06 at 10:16:58AM

US#036175 Created: 12/2/2006 4:22:20PM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 12/4/2006 1:25:56AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Fred Adams

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 12/01/06 16:22

Timezone: Eastern Standard Time - EST

Identified By: 3rd Party

Incident Status: Open

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Not Reported

AV: Not Reported

Agency reports that a laptop was stolen in a department store parking lot. The laptop contained PII but needed an access card and PIN to view the information.

Ticket Status: CLOSED On 12/02/06 at 4:25:03PM

US#036124 Created: 12/1/2006 9:58:11PM

Problem Type: 01-Unauthorized Access

Sub-Type: Privileged Account or System Access

PII Involved: Yes

Last Edited: 12/4/2006 6:29:41AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: John Joray

Tracking #: 07C03837

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 11/28/06 15:46

Timezone: Eastern Standard Time - EST

Identified By: Not Reported

Incident Status: Not Reported

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Windows XP

AV: Not Reported

DOD Agency reported a system had been compromised by malware, which created a back door.

Ticket Status: CLOSED On 12/01/06 at 10:12:33PM

US#035847 Created: 11/29/2006 5:32:22PM

Problem Type: 04-Improper Usage

Sub-Type: Data Spillage

PII Involved: Yes

Last Edited: 11/30/2006 2:19:59AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Frank Richard

Tracking #: 2006-USCERT1UAV9J

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)

Occurred: 11/29/06 0:00

Timezone: Eastern Standard Time - EST

Identified By: Other

Incident Status: Unknown

Impact: Medium

Sites: 1

Systems: 1

Function: Web Server

OS: Windows XP

AV: Installed

An agency has reported a questionnaire that is used for acquiring data, was placed on a website, with PII stored on it. The questionnaire contains individual's names, home addresses, phone numbers, social security numbers, and emergency POC'S.

Ticket Status: SUSPEND

US#034665 Created: 11/20/2006 3:13:12PM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 11/29/2007 2:26:54AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: UNITED STATES ARMY RECRUITING COMMAND

Tracking #: 2006-USCERT2RJ2X7

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA) / 1

Occurred: 11/20/06 11:13

Timezone: Eastern Standard Time - EST

Identified By: 3rd Party

Incident Status: Open

Impact: High

Sites: 1

Systems: 1

Function: Other

OS: Windows XP

AV: Installed

An agency reported a Docking Station with hard disk used for laptop backup was FedEx to Dell for repair. The disk contained PII.

Ticket Status: CLOSED On 12/03/06 at 12:56:50PM

US#034099 Created: 11/15/2006 1:44:35PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 11/16/2006 8:07:27AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Fred Adams**Tracking #:** 2006-USCERT2UBYP5

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 11/14/06 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Other**Incident Status:** Unknown**Impact:** Medium**# Sites:** 1**# Systems:** 1**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

An agency has reported a stolen laptop from a personal vehicle. The vehicle was forced into and the computer removed. Impact of PII is unknown. Local police authorities are investigating.

Ticket Status: CLOSED On 11/15/06 at 1:47:59PM

US#032804 Created: 11/6/2006 6:03:12PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 11/6/2006 6:21:22AM

Report Method: Web**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Deborah Joseph**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 11/03/06 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Other**Incident Status:** Not Reported**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** 1**Function:** Laptop**OS:** Windows XP**AV:** Installed

An agency reports the theft of a laptop. The laptop contained PII.

Ticket Status: CLOSED On 11/06/06 at 6:08:59PM

US#032786 Created: 11/6/2006 3:34:55PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 11/7/2006 7:15:23AM

Report Method: Web**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Fred Adams**Tracking #:** 2006-USCERT4780WJ

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA) / UNITED STATES ARMY RECRUITING COMMAND**Occurred:** 11/05/06 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** 3rd Party**Incident Status:** Not Reported**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** 1**Function:** Laptop**OS:** Not Reported**AV:** Not Reported

An agency reports the theft of a laptop containing PII of approximately 30,000 individuals.

Ticket Status: CLOSED On 11/06/06 at 3:39:34PM

US#031951 Created: 10/30/2006 2:54:40PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 10/30/2006 2:05:46AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Fred Adams**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA) / UNITED STATES ARMY RECRUITING COMMAND**Occurred:** 10/30/06 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** User**Incident Status:** Closed**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** 1**Function:** Laptop**OS:** Not Reported**AV:** Not Reported

Agency reports a member was held up at gunpoint while at an ATM in his POV. The member's wallet and Government computer were stolen. Local police are investigating whether or not PII information was present on the laptop.

Ticket Status: CLOSED On 10/30/06 at 2:59:32PM

US#031348 Created: 10/24/2006 7:51:53PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 10/25/2006 7:31:09AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** FREDERICK ADAMS**Tracking #:** 2006-USCERT24DOTM

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 10/24/06 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Other**Incident Status:** Unknown**Impact:** Medium**# Sites:** 1**# Systems:** 1**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

An agency has reported that one of their employees was carjacked while conducting business. The vehicle was recovered, but the laptop was stolen. Individual employees PII was stored on the laptop. The local police departments were notified, and are conducting an investigation.

Ticket Status: CLOSED On 10/24/06 at 8:09:23PM

US#031239 Created: 10/24/2006 8:07:42AM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 10/31/2006 2:11:49AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Frederick Adams**Tracking #:** 07-USAAC-2

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 10/24/06 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Not Reported**Incident Status:** Not Reported**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Laptop**OS:** Not Reported**AV:** Not Reported

US-CERT received an incident report involving PII. A laptop was reported stolen from a cubicle inside a government building. The laptop contained names, addresses, SSN, DOB, phone numbers, and mother's maiden names. The reporting party didn't reveal how many people are affected.

Ticket Status: CLOSED On 10/25/06 at 6:20:10AM

US#030680 Created: 10/18/2006 11:29:12AM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 11/13/2006 7:31:00AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** James Mark**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 10/18/06 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Not Reported**Incident Status:** Open**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Laptop**OS:** Windows XP**AV:** Not Reported

Agency reports the theft of a government laptop. The notebook was access controlled by smart card. It contains Privacy Act information on an estimated 15 personnel, which can be identified. The initial start up screen identifies the system as a federal government computer and that further access is a federal crime. The hard drive was not encrypted.

Ticket Status: CLOSED On 11/13/06 at 7:30:54AM

US#030506 Created: 10/16/2006 8:02:35PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 10/17/2006 2:28:07AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Fred Adams**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA) / UNITED STATES ARMY RECRUITING COMMAND**Occurred:** 10/15/06 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** 3rd Party**Incident Status:** Closed**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** 1**Function:** Laptop**OS:** Not Reported**AV:** Not Reported

Agency reports that a laptop stolen from an POV that was secured. Laptop may have had unknown number of possible agency prospects names, addresses and phone numbers. Police were notified.

Ticket Status: CLOSED On 10/16/06 at 8:07:52PM

US#029920 Created: 10/11/2006 2:51:22PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 10/18/2006 2:56:18AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Linda Genovese**Tracking #:** 2006-USCERT1D7V62

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Army (USA)**Occurred:** 09/20/06 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Other**Incident Status:** Unknown**Impact:** Medium**# Sites:** 1**# Systems:** 1**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

An agency has reported a total of 4 laptop computers were stolen by an individual. The intruder was photographed by security cameras where each laptop was stolen. Federal police arrived, initiating an investigation.

Ticket Status: CLOSED On 10/18/06 at 2:55:52PM

US#052063 Created: 4/11/2007 3:39:16PM

Problem Type: 06-Investigation**Sub-Type:** Non Cyber**PII Involved:** Yes

Last Edited: 4/12/2007 4:00:56AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Donna Williamson**Tracking #:** #2007-USCERT1Z0CKA

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Defense Commissary Agency**Occurred:** 04/11/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Other**Incident Status:** Unknown**Impact:** Medium**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

An agency reports an employee erroneously addressed the wrong address and sent a PII record on an individual to the wrong employee. The record is being shipped back to the agency.

Ticket Status: CLOSED On 04/11/07 at 3:45:00PM

US#051455 Created: 4/5/2007 1:32:28PM

Problem Type: 04-Improper Usage**Sub-Type:** Policy Violation**PII Involved:** Yes

Last Edited: 4/5/2007 11:47:06AM

Report Method: Web**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Donna Williamson**Tracking #:** PV 07-001

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Defense Commissary Agency**Occurred:** 04/05/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Not Reported**Incident Status:** Open**Impact:** Unknown**# Sites:** 1**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

An agency reports a store timekeeper kept a document containing PII in a personal locker. An attached post-it-note also containing PII fell off the document and was found by another employee.

Ticket Status: CLOSED On 04/05/07 at 2:32:44PM

US#053275 Created: 4/23/2007 2:52:46PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 4/24/2007 3:51:44AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:****Tracking #:** 15160

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Defense Contract and Audit Agency (DCAA)**Occurred:** 04/21/07 14:52**Timezone:** Eastern Standard Time - EST**Identified By:** 3rd Party**Incident Status:** Open**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

Agency reports laptop stolen from vehicle. PII was involved.

Ticket Status: CLOSED On 04/23/07 at 2:57:38PM

US#051257 Created: 4/3/2007 1:52:05PM

Last Edited: 4/3/2007 10:56:39AM

Assigned To: Incident Handling

Problem Type: 01-Unauthorized Access**Report Method:** Email**Sub-Type:** Equipment**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Mark Frank**Tracking #:** 14780**Impacted Party:** Department of Defense (DOD) / Defense Contract and Audit Agency (DCAA)**Occurred:** 02/09/07 0:00**Impact:** Medium**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** 1**OS:** Not Reported**Identified By:** Other**# Systems:** 1**AV:** Not Reported**Incident Status:** Unknown

An agency reports a missing desktop computer with possible PII data stored on it. The computer was discovered missing during an agency inventory.

Ticket Status: CLOSED On 04/03/07 at 1:54:55PM

US#042577 Created: 1/29/2007 5:34:55PM

Last Edited: 1/30/2007 3:44:56AM

Assigned To: Incident Handling

Problem Type: 01-Unauthorized Access**Report Method:** Web**Sub-Type:** Equipment**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** JTF-GNO**Tracking #:** 13588**Impacted Party:** Department of Defense (DOD) / Defense Contract and Audit Agency (DCAA)**Occurred:** 01/26/07 18:30**Impact:** Not Reported**Function:** Laptop**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Windows XP**Identified By:** User**# Systems:** 1**AV:** Installed**Incident Status:** Not Reported

An agency reports an employee's laptop was stolen. The laptop contained PII on 16 individuals.

Ticket Status: CLOSED On 01/29/07 at 5:39:40PM

US#034377 Created: 11/17/2006 5:17:11PM

Last Edited: 1/29/2007 2:37:03AM

Assigned To: Incident Handling

Problem Type: 01-Unauthorized Access**Report Method:** Web**Sub-Type:** Equipment**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Mark.Frank**Tracking #:** 12481**Impacted Party:** Department of Defense (DOD) / Defense Contract and Audit Agency (DCAA)**Occurred:** 11/17/06 0:00**Impact:** Not Reported**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Not Reported**Identified By:** User**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Not Reported

Agency reports lost laptop that may have contained PII. Incident is being investigated.

Ticket Status: CLOSED On 11/17/06 at 5:21:49PM

US#039939 Created: 1/5/2007 12:05:24PM

Last Edited: 2/8/2007 8:59:25AM

Assigned To: Incident Handling

Problem Type: 01-Unauthorized Access**Report Method:** Email**Sub-Type:** Privileged Account or System Access**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Renee Speed**Tracking #:** 01042007**Impacted Party:** Department of Defense (DOD) / Defense Finance and Accounting Service (DFAS)**Occurred:** 01/03/07 0:00**Impact:** Not Reported**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Windows XP**Identified By:** 3rd Party**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Open

Four individuals had their pay accounts accessed. Their direct deposit information was changed. The accounts where the funds were deposited were pre-paid debit card accounts. All accounts were locked by the servicing bank. The Defense Criminal Investigative Service (DCIS) is currently investigating.

Ticket Status: ASSIGNED

US#054148 Created: 5/3/2007 10:36:20AM

Last Edited: 5/4/2007 12:24:36PM

Assigned To: Incident Handling

Problem Type: 04-Improper Usage**Report Method:** Email**Sub-Type:** Policy Violation**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Defense Logistics Agency CERT**Tracking #:** # 2007-0503-8108**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)**Occurred:** 05/03/07 0:00**Impact:** Medium**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** 1**OS:** Not Reported**Identified By:** Other**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Unknown

An agency reports an employee sent several unencrypted emails containing PII to other individuals on the network.

Ticket Status: CLOSED On 05/03/07 at 10:39:52AM

US#054109 Created: 5/2/2007 3:03:08PM

Last Edited: 5/3/2007 10:18:31AM

Assigned To: Incident Handling

Problem Type: 04-Improper Usage**Report Method:** Email**Sub-Type:** Policy Violation**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Defense Logistics Agency CERT**Tracking #:** 2007-0502-8107**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)**Occurred:** 05/02/07 0:00**Impact:** Medium**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** 1**OS:** Not Reported**Identified By:** Other**# Systems:** 1**AV:** Not Reported**Incident Status:** Unknown

An agency reports an employee sent an unencrypted email containing PII to another employee.

Ticket Status: CLOSED On 05/02/07 at 3:05:25PM

US#053666 Created: 4/27/2007 6:06:10PM

Last Edited: 4/27/2007 6:13:08AM

Assigned To: Incident Handling

Problem Type: 04-Improper Usage**Report Method:** Email**Sub-Type:** Policy Violation**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Defense Logistics Agency CERT**Tracking #:** 2007-0427-9518**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)**Occurred:** 04/27/07 0:00**Impact:** Not Reported**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Not Reported**Identified By:** Not Reported**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Not Reported

Agency reports that an email with four people's PII was sent without proper encryption. Agency is cleaning email servers of the information.

Ticket Status: CLOSED On 04/27/07 at 6:08:41PM

US#052681 Created: 4/18/2007 10:58:58AM

Last Edited: 4/20/2007 1:55:40AM

Assigned To: Incident Handling

Problem Type: 04-Improper Usage**Report Method:** Email**Sub-Type:** Policy Violation**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Defense Logistics Agency CERT**Tracking #:** 2007-0419-8106**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)**Occurred:** 04/18/07 0:00**Impact:** Medium**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** 1**OS:** Not Reported**Identified By:** Other**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Closed

An agency reports an individual received an unencrypted email containing personal identifiable information (PII).

Ticket Status: CLOSED On 04/18/07 at 11:03:20AM

US#051796 Created: 4/9/2007 10:00:04AM

Last Edited: 4/10/2007 3:01:59AM

Assigned To: Analysis

Problem Type: 06-Investigation**Report Method:** Email**Sub-Type:** Non Cyber**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Defense Logistics Agency CERT**Tracking #:** 2007-0406-5501**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)**Occurred:** 04/09/07 0:00**Impact:** Not Reported**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Not Reported**Identified By:** 3rd Party**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Open

An agency reports that documentation containing PII was found in a dumpster. The documentation was removed from the dumpster and the agency is investigating.

Ticket Status: CLOSED On 04/09/07 at 10:13:00AM

US#049944 Created: 3/23/2007 2:03:34PM

Last Edited: 3/28/2007 4:41:34AM

Assigned To: Incident Handling

Problem Type: 01-Unauthorized Access**Report Method:** Email**Sub-Type:** Data Exfiltration**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Defense Logistics Agency CERT**Tracking #:** 2007-0323-3050**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)**Occurred:** 03/23/07 14:03**Impact:** Not Reported**Function:** Web Server**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Not Reported**Identified By:** Not Reported**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Not Reported

Agency reports an incident involving PII. A webpage allows browser to search for and obtain information regarding employee cases filed with The Equal Employment Opportunity Commission (EEOC). Search feature has been disabled and appropriate actions are being taken to fully resolve the issue.

Ticket Status: ASSIGNED

US#049863 Created: 3/22/2007 5:20:43PM

Last Edited: 3/23/2007 4:34:06AM

Assigned To: Incident Handling

Problem Type: 01-Unauthorized Access**Report Method:** Email**Sub-Type:** Equipment**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Defense Logistics Agency CERT**Tracking #:** 2007-0322-9505**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)**Occurred:** 03/22/07 0:00**Impact:** Medium**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** 1**OS:** Not Reported**Identified By:** Other**# Systems:** 1**AV:** Not Reported**Incident Status:** Unknown

An agency reports a laptop missing. The laptop has PII data stored on it. The agency is unsure if the data was compromised.

Ticket Status: CLOSED On 03/22/07 at 5:22:52PM

US#049432 Created: 3/19/2007 12:37:17PM

Last Edited: 3/20/2007 4:16:34AM

Assigned To: Incident Handling

Problem Type: 06-Investigation**Report Method:** Email**Sub-Type:** Non Cyber**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Defense Logistics Agency CERT**Tracking #:** 2007-0319-9504**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)**Occurred:** 03/19/07 0:00**Impact:** Not Reported**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Not Reported**Identified By:** Not Reported**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Unknown

An agency reports PII was found in a public internal folder. The data was openly accessible to a sub-agency's personnel.. The information was removed.

Ticket Status: CLOSED On 03/19/07 at 12:45:05PM

US#048932 Created: 3/15/2007 4:38:42PM

Last Edited: 3/16/2007 6:26:09AM

Assigned To: Incident Handling

Problem Type: 04-Improper Usage**Report Method:** Email**Sub-Type:** Policy Violation**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Defense Logistics Agency CERT**Tracking #:** 2007-0315-1445**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)**Occurred:** 03/15/07 0:00**Impact:** Medium**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** 1**OS:** Not Reported**Identified By:** Other**# Systems:** 1**AV:** Not Reported**Incident Status:** Unknown

An agency reported an employee accidentally emailed one employee's records that were being scanned.

Ticket Status: CLOSED On 03/15/07 at 4:40:44PM

US#047605 Created: 3/6/2007 2:24:28PM

Last Edited: 4/26/2007 12:31:24PM

Assigned To: Incident Handling

Problem Type: 04-Improper Usage**Report Method:** Email**Sub-Type:** Data Spillage**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Defense Logistics Agency CERT**Tracking #:** 2007-0301-2130**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)**Occurred:** 03/06/07 0:00**Impact:** Medium**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** 1**OS:** Not Reported**Identified By:** Other**# Systems:** 1**AV:** Not Reported**Incident Status:** Unknown

An agency reported a shared folder with approximately 8000 individuals PII data. The permissions allowed unauthorized individuals to gain access.

Ticket Status: CLOSED On 04/26/07 at 12:30:36AM

US#040425 Created: 1/10/2007 1:54:19PM

Last Edited: 1/10/2007 2:04:17AM

Assigned To: Incident Handling

Problem Type: 04-Improper Usage**Report Method:** Email**Sub-Type:** Policy Violation**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Defense Logistics Agency CERT**Tracking #:** 2007-0110-9501**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)**Occurred:** 01/10/07 0:00**Impact:** Not Reported**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Not Reported**Identified By:** Not Reported**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Not Reported

Agency reports an e-mail containing PII was discovered in a public folder. The e-mail has been removed from the folder.

Ticket Status: CLOSED On 01/10/07 at 1:56:59PM

US#038167 Created: 12/15/2006 2:10:34PM

Last Edited: 1/3/2007 9:28:02AM

Assigned To: Incident Handling

Problem Type: 04-Improper Usage**Report Method:** Email**Sub-Type:** Policy Violation**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Defense Logistics Agency CERT**Tracking #:** 2006-1213-9989**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)**Occurred:** 12/15/06 0:00**Impact:** Not Reported**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Not Reported**Identified By:** User**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Not Reported

Agency reports employee emailed PII to wrong recipient. Agency is investigating incident.

Ticket Status: CLOSED On 01/03/07 at 9:27:55AM

US#037132 Created: 12/8/2006 6:02:38PM

Last Edited: 12/27/2006 5:19:44AM

Assigned To: Analysis

Problem Type: 06-Investigation**Report Method:** Email**Sub-Type:** Unconfirmed Report**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Defense Logistics Agency CERT**Tracking #:** Not Reported**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)**Occurred:** 12/08/06 18:02**Impact:** Not Reported**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Not Reported**Identified By:** Not Reported**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Not Reported

Agency reported removing a .pdf document from its web page because it may have contained PII in its metadata.

Ticket Status: CLOSED On 12/27/06 at 2:28:58PM

US#036801 Created: 12/6/2006 5:37:19PM

Last Edited: 12/27/2006 7:40:43AM

Assigned To: Incident Handling

Problem Type: 04-Improper Usage**Report Method:** Email**Sub-Type:** Policy Violation**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Defense Logistics Agency**Tracking #:** 2006-1206-3056**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)**Occurred:** 12/06/06 0:00**Impact:** Not Reported**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Not Reported**Identified By:** User**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Not Reported

An agency reported the HRC released a Personnel Employee Bulletin, a released newsletter contained two names, social security numbers and birth dates for two employees. Bulletin is being removed from systems. PII Involved.

Ticket Status: CLOSED On 12/27/06 at 7:40:33PM

US#047400 Created: 3/5/2007 3:19:11PM

Last Edited: 3/12/2007 4:01:46AM

Assigned To: Incident Handling

Problem Type: 04-Improper Usage**Report Method:** Email**Sub-Type:** Policy Violation**Reporting Sector:** Agency (Department of Veterans Affairs)**PII Involved:** Yes**Reported By:** VASOC**Tracking #:** VA03566**Impacted Party:** Department of Defense (DOD) / Joint Task Force-Global Network Operations (JTF-GNO)**Occurred:** 03/05/07 19:52**Impact:** Not Reported**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Not Reported**Identified By:** Not Reported**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Open

Agency reports unencrypted email received by an employee containing PII.

Ticket Status: CLOSED On 03/05/07 at 3:21:19PM

US#038078 Created: 12/14/2006 11:17:51PM

Last Edited: 1/4/2007 1:21:09AM

Assigned To: Incident Handling

Problem Type: 06-Investigation**Report Method:** Email**Sub-Type:** Non Cyber**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:****Tracking #:** Not Reported**Impacted Party:** Department of Defense (DOD) / Joint Task Force-Global Network Operations (JTF-GNO)**Occurred:** 12/14/06 0:00**Impact:** Not Reported**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Not Reported**Identified By:** Not Reported**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Not Reported

An organization reports the possible compromise of 100 military member records. Forwarded information to the DOD contingency for there action.

Ticket Status: CLOSED On 01/04/07 at 1:19:37AM

US#036084 Created: 12/1/2006 4:15:57PM

Last Edited: 4/11/2007 11:48:13AM

Assigned To: Incident Handling

Problem Type: 01-Unauthorized Access**Report Method:** Email**Sub-Type:** Network**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Joseph Gudsnuk**Tracking #:** US-CERT - 2006-USCERT3USU76**Impacted Party:** Department of Defense (DOD) / Joint Task Force-Global Network Operations (JTF-GNO)**Occurred:** 12/01/06 0:00**Impact:** Not Reported**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Not Reported**Identified By:** 3rd Party**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Not Reported

Agency reports network compromised by an attack on its Domain Controller. Initial investigation was performed. Forensics and mitigation are ongoing. Agency reports potential PII compromised.

Ticket Status: CLOSED On 04/11/07 at 11:48:02PM

US#034384 Created: 11/17/2006 6:36:16PM

Last Edited: 1/29/2007 2:39:25AM

Assigned To: Incident Handling

Problem Type: 01-Unauthorized Access**Report Method:** Web**Sub-Type:** Non Privileged Account or System Access**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** dennis.eger**Tracking #:** 2006-USCERTD9F89**Impacted Party:** Department of Defense (DOD) / Joint Task Force-Global Network Operations (JTF-GNO)**Occurred:** 11/17/06 0:00**Impact:** Not Reported**Function:** Other**Timezone:** Eastern Standard Time - EST**# Sites:** 1**OS:** Windows XP**Identified By:** Log Review**# Systems:** 1**AV:** Installed**Incident Status:** Open

Agency reports malicious code used to compromise an admin host that has PII contained on it. System has been taken off-line and the drive is being analyzed by the agency's incident response team.

Ticket Status: CLOSED On 01/07/07 at 8:55:01AM

US#054328 Created: 5/5/2007 1:11:41PM

Last Edited: 5/7/2007 12:38:53PM

Assigned To: Incident Handling

Problem Type: 06-Investigation**Report Method:** Email**Sub-Type:** Non Cyber**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Steven Michel**Tracking #:** Not Reported**Impacted Party:** Department of Defense (DOD) / Marine Corps (USMC)**Occurred:** 05/04/07 0:00**Impact:** Not Reported**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Not Reported**Identified By:** User**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Not Reported

Agency reports lost thumbdrive containing PII.

Ticket Status: CLOSED On 05/05/07 at 1:22:41PM

US#051249 Created: 4/3/2007 12:22:02PM

Last Edited: 4/3/2007 10:53:28AM

Assigned To: Incident Handling

Problem Type: 01-Unauthorized Access**Report Method:** Email**Sub-Type:** Equipment**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** MDACIRT**Tracking #:** MIRS 7082**Impacted Party:** Department of Defense (DOD) / Missile Defense Agency (MDA)**Occurred:** 04/02/07 0:00**Impact:** Medium**Function:** Blackberry/PDA/Mobile Agent**Timezone:** Eastern Standard Time - EST**# Sites:** 1**OS:** Not Reported**Identified By:** Other**# Systems:** 1**AV:** Not Reported**Incident Status:** Unknown

An agency reports an employee lost their agency issued blackberry, while fulfilling a Temporary Duty Assignment in a foreign country. The Blackberry contained PII data.

Ticket Status: CLOSED On 04/03/07 at 12:25:32PM

US#041820 Created: 1/23/2007 10:38:44AM

Last Edited: 1/23/2007 10:46:04AM

Assigned To: Incident Handling

Problem Type: 04-Improper Usage**Report Method:** Email**Sub-Type:** Policy Violation**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Chris Lee**Tracking #:** 2007-490**Impacted Party:** Department of Defense (DOD) / National Security Agency (NSA)**Occurred:** 01/23/07 0:00**Impact:** Medium**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** 1**OS:** Windows 2000 Professional**Identified By:** 3rd Party**# Systems:** 1**AV:** Installed**Incident Status:** Unknown

Agency reports an email was sent to 40+ people containing SSNs. The SSNs of 24 individuals were compromised.

Ticket Status: CLOSED On 01/23/07 at 10:42:36AM

US#039692 Created: 1/3/2007 9:54:40AM

Last Edited: 1/4/2007 3:02:54AM

Assigned To: Incident Handling

Problem Type: 04-Improper Usage**Report Method:** Email**Sub-Type:** Policy Violation**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:****Tracking #:** 1566**Impacted Party:** Department of Defense (DOD) / National Security Agency (NSA)**Occurred:** 12/29/06 0:00**Impact:** Medium**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** 1**OS:** Not Reported**Identified By:** Other**# Systems:** 1**AV:** Not Reported**Incident Status:** Unknown

An agency reports documents with PII data on several individuals is posted on four different unencrypted websites. The agency states some PII data may have been compromised.

Ticket Status: CLOSED On 01/03/07 at 3:22:51PM

US#039235 Created: 12/27/2006 11:40:31AM

Last Edited: 2/9/2007 1:21:13AM

Assigned To: Incident Handling

Problem Type: 01-Unauthorized Access**Report Method:** Email**Sub-Type:** Equipment**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:****Tracking #:** 1422**Impacted Party:** Department of Defense (DOD) / National Security Agency (NSA)**Occurred:** 11/14/06 0:00**Impact:** Medium**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** 1**OS:** Not Reported**Identified By:** Other**# Systems:** 1**AV:** Not Reported**Incident Status:** Unknown

An agency has reported the loss of a laptop with PII stored on it. The data contains SSN's, full names, and test results that effect 73 individuals. The laptop has not been found, and is believed to have possibly been compromised.

Ticket Status: CLOSED On 02/09/07 at 1:21:03AM

US#030679 Created: 10/18/2006 11:19:01AM

Last Edited: 10/25/2006 11:01:40AM

Assigned To: Incident Handling

Problem Type: 04-Improper Usage**Report Method:** Email**Sub-Type:** Policy Violation**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** NSA**Tracking #:** CSIR-2006-1295**Impacted Party:** Department of Defense (DOD) / National Security Agency (NSA)**Occurred:** 10/18/06 0:00**Impact:** Medium**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** 1**OS:** Not Reported**Identified By:** Other**# Systems:** 1**AV:** Not Reported**Incident Status:** Unknown

An agency has reported a user on an internal classified network discovered a shared folder after a review for PII criteria reporting. PII was stored in the folder.

Ticket Status: CLOSED On 10/25/06 at 11:01:33AM

US#054416 Created: 5/7/2007 8:18:02AM

Problem Type: 06-Investigation

Sub-Type: Other

PII Involved: Yes

Last Edited: 5/7/2007 11:54:59AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: David German

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Navy (USN)

Occurred: 05/04/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Not Reported

Incident Status: Closed

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Not Reported

AV: Not Reported

An agency reports potential compromise of fitness report data. The data was inadvertently posted to a non-agency website. The file was immediately removed from the site. PII was involved.

Ticket Status: CLOSED On 05/07/07 at 8:21:24AM

US#054282 Created: 5/4/2007 6:17:01PM

Problem Type: 04-Improper Usage

Sub-Type: Policy Violation

PII Involved: Yes

Last Edited: 5/4/2007 6:24:07AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: LCDR Bill Batson

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Navy (USN)

Occurred: 05/04/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Not Reported

Incident Status: Not Reported

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Not Reported

AV: Not Reported

Agency reports that PII was posted on an internal webpage. Once the error was found, the material was removed. Two individuals were affected.

Ticket Status: CLOSED On 05/04/07 at 6:20:37PM

US#053584 Created: 4/26/2007 10:34:41AM

Problem Type: 04-Improper Usage

Sub-Type: Policy Violation

PII Involved: Yes

Last Edited: 4/26/2007 11:37:10AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Bill Batson

Tracking #: #2007-USCERT24W5IY

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Navy (USN)

Occurred: 04/25/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Other

Incident Status: Unknown

Impact: Medium

Sites: 1

Systems: 1

Function: Not Reported

OS: Not Reported

AV: Not Reported

An agency reports an employee sent an email that contained an attachment with a spreadsheet. The spreadsheet contained PII data. The spreadsheet was sent to several senior leaders.

Ticket Status: CLOSED On 04/26/07 at 10:37:14AM

US#053257 Created: 4/23/2007 1:52:21PM

Problem Type: 06-Investigation

Sub-Type: Non Cyber

PII Involved: Yes

Last Edited: 4/24/2007 4:55:46AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: william batson

Tracking #: 301540ZNOV06

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Navy (USN) / DON CIO (Naval Information Systems Management)

Occurred: 04/23/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: 3rd Party

Incident Status: Not Reported

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Not Reported

AV: Not Reported

An agency reports web application containing guides used for training have actual PII listed within training screen shots. The guides are scheduled to be rewritten using fictional information.

Ticket Status: CLOSED On 04/23/07 at 2:01:35PM

US#052835 Created: 4/19/2007 1:20:20PM

Last Edited: 4/23/2007 8:44:47AM

Assigned To: Incident Handling

Problem Type: 01-Unauthorized Access**Report Method:** Email**Sub-Type:** Non Privileged Account or System Access**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Matthew Haws**Tracking #:** 2007.103558**Impacted Party:** Department of Defense (DOD) / Navy (USN)**Occurred:** 04/19/07 0:00**Impact:** Medium**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** 1**OS:** Not Reported**Identified By:** Other**# Systems:** 1**AV:** Not Reported**Incident Status:** Unknown

An agency reports an individual accessed an agency system and obtained PII data on several individuals and he created false ID cards with their information. The local law enforcement is investigating this incident.

Ticket Status: CLOSED On 04/19/07 at 1:22:54PM

US#052350 Created: 4/16/2007 9:56:56AM

Last Edited: 4/17/2007 2:04:50AM

Assigned To: Incident Handling

Problem Type: 01-Unauthorized Access**Report Method:** Email**Sub-Type:** Equipment**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Jennie Humes**Tracking #:** none present**Impacted Party:** Department of Defense (DOD) / Navy (USN)**Occurred:** 03/09/07 0:00**Impact:** Not Reported**Function:** Laptop**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Not Reported**Identified By:** Not Reported**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Not Reported

An agency reports 148 new and 3 used laptop computers were stolen. The older laptops contained PII and college course information of students from 2003 to 2005.

Ticket Status: RE-OPENED

US#051635 Created: 4/6/2007 4:51:46PM

Last Edited: 4/6/2007 5:12:32AM

Assigned To: Incident Handling

Problem Type: 06-Investigation**Report Method:** Email**Sub-Type:** Non Cyber**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Angela Hanson**Tracking #:** Not Reported**Impacted Party:** Department of Defense (DOD) / Navy (USN)**Occurred:** 02/26/07 0:00**Impact:** Not Reported**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** Not Reported**OS:** Not Reported**Identified By:** Not Reported**# Systems:** Not Reported**AV:** Not Reported**Incident Status:** Open

An agency reports PII was lost in a FedEx shipment affecting two individuals.

Ticket Status: ASSIGNED

US#049737 Created: 3/21/2007 6:19:16PM

Last Edited: 3/22/2007 4:29:53AM

Assigned To: Incident Handling

Problem Type: 06-Investigation**Report Method:** Email**Sub-Type:** Non Cyber**Reporting Sector:** Agency (Department of Defense (DOD))**PII Involved:** Yes**Reported By:** Ellen J. Sharp**Tracking #:** 2007.76029**Impacted Party:** Department of Defense (DOD) / Navy (USN)**Occurred:** 03/21/07 0:00**Impact:** Medium**Function:** Not Reported**Timezone:** Eastern Standard Time - EST**# Sites:** 1**OS:** Not Reported**Identified By:** Other**# Systems:** 1**AV:** Not Reported**Incident Status:** Unknown

An agency reported application paperwork for three individuals is missing. The documents were left on a desk overnight and cannot be located. PII was involved.

Ticket Status: CLOSED On 03/21/07 at 6:22:23PM

US#049448 Created: 3/19/2007 1:44:25PM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 3/30/2007 10:27:05AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Sims, Pettis N USA ENS USN NMCB 133

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Navy (USN)

Occurred: 03/12/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: User

Incident Status: Closed

Impact: Not Reported

Sites: 1

Systems: 1

Function: Other

OS: Not Reported

AV: Not Reported

An agency has reported that a thumb drive containing PII on 653 personnel was lost. The data was not encrypted or password protected.

Ticket Status: ASSIGNED

US#049016 Created: 3/16/2007 9:17:00AM

Problem Type: 04-Improper Usage

Sub-Type: Policy Violation

PII Involved: Yes

Last Edited: 3/16/2007 9:25:36AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Cain, Danny K CNRFC

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Navy (USN)

Occurred: 03/16/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Administrator

Incident Status: Closed

Impact: Not Reported

Sites: 1

Systems: Not Reported

Function: Not Reported

OS: Not Reported

AV: Not Reported

An agency is reporting that an excel spreadsheet was published on a public facing website on the 7th of Dec 2006. The spreadsheet contained 105 SSNs of individuals.

Ticket Status: CLOSED On 03/16/07 at 9:21:37AM

US#048695 Created: 3/13/2007 2:04:52PM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 3/14/2007 5:40:28AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By:

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Navy (USN)

Occurred: 11/30/06 0:00

Timezone: Eastern Standard Time - EST

Identified By: User

Incident Status: Closed

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Other

OS: Not Reported

AV: Not Reported

An agency reports that a members car was broken into, and a flash drive containing evaluations for four unit members was stolen. The drive was not encrypted or password protected. PII was involved.

Ticket Status: CLOSED On 03/13/07 at 2:07:38PM

US#048522 Created: 3/12/2007 5:19:42PM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 3/13/2007 6:27:18AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: JTF-GNO

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Navy (USN) / DON CIO (Naval Information Systems Management)

Occurred: 03/12/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Other

Incident Status: Closed

Impact: High

Sites: 1

Systems: 153

Function: Laptop

OS: Not Reported

AV: Not Reported

An agency reports the lost of around 150 laptops, 3 of which contain personally identifiable information.

Ticket Status: CLOSED On 03/12/07 at 5:22:42PM

US#047805 Created: 3/7/2007 7:09:55PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 3/13/2007 1:59:40AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:****Tracking #:** Thumb Drive - US-CERT - 2007-USCERT339RHX

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Navy (USN)**Occurred:** 03/05/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** User**Incident Status:** Closed**Impact:** Not Reported**Function:** Other**# Sites:** Not Reported**OS:** Windows XP**# Systems:** Not Reported**AV:** Not Installed

An agency reports a lost USB drive that contained an alpha roster. The alpha roster accounts for 200 assigned personnel. PII was involved.

Ticket Status: CLOSED On 03/07/07 at 7:16:33PM

US#043968 Created: 2/7/2007 9:11:21AM

Problem Type: 06-Investigation**Sub-Type:** Non Cyber**PII Involved:** Yes

Last Edited: 2/7/2007 9:56:35AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** JTF-GNO**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Navy (USN)**Occurred:** 02/02/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Not Reported**Incident Status:** Not Reported**Impact:** Not Reported**Function:** Not Reported**# Sites:** Not Reported**OS:** Not Reported**# Systems:** Not Reported**AV:** Not Reported

Agency member reports a list of names and SSN's were lost while being transported. The individuals affected were notified.

Ticket Status: CLOSED On 02/07/07 at 9:17:02AM

US#042891 Created: 1/31/2007 5:24:24PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Privileged Account or System Access**PII Involved:** Yes

Last Edited: 2/1/2007 1:45:57AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:****Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Navy (USN)**Occurred:** 01/29/07 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** 3rd Party**Incident Status:** Closed**Impact:** Not Reported**Function:** Database Server**# Sites:** Not Reported**OS:** Not Reported**# Systems:** Not Reported**AV:** Not Reported

Agency reports a database system was compromised. The database contained PII information. The agency has notified personnel involved, implemented a forced password change for all users and patched system configuration files.

Ticket Status: CLOSED On 01/31/07 at 5:33:58PM

US#041523 Created: 1/20/2007 8:27:35PM

Problem Type: 01-Unauthorized Access**Sub-Type:** Equipment**PII Involved:** Yes

Last Edited: 1/21/2007 5:51:23AM

Report Method: EMail**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** LCDR Meghan Michael**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Navy (USN)**Occurred:** 01/12/07 1:45**Timezone:** GMT - 07 (UTC - 07) Pacific Daylight Time - PDT**Identified By:** User**Incident Status:** Not Reported**Impact:** Not Reported**Function:** Laptop**# Sites:** 1**OS:** Not Reported**# Systems:** 1**AV:** Not Reported

Federal employee reports the theft of a laptop and memory stick containing PII.

Ticket Status: CLOSED On 01/20/07 at 9:08:00PM

US#040295 Created: 1/9/2007 10:44:16AM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 1/10/2007 4:09:23AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By:

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Navy (USN)

Occurred: 11/30/06 0:00

Timezone: Eastern Standard Time - EST

Identified By: Other

Incident Status: Unknown

Impact: Medium

Sites: 1

Systems: 1

Function: Not Reported

OS: Not Reported

AV: Not Reported

An agency has reported a laptop is missing with 37 individuals PII stored on it. The local authorities have been notified.

Ticket Status: CLOSED On 01/09/07 at 11:13:04AM

US#038313 Created: 12/17/2006 11:57:46AM

Problem Type: 01-Unauthorized Access

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 2/8/2007 11:44:59AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Fountain, Shellie

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Navy (USN)

Occurred: 12/14/06 0:00

Timezone: Eastern Standard Time - EST

Identified By: Administrator

Incident Status: Closed

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Laptop

OS: Not Reported

AV: Not Reported

Agency reports that a laptop had been stolen. Contained on a CD, that was inserted in the drive at the time of theft, contained sensitive information on 114 agency personnel.

Ticket Status: CLOSED On 02/08/07 at 11:44:40PM

US#037756 Created: 12/12/2006 3:57:04PM

Problem Type: 04-Improper Usage

Sub-Type: Policy Violation

PII Involved: Yes

Last Edited: 2/8/2007 7:29:52AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Kirk A Lagerquist

Tracking #: 200061212

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Navy (USN)

Occurred: 12/12/06 0:00

Timezone: Eastern Standard Time - EST

Identified By: Other

Incident Status: Unknown

Impact: Medium

Sites: 1

Systems: 1

Function: Not Reported

OS: Not Reported

AV: Not Reported

An agency has reported employees sent an email from an AOL account with an attachment, courtesy copied to a civilian with the same name as an employee. The attachment contained unaccounted for PII on 78 individuals.

Ticket Status: CLOSED On 02/08/07 at 7:29:44AM

US#036736 Created: 12/6/2006 10:58:48AM

Problem Type: 06-Investigation

Sub-Type: Non Cyber

PII Involved: Yes

Last Edited: 12/7/2006 6:46:59AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Lawrence Haws

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD) / Navy (USN)

Occurred: 11/30/06 0:00

Timezone: Eastern Standard Time - EST

Identified By: Not Reported

Incident Status: Not Reported

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Not Reported

AV: Not Reported

Agency reports a PII incident involving 33 individuals. Their names and SSN were inadvertently mailed to the wrong address. Steps have been taken to retrieve the package and new procedures were put in place.

Ticket Status: CLOSED On 12/06/06 at 11:16:03AM

US#036112 Created: 12/1/2006 7:55:53PM

[Problem Type: 01-Unauthorized Access](#)

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 5/1/2007 2:31:57AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By:

Tracking #: Not Reported

Assigned To: Incident Handling

[Impacted Party: Department of Defense \(DOD\) / Navy \(USN\)](#)

Occurred: 11/29/06 0:00

Timezone: Eastern Standard Time - EST

Identified By: 3rd Party

Incident Status: Closed

Impact: Not Reported

Sites: Not Reported

Systems: 1

Function: Laptop

OS: Not Reported

AV: Not Reported

Agency reports their laptop computers, containing the names and SSNs of crewmembers were stolen. The laptop was in the trunk of a car which was stolen on 29 Nov.

Ticket Status: CLOSED On 12/01/06 at 8:02:05PM

US#030240 Created: 10/13/2006 8:06:39PM

[Problem Type: 01-Unauthorized Access](#)

Sub-Type: Network

PII Involved: Yes

Last Edited: 11/22/2006 3:18:23AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: JTF-GNO

Tracking #: Not Reported

Assigned To: Incident Handling

[Impacted Party: Department of Defense \(DOD\) / Navy \(USN\) / DON CIO \(Naval Information Systems Management\)](#)

Occurred: 10/13/06 0:00

Timezone: Eastern Standard Time - EST

Identified By: Not Reported

Incident Status: Closed

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Not Reported

AV: Not Reported

Agency reports receiving a report of PII disclosure of several employees through google cache of Agency employees. Requests were sent to Google to have many websites removed from Google cache. It is unknown how the cached data has been stored on Google servers.

Ticket Status: CLOSED On 11/22/06 at 3:18:09PM

US#029896 Created: 10/11/2006 11:31:01AM

[Problem Type: 01-Unauthorized Access](#)

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 10/25/2006 10:57:49AM

Report Method: Email

Reporting Sector: Company/Business (Lincoln BP Management)

Reported By: Sandra Kline

Tracking #: 2006-USCERTUUX06

Assigned To: Incident Handling

[Impacted Party: Department of Defense \(DOD\)](#)

Occurred: 10/11/06 0:00

Timezone: Eastern Standard Time - EST

Identified By: Other

Incident Status: Unknown

Impact: Medium

Sites: 1

Systems: 1

Function: Not Reported

OS: Not Reported

AV: Not Reported

An agency has reported the theft of a laptop computer and CD's containing files with PII stored on them. The company and the local criminal investigative division are investigating.

Ticket Status: CLOSED On 10/25/06 at 10:57:41AM

US#054398 Created: 5/7/2007 1:22:14AM

[Problem Type: 06-Investigation](#)

Sub-Type: Suspicious System Activity

PII Involved: Yes

Last Edited: 5/7/2007 2:00:53AM

Report Method: Email

Reporting Sector: Agency (Department of Homeland Security (DHS))

Reported By: KeyLogger

Tracking #: Not Reported

Assigned To: Incident Handling

[Impacted Party: Department of Defense \(DOD\)](#)

Occurred: 05/07/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: Not Reported

Incident Status: Not Reported

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Not Reported

AV: Not Reported

US-CERT has received data from a third party potentially indicating that some agency customers and/or employees have had Personal Identifiable Information (PII) captured via a keylogger installed on their systems.

Ticket Status: CLOSED On 05/07/07 at 1:22:35AM

US#054252 Created: 5/4/2007 1:36:21PM

Problem Type: 06-Investigation

Sub-Type: Other

PII Involved: Yes

Last Edited: 5/4/2007 1:46:49AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: Walter Richard

Tracking #: Google PII

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD)

Occurred: 05/04/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: User

Incident Status: Closed

Impact: Not Reported Function: Not Reported

Sites: Not Reported OS: Not Reported

Systems: Not Reported AV: Not Reported

An agency reports that PII information found about members of the agency through a Google search. PII included name, rank, SSN, and bloodtypes.

Ticket Status: CLOSED On 05/04/07 at 1:39:31PM

US#053738 Created: 4/28/2007 4:27:16PM

Problem Type: 06-Investigation

Sub-Type: Suspicious System Activity

PII Involved: Yes

Last Edited: 4/28/2007 6:21:40AM

Report Method: Email

Reporting Sector: Agency (Department of Homeland Security (DHS))

Reported By: KeyLogger

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD)

Occurred: 04/28/07 16:27

Timezone: Eastern Standard Time - EST

Identified By: 3rd Party

Incident Status: Closed

Impact: Not Reported Function: Not Reported

Sites: Not Reported OS: Not Reported

Systems: Not Reported AV: Not Reported

US-CERT has received data from a third party potentially indicating that some agency customers and/or employees have had Personal Identifiable Information (PII) captured via a keylogger installed on their systems.

Ticket Status: CLOSED On 04/28/07 at 4:30:24PM

US#053553 Created: 4/25/2007 8:03:49PM

Problem Type: 06-Investigation

Sub-Type: Unconfirmed Report

PII Involved: Yes

Last Edited: 4/26/2007 2:04:06AM

Report Method: Web

Reporting Sector: Agency (Department of Defense (DOD))

Reported By:

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD)

Occurred: 04/25/07 0:00

Timezone: Eastern Standard Time - EST

Identified By: 3rd Party

Incident Status: Not Reported

Impact: Not Reported Function: Not Reported

Sites: Not Reported OS: Not Reported

Systems: Not Reported AV: Not Reported

An agency reports disclosure of hard copy personnel report at the agency resulted in an unconfirmed number of identity theft attempts. Local law enforcement is investigating.

Ticket Status: ASSIGNED

US#048947 Created: 3/15/2007 6:32:52PM

Problem Type: 06-Investigation

Sub-Type: Suspicious System Activity

PII Involved: Yes

Last Edited: 3/18/2007 8:15:25AM

Report Method: Email

Reporting Sector: Agency (Department of Homeland Security (DHS))

Reported By: KeyLogger

Tracking #: Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD)

Occurred: 03/15/07 18:32

Timezone: Eastern Standard Time - EST

Identified By: 3rd Party

Incident Status: Closed

Impact: Not Reported Function: Not Reported

Sites: Not Reported OS: Not Reported

Systems: Not Reported AV: Not Reported

US-CERT has received data from a third party potentially indicating that some agency customers and/or employees have had Personal Identifiable Information (PII) captured via a keylogger installed on their systems.

Ticket Status: CLOSED On 03/15/07 at 6:33:09PM

US#046377 Created: 2/26/2007 1:25:10PM

Problem Type: 06-Investigation**Sub-Type:** Non Cyber**PII Involved:** Yes

Last Edited: 2/27/2007 1:46:36AM

Report Method: Email**Reporting Sector:** Agency (Department of Homeland Security (DHS))**Reported By:** SOC**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD)**Occurred:** 02/26/07 13:25**Timezone:** Eastern Standard Time - EST**Identified By:** 3rd Party**Incident Status:** Closed**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

US-CERT has received data from a third party potentially indicating that some agency customers and/or employees have had Personal Identifiable Information (PII) captured via a keylogger installed on their systems.

Ticket Status: CLOSED On 02/26/07 at 1:25:46PM

US#044361 Created: 2/10/2007 4:27:37PM

Problem Type: 06-Investigation**Sub-Type:** Non Cyber**PII Involved:** Yes

Last Edited: 2/10/2007 4:27:54AM

Report Method: Email**Reporting Sector:** Agency (Department of Homeland Security (DHS))**Reported By:** KeyLogger**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD)**Occurred:** 02/10/07 16:27**Timezone:** Eastern Standard Time - EST**Identified By:** 3rd Party**Incident Status:** Closed**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

US-CERT has received data from a third party potentially indicating that some agency customers and/or employees have had Personal Identifiable Information (PII) captured via a keylogger installed on their systems.

Ticket Status: CLOSED On 02/10/07 at 4:27:50PM

US#043291 Created: 2/3/2007 3:38:44PM

Problem Type: 06-Investigation**Sub-Type:** Non Cyber**PII Involved:** Yes

Last Edited: 2/3/2007 3:40:13AM

Report Method: Email**Reporting Sector:** Agency (Department of Homeland Security (DHS))**Reported By:** KeyLogger**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD)**Occurred:** 02/03/07 15:38**Timezone:** Eastern Standard Time - EST**Identified By:** 3rd Party**Incident Status:** Closed**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

US-CERT has received data from a third party potentially indicating that some agency customers and/or employees have had Personal Identifiable Information (PII) captured via a keylogger installed on their systems.

Ticket Status: CLOSED On 02/03/07 at 3:40:08PM

US#040733 Created: 1/13/2007 1:18:26PM

Problem Type: 06-Investigation**Sub-Type:** Non Cyber**PII Involved:** Yes

Last Edited: 1/13/2007 1:18:49AM

Report Method: Email**Reporting Sector:** Agency (Department of Homeland Security (DHS))**Reported By:** KeyLogger**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD)**Occurred:** 01/13/07 13:18**Timezone:** Eastern Standard Time - EST**Identified By:** 3rd Party**Incident Status:** Closed**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

US-CERT has received data from a third party potentially indicating that some agency customers and/or employees have had Personal Identifiable Information (PII) captured via a keylogger installed on their systems.

Ticket Status: CLOSED On 01/13/07 at 1:18:45PM

US#038257 Created: 12/16/2006 3:11:03PM

Problem Type: 06-Investigation**Sub-Type:** Non Cyber**PII Involved:** Yes

Last Edited: 12/21/2006 2:34:07AM

Report Method: Email**Reporting Sector:** Agency (Department of Homeland Security (DHS))**Reported By:** KeyLogger**Tracking #:** Not Reported

Assigned To: Analysis

Impacted Party: Department of Defense (DOD)**Occurred:** 12/07/06 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** 3rd Party**Incident Status:** Closed**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

US-CERT has received data from a third party potentially indicating that some agency customers and/or employees have had Personal Identifiable Information (PII) captured via a keylogger installed on their systems.

Ticket Status: CLOSED On 12/16/06 at 3:11:30PM

US#037083 Created: 12/8/2006 2:05:12PM

Problem Type: 04-Improper Usage**Sub-Type:** Policy Violation**PII Involved:** Yes

Last Edited: 12/8/2006 2:16:14AM

Report Method: Email**Reporting Sector:** Agency (Department of Defense (DOD))**Reported By:** Donna Williamson**Tracking #:** -

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD)**Occurred:** 12/08/06 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Not Reported**Incident Status:** Not Reported**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

Agency reports a compromise involving a form containing the personal information of a newly hired employee. The form was found on a printer. The agency is attempting to identify who sent the document to the printer so that proper corrective action may be taken.

Ticket Status: CLOSED On 12/08/06 at 2:13:50PM

US#035744 Created: 11/29/2006 9:49:32AM

Problem Type: 06-Investigation**Sub-Type:** Suspicious System Activity**PII Involved:** Yes

Last Edited: 11/29/2006 9:51:12AM

Report Method: Email**Reporting Sector:** Agency (Department of Homeland Security (DHS))**Reported By:** KeyLogger**Tracking #:** Not Reported

Assigned To: Analysis

Impacted Party: Department of Defense (DOD)**Occurred:** 11/29/06 9:49**Timezone:** Eastern Standard Time - EST**Identified By:** 3rd Party**Incident Status:** Closed**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

US-CERT has received data from a third party potentially indicating that some agency customers and/or employees have had Personal Identifiable Information (PII) captured via a keylogger installed on their systems.

Ticket Status: CLOSED On 11/29/06 at 9:51:05AM

US#034223 Created: 11/16/2006 3:38:57PM

Problem Type: 06-Investigation**Sub-Type:** Suspicious System Activity**PII Involved:** Yes

Last Edited: 11/16/2006 3:51:21AM

Report Method: Email**Reporting Sector:** Agency (Department of Homeland Security (DHS))**Reported By:** KeyLogger**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD)**Occurred:** 11/16/06 0:00**Timezone:** Eastern Standard Time - EST**Identified By:** Not Reported**Incident Status:** Not Reported**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

US-CERT has received data from a third party potentially indicating that some agency customers and/or employees have had Personal Identifiable Information (PII) captured via a keylogger installed on their systems.

Ticket Status: CLOSED On 11/16/06 at 3:47:22PM

US#033795 Created: 11/13/2006 5:22:01PM

[Problem Type: 01-Unauthorized Access](#)

Sub-Type: Equipment

PII Involved: Yes

Last Edited: 11/14/2006 6:54:29AM

Report Method: Web

Reporting Sector: Agency (Department of Defense (DOD))

Reported By: JTF-GNO

Tracking #: DSS-0001

Assigned To: Incident Handling

[Impacted Party: Department of Defense \(DOD\)](#)

Occurred: 11/11/06 14:30

Timezone: Eastern Standard Time - EST

Identified By: Not Reported

Incident Status: Closed

Impact: Not Reported

Sites: 1

Systems: 4

Function: Laptop

OS: Not Reported

AV: Not Reported

Agency reports 4 laptops containing PII were stolen. Local law enforcement and the agency are conducting an investigation.

Ticket Status: CLOSED On 11/13/06 at 5:29:24PM

US#032583 Created: 11/4/2006 5:24:48PM

[Problem Type: 06-Investigation](#)

Sub-Type: Suspicious System Activity

PII Involved: Yes

Last Edited: 11/4/2006 4:26:15AM

Report Method: Email

Reporting Sector: Agency (Department of Homeland Security (DHS))

Reported By: KeyLogger

Tracking #: Not Reported

Assigned To: Analysis

[Impacted Party: Department of Defense \(DOD\)](#)

Occurred: 11/04/06 16:24

Timezone: Eastern Standard Time - EST

Identified By: 3rd Party

Incident Status: Closed

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Not Reported

AV: Not Reported

US-CERT has received data from a third party potentially indicating that some agency customers and/or employees have had Personal Identifiable Information (PII) captured via a keylogger installed on their systems.

Ticket Status: CLOSED On 11/04/06 at 5:26:02PM

US#032071 Created: 10/31/2006 2:41:46PM

[Problem Type: 06-Investigation](#)

Sub-Type: Non Cyber

PII Involved: Yes

Last Edited: 10/31/2006 2:27:43AM

Report Method: Email

Reporting Sector: Agency (Department of Defense (DOD))

Reported By:

Tracking #: Not Reported

Assigned To: Incident Handling

[Impacted Party: Department of Defense \(DOD\)](#)

Occurred: 10/31/06 0:00

Timezone: Eastern Standard Time - EST

Identified By: Not Reported

Incident Status: Not Reported

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Not Reported

AV: Not Reported

An organization reports over 11,000 pieces of mail sent to incorrect addresses. There was PII in the pieces of mail that was sent to the incorrect members.

Ticket Status: CLOSED On 10/31/06 at 2:48:20PM

US#031393 Created: 10/25/2006 7:58:14AM

[Problem Type: 06-Investigation](#)

Sub-Type: Suspicious System Activity

PII Involved: Yes

Last Edited: 10/27/2006 12:47:57PM

Report Method: Email

Reporting Sector: Agency (Department of Homeland Security (DHS))

Reported By: KeyLogger

Tracking #: Not Reported

Assigned To: Analysis

[Impacted Party: Department of Defense \(DOD\)](#)

Occurred: 10/25/06 7:58

Timezone: Eastern Standard Time - EST

Identified By: 3rd Party

Incident Status: Closed

Impact: Not Reported

Sites: Not Reported

Systems: Not Reported

Function: Not Reported

OS: Not Reported

AV: Not Reported

US-CERT has received data from a third party potentially indicating that some agency customers and/or employees have had Personal Identifiable Information (PII) captured via a keylogger installed on their systems.

Ticket Status: CLOSED On 10/25/06 at 7:59:42AM

US#030407 Created: 10/16/2006 11:03:08AM**Problem Type:** 06-Investigation**Sub-Type:** Suspicious System Activity**PII Involved:** Yes**Last Edited:** 1/4/2007 6:18:13AM**Report Method:** Email**Reporting Sector:** Agency (Department of Homeland Security (DHS))**Reported By:** KeyLogger**Tracking #:** Not Reported

Assigned To: Incident Handling

Impacted Party: Department of Defense (DOD)**Occurred:** 10/16/06 11:03**Timezone:** Eastern Standard Time - EST**Identified By:** 3rd Party**Incident Status:** Closed**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

US-CERT has received data from a third party potentially indicating that some agency customers and/or employees have had Personal Identifiable Information (PII) captured via a keylogger installed on their systems.

Ticket Status: CLOSED On 01/04/07 at 6:17:20AM

US#030109 Created: 10/13/2006 8:58:55AM**Problem Type:** 06-Investigation**Sub-Type:** Suspicious System Activity**PII Involved:** Yes**Last Edited:** 10/13/2006 9:31:38AM**Report Method:** Email**Reporting Sector:** Agency (Department of Homeland Security (DHS))**Reported By:** KeyLogger**Tracking #:** Not Reported

Assigned To: Analysis

Impacted Party: Department of Defense (DOD)**Occurred:** 10/13/06 8:58**Timezone:** Eastern Standard Time - EST**Identified By:** 3rd Party**Incident Status:** Closed**Impact:** Not Reported**# Sites:** Not Reported**# Systems:** Not Reported**Function:** Not Reported**OS:** Not Reported**AV:** Not Reported

US-CERT has received data from a third party potentially indicating that some agency customers and/or employees have had Personal Identifiable Information (PII) captured via a keylogger installed on their systems.

Ticket Status: CLOSED On 10/13/06 at 9:01:43AM