Data Spillage and Unauthorized Disclosure Policy
Enclosure 6: Remediation, Mitigation, and Cost Determination

1. Remediation and/or Mitigation.

a. Cybersecurity/information assurance (CS/IA) personnel and organizations in the reporting chain must prevent compromise/destruction of evidence by obtaining authorization from the cognizant activity security managers/program security managers (ASM/PSM) of affected assets prior to any sanitization or “clean-up” activities.

b. Pre-existing mitigation measures (e.g., data-at-rest encryption, self-encrypting drives) may reduce the remediation and/or additional mitigation required.

c. All affected storage/media/devices must be protected at the same classification level, caveats and sensitivity as the spilled information. They also:

(1) Must be labeled with the highest classification level, caveats and sensitivity of the spilled information, until the appropriate remediation processes have been executed and verified.

(2) Must be labeled to indicate that they must remain under DoD control and are not authorized for release outside DoD.

(3) May have sanitization and/or destruction deferred until they are being prepared to be removed from DoD control and/or released outside DoD, per DoD and national policy (e.g., references o, p, v and w).

(4) If the information spilled has been determined to contain Top Secret, Sensitive Compartmented Information or Special Access Program data: May only be released outside DoD (e.g., for disposal or recycling) upon appropriate destruction in accordance with Army Cyber Command (ARCYBER) and Second Army procedures (reference l), IA Best Business Practices 03-PE-O-0003, National Security Agency/Central Security Service (NSA/CSS) policy/guidance (references bb and cc) and National Institute of Standards and Technology (NIST) Special Publication 800-88.

(5) If the information spilled has been determined to contain Secret or below: May only be released outside DoD (e.g., for disposal or recycling) upon appropriate sanitization and/or destruction in accordance with ARCYBER and Second Army procedures (reference l), IA Best Business Practices 03-PE-O-0003, NSA/CSS policy/guidance (references bb and cc) and NIST Special Publication 800-88.

d. Technical remediation must be performed by personnel authorized access to the highest classification level, caveats and sensitivity of the spilled information. If necessary, personnel may be granted “one-time” or short-duration access to the information in accordance with AR 25-2, AR 380-5, AR 380-67 and AR 380-381.

e. Remediation and mitigation measures will be performed in accordance with ARCYBER and Second Army procedures (e.g., reference l). Except where mandatory, these measures will be tailored and implemented based upon risk management, damage assessment, mission requirements, operational needs and continuity of operations.

f. The cognizant Risk Management Framework authorizing official/designated approval authority for each affected system/network will determine whether remediation and mitigation have reached an acceptable level of risk, per the authority granted in AR 25-2 and subject to applicable Army, DoD and national policies, regulations and laws.

2. Cost Determination and Reimbursement.

a. All organizations or activities affected by a potential data spill or unauthorized disclosure must document and report costs in accordance with ARCYBER and Second Army procedures (e.g., reference l).

b. Cost documentation and reporting is U//FOUO and must be handled accordingly, per the Security Classification Guide for Cyberspace Operations and Security.

c. Per the Deputy Secretary of Defense (reference s), the DoD component responsible for a willful or negligent data spill of classified information (e.g., willful or negligent data spill caused by their personnel) will pay the reimbursable enterprise service providers for clean-up costs across the enterprise to restore the affected system/network to a normal operating configuration, in accordance with service level agreements that include such provisions.

d. Clean-up costs directly associated with the following scenarios are not currently mandated for reimbursement per the Deputy Secretary of Defense memorandum (reference s), DoD policy or Army policy.

(1) Inadvertent spillage of classified information.

(2) Spillage of unclassified sensitive information/controlled unclassified information.

(3) Not a reimbursable enterprise service provider.

(4) Not formally authorized for reimbursement per the Army Budget Office.

e. Clean-up costs not mandated for reimbursement per the Deputy Secretary of Defense memorandum (reference s), DoD policy or Army policy may still be collected if

the funding account is formally authorized for reimbursement per the Army Budget Office and the provision is added to applicable contracts, memoranda of agreement, memoranda of understanding and/or service level agreements.