Personally Identifiable Information (PII) Reporting Actions

The term PII means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, employment history or information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

1. Within 1 hour of discovery, report all incidents involving the actual or suspected compromise of PII to the US-CERT at http://www.us-cert.gov/. If computer access is not available, incidents can be reported 24/7 to 1-866-606-9580 (OAA SEC) or 1-703-235-5110 (US-CERT).
2. Immediately after reporting, an email, including the US-CERT reporting number and a brief synopsis with POC information for the incident, should also be sent to the following accounts:
   pii.reporting@us.army.mil
   usarmy.mannheim.arcyber.mbx.rcerte@mail.mil
3. Within 24 hours, the individual or chain of command must submit PII incident report to the Army Freedom of Information Act and Privacy office at: army_privacy_alert@conus.army.mil.
4. Contact the USAREUR Privacy Officer as well as continue to follow existing internal command procedures to notify local command officials.

Contact Information:

GRAFENWOEHR/VILSECK

Mr. John Sholes
Information Assurance Manager
DSN 526-6001

Mr. Steve Gerding
Deputy Regional NEC Director
DSN 569-6960

HOHENFELS

Mr. Mike Mullen
Information Management Officer
DSN 466-2244

Mr. Julio Hernandez
NEC Director
DSN 520-5690

GARMISCH

Mr. Harold Irwin
Information Management Officer
DSN 440-3322

Mr. Alan Arnold
NEC Chief
DSN 440-3675

USAREUR FOIA/Privacy Officer
DSN: 370-8216

Computer Incident Handling and Reporting Procedures

USAG Bavaria
Bavarian Military Community
Information Assurance

Unit 28130, CMR 415
APO, AE 09114

Incident and Intrusion Reporting Overview

Incidents and intrusions may be the result of deliberate malicious activity or the result of accidental mishandling of government equipment and information. In either case, significant damage to the Army's security posture can be the result. It is imperative that timely, mindful, and informed action be taken to ensure the safeguarding of Army information. This quick reference guide will give you the information needed to report incidents or suspected incidents in the proper manner.

EXAMPLES OF REPORTABLE INCIDENTS:

1. Anti-Virus alerts indicating a worm, virus, Trojan, or other infection.
2. Personnel alerting you about virus emails coming from your account.
3. *Suspicious email in which you responded to, clicked a link, or opened an attachment from.*
4. Occurrence of multiple pop-ups from your browser with inappropriate or other unsolicited content
5. Unexpected events in your daily work routine (system slows to a crawl for no apparent reason, repeated system crashes and error messages, inability to open files or run applications)
6. Unexplained modifications to your background, files, or applications.
7. Presence of suspicious files, shortcuts, or programs on your system
8. Witness the use of unauthorized systems or devices on the network
9. Observe a Spillage/(UDCI) (Unauthorized Disclosure of Classified Information) on the UNCLASS network.
10. Note: The above list is not all inclusive. If you suspect malicious or suspicious activity ALWAYS REPORT IT!

Incident and Intrusion Reporting Actions

If you suspect you are involved in a computer incident or intrusion you must perform the following actions:

1. Contact your IMO, Systems Administrator, Information Assurance personnel, or 119 IMMEDIATELY.
2. Restrict physical access to the Information System or media until your IMO, Systems Administrator or Information Assurance personnel arrive.
3. DO NOT disconnect your network connection (unplug your network cable)
4. DO NOT turn off your computer
5. NEVER perform investigative actions on your own.
6. Turn of the monitor and place a "Hands Off" notice over the computer monitor to notify people not to tamper with the system.
7. If a spillage is involved, complete the immediate action checklist and work with your Security/IA personnel.

Classified Spillage Reporting Actions

The majority of spillage incidents result from careless methods, shortcuts, or untrained users who have intentionally or accidentally compromised sensitive and classified information vital to national security and operational processes. Follow these quick reference guidelines in the advent of a Spillage.

DO:

- Isolate and guard the affected IS(s) immediately.
- Disconnect network connections.
- Implement your Command's spillage incident response plan immediately.
- Restrict physical access to the IS or media until your security manager or IAM/IASO provides guidance.
- Complete initial unit information and Immediate Action Checklist.
- Provide Immediate Action Checklist to designated individuals (i.e. IASO/IAM/SA/NA etc).
- Notify Servicing Signal Battalion Information Assurance Staff.

DO NOT:

- Investigate actions on the IS until authorized by Commander or information security personnel.
- Contact any commercial Internet service provider (ISP) or ISP account identified.
- Confirm or deny a spillage incident occurrence in the public sector.
- Confirm or deny the compromise of sensitive or classified information in the public sector.
- Delay implementation of containment procedures awaiting notifications of key personnel.