Data Spillage and Unauthorized Disclosure Policy
Enclosure 1: References

a. Army Regulation (AR) 25-2, Information Assurance (IA), 23 March 2009. (http://www.apd.army.mil)

b. AR 25-1, Army Information Technology (IT), 25 June 2013. (http://www.apd.army.mil)

c. AR 380-5, Department of the Army Information Security Program, 29 September 2000. (http://www.apd.army.mil)

d. AR 380-67, Personnel Security Program, 24 January 2014. (http://www.apd.army.mil)

e. AR 15-6, Procedures for Investigating Officers and Boards of Officers, 2 October 2006. (http://www.apd.army.mil)

f. AR 380-381, Special Access Programs (SAPs) and Sensitive Activities, 21 April 2004. (http://www.apd.army.mil)

g. AR 380-40, Safeguarding and Controlling Communications Security Material, 9 July 2012. (U//FOUO) (http://www.apd.army.mil)

h. Memorandum, Under Secretary of the Army, 10 May 2013, subject: Commander and Leader Responsibilities for Cybersecurity/Information Assurance (CS/IA) Incidents. (https://informationassurance.us.army.mil)

i. Army Information Assurance Best Business Practices (IA BBP) 03-PE-O-0003, Sanitization of Media, 22 August 2012, as amended. (https://informationassurance.us.army.mil)

j. Army IA BBP 03-EC-T-0002, Data Transfer Across Security Domains, 23 May 2006, as amended. (https://informationassurance.us.army.mil)

k. ALARACT 224/2013, 11 September 2013, subject: Emphasizing the Protection of Classified Information and the Integrity of Unclassified Government Information Technology (IT) Systems. (http://www.apd.army.mil)

l. Army Cyber Command Execute Order (EXORD) 2012-276, 7 June 2012, subject: Unauthorized Disclosure of Classified Information via Electronic Communication Reporting Procedures; and associated Fragmentary Orders (FRAGO). (U//FOUO)

m. DoD Directive (DoDD) 5210.50, Management of Serious Security Incidents Involving Classified Information, 27 October 2014. (http://www.dtic.mil/whs/directives)

n. DoDD 5240.06, Counterintelligence Awareness and Reporting (CIAR), 30 May 2013. (http://www.dtic.mil/whs/directives)

o. DoD Manual (DoDM) 5200.01 Volume 3, DoD Information Security Program: Protection of Classified Information, 19 March 2013. (http://www.dtic.mil/whs/directives)

p. DoDM 5200.01 Volume 4, DoD Information Security Program: Controlled Unclassified Information (CUI), 13 February 2012. (http://www.dtic.mil/whs/directives)

q. DoDM 5105.21 Volume 3, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities, 19 October 2012. (http://www.dtic.mil/whs/directives)

r. DoDM 5205.07 Volume 1, DoD Special Access Program (SAP) Security Manual: General Procedures, 18 June 2015. (http://www.dtic.mil/whs/directives)

s. Memorandum, Deputy Secretary of Defense, 14 August 2014, subject: Unauthorized Disclosures of Classified Information or Controlled Unclassified Information on DoD Information Systems. (https://informationassurance.us.army.mil)

t. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), 9 February 2011, as amended. (http://www.dtic.mil/cjcs_directives)

u. Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B, Cyber Incident Handling Program, 10 July 2012, as amended. (http://www.dtic.mil/cjcs_directives)

v. DoD Risk Management Framework Knowledge Service (RMF KS), as amended. (https://rmfks.osd.mil)

w. Committee on National Security Systems (CNSS) Policy No. 18, National Policy on Classified Information Spillage, June 2006. (http://www.cnss.gov)

x. CNSS Instruction (CNSSI) 1001, National Instruction on Classified Information Spillage, February 2008. (http://www.cnss.gov)

y. CNSSI 4003, Reporting and Evaluating Communications Security (COMSEC) Incidents, 27 May 2014, as amended. (U//FOUO) (http://www.cnss.gov)

z. Intelligence Community Directive (ICD) 701, Security Policy Directive for Unauthorized Disclosures of Classified Information, 14 March 2007. (U//FOUO)

aa. United States Computer Emergency Readiness Team (US-CERT) Federal Incident Notification Guidelines, 1 October 2014, as amended. (https://www.us-cert.gov/incident-notification-guidelines)

bb. National Security Agency (NSA) / Central Security Service (CSS) Policy Manual 9-12, NSA/CSS Storage Device Sanitization Manual, 15 December 2014, as amended. (https://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance)

cc. NSA/CSS Media Destruction Guidance, as amended. (https://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance)

dd. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, May 2013, as amended. (http://csrc.nist.gov/publications)

ee. NIST SP 800-88 Revision 1, Guidelines for Media Sanitization, December 2014, as amended. (http://csrc.nist.gov/publications)

ff. U.S. Cyber Command Task Order J3-14-0035, Approved Cross-Domain Violation(s) (CDV) Mitigation Strategies, 11 February 2014. (U//FOUO)

gg. Headquarters, Department of the Army General Orders No. 2014-02, Affirmation of Secretary of the Army Commitment to Unity of Effort; Designation of U.S. Army Cyber Command as an Army Force Component Headquarters; Reactivation of Second Army and Designation as a Direct Reporting Unit; Disestablishment of the U.S. Army Network Enterprise Technology Command/9th Signal Command (Army) as a Direct Reporting Unit and Reassignment to Second Army; Designation of General Court-Martial Convening Authorities, 6 March 2014.

hh. Army Cyber Command and Second Army, Security Classification Guide for Cyberspace Operations and Security, 29 May 2015, as amended. (U//FOUO) (https://army.deps.mil/Army/CMDS/ARCYBER/External/G2/Security/Lists/Announcements/)