Data Spillage and Unauthorized Disclosure Policy
Enclosure 5: Categorization and Investigations

1. Categorization. Data spillage and unauthorized disclosure incidents must be formally categorized by Army Cyber Command and Second Army as listed below, per the Deputy Secretary of Defense memorandum regarding unauthorized disclosure of classified information or controlled unclassified information on DoD information systems (reference s). The category may be changed as a result of findings during a preliminary inquiry or other formal investigation in accordance with AR 380-5, AR 380-67, AR 15-6 and AR 380-381.

a. Willful. An incident is categorized as willful if the person purposely disregarded DoD security or information-safeguarding policies or requirements (e.g., intentionally bypassing a known security control).

b. Negligent. An incident is categorized as negligent if the person acted unreasonably in causing the incident (e.g., a careless lack of attention to detail or reckless disregard for proper procedures).

c. Inadvertent. An incident is categorized as inadvertent if the person did not know, and had no reasonable basis to know, that the incident was occurring (e.g., the person reasonably relied on improper markings).

2. Investigations.

a. Potential unauthorized disclosure of classified information must be formally investigated in accordance with Army G-2 policies and procedures (e.g., reference c). Preliminary inquiries and other formal investigations for cybersecurity/information assurance (CS/IA) incidents potentially involving classified information will be conducted by the assigned lead organization in accordance with AR 380-5.

b. Disclosure of unclassified sensitive information/controlled unclassified information (CUI) does not require a formal security inquiry or formal investigation; however, an informal inquiry and other actions will be conducted as appropriate in accordance with DoD Manual 5200.01, Volume 4.

c. Commanders will conduct formal investigations in accordance with AR 380-67 and AR 15-6 upon suspicion or evidence of misconduct. Commanders will report adverse and/or credible derogatory information on personnel associated with CS/IA incidents to the designated central adjudication facility in accordance with AR 380-67.

d. Commanders and leaders will, as they deem appropriate, suspend user accounts or specific user account privileges for willful or negligent violations while corrective actions are pending. Prior to reinstatement of privileges, the user will be required to complete corrective training tailored to the nature of the CS/IA incident.