Data Spillage and Unauthorized Disclosure Policy
Enclosure 2: Terms, Responsibilities and Prevention

1. Terms. For the purposes of this memorandum, the following terms are used.

a. Cross-Domain Violation (CDV). Physical or logical connection of a system, device or equipment to a network for which it is not authorized and/or accredited. This is a cybersecurity/information assurance incident that must be reported, and that greatly increases the risk of data spillage and/or unauthorized disclosure; however, the presence of a CDV does not necessarily mean there has already been a data spill or unauthorized disclosure.

b. Cybersecurity/Information Assurance (CS/IA) personnel. Includes privileged users, those personnel responsible for CS/IA and those personnel appointed to CS/IA positions (e.g., system administrators, network administrators, database administrators, information system security officers, IA support officers, information system security managers, IA managers, IA network managers, IA program managers, designated Risk Management Framework authorizing officials, designated approving authorities, chief information officers).

c. Data spillage/data spill. Security incident that results in the transfer of classified information or unclassified sensitive information/controlled unclassified information to an information system not authorized to store or process that information.

d. Inadvertent incident. 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).

e. Negligent incident. 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).

f. Responding personnel. Personnel performing in an incident response and/or incident reporting capacity, regardless of their assigned job function.

g. Sensitive information/unclassified sensitive information. Unclassified information that requires safeguarding and/or dissemination controls. Examples include, but are not limited to, information that contains, is labeled with, or is subject to: Controlled Unclassified Information (CUI); For Official Use Only (FOUO); Sensitive But Unclassified (SBU); Personally Identifiable Information (PII); Protected Health Information (PHI); Source Selection Information (SSI); Procurement Sensitive; Limited Distribution (LIMDIS); Law Enforcement Sensitive (LES); Privacy Act; and Export Control Act (ECA).

h. Servers. Includes cloud servers, network server resources (e.g., network attached storage), virtual servers, virtualized/shared server resources, containers, and instances and servers used for testing, staging and/or training.

i. Unauthorized disclosure. An event involving the exposure of information to entities not authorized access to the information.

j. Willful incident. 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).

2. Responsibilities.

a. All personnel must: access and carefully review the Security Classification Guides (SCGs) that apply to the systems/networks and operations they support; safeguard and protect classified and unclassified sensitive information/CUI from data spillage and unauthorized disclosure; immediately provide initial notification of all suspected or confirmed CS/IA incidents as directed in Enclosure 3; and render full cooperation in any inquiry and investigation.

b. Responding personnel must: ensure that actions are taken to appropriately isolate and contain a data spill; prevent unauthorized access to information in question while applying risk management principles to maintain continuity of operations, in accordance with AR 25-2, Army Cyber Command and Second Army procedures; preserve evidence; and ensure that all necessary notifications and reporting occur.

c. Activity security managers/program security managers (ASMs/PSMs) are the overall lead for addressing classified spillage incidents and must closely coordinate with cybersecurity/information assurance personnel (i.e., information assurance managers and information system security managers (IAMs/ISSMs)) per DoD Manual 5200.01, Volume 3.

d. IAMs/ISSMs are the overall lead for coordinating the cybersecurity/information assurance (CS/IA) personnel's reporting of and response to all CS/IA incidents. They must: coordinate the initiation of protective and/or corrective measures; closely coordinate with the activity security manager/program security manager on CS/IA incidents potentially involving classified systems, networks, information or data; and direct their CS/IA personnel in assisting with CS/IA incident response, notifications, reporting, inquiries, investigations, remediation and mitigation.

e. Commanders and leaders will ensure that:

(1) All Security Classification Guides for systems/networks and operations are developed and maintained in accordance with AR 380-5; entries for pertinent unclassified sensitive information/CUI that must be protected are considered for inclusion within SCGs; all personnel are provided access to and are familiar with current SCGs that apply to the systems/networks and operations they support; SCG files are searchable wherever possible (i.e., not scanned); and all SCGs, with the exception of those for Sensitive Compartmented Information and Special Access Programs, are submitted to the DoD Index of Security Classification Guides hosted by the Defense Technical Information Center (https://www.dodtechipedia.mil/dodwiki/display/techipedia/Security+Classification+Guide+-+Formerly+Security+Classification+Guide+Index).

(2) Existing Incident Response Plans (IRPs) are promptly updated to reflect this memorandum, its enclosures, and Army Cyber Command and Second Army procedures (e.g., reference l); all IRPs incorporate current policies, processes and procedures for data spillage and unauthorized disclosure; all IRPs include procedures for remediation, mitigation and sanitization, using tools approved by Army Cyber Command and Second Army (e.g., reference l); all IRPs list the common data owners, information owners, and other personnel and organizations delineated in the Initial Notification and Reporting sections of this memorandum (Enclosures 3 and 4); and the overall requirements from this memorandum and its enclosures, to specifically include notification and reporting to the Army, are incorporated into memoranda of agreement (MOAs), memoranda of understanding (MOUs) and service level agreements (SLAs), such as those with other programs, systems, networks, organizations, agencies, IT service providers and contractors.

(3) In coordination with the ASM/PSM, and in accordance with AR 380-5 and DoDM 5200.01, Volume 3, all users receive annual training: on the proper marking, labeling, storage, handling, transmission, destruction, communication and data transfer of both classified information and unclassified sensitive information/CUI; on any Privacy Act information (e.g., Personally Identifiable Information, Protected Health Information) processed by the information system; specific to each SCG and IRP that applies to the systems/networks and operations the person supports; and on the policy, processes and procedures for the prevention, identification, notification and reporting of CS/IA incidents (including, but not limited to, data spillage, unauthorized disclosure and unauthorized disclosure in the public domain).

(4) All personnel are held accountable for their actions or lack thereof, such that administrative, judicial, contractual or other disciplinary/corrective actions and civil and/or criminal penalties may be imposed when appropriate, and may be increased for repeat offenses.

(5) Plans to prevent recurrence of each CS/IA incident are formally documented, and address the root cause and contributing factors of each incident (e.g., after action report, lessons learned).

(6) The additional responsibilities designated in the May 2013 Under Secretary of the Army memorandum regarding commander and leader responsibilities for CS/IA incidents (reference h) are followed.

f. Theater Signal Commands (TSCs) will ensure that all actions to identify, contain, eradicate and report CS/IA incidents are conducted within their theater of operations. Each TSC information system security manager/IA program manager will ensure and verify that all remediation, reporting and cost determination requirements are met prior to the closure of each incident.

g. Regional Cyber Centers (RCCs) will coordinate all CS/IA incident response procedures and measures for containment, eradication and verification among the reporting organization, TSCs, Network Enterprise Centers (NECs), Regional Network Enterprise Centers (RNECs), IT, cloud and enterprise service providers, Network Enterprise Technology Command (NETCOM), Army Cyber Command, Second Army, law enforcement and counterintelligence.

h. Army Cyber Command and Second Army will, in accordance with General Orders No. 2014-02:

(1) Where authorized or directed, develop and publish Army-wide orders, procedures, lists of approved tools/technologies and training for the full life cycle of data spillage and unauthorized disclosure in accordance with Army, DoD and national policies, to include CJCSI 6510.01 and CJCSM 6510.01; update these documents as needed; publish these documents on both the NIPRNet and SIPRNet, classification permitting; and coordinate CS/IA incident response among the Army, U.S. Cyber Command, the U.S. Computer Emergency Readiness Team, the Defense Information Systems Agency, other DoD components and federal agencies.

(2) Advise, recommend and/or implement incorporation into Army-wide orders of, and procedures and training for: the specific requirements within this memorandum and its enclosures; the specific requirements within Enclosure 6 of DoDM 5200.01, Volume 3; and the “incident response” family of security controls in NIST SP 800-53 as selected, and their implementation as defined per the DoD Risk Management Framework (RMF) Knowledge Service and applicable RMF overlays.

(3) Advise, recommend and/or implement incorporation into Army-wide orders of, and procedures and training for up-to-date and validated contact information for notification/reporting to all Army and non-Army incident response organizations (as cited

by this memorandum and its enclosures), in order to expedite incident response activities conducted by any personnel and all Army organizations. Where available, this contact information must include commercial phone numbers, commercial fax numbers, Defense Switched Network (DSN) phone numbers, secure phone numbers, secure fax numbers, unclassified network email addresses, classified network email addresses, organizational websites and any relevant reporting pages on these websites.

3. Prevention.

a. All personnel must conduct any data transfer across security domains in accordance with IA Best Business Practices 03-EC-T-0002 (reference j); and applicable policies, processes and procedures from Army G-2, Army CIO/G-6, Army Cyber Command, Second Army and their Commands, systems and programs.

(1) Prior to manual data transfer, all personnel must ensure that all classified and/or unclassified sensitive information/CUI has undergone a thorough, reliable human review, appropriate overall marking and appropriate portion marking.

(2) Reliable human review of the data must be conducted by a subject matter expert prior to requesting or conducting a manual data transfer; where feasible, must include a “dirty word” search that checks for inclusion of words/phrases identified by the organization as potential indicators of non-releasable content; must follow applicable SCGs; and must use tools approved specifically for that purpose by Army G-2, Army Cyber Command and Second Army (e.g., reference l) or Army CIO/G-6 (e.g., reference j).

(3) Two-Person Integrity (TPI) is mandatory for manual data transfer from a higher classification system/domain to a lower classification system/domain (i.e., “high to low”). TPI requires that the reliable human review be performed by more than one person and that execution of the manual data transfer process be validated by more than one person.

(4) Exceptions to TPI may only be granted by signed (physically/digitally) authorization from the commander or RMF authorizing official/designated approval authority in order to meet compelling mission-essential operational requirements. Exceptions must be based upon recommendations given by the cognizant ASM/PSM and/or Command security manager; and the cognizant ISSM/IAM and/or IA program manager. Exceptions must be documented in the system/network Plan of Action and Milestones (POA&M) as non-compliance with security control “AC-4” (Information Flow Enforcement).

b. Commanders, leaders and Army organizations issuing acceptable use policies (AUP) must ensure that the following preventative requirements are included in all AUPs for programs, systems and networks.

(1) Classified and unclassified sensitive information/CUI must only be accessed, stored and processed on those devices, equipment, systems and networks that are formally and explicitly authorized for the classification level, caveats and sensitivity of the information.

(2) Personnel must not access, store or process classified and unclassified sensitive information/CUI in an insecure and/or unapproved manner.

(3) Personnel must not connect any device, system or equipment to a network for which it is not authorized and/or accredited.

(4) Personnel must not use any unauthorized device, equipment, system or network to view, access, download, post, communicate or transfer any material known or suspected to contain classified information or unclassified sensitive information/CUI.

(5) Personnel must not directly access, download or view emails and email attachments containing or labeled as classified or unclassified sensitive information/CUI from a device, equipment, system or network (e.g., cellphone, tablet, computer) not specifically authorized to process such information – either directly or through a website (e.g., webmail) – unless this is done in a formally authorized and secured manner (e.g., virtual environment, secure viewing application, sandbox application, secure thin client) that prevents such information from being either temporarily or permanently stored on the device, equipment, system or network.

c. Commanders, program managers, NECs, IT service providers, CS/IA personnel and ASMs/PSMs must ensure that:

(1) Data spillage prevention is incorporated into the design, configuration and user training for devices, equipment, systems and networks as part of the overall data loss prevention (DLP) program and architecture. Examples of this include, but are not limited to: strict access controls; encryption (communication, storage, database fields); classification/sensitivity warning banners, notifications and reminders; validation of data fields (versus permitting arbitrary text); policies for data inventory, classification and handling; monitoring tools for data creation, use, storage, transmission, disposition and disposal; and DLP solutions that detect abnormal access, evasion techniques and data exfiltration attempts.

(2) All laptops and government-furnished portable electronic devices have full disk data-at-rest encryption (e.g., Bitlocker), where supported, and/or file-based encryption (e.g., Encrypted File System) that is active and properly configured.

(3) Encryption of communication (e.g., email), transmission (e.g., data in transit) and storage (e.g., data at rest) of both classified and unclassified sensitive information/CUI occurs per AR 25-2, AR 25-1, other Army/DoD policies and Army orders. Wherever reasonable, per available technical resources and mission impact, additionally encrypt: unclassified and classified server storage; unclassified and classified workstation storage; and database fields that may contain classified or unclassified sensitive information/CUI. Encryption methods that are appropriate to the classification level, caveats and sensitivity of the information must be used.

(4) Procedures are developed for any manual data transfers (e.g., sneakernet, air-gapping), semi-automated data transfers (human initiated) and/or fully automated data transfers (machine to machine) between systems/networks that are lower classification, higher classification or in different security domains.

(5) Manual data transfers are minimized as much as possible and are only authorized if a valid mission requirement exists and there is no other option to support the requirement within the necessary timeframe.

(6) Personnel are trained at least annually in accordance with AR 380-5 and this memorandum in the proper protection, safeguarding, marking, labeling, storage, handling, transmission, destruction and data transfer of both classified and unclassified sensitive information/CUI. This includes training in reporting of theft and loss.

(7) Personnel are trained at least biennially in accordance with AR 380-5 in the proper application of relevant SCGs, to include any SCG instructions regarding data compilation and aggregation.