UNCLASSIFIED//FOUO

UNITED STATES COMPUTER EMERGENCY READINESS TEAM (US-CERT)

US-CERT OPERATIONS

Incident & Event Summary
Department of Defense (DOD)

Tuesday 5/8/2007

UNCLASSIFIED//FOUO
Executive Summary
The National Cyber Security Division (NCSD) 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

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAT 1</td>
<td>Unauthorized Access</td>
<td>In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.</td>
</tr>
<tr>
<td>CAT 2</td>
<td>Denial of Service (DoS)</td>
<td>An attack that successfully 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.</td>
</tr>
<tr>
<td>CAT 3</td>
<td>Malicious Code</td>
<td>Successful 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 successfully quarantined by antivirus (AV) software.</td>
</tr>
<tr>
<td>CAT 4</td>
<td>Improper Usage</td>
<td>A person violates acceptable computing use policies.</td>
</tr>
</tbody>
</table>

Table 2: Federal Agency Event Categories

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAT 5</td>
<td>Scans / Probes / Attempted Access</td>
<td>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.</td>
</tr>
<tr>
<td>CAT 6</td>
<td>Investigation</td>
<td>Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.</td>
</tr>
</tbody>
</table>
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**

- 10/06: 13
- 11/06: 11
- 12/06: 20
- 01/07: 22
- 02/07: 14
- 03/07: 24
- 04/07: 25
- 05/07: 9

**Figure 1.4: Top Incident or Event Reported by Month**

- 10/06: 7
- 11/06: 6
- 12/06: 8
- 01/07: 12
- 02/07: 7
- 03/07: 13
- 04/07: 13
- 05/07: 4

**Figure 1.5: Tickets by Sub Organization**

- **DCAA**: 4
- **Defense Commissary Agency**: 2
- **DFAS**: 1
- **DOD**: 14
- **JTF-GNO**: 19
- **MDA**: 4
- **NSA**: 1
- **USA**: 62
- **USAF**: 3
- **USMC**: 1
- **USN**: 23

UNCLASSIFIED//FOUO
UNCLASSIFIED//FOUO

**US#042024**  Created: 1/24/2007  7:26:50PM  Assigned To: Incident Handling

**Problem Type:** 04-Improper Usage

**Sub-Type:** Policy Violation

**PII Involved:** Yes

**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

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  Assigned To: Incident Handling

**Problem Type:** 01-Unauthorized Access

**Sub-Type:** Equipment

**PII Involved:** Yes

**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

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  7:29:12PM

**US#040308**  Created: 1/9/2007  12:11:34PM  Assigned To: Incident Handling

**Problem Type:** 04-Improper Usage

**Sub-Type:** Policy Violation

**PII Involved:** Yes

**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

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  7:19:54PM

**US#054497**  Created: 5/7/2007  9:33:04PM  Assigned To: Incident Handling

**Problem Type:** 01-Unauthorized Access

**Sub-Type:** Equipment

**PII Involved:** Yes

**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

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
An 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.

An agency reports 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.

An agency reports a stolen laptop containing PII. Incident has been reported to local law enforcement. PII was involved. Law enforcement has been notified and the incident is under investigation.

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.
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.

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

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.

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.

<table>
<thead>
<tr>
<th>Ticket Status: CLOSED On 04/24/07 at 12:31:58PM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem Type: 01-Unauthorized Access</td>
</tr>
<tr>
<td>Sub-Type: Equipment</td>
</tr>
<tr>
<td>PII Involved: Yes</td>
</tr>
<tr>
<td>Impact Party: Department of Defense (DOD) / Army (USA)</td>
</tr>
<tr>
<td>Occurred: 04/17/07 0:00</td>
</tr>
<tr>
<td>Timezone: Eastern Standard Time - EST</td>
</tr>
<tr>
<td>Identified By: Other</td>
</tr>
<tr>
<td>Incident Status: Unknown</td>
</tr>
<tr>
<td>Impact: Medium</td>
</tr>
<tr>
<td>Function: Laptop</td>
</tr>
<tr>
<td># Sites: 1</td>
</tr>
<tr>
<td>OS: Not Reported</td>
</tr>
<tr>
<td># Systems: 1</td>
</tr>
<tr>
<td>AV: Not Reported</td>
</tr>
<tr>
<td>Tracking #: #2007-USCERT3MKCYN</td>
</tr>
</tbody>
</table>

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

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.

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.

<table>
<thead>
<tr>
<th>Ticket Status: CLOSED On 04/10/07 at 10:55:00AM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem Type: 01-Unauthorized Access</td>
</tr>
<tr>
<td>Sub-Type: Equipment</td>
</tr>
<tr>
<td>PII Involved: Yes</td>
</tr>
<tr>
<td>Impact Party: Department of Defense (DOD) / Army (USA)</td>
</tr>
<tr>
<td>Occurred: 04/10/07 0:00</td>
</tr>
<tr>
<td>Timezone: Eastern Standard Time - EST</td>
</tr>
<tr>
<td>Identified By: Other</td>
</tr>
<tr>
<td>Incident Status: Unknown</td>
</tr>
<tr>
<td>Impact: Medium</td>
</tr>
<tr>
<td>Function: Blackberry/PDA/Mobile Agent,Laptop</td>
</tr>
<tr>
<td># Sites: 1</td>
</tr>
<tr>
<td>OS: Not Reported</td>
</tr>
<tr>
<td># Systems: 1</td>
</tr>
<tr>
<td>AV: Not Reported</td>
</tr>
<tr>
<td>Tracking #: 2007-USCERT1RUV9S</td>
</tr>
</tbody>
</table>

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.

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

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

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

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.
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

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

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 12:09:09PM

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.
An agency reports a PII compromise. A sensitive file had shared permission 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

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

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

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

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

Ticket Status: ASSIGNED

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

An agency reports a laptop computer missing from an individual's section. The laptop was up to date on all patches.
An agency has reported several laptop computers were taken from an individual's home. The Albuquerque Police Department was notified and a report filed.

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

An 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

An 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 02/20/07 at 4:02:36PM
<table>
<thead>
<tr>
<th>Ticket Number</th>
<th>Created Date</th>
<th>Last Edited Date</th>
<th>Assigned To:</th>
<th>Problem Type:</th>
<th>Sub-Type:</th>
<th>PII Involved:</th>
<th>Impact Party:</th>
<th>Occurred</th>
<th>Timezone</th>
<th>Identified By:</th>
<th>Incident Status</th>
<th>Impact</th>
<th>Function</th>
<th>OS</th>
<th>AV</th>
<th># Systems</th>
<th># Sites</th>
<th>Ticket Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>US044607</td>
<td>2/12/2007</td>
<td>2/12/2007</td>
<td>Incident Handling</td>
<td>01-Unauthorized Access</td>
<td>Equipment</td>
<td>Yes</td>
<td>Department of Defense (DOD) / Army (USA)</td>
<td>02/12/07 0:00</td>
<td>Eastern Standard Time - EST</td>
<td>User</td>
<td>Closed</td>
<td>PII Involved:</td>
<td>impacted Party:</td>
<td>Ticket Status:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>US044121</td>
<td>2/8/2007</td>
<td>2/9/2007</td>
<td>Incident Handling</td>
<td>01-Unauthorized Access</td>
<td>Equipment</td>
<td>Yes</td>
<td>Department of Defense (DOD) / Army (USA)</td>
<td>02/08/07 0:00</td>
<td>Eastern Standard Time - EST</td>
<td>User</td>
<td>Open</td>
<td>PII Involved:</td>
<td>impacted Party:</td>
<td>Ticket Status:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>US043001</td>
<td>2/1/2007</td>
<td>2/28/2007</td>
<td>Incident Handling</td>
<td>04-Improper Usage</td>
<td>Policy Violation</td>
<td>Yes</td>
<td>Department of Defense (DOD) / Army (USA)</td>
<td>02/01/07 0:00</td>
<td>Eastern Standard Time - EST</td>
<td>Other</td>
<td>Unknown</td>
<td>PII Involved:</td>
<td>impacted Party:</td>
<td>Ticket Status:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>US042997</td>
<td>2/1/2007</td>
<td>2/1/2007</td>
<td>Incident Handling</td>
<td>01-Unauthorized Access</td>
<td>Network</td>
<td>Yes</td>
<td>Department of Defense (DOD) / Army (USA)</td>
<td>02/01/07 0:00</td>
<td>Eastern Standard Time - EST</td>
<td>Not Reported</td>
<td>Not Reported</td>
<td>PII Involved:</td>
<td>impacted Party:</td>
<td>Ticket Status:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

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.
**UNCLASSIFIED//FOUO**

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

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

**Assigned To:** Incident Handling  
**Last Edited:** 2/21/2007 8:35:23AM  
**Created:** 1/29/2007 4:09:41PM

**Impact:** Department of Defense (DOD) / Army (USA)

- **Occured:** 01/29/07 0:00  
- **Timezone:** Eastern Standard Time - EST

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

An agency reports that an 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

**Assigned To:** Incident Handling  
**Last Edited:** 1/26/2007 10:58:33AM

**Impact:** Department of Defense (DOD) / Army (USA)

- **Occured:** 01/26/07 10:50  
- **Timezone:** Eastern Standard Time - EST

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

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

**Assigned To:** Incident Handling  
**Last Edited:** 2/2/2007 10:44:17AM

**Impact:** Department of Defense (DOD) / Army (USA)

- **Occured:** 01/25/07 11:24  
- **Timezone:** Eastern Standard Time - EST

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

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

**Assigned To:** Incident Handling  
**Last Edited:** 1/29/2007 2:31:58AM

**Impact:** Department of Defense (DOD) / Army (USA)

- **Occured:** 01/21/07 0:00  
- **Timezone:** Eastern Standard Time - EST

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

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

**Ticket Status:** RE-OPENED
Federal agency reports the theft of a government laptop which contained PII

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

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

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

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

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.
<table>
<thead>
<tr>
<th>Ticket Status</th>
<th>Created</th>
<th>Last Edited</th>
<th>Assigned To:</th>
</tr>
</thead>
</table>

**US#040019**

**Problem Type:** 01-Unauthorized Access

**PII Involved:** Yes

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

**Occurred:** 01/06/07 0:00

**Timezone:** Eastern Standard Time - EST

**Identified By:** 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.

**US#039825**

**Problem Type:** 01-Unauthorized Access

**PII Involved:** Yes

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

**Occurred:** 12/31/06 0:00

**Timezone:** Eastern Standard Time - EST

**Identified By:** Other

**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.

**US#039363**

**Problem Type:** 01-Unauthorized Access

**PII Involved:** Yes

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

**Occurred:** 12/16/06 0:00

**Timezone:** Eastern Standard Time - EST

**Identified By:** 3rd Party

**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.

**US#038642**

**Problem Type:** 01-Unauthorized Access

**PII Involved:** Yes

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

**Occurred:** 12/16/06 0:00

**Timezone:** Eastern Standard Time - EST

**Identified By:** 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.

**US#040019**

**Problem Type:** 01-Unauthorized Access

**PII Involved:** Yes

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

**Occurred:** 01/06/07 0:00

**Timezone:** Eastern Standard Time - EST

**Identified By:** 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.

**US#039825**

**Problem Type:** 01-Unauthorized Access

**PII Involved:** Yes

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

**Occurred:** 12/31/06 0:00

**Timezone:** Eastern Standard Time - EST

**Identified By:** Other

**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.

**US#039363**

**Problem Type:** 01-Unauthorized Access

**PII Involved:** Yes

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

**Occurred:** 12/16/06 0:00

**Timezone:** Eastern Standard Time - EST

**Identified By:** 3rd Party

**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.

**US#038642**

**Problem Type:** 01-Unauthorized Access

**PII Involved:** Yes

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

**Occurred:** 12/16/06 0:00

**Timezone:** Eastern Standard Time - EST

**Identified By:** 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 1
**US#038027**
**Created:** 12/14/2006 3:41:32PM  
**Last Edited:** 1/11/2007 2:28:31AM  
**Assigned To:** Incident Handling  
**Problem Type:** 01-Unauthorized Access  
**Sub-Type:** Equipment  
**PII Involved:** Yes  
**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  

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 SSNs 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 their personal information.

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

### Ticket 2
**US#037642**
**Created:** 12/11/2006 8:53:37PM  
**Last Edited:** 2/8/2007 9:26:32AM  
**Assigned To:** Incident Handling  
**Problem Type:** 01-Unauthorized Access  
**Sub-Type:** Privileged Account or System Access  
**PII Involved:** Yes  
**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  

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

### Ticket 3
**US#036361**
**Created:** 12/4/2006 12:32:39PM  
**Last Edited:** 12/5/2006 12:44:54PM  
**Assigned To:** Incident Handling  
**Problem Type:** 04-Improper Usage  
**Sub-Type:** Policy Violation  
**PII Involved:** Yes  
**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  

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

### Ticket 4
**US#036313**
**Created:** 12/4/2006 9:59:31AM  
**Last Edited:** 12/5/2006 6:05:43AM  
**Assigned To:** Incident Handling  
**Problem Type:** 01-Unauthorized Access  
**Sub-Type:** Equipment  
**PII Involved:** Yes  
**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  

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
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.

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

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.

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

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

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

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.
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.

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.

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.

Agency reports that a laptop stolen from an POV that was secured. The laptop may have had unknown number of possible agency prospects names, addresses and phone numbers, and mother’s maiden names. The reporting party didn't reveal how many people are affected.

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

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

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

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

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.

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.

Agency reports laptop stolen from vehicle. PII was involved.
An agency reports a missing desktop computer with possible PII data stored on it. The computer was discovered missing during an agency inventory.

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

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

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.
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

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

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

An agency reports an individual received an unencrypted email containing personal identifiable information (PII).
An agency reports that documentation containing PII was found in a dumpster. The documentation was removed from the dumpster and the agency is investigating.

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.

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

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.
### Incident 1

**Problem Type:** 04-Improper Usage  
**Sub-Type:** Policy Violation  
**PII Involved:** Yes  
**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)  
**Occur:** 03/15/07  0:00  
**Function:** Other  
**OS:** Not Reported  
**AV:** Not Reported  
**Impact:** Medium  
**Timezone:** Eastern Standard Time - EST  
**Identified By:** Other  
**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

### Incident 2

**Problem Type:** 04-Improper Usage  
**Sub-Type:** Data Spillage  
**PII Involved:** Yes  
**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)  
**Occur:** 03/06/07  0:00  
**Function:** Other  
**OS:** Not Reported  
**AV:** Not Reported  
**Impact:** Medium  
**Timezone:** Eastern Standard Time - EST  
**Identified By:** Other  
**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

### Incident 3

**Problem Type:** 04-Improper Usage  
**Sub-Type:** Policy Violation  
**PII Involved:** Yes  
**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)  
**Occur:** 01/10/07  0:00  
**Function:** Other  
**OS:** Not Reported  
**AV:** Not Reported  
**Impact:** Not Reported  
**Timezone:** Eastern Standard Time - EST  
**Identified By:** Other  
**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 01/03/07 at 9:27:55AM

### Incident 4

**Problem Type:** 04-Improper Usage  
**Sub-Type:** Policy Violation  
**PII Involved:** Yes  
**Impacted Party:** Department of Defense (DOD) / Defense Logistics Agency (DLA)  
**Occur:** 12/15/06  0:00  
**Function:** User  
**OS:** Not Reported  
**AV:** Not Reported  
**Impact:** Not Reported  
**Timezone:** Eastern Standard Time - EST  
**Identified By:** Other  
**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
<table>
<thead>
<tr>
<th>Ticket ID</th>
<th>Created Date</th>
<th>Last Edited Date</th>
<th>Assigned To:</th>
</tr>
</thead>
</table>

**Problem Type:**
- 06-Investigation
- 04-Improper Usage
- 06-Investigation
- Non Cyber

**Sub-Type:**
- Unconfirmed Report
- Policy Violation
- Non Cyber
- Non Cyber

**PII Involved:**
- Yes
- Yes
- Yes
- Yes

**Report Method:**
- Email
- Email
- Email
- Email

**Reporting Sector:**
- Agency (Department of Defense (DOD))
- Agency (Department of Defense (DOD))
- Agency (Department of Veterans Affairs)
- Agency (Department of Defense (DOD))

**Tracking #:**
- Not Reported
- 2006-1206-3056
- VA03566
- Not Reported

**Impacted Party:**
- Department of Defense (DOD) / Defense Logistics Agency (DLA)
- Department of Defense (DOD) / Defense Logistics Agency (DLA)
- Department of Defense (DOD) / Joint Task Force-Global Network Operations (JTF-GNO)
- Department of Defense (DOD) / Joint Task Force-Global Network Operations (JTF-GNO)

**Occurred:**
- 12/08/06 18:02
- 12/06/06 0:00
- 03/05/07 19:52
- 12/14/06 0:00

**Timezone:**
- Eastern Standard Time - EST
- Eastern Standard Time - EST
- Eastern Standard Time - EST
- Eastern Standard Time - EST

**Identified By:**
- User
- Not Reported
- Not Reported
- Not Reported

**Incident Status:**
- Not Reported
- Not Reported
- Open
- Not Reported

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

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.

An agency reported unencrypted email received by an employee containing PII.

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

---

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.

---

Agency reports lost thumbdrive containing PII.

---

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.
UNCLASSIFIED//FOUO

US#041820  Created: 1/23/2007  10:38:44AM  Assigned To: Incident Handling

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

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  Assigned To: Incident Handling

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

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  Assigned To: Incident Handling

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

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  Assigned To: Incident Handling

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

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 11:01:40AM

UNCLASSIFIED//FOUO
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

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

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

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

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.
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

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

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

Ticket Status: ASSIGNED

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

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.

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.

An agency reports the lost of around 150 laptops, 3 of which contain personally identifiable information.
An agency reports a lost USB drive that contained an alpha roster. The alpha roster accounts for 200 assigned personnel. PII was involved.

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

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.

Federal employee reports the theft of a laptop and memory stick containing PII.
An agency has reported a laptop is missing with 37 individuals PII stored on it. The local authorities have been notified.

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.

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.

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.
Problem Type: 01-Unauthorized Access  
Sub-Type: Equipment  
PII Involved: Yes  
Reporting Sector: Agency (Department of Defense (DOD))  
Reporting By: Not Reported  
Tracking #: Not Reported

**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

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

Problem Type: 01-Unauthorized Access  
Sub-Type: Network  
PII Involved: Yes  
Reporting Sector: JTF-GNO  
Tracking #: Not Reported

**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

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

Problem Type: 01-Unauthorized Access  
Sub-Type: Equipment  
PII Involved: Yes  
Reporting Sector: Company/Business (Lincoln BP Management)  
Reported By: Sandra Kline  
Tracking #: 2006-USCERTUUXO6

**Impacted Party: Department of Defense (DOD)**

Occurred: 10/11/06 0:00  
Timezone: Eastern Standard Time - EST  
Identified By: Other  
Incident Status: Unknown

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

Problem Type: 66-Investigation  
Sub-Type: Suspicious System Activity  
PII Involved: Yes  
Reporting Sector: Agency (Department of Homeland Security (DHS))  
Reported By: KeyLogger  
Tracking #: Not Reported

**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

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
A ticket is assigned to the Incident Handling team. An agency reports that Personal Identifiable Information (PII) information found by a Google search. PII included name, rank, SSN, and bloodtypes. The ticket status is CLOSED on 05/04/07 at 1:39:31PM.

Another ticket is assigned to the Incident Handling team. US-CERT has received data from a third party potentially indicating that some agency customers and/or employees have had PII captured via a keylogger installed on their systems. The ticket status is CLOSED on 04/28/07 at 4:30:24PM.

A third ticket is assigned to the Incident Handling team. An agency reports disclosure of hard copy personnel report at the agency resulted in an unconfirmed number of identity theft attempts. The ticket status is CLOSED on 03/15/07 at 6:33:09PM.
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-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-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-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.
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.

**Incident Status:** Closed

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.

**Incident Status:** Closed

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.

**Incident Status:** Closed

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.
UNCLASSIFIED//FOUO

Ticket Status: CLOSED On 11/11/06 at 14:30


**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 #:** DSS-0001

**Impacted Party: Department of Defense (DOD)**

**Occurred:** 11/11/06 14:30
**Impact:** Not Reported
**Timezone:** Eastern Standard Time - EST
**Function:** Laptop
**Identified By:** Not Reported
**# Sites:** 1
**# Systems:** 4
**OS:** Not Reported
**AV:** Not Reported
**Incident Status:** Closed

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: 11/04/2006   16:24   Last Edited: 11/04/2006   5:26:02PM   Assigned To: Analysis

**Problem Type:** 06-Investigation
**Sub-Type:** Suspicious System Activity
**Report Method:** Email
**PII Involved:** Yes
**Reported By:** KeyLogger
**Tracking #:** Not Reported

**Impacted Party: Department of Defense (DOD)**

**Occurred:** 11/04/06 16:24
**Impact:** Not Reported
**Timezone:** Eastern Standard Time - EST
**Function:** Not Reported
**Identified By:** 3rd Party
**# Sites:** Not Reported
**# Systems:** Not Reported
**OS:** Not Reported
**AV:** Not Reported
**Incident Status:** Closed

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   0:00   Last Edited: 10/31/2006   2:48:20PM   Assigned To: Incident Handling

**Problem Type:** 06-Investigation
**Sub-Type:** Non Cyber
**PII Involved:** Yes
**Report Method:** Email
**Reporting Sector:** Agency (Department of Defense (DOD))
**Reported By:** KeyLogger
**Tracking #:** Not Reported

**Impacted Party: Department of Defense (DOD)**

**Occurred:** 10/31/06 0:00
**Impact:** Not Reported
**Timezone:** Eastern Standard Time - EST
**Function:** Not Reported
**Identified By:** Not Reported
**# Sites:** Not Reported
**# Systems:** Not Reported
**OS:** Not Reported
**AV:** Not Reported
**Incident Status:** 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


**Problem Type:** 06-Investigation
**Sub-Type:** Suspicious System Activity
**PII Involved:** Yes
**Report Method:** Email
**Reporting Sector:** Agency (Department of Homeland Security (DHS))
**Reported By:** KeyLogger
**Tracking #:** Not Reported

**Impacted Party: Department of Defense (DOD)**

**Occurred:** 10/25/06 7:58
**Impact:** Not Reported
**Timezone:** Eastern Standard Time - EST
**Function:** Not Reported
**Identified By:** 3rd Party
**# Sites:** Not Reported
**# Systems:** Not Reported
**OS:** Not Reported
**AV:** Not Reported
**Incident Status:** Closed

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-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.

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.

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.