1003 Privacy and Security Incident Reporting

I. Applicability

All employees, contractors, and workforce members are required to report privacy and security incidents in accordance with this policy. Failure to do so is subject to disciplinary action as outlined in DHS Policy 4002, "Privacy and Security Sanctions," as well as DHS Policy 1084, "Employee Discipline: Conduct/Performance."

II. Policy

(A) All privacy or security incidents must be reported immediately by all DHS employees, contractors, and workforce members by utilizing the DHS Real Time Incident Reporting System (http://kadril.dhhs.arkgov.net/itsec5/incidentreportform.aspx) or by contacting the Chief Information Security Officer by email or phone. A privacy or security incident is an occurrence, or suspected occurrence, that affects the confidentiality or integrity of DHS information.

(B) Examples of privacy or security incidents include, without limitation:

(1) Failure to follow any DHS Privacy or Security Policy (1001, 1002, 4000s-5000s);

(2) Lost, missing, or stolen DHS electronic devices, (laptops, iPads, tablets, cell phones, cameras, flash drives--whether encrypted or not, it must be reported);

(3) Lost, missing, or stolen files or documents containing confidential information of DHS clients or employees;

(4) Confidential information emailed, post mailed, faxed, or otherwise disclosed to the wrong or unauthorized recipient;

(5) Failure to e-mail confidential information outside of DHS with "SENSITIVE" in the subject line or body of the email;

(6) Unauthorized access, acquisition, use, or disclosure of confidential information (personally identifiable information (PII) or protected health information (PHI));

(7) Password sharing or any misuse of a DHS computer or electronic device;

(8) Unauthorized devices connected to or unauthorized software installed on a DHS Information System;

(9) Suspected hacking attempts, email hoaxes, phishing scams, social engineering attempts, virus, worm, or "Trojan Horse" activity, website defacement, exploiting system vulnerabilities, port or network scans or probes (email that is what is commonly known as SPAM that does not appear to be looking for information

should be deleted and does not need to be reported, but other attempts as listed in this point should be reported);

(10) Physical intrusion or attempted intrusions into DHS facilities containing DHS Information Systems or confidential information; or,

(11) Any behavior that might threaten the safety or security of DHS Information Systems or confidential information.

(12) Any loss of PII or a security incident, which includes Social Security Administration (SSA)-provided information, must be reported by the DHS incident response team to the SSA Regional Office Contact or the SSA Systems Security Contact identified in the data sharing agreement with SSA. If, for any reason, the DHS incident response team is unable to notify the SSA Regional Office or the SSA Systems Security Contact within one hour, the responsible State Agency official or delegate must report the incident by contacting SSA's National Network Service Center (NNSC) toll free at 1-877-697-4889 (select "Security and PII Reporting" from the options list).

(C) If it is discovered during the course of an investigation that other employees failed to report a privacy or security incident or violated any other privacy or security policies or procedures, then those employees are subject to disciplinary action as specifically outlined in DHS Policy 4002, "Privacy and Security Sanctions." DHS Policy 1084, "Employee Discipline" may also be cited for violations.

(D) Reporting a privacy or security incident to a supervisor is not sufficient to comply with the reporting requirement. If an employee reports an incident to a supervisor, it becomes both the employee's and the supervisor's responsibility to ensure that the incident is immediately reported via the Incident Reporting System. Any questions can be directed to the DHS Privacy Office or IT Security Office.

(E) If an employee with the DHS Privacy or IT Security Offices instructs an employee to file a report via the Incident Reporting System and the employee fails to do so, that will be considered a Failure to Report Class II Offense and subject to a Class II Sanction per DHS Policy 4002, "Privacy and Security Sanctions."

(F) All DHS employees are expected to cooperate with the DHS Privacy and IT Security Offices throughout the investigation of an incident. Lying or misrepresenting facts during such an investigation is subject to termination as detailed in DHS Policy 4002, "Privacy and Security Sanctions."

(G) Various divisions and other agencies may be called upon to assist during an investigation. The DHS Privacy Officer or the Chief Information Security Officer (CISO) will make divisional contact through the appropriate divisional executive, supervisor, or designated IT security manager. Division Directors or their designees will assist in determining the appropriate disciplinary action for employees involved in

privacy and security incidents, as long as it is consistent with DHS Policy 4002, "Privacy and Security Sanctions."

(H) The IT Security and Privacy Offices will diligently attempt to complete an investigation promptly after receiving an incident report. However, circumstances regarding the incident could lengthen an investigation. The CISO or the DHS Privacy Officer will submit a final report to the employee's supervisor and Director or designee. The final report will contain a detailed account of the investigation, evidence, findings, and any appropriate sanctions.

(I) Pursuant to Ark. Code Ann. § 10-4-29, DHS must report security incidents (as defined in the Arkansas Code) to Arkansas Legislative Audit (ALA) within five (5) state business days of learning of the security incident. The Office of Security and Compliance is responsible for all reports to ALA.

III. Failure to Comply

Violations of this policy may result in disciplinary action as outlined in DHS policies 4002, "DHS Privacy and Security Sanctions," and 1084, "Employee Discipline: Conduct/Performance."