Data Spillage and Unauthorized Disclosure Policy
Enclosure 4: Immediate Actions, Reporting, and Record Keeping

1. Immediate Actions.

a. Individual personnel and responding personnel must make every reasonable effort to immediately isolate and contain a potential data spill in order to minimize its spread and impact. Actions must be taken in accordance with the Incident Response Plan (IRP) and relevant procedures and checklists (e.g., recalling an email and informing recipients not to distribute it further; and changing permissions on a server to restrict access to the information).

b. Personnel must not do any of the following unless and until instructed to do so by cybersecurity/information assurance (CS/IA) personnel or an organization in the CS/IA incident reporting chain. This will help ensure continuity of operations and preserve evidence.

(1) Do not delete data (e.g., files, email, database records), destroy information or remove storage devices.

(2) Do not power down any devices, systems or equipment.

(3) Do not disconnect any devices, systems or equipment from the network. Although effective against the spread of viruses, disconnection may not be necessary, may impact operations and may actually interfere with immediate actions needed to contain and investigate the data spill (e.g., recall of an email message, remote access by responding personnel).

c. Secure potentially affected information and devices/equipment not powered on, not connected to the network or not actively supporting operations: in an environment accredited for open or closed storage of the classification level, caveats and sensitivity; in a manner appropriate for the handling requirements; and in accordance with the Incident Response Plan (IRP).

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

e. CS/IA personnel and organizations in the reporting chain must avoid unnecessary or prolonged sanitization, powering down and/or disconnection of affected devices, systems and equipment.

(1) When deemed necessary, the affected devices, systems and equipment will only remain out of operation as long as they are deemed to be, by the CS/IA personnel or organizations in the reporting chain, a credible risk of further data spillage,

unauthorized disclosure or contamination of evidence. The mere occurrence of a CS/IA incident, the mere presence of spilled data or a delayed investigation or “clean-up” of the incident is not a credible risk that justifies degradation to operations.

(2) The following must not be significantly degraded in mission performance and must not be blocked, isolated, quarantined or disconnected from the network unless absolutely necessary and with signed authorization (physically/digitally) from the Commander or Risk Management Framework authorizing official/designated approving authority (RMF AO/DAA), based upon recommendations from the cognizant information system security manager/IA manager (ISSM/IAM) and/or IA program manager (IAPM).

(a) Servers that actively support operations, whether or not these servers are tactical, non-tactical, mission support or administrative. For these, personnel will follow the procedures in their IRP regarding any isolation or containment.

(b) Devices, equipment, systems and networks that actively support tactical operations, to include those used in exercises and deployments. For these, personnel will follow the procedures in their IRP regarding any isolation or containment.

(3) Server disk storage (to include network-based, shared and virtualized storage) will only be sanitized and/or restored from backup if formally determined to be necessary by Army Cyber Command and Second Army after consultation with the cognizant ISSM/IAM, IAPM and/or RMF AO/DAA.

2. Reporting.

a. CS/IA incidents must be reported in information system-related status briefings to senior leadership and throughout the chain of command.

b. Reporting of 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.

c. As detailed in ARCYBER and Second Army procedures (e.g., reference l), the NEC or installation ISSM/IAM must ensure that the following personnel for the affected system/program have been identified and appropriately notified of the suspected or confirmed CS/IA incident.

(1) ASM/PSM.

(2) ISSM/IAM.

(3) System owner and/or program manager.

(4) Data owner and/or information owner.

(5) RMF AO/DAA.

(6) Command security manager.

(7) Commander and/or director.

(8) Original classification authority or formal designee.

d. Reporting of all CS/IA incidents is in addition to initial notification (Enclosure 3), must occur throughout the appropriate chain of command, and will include reporting in the order listed as follows, in accordance with Army Cyber Command and Second Army procedures (e.g., reference l).

(1) All personnel to their CS/IA personnel.

(2) CS/IA personnel to the ASM/PSM.

(3) CS/IA personnel to the ISSM/IAM for the Network Enterprise Center (NEC), installation, region or state.

(4) ISSM/IAM for the NEC, installation, region or state to the Regional Cyber Center (RCC).

(5) RCC to the Network Enterprise Technology Command (NETCOM) Signal Brigade.

(6) NETCOM Signal Brigade to the Theater Signal Command.

(7) Incidents meeting Army Cyber Command and Second Army reporting requirements: RCC to the Army Cyber Operations and Integration Center (ACOIC).

(8) Incidents involving non-Army assets: Army Cyber Command and Second Army to U.S. Cyber Command, the U.S. Computer Emergency Readiness Team (US-CERT), other DoD components and federal agencies.

e. The following types of incidents require additional reporting in accordance with Army Cyber Command (ARCYBER) and Second Army procedures (e.g., reference l).

(1) Privacy Act information (e.g., Personally Identifiable Information, Protected Health Information): Within one hour of receiving a report, ARCYBER must report to US-CERT per their Federal Incident Notification Guidelines (reference aa); followed by ARCYBER's reporting within 24 hours to the Army Privacy Office using DoD Form 2959 ("Breach of PII Report") (https://www.rmda.army.mil/privacy/RMDA-PO-Division.html).

(2) Cross-Domain Violations: By ARCYBER per U.S. Cyber Command orders and procedures (e.g., reference ff).

(3) Confirmed (functional or informational) compromise of confidentiality, integrity or availability: Within one hour of being positively identified and reported to/by ARCYBER, ARCYBER will report to US-CERT per their Federal Incident Notification Guidelines (reference aa).

(4) Incidents involving Special Access Programs (SAP), Sensitive Activities, Special Access Required, Alternative Compensatory Control Measures, in accordance with DoD Manual 5205.07, Volume 1: Immediately by all personnel to the program security officer (PSO) and program security manager (PSM); followed by the PSO/PSM to the CIO/G-6 SAP Special Program Office and Army Special Programs Directorate (ASPD); then ASPD to the DoD SAP Central Office (SAPCO), after which SAPCO reports to the Office of the Under Secretary of Defense for Intelligence (OUSD(I)).

(5) Incidents involving COMSEC material or cryptologic information, including Controlled Cryptographic Items, Cryptographic High-Value Products and other NSA Suite B equipment: COMSEC account manager/Key Management Infrastructure operating account manager to the Communications Security Logistics Activity (CSLA); followed by the CSLA to the National COMSEC Incident Reporting System.

(6) Incidents involving Special Intelligence (SI): In addition to the Secure Compartmented Information (SCI) reporting procedures listed below, ARCYBER and Second Army to the NSA National Security Operations Center (NSOC).

(7) Incidents confirmed to involve classified information that may become public, attract media attention or attract significant public attention, categorized as "serious security incidents" by DoD Directive 5210.50: ARCYBER and Second Army to the Army G-2; followed by the Army G-2 to OUSD(I) and the Army Public Affairs Office.

(8) Incidents confirmed to involve classified information about an intelligence activity or intelligence personnel, categorized as "serious security incidents" per DoD Directive 5210.50: ARCYBER and Second Army to the Army G-2; then the Army G-2 to OUSD(I) and the DoD senior intelligence oversight officer.

(9) Incidents that have been reported to a congressional oversight committee, confirmed to involve espionage, involve large amounts of classified information or may reveal a potential systemic weakness in classification, safeguarding or declassification policy or practices: ARCYBER and Second Army to the Army G-2; followed by the Army G-2 to OUSD(I).

(10) Incidents associated with foreign intelligence entities, in accordance with DoD Directive 5240.06: Reported within 72 hours by ARCYBER and Second Army to the Army Intelligence and Security Command (INSCOM) Counterintelligence (CI) or other responsible Defense CI component.

f. Incidents involving the following “special circumstances” per Enclosure 6 of DoD Manual 5200.01, Volume 3, require additional reporting in accordance with ARCYBER and Second Army procedures (e.g., reference l).

(1) Incidents suspected to involve deliberate compromise of classified information, espionage, a foreign intelligence service or a terrorist organization: Immediately reported by ARCYBER and Second Army to INSCOM CI or other responsible Defense CI component.

(2) Incidents suspected to involve an apparent violation of criminal law: Reported by ARCYBER and Second Army to Army Criminal Investigation Command.

(3) Incidents that actually or potentially involve SCI, in accordance with DoD Manual 5105.21, Volume 3 and Intelligence Community Directive 701: Reported by ARCYBER and Second Army to the Army G-2; followed by the Army G-2 to the National Counterintelligence Security Center (NCSC).

(4) Incidents involving inadvertent disclosure of Restricted Data (RD) and/or Formerly Restricted Data (FRD) occurring pursuant to automatic declassification processes: Reported by ARCYBER and Second Army to the Army G-2; followed by the Army G-2 to the Department of Energy, with the Army G-2 sending a copy of the report to both OUSD(I) and the Deputy Assistant Secretary of Defense for Nuclear Matters.

(5) Incidents that actually or potentially involve foreign government information (FGI) or North Atlantic Treaty Organization (NATO) information: Reported by ARCYBER and Second Army to the Army G-2; followed by the Army G-2 to the Office of the Under Secretary of Defense for Policy (OUSD(P)).

(6) Incidents that actually or potentially involve United States classified information provided to foreign governments: Reported by ARCYBER and Second Army to the Army G-2; followed by the Army G-2 to the originating DoD component, original classification authority, OUSD(I) and OUSD(P).

(7) Incidents that actually or potentially involve Critical Program Information (CPI) or CPI related to classified contracts: Reported by ARCYBER and Second Army to the program manager of record; followed by the program manager of record to Army INSCOM CI or other responsible Defense CI component.

(8) Incidents involving Alternative Compensatory Control Measures (ACCM) - protected information: Reported by the ASM/PSM to the local ACCM control officer and the Army G-2.

3. Record Keeping.

a. Responding personnel will: keep a log of all actions taken regarding the CS/IA incident response, including the date/time of the action and who performed the action; and will create and maintain records, such as tickets, as appropriate for their role.

b. IAMs/ISSMs will ensure appropriate accountability, chain of custody and handling for hardware, equipment or devices potentially affected by the CS/IA incident.

c. Records associated with the CS/IA incident (e.g., audit logs, investigation documents) must be kept in accordance with ARCYBER and Second Army procedures (e.g., reference l), AR 25-2, AR 380-5, AR 380-67, AR 15-6 and AR 380-381.