Data Spillage and Unauthorized Disclosure Policy
Enclosure 3: Initial Notification and Public Disclosure

1. Initial Notification.

a. Personnel who suspect or observe a potential cybersecurity/information assurance (CS/IA) incident on any Army, DoD or federal device, equipment, system or network must immediately notify their information system security officer/IA support officer (ISSO/IASO) or information system security manager/IA manager (ISSM/IAM).

(1) Notification of a potential data spillage or unauthorized disclosure (i.e., unauthorized disclosure of classified information) is at least U//FOUO (minimal detail) and may be classified depending upon the level of detail, per the Security Classification Guide for Cyberspace Operations and Security (reference hh).

(2) Personnel who suspect or know that a CS/IA incident potentially involves classified systems, networks, information or data must also immediately notify their activity security manager/program security manager (ASM/PSM) and/or the ASM/PSM for the affected system/program, if known.

(3) Personnel not able to make immediate contact with their ISSO/IASO or ISSM/IAM must continue to attempt to contact them while also contacting the supporting incident response organization listed in their Incident Response Plan (IRP). If that organization is not readily known, available or able to initiate incident response, personnel will contact one of the following organizations until incident response is initiated: their local help desk; their servicing Network Enterprise Center or designated IT service provider; and their Regional Cyber Center or the Army Enterprise Service Desk (AESD).

(4) Personnel must subsequently notify their supervisor of the suspected or observed CS/IA incident.

(5) All personnel who are senders, recipients and observers of CS/IA incidents are equally responsible for ensuring that initial notification has occurred promptly and properly. This shared responsibility for initial notification from all parties involved potentially reduces response times and ensures that all affected devices, equipment, systems, networks and personnel are identified for the remediation/mitigation process.

b. Personnel who know or reasonably should know that they may be involved in a CS/IA incident must report it (i.e., “self-reporting”).

(1) Self-reporting will be considered as a positive factor in the consideration of any appropriate administrative, judicial, contractual or other sanctions and/or disciplinary/corrective actions.

(2) Failure to self-report may be considered as a factor for categorizing the incident as “willful”, “negligent” or “inadvertent”.

(3) Commanders and supervisors may consider failure to self-report to be an adverse factor or credible derogatory information against the personnel who failed to self-report, which may adversely impact their security clearance/position of trust and continued access to classified or unclassified sensitive information/CUI.

c. Any activity/organization in receipt of a potential data spill, unauthorized disclosure or improper transfer of classified information (physical or transmitted) must notify the sending activity/organization. The sending activity/organization will then become the lead organization, responsible per DoDM 5200.01, Volume 3, for further reporting, inquiries and investigations.

d. Unclassified communication of suspected or confirmed CS/IA incidents will be avoided where classified communication is available. Any unclassified communication must not include potentially classified information or specifics about the incident that are often themselves classified, such as: a description of the information content; specific details about the incident; computer/server names; IP addresses; and specific locations on a system, network or website. Unclassified communication must be encrypted if it contains specific details about the incident and/or unclassified sensitive information/CUI. Where readily available, communicate using encrypted email, secure telephones, secure faxes and secured or classified devices, systems and networks.

e. CS/IA personnel must collaborate with the ASM/PSM immediately upon notification of a potential CS/IA incident, and continue collaborating until the incident is closed.

f. Those personnel and organizations receiving notification of a potential CS/IA incident will be considered “responding personnel” and will provide immediate and appropriate assistance for the incident, to include assistance with notifications, immediate actions and reporting.

g. Responding personnel will coordinate notifications/reports received and consolidate efforts across the Army by assigning a lead organization to be responsible for working with responding personnel and conducting a preliminary inquiry or other formal investigation in accordance with AR 380-5, AR 380-67, AR 15-6 and AR 380-381.

(1) Lead organization is by default assigned to the sending activity/organization, if that is known.

(2) The lead organization is typically the one that appears: to have originated the incident; to be most impacted by the incident; to be best suited for coordinating a prompt and thorough response (e.g., system storing the data, organization of the affected system); or to be the organization of the data owner/information owner.

(3) The assigned lead organization must promptly execute its responsibilities unless and until its assignment is changed.

(4) The assigned lead organization is responsible for identifying and notifying all recipients, organizations, programs and units potentially affected by the incident.

(5) Lead organization assignment may be changed as deemed appropriate by Theater Signal Commands or the Commander of Army Cyber Command and Second Army.

h. The following types of CS/IA incidents have special additional immediate notification requirements, to be performed by responding personnel in accordance with Army Cyber Command and Second Army procedures (e.g., reference l).

(1) Privacy Act information (e.g., Personally Identifiable Information, Protected Health Information): Immediately reported to the privacy officer.

(2) Sensitive Compartmented Information (SCI): Immediately reported to the special security officer (SSO) and, where applicable, the contractor SSO, special security representatives (SSRs) and contractor SSRs.

(3) Special Access Program, Sensitive Activities, Special Access Required, Alternative Compensatory Control Measures (SAP, SA, SAR, ACCM): Immediately reported to the program security officer (PSO) and the program security manager (PSM) in accordance with AR 380-381. The PSO and PSM must coordinate further incident response and reporting with the ISSM/IAM; and within 24 hours notify the CIO/G-6 SAP Special Program Office and the Army Special Programs Directorate (formerly known as the Technology Management Office) in accordance with AR 380-381.

(4) COMSEC material and cryptologic information, including Controlled Cryptographic Items, Cryptographic High-Value Products and other NSA Suite B equipment: Immediately reported to the COMSEC account manager/Key Management Infrastructure operating account manager, who then reports to the Communications Security Logistics Activity in accordance with AR 380-40 and CNSSI 4003.

2. Public Disclosure.

a. Classified information that has been publicly disclosed (e.g., in the public media, on the Internet, open source, in the public domain) remains at the original classification level and caveats until formally declassified or downgraded by an appropriate original classification authority (OCA).

b. Unclassified sensitive information/CUI that has been publicly disclosed will maintain its sensitivity unless that sensitivity is changed by the appropriate data owner/information owner.

c. Personnel must not make any statement or comment to unauthorized personnel or members of the public that confirms or denies the occurrence of any CS/IA incident, such as a data spill, unauthorized disclosure, loss or theft. Personnel must refer any public inquiry to the Army Public Affairs Office.

d. Personnel must not make any statement or comment to unauthorized personnel or members of the public that would either confirm or deny the existence of classified information or the accuracy of that information. Personnel must refer any public inquiry to the Army Public Affairs Office.

e. Personnel who seek classified information in the public domain, acknowledge its accuracy or existence, and/or propagate the information in any way may be subject to disciplinary action in accordance with AR 25-2, AR 380-5, AR 380-67, AR 15-6, AR 380-381 and other applicable policy, regulations and laws.

f. The cognizant ISSM/IAM or ASM/PSM will make an initial determination of whether the classified information in the public disclosure is “widely available” (i.e., easily accessible and made known to the public, such as reported via a public news source) versus a “limited disclosure” (i.e., requiring a concerted effort for the public to locate and/or access the information, not made known to the public, not reported via a public news source) in accordance with ALARACT 224/2013 and DoD Directive 5210.50.

(1) Responding personnel will use this initial determination (if readily available) to govern the initial response to the CS/IA incident, in accordance with Army Cyber Command and Second Army procedures (e.g., reference l).

(2) Public disclosures are still CS/IA incidents and must be reported in accordance with Army Cyber Command and Second Army procedures (e.g., reference l) regardless of whether the public disclosure is “widely available” or a “limited disclosure”.

(3) CS/IA incidents determined to be “widely available” disclosures must still be reported; however, these incidents will not require full incident response, investigation and remediation (sanitization/destruction.) Remediation of these incidents will only require destruction of printed information and permanent deletion of data by the system administrator/network administrator/database administrator (SA/NA/DBA) from all reasonably accessible areas of a system/device (to include temporary data, cache data, user data and data only accessible to the SA/NA/DBA).

(4) CS/IA incidents determined to be “limited disclosures” will be handled in the same manner as other unauthorized disclosures.

(5) The Regional Cyber Center will promptly make the final determination of “widely available” versus “limited disclosure” upon receiving the CS/IA incident, and will notify the incident’s points of contact of that final determination. Responding personnel, Army Cyber Command and Second Army will use this final determination to govern responses to future CS/IA incidents directly related to the information disclosed. Army Cyber Command and Second Army will reduce unnecessary incident response by disseminating final determinations of “widely available” disclosures to all Army Cyber Command and Second Army incident reporting organizations, NETCOM, Network Enterprise Centers and IT service providers.