

Table of Contents

[Exhibit A–Internal District Computer Security Incident Reporting Form](#)

[Exhibit B–Texas Department of Public Safety Computer Security Incident Reporting Form](#)

Exhibit A—Internal District Computer Security
Incident Reporting Form

Note: This form is to be used at the District level for reporting and tracking a computer security incident involving criminal history records information. See Exhibit B for reporting requirements to the Texas Department of Public Safety.

If the incident involves unauthorized use of or access to the District's cyberinfrastructure, the incident should also be reported in accordance with the District's cybersecurity plan. [See CQB]

Name of person reporting
incident (*print*): _____

Date of report
(*mm/dd/yyyy*): _____

Date of incident
(*mm/dd/yyyy*): _____

Name of
person to whom report was
submitted (*print*): _____

Phone: _____

Email: _____

Location(s) of incident: _____

Area(s) affected: _____

Method of detection: _____

Description of incident: _____

Actions taken
in response to the incident: _____

Submit copies of this form to Dr. Gregory Nelson, Assistant Superintendent for Human Resources as soon as possible but no later than 245 hours of the time of detection.

Exhibit B—Texas Department of Public Safety
Computer Security Incident Reporting Form

Note: To report a computer security incident to the Texas Department of Public Safety (DPS) involving criminal history record information, a District must use the online incident response form¹ provided by the DPS's Criminal Justice Information Service (CJIS) Security Office.

¹ Texas Department of Public Safety Criminal Justice Information Service (CJIS) Security Office:
<http://www.dps.texas.gov/SecurityReview/documents.htm>