# HOUSE RESEARCH

## Bill Summary

**FILE NUMBER:** H.F. 183 **DATE:** March 21, 2013
**Version:** First Engrossment

**Authors:** Holberg and others

**Subject:** Government data; breaches of security

**Analyst:** Matt Gehring, 651-296-5052



## Overview

This bill expands disclosure requirements and modifies penalties related to unauthorized access to government data classified as not public.

**Section**

**1** **Access to data by individual.** Permits an individual data subject to request the name of any persons who have obtained access to private data on the individual, unless the data would identify an undercover law enforcement officer or are active investigative data.

**2** **Data protection.** Requires the responsible authority to establish procedures for ensuring that not public data are accessible only to persons whose work assignments reasonably require access, and that it is only accessed for those purposes, and requires the responsible authority to develop a policy incorporating these procedures, which may include a model policy governing access if data is shared with other government entities.

**3** **Disclosure of breach in security; notice and investigation report required.** Expands an existing section of law requiring data subjects to be notified of a breach in the security of data to include all government entities. The current law applies only to state agencies.

This section also clarifies the definition of "breach in the security of data" and requires a report to be published upon completion of an investigation into a breach once all rights of appeal have been exhausted. The report must include a description of the data accessed or acquired, and, if disciplinary action was imposed against an employee, the number of individual data subjects affected, the names of employees determined responsible, and the final disposition of disciplinary action.

**Section**

The report must be posted on the government entity's website or bulletin board, and provided to a data subject who requests it.

**4** **Penalties.** Provides that conduct which constitutes a knowing unauthorized acquisition of not public data is a misdemeanor, and is just cause for suspension without pay or dismissal of the offending employee.

**5** **Data classification; general rule.** Provides that the name of agencies submitting data to the Comprehensive Incident-Based Reporting System (CIBRS) are public, along with a general description of the types of data submitted by the agency to the CIBRS system.