# HOUSE BILL 959

P1, L6 3lr2326
CF SB 676

By: **Delegate Lee (Commission on Maryland Cybersecurity Innovation and Excellence) and Delegates Bobo, Cullison, DeBoy, Dumais, Eckardt, Healey, Hough, McDonough, A. Miller, Mizeur, Pendergrass, B. Robinson, S. Robinson, Stocksdale, F. Turner, and Valderrama**

Introduced and read first time: February 7, 2013
Assigned to: Health and Government Operations

A BILL ENTITLED

AN ACT concerning

**Governmental Procedures – Security and Protection of Information**

FOR the purpose of requiring a certain unit, when destroying a resident's records that contain certain personal or private information of the resident, to take certain steps to protect against the unauthorized acquisition or use of the personal or private information under certain circumstances; requiring certain units that collect certain personal or private information of a resident to implement and maintain certain security procedures and practices under certain circumstances; requiring certain units that collect or maintain computerized data that include certain personal or private information of a resident to conduct a certain investigation under certain circumstances and notify certain persons of a breach of the security of a system under certain circumstances; specifying the time at which notification must be given; specifying the contents of the notification; authorizing notification to be given in a certain manner; requiring certain units to retain certain records for a certain period of time under certain circumstances; providing that a waiver of certain provisions of this Act is contrary to public policy and is void and unenforceable; providing that compliance with certain provisions of this Act does not relieve a certain unit from a duty to comply with certain other requirements of federal law; providing that the provisions of this Act are exclusive and shall preempt any provision of local law; requiring a unit to report to certain consumer reporting agencies on the breach of the security of a system under certain circumstances; requiring a unit to provide notice of a breach of the security of a system to the Office of Attorney General and the Department of Information Technology under certain circumstances; establishing a private right of action for a resident affected by a violation of this Act; requiring the Department, in consultation with the Office of the Attorney General and the Department of Budget and Management, to adopt certain rules and regulations; defining certain terms; providing for the

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.**
**[**Brackets**]** indicate matter deleted from existing law.

applicability of a certain provision of this Act; and generally relating to the protection of information collected by units or included in computerized data that is collected and maintained by units.

BY adding to
Article – State Government
Section 10–1301 through 10–1309 to be under the new subtitle "Subtitle 13. Protection of Information by Government Agencies"
Annotated Code of Maryland
(2009 Replacement Volume and 2012 Supplement)

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:

**Article – State Government**

**SUBTITLE 13. PROTECTION OF INFORMATION BY GOVERNMENT AGENCIES.**

**10–1301.**

**(A) IN THIS SUBTITLE THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.**

**(B) "ENCRYPTED" MEANS THE PROTECTION OF DATA IN ELECTRONIC OR OPTICAL FORM, IN STORAGE OR IN TRANSIT USING AN ENCRYPTION TECHNOLOGY THAT HAS BEEN ADOPTED BY AN ESTABLISHED STANDARDS SETTING BODY OF THE FEDERAL GOVERNMENT, INCLUDING THE FEDERAL INFORMATION PROCESSING STANDARDS ISSUED BY THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, WHICH RENDERS SUCH DATA INDECIPHERABLE WITHOUT AN ASSOCIATED CRYPTOGRAPHIC KEY NECESSARY TO ENABLE DECRYPTION OF SUCH DATA.**

**(C) (1) "PERSONAL INFORMATION" MEANS ANY INFORMATION CONCERNING A NATURAL PERSON THAT, BECAUSE OF NAME, NUMBER, PERSONAL MARK, UNIQUE BIOMETRIC OR GENERIC PRINT, IMAGE OR DATA, OR OTHER IDENTIFIER, CAN BE USED TO IDENTIFY SUCH A NATURAL PERSON.**

**(2) "PERSONAL INFORMATION" DOES NOT INCLUDE:**

**(I) PUBLICLY AVAILABLE INFORMATION THAT IS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC FROM FEDERAL, STATE, OR LOCAL GOVERNMENT RECORDS;**

**(II) INFORMATION THAT AN INDIVIDUAL HAS CONSENTED TO HAVE PUBLICLY DISSEMINATED OR LISTED; OR**

**(III) INFORMATION THAT IS DISSEMINATED OR LISTED IN ACCORDANCE WITH THE FEDERAL HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT.**

**(D) "PRIVATE INFORMATION" MEANS PERSONAL INFORMATION IN COMBINATION WITH ANY ONE OR MORE OF THE FOLLOWING DATA ELEMENTS, WHETHER OR NOT ANY OF THE ELEMENTS ARE ENCRYPTED:**

**(1) SOCIAL SECURITY NUMBER;**

**(2) DRIVER'S LICENSE OR STATE IDENTIFICATION CARD NUMBER;**

**(3) PASSPORT NUMBER OR OTHER UNITED STATES ISSUED IDENTIFICATION NUMBER; OR**

**(4) ACCOUNT NUMBER, CREDIT OR DEBIT CARD NUMBER, IN COMBINATION WITH ANY REQUIRED SECURITY CODE, ACCESS CODE, OR PASSWORD THAT WOULD PERMIT ACCESS TO THE FINANCIAL ACCOUNT OF AN INDIVIDUAL.**

**(E) "REASONABLE SECURITY PROCEDURES AND PRACTICES" MEANS DATA SECURITY PROCEDURES AND PRACTICES DEVELOPED, IN GOOD FAITH, AND SET FORTH IN A WRITTEN INFORMATION SECURITY POLICY THAT CLEARLY DEMONSTRATES THAT THE PROCEDURES AND PRACTICES:**

**(1) COORDINATE AN INFORMATION SECURITY PROGRAM;**

**(2) REQUIRE A RISK ASSESSMENT TO IDENTIFY REASONABLY FORESEEABLE INTERNAL AND EXTERNAL RISKS TO THE SECURITY, CONFIDENTIALITY, AND INTEGRITY OF CUSTOMER INFORMATION AND TO ASSESS THE SUFFICIENCY OF ANY SAFEGUARDS IN PLACE TO CONTROL THESE RISKS;**

**(3) ONCE A RISK ASSESSMENT IS COMPLETED, INCLUDE DESIGN SAFEGUARDS TO CONTROL THE IDENTIFIED RISKS AND TO MONITOR REGULARLY THE EFFECTIVENESS OF THE CONTROLS;**

**(4) CONTRACTUALLY ENSURE THAT SPECIFIED SERVICE PROVIDERS ARE CAPABLE OF PROVIDING APPROPRIATE SAFEGUARDS FOR THE PERSONAL AND PRIVATE INFORMATION OF CUSTOMERS; AND**

**(5) EVALUATE AND ADJUST THE INFORMATION SECURITY PROGRAM BASED ON THE FOLLOWING:**

**(I) THE FINDINGS OF THE REGULAR MONITORING AND TESTING OF INFORMATION SAFEGUARDS;**

**(II) MATERIAL CHANGES TO OPERATIONS OR BUSINESS ARRANGEMENTS; OR**

**(III) CIRCUMSTANCES THAT THE BUSINESS KNOWS OR HAS REASON TO KNOW MAY HAVE A MATERIAL IMPACT ON THE INFORMATION SECURITY PROGRAM OF THE BUSINESS.**

**(F) "RECORDS" MEANS INFORMATION THAT IS INSCRIBED ON A TANGIBLE MEDIUM OR THAT IS STORED IN AN ELECTRONIC OR OTHER MEDIUM AND IS RETRIEVABLE IN PERCEIVABLE FORM.**

**(G) "RESIDENT" MEANS AN INDIVIDUAL RESIDING IN THE STATE WHO PROVIDES PERSONAL OR PRIVATE INFORMATION TO A UNIT FOR THE PURPOSE OF OBTAINING A SERVICE, PRODUCT, OR DOCUMENT FROM THE GOVERNMENT AGENCY.**

**(H) "UNIT" MEANS:**

**(1) AN EXECUTIVE, LEGISLATIVE, OR JUDICIAL AGENCY, OR A DEPARTMENT, A BOARD, A COMMISSION, AN AUTHORITY, AN INSTITUTION, A UNIT OR AN INSTRUMENTALITY OF THE STATE; OR**

**(2) A COUNTY, MUNICIPALITY, BI–COUNTY AGENCY, COUNTY BOARD OF EDUCATION, PUBLIC AUTHORITY, OR ANY OTHER POLITICAL SUBDIVISION OF THE STATE.**

**10–1302.**

**WHEN A UNIT IS DESTROYING RECORDS OF A RESIDENT THAT CONTAIN PERSONAL OR PRIVATE INFORMATION OF THE RESIDENT, THE UNIT SHALL TAKE REASONABLE STEPS TO PROTECT AGAINST UNAUTHORIZED ACCESS TO OR USE OF THE PERSONAL OR PRIVATE INFORMATION, TAKING INTO ACCOUNT:**

**(1) THE SENSITIVITY OF THE RECORDS;**

**(2) THE NATURE AND SIZE OF THE UNIT AND ITS OPERATIONS;**

**(3) THE COSTS AND BENEFITS OF DIFFERENT DESTRUCTION METHODS; AND**

**(4) AVAILABLE TECHNOLOGY.**

**10–1303.**

**(A) TO PROTECT PRIVATE INFORMATION FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, OR DISCLOSURE, A UNIT THAT COLLECTS PERSONAL INFORMATION OF A RESIDENT SHALL IMPLEMENT AND MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT ARE APPROPRIATE TO THE NATURE OF THE PERSONAL OR PRIVATE INFORMATION COLLECTED AND THE NATURE AND SIZE OF THE UNIT AND ITS OPERATIONS.**

**(B) (1) THIS SUBSECTION SHALL APPLY TO A WRITTEN CONTRACT THAT IS ENTERED INTO ON OR AFTER JANUARY 1, 2014.**

**(2) A UNIT THAT USES A NONAFFILIATED THIRD PARTY AS A SERVICE PROVIDER TO PERFORM SERVICES FOR THE UNIT AND DISCLOSES PERSONAL OR PRIVATE INFORMATION ABOUT A RESIDENT UNDER A WRITTEN CONTRACT WITH THE THIRD PARTY SHALL REQUIRE BY CONTRACT THAT THE THIRD PARTY IMPLEMENT AND MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT:**

**(I) ARE APPROPRIATE TO THE NATURE OF THE PERSONAL OR PRIVATE INFORMATION DISCLOSED TO THE NONAFFILIATED THIRD PARTY; AND**

**(II) ARE REASONABLY DESIGNED TO HELP PROTECT THE PERSONAL OR PRIVATE INFORMATION FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR DESTRUCTION.**

**10–1304.**

**(A) (1) IN THIS SECTION THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.**

**(2) (I) "BREACH OF THE SECURITY OF A SYSTEM" MEANS THE UNAUTHORIZED ACQUISITION OF COMPUTERIZED DATA THAT COMPROMISES THE SECURITY, CONFIDENTIALITY, OR INTEGRITY OF THE PERSONAL OR PRIVATE INFORMATION MAINTAINED BY A UNIT.**

**(II) "BREACH OF THE SECURITY OF A SYSTEM" DOES NOT INCLUDE THE GOOD FAITH ACQUISITION OF PERSONAL INFORMATION BY AN EMPLOYEE OR AGENT OF A UNIT FOR THE PURPOSES OF THE UNIT, PROVIDED THAT THE PERSONAL OR PRIVATE INFORMATION IS NOT USED OR SUBJECT TO FURTHER UNAUTHORIZED DISCLOSURE.**

**(3) "IDENTITY FRAUD" HAS THE MEANING STATED IN § 8–301(B) OR (C) OF THE CRIMINAL LAW ARTICLE.**

**(B) (1) IF A UNIT THAT COLLECTS COMPUTERIZED DATA THAT INCLUDES PRIVATE INFORMATION OF A RESIDENT DISCOVERS OR IS NOTIFIED OF A BREACH OF THE SECURITY OF A SYSTEM, THE UNIT SHALL CONDUCT IN GOOD FAITH A REASONABLE AND PROMPT INVESTIGATION TO DETERMINE WHETHER THE UNAUTHORIZED ACQUISITION OF PRIVATE INFORMATION OF THE RESIDENT HAS CREATED OR IS REASONABLY LIKELY TO CREATE A MATERIAL RISK OF IDENTITY FRAUD.**

**(2) IF AFTER THE INVESTIGATION IS CONCLUDED, THE UNIT DETERMINES THAT THE UNAUTHORIZED ACQUISITION OF THE RESIDENT'S PERSONAL OR PRIVATE INFORMATION HAS CREATED OR IS REASONABLY LIKELY TO CREATE A MATERIAL RISK OF IDENTITY FRAUD, THE UNIT SHALL NOTIFY THE RESIDENT OF THE BREACH.**

**(3) EXCEPT AS PROVIDED IN SUBSECTION (D) OF THIS SECTION, THE NOTIFICATION REQUIRED UNDER PARAGRAPH (2) OF THIS SUBSECTION SHALL BE GIVEN AS SOON AS REASONABLY PRACTICABLE, BUT NOT LATER THAN 45 DAYS AFTER THE UNIT CONDUCTS THE INVESTIGATION REQUIRED UNDER PARAGRAPH (1) OF THIS SUBSECTION.**

**(4) IF, AFTER THE INVESTIGATION REQUIRED UNDER PARAGRAPH (1) OF THIS SUBSECTION IS CONCLUDED, THE UNIT DETERMINES THAT NOTIFICATION UNDER PARAGRAPH (2) OF THIS SUBSECTION IS NOT REQUIRED, THE UNIT SHALL MAINTAIN RECORDS THAT REFLECT ITS DETERMINATION FOR 3 YEARS AFTER THE DETERMINATION IS MADE.**

**(C) (1) A PARTY THAT MAINTAINS COMPUTERIZED DATA THAT INCLUDES PRIVATE INFORMATION PROVIDED BY A UNIT SHALL NOTIFY THE UNIT OF A BREACH OF THE SECURITY OF A SYSTEM IF THE UNAUTHORIZED ACQUISITION OF THE RESIDENT'S PRIVATE INFORMATION HAS CREATED OR IS REASONABLY LIKELY TO CREATE A MATERIAL RISK OF IDENTITY FRAUD.**

**(2) EXCEPT AS PROVIDED IN SUBSECTION (D) OF THIS SECTION, THE NOTIFICATION REQUIRED UNDER PARAGRAPH (1) OF THIS SUBSECTION**

**SHALL BE GIVEN AS SOON AS REASONABLY PRACTICABLE, BUT NOT LATER THAN 45 DAYS AFTER THE UNIT DISCOVERS OR IS NOTIFIED OF THE BREACH OF THE SECURITY OF A SYSTEM.**

**(3) A PARTY THAT IS REQUIRED TO NOTIFY A UNIT OF A BREACH OF THE SECURITY OF A SYSTEM UNDER PARAGRAPH (1) OF THIS SUBSECTION SHALL SHARE WITH THE UNIT INFORMATION RELATING TO THE BREACH.**

**(D) (1) THE NOTIFICATION REQUIRED UNDER SUBSECTIONS (B) AND (C) OF THIS SECTION MAY BE DELAYED:**

**(I) IF A LAW ENFORCEMENT AGENCY DETERMINES THAT THE NOTIFICATION WILL IMPEDE A CRIMINAL INVESTIGATION OR JEOPARDIZE HOMELAND OR NATIONAL SECURITY; OR**

**(II) TO DETERMINE THE SCOPE OF THE BREACH OF THE SECURITY OF A SYSTEM, IDENTIFY THE INDIVIDUALS AFFECTED, OR RESTORE THE INTEGRITY OF THE SYSTEM.**

**(2) IF NOTIFICATION IS DELAYED UNDER PARAGRAPH (1)(I) OF THIS SUBSECTION, NOTIFICATION SHALL BE GIVEN AS SOON AS REASONABLY PRACTICABLE, BUT NOT LATER THAN 45 DAYS AFTER THE LAW ENFORCEMENT AGENCY DETERMINES THAT THE NOTIFICATION WILL NOT IMPEDE A CRIMINAL INVESTIGATION AND WILL NOT JEOPARDIZE HOMELAND OR NATIONAL SECURITY.**

**(E) THE NOTIFICATION REQUIRED UNDER SUBSECTION (B) OF THIS SECTION MAY BE GIVEN:**

**(1) BY WRITTEN NOTICE SENT TO THE MOST RECENT ADDRESS OF THE INDIVIDUAL IN THE RECORDS OF THE UNIT;**

**(2) BY ELECTRONIC MAIL TO THE MOST RECENT ELECTRONIC MAIL ADDRESS OF THE RESIDENT IN THE RECORDS OF THE UNIT IF:**

**(I) THE RESIDENT HAS EXPRESSLY CONSENTED TO RECEIVE ELECTRONIC NOTICE; OR**

**(II) THE UNIT CONDUCTS ITS DUTIES PRIMARILY THROUGH INTERNET ACCOUNT TRANSACTIONS OR THE INTERNET;**

**(3) BY TELEPHONIC NOTICE, TO THE MOST RECENT TELEPHONE NUMBER OF THE RESIDENT IN THE RECORDS OF THE UNIT; OR**

**(4) BY SUBSTITUTE NOTICE AS PROVIDED IN SUBSECTION (F) OF THIS SECTION IF:**

**(I) THE UNIT DEMONSTRATES THAT THE COST OF PROVIDING NOTICE WOULD EXCEED $100,000 OR THAT THE AFFECTED CLASS OF INDIVIDUALS TO BE NOTIFIED EXCEEDS 175,000; OR**

**(II) THE UNIT DOES NOT HAVE SUFFICIENT CONTACT INFORMATION TO GIVE NOTICE IN ACCORDANCE WITH ITEM (1), (2), OR (3) OF THIS SUBSECTION.**

**(F) SUBSTITUTE NOTICE UNDER SUBSECTION (E)(4) OF THIS SECTION SHALL CONSIST OF:**

**(1) ELECTRONICALLY MAILING THE NOTICE TO A RESIDENT ENTITLED TO NOTIFICATION UNDER SUBSECTION (B) OF THIS SECTION IF THE UNIT HAS AN ELECTRONIC MAIL ADDRESS FOR THE RESIDENT TO BE NOTIFIED;**

**(2) CONSPICUOUS POSTING OF THE NOTICE ON THE WEB SITE OF THE UNIT IF THE UNIT MAINTAINS A WEB SITE; AND**

**(3) NOTIFICATION TO STATEWIDE MEDIA.**

**(G) THE NOTIFICATION REQUIRED UNDER SUBSECTION (B) OF THIS SECTION SHALL INCLUDE:**

**(1) TO THE EXTENT POSSIBLE, A DESCRIPTION OF THE CATEGORIES OF INFORMATION THAT WERE, OR ARE REASONABLY BELIEVED TO HAVE BEEN, ACQUIRED BY AN UNAUTHORIZED PERSON, INCLUDING WHICH OF THE ELEMENTS OF PERSONAL OR PRIVATE INFORMATION WERE, OR ARE REASONABLY BELIEVED TO HAVE BEEN, ACQUIRED;**

**(2) CONTACT INFORMATION FOR THE UNIT MAKING THE NOTIFICATION, INCLUDING THE UNIT'S ADDRESS, TELEPHONE NUMBER, AND TOLL–FREE TELEPHONE NUMBER IF ONE IS MAINTAINED;**

**(3) THE TOLL–FREE TELEPHONE NUMBERS AND ADDRESSES FOR THE MAJOR CONSUMER REPORTING AGENCIES; AND**

**(4) (I) THE TOLL–FREE TELEPHONE NUMBERS, ADDRESSES, AND WEB SITE ADDRESSES FOR:**

**1. THE FEDERAL TRADE COMMISSION; AND**

**2. THE OFFICE OF THE ATTORNEY GENERAL; AND**

**(II) A STATEMENT THAT A RESIDENT CAN OBTAIN INFORMATION FROM THESE SOURCES ABOUT STEPS THE RESIDENT CAN TAKE TO AVOID IDENTITY THEFT.**

**(H) (1) BEFORE GIVING THE NOTIFICATION REQUIRED UNDER SUBSECTION (B) OF THIS SECTION AND SUBJECT TO SUBSECTION (D) OF THIS SECTION, A UNIT SHALL PROVIDE NOTICE OF A BREACH OF THE SECURITY OF A SYSTEM TO THE OFFICE OF THE ATTORNEY GENERAL.**

**(2) IN ADDITION TO THE NOTICE REQUIRED UNDER PARAGRAPH (1) OF THIS SUBSECTION, A UNIT, AS DEFINED IN § 10–1301(H)(1) OF THIS SUBTITLE, SHALL PROVIDE NOTICE OF A BREACH OF SECURITY TO THE DEPARTMENT OF INFORMATION TECHNOLOGY.**

**(I) A WAIVER OF ANY PROVISION OF THIS SECTION IS CONTRARY TO PUBLIC POLICY AND IS VOID AND UNENFORCEABLE.**

**(J) COMPLIANCE WITH THIS SECTION DOES NOT RELIEVE A UNIT FROM A DUTY TO COMPLY WITH ANY OTHER REQUIREMENTS OF FEDERAL LAW RELATING TO THE PROTECTION AND PRIVACY OF PERSONAL OR PRIVATE INFORMATION.**

**10–1305.**

**THE PROVISIONS OF THIS SUBTITLE ARE EXCLUSIVE AND SHALL PREEMPT ANY PROVISION OF LOCAL LAW.**

**10–1306.**

**(A) IF A UNIT IS REQUIRED UNDER § 10–1304 OF THIS SUBTITLE TO GIVE NOTICE OF A BREACH OF THE SECURITY OF A SYSTEM TO 1,000 OR MORE INDIVIDUALS, THE UNIT ALSO SHALL NOTIFY, WITHOUT UNREASONABLE DELAY, EACH CONSUMER REPORTING AGENCY THAT COMPILES AND MAINTAINS FILES ON CONSUMERS ON A NATIONWIDE BASIS, AS DEFINED BY 15 U.S.C. § 1681A(P), OF THE TIMING, DISTRIBUTION, AND CONTENT OF THE NOTICES.**

**(B) THIS SECTION DOES NOT REQUIRE THE INCLUSION OF THE NAMES OR OTHER PERSONAL IDENTIFYING INFORMATION OF RECIPIENTS OF NOTICES OF THE BREACH OF THE SECURITY OF A SYSTEM.**

**10–1307.**

**(A) IN THIS SECTION, "AFFILIATE" MEANS AN ENTITY THAT CONTRACTS WITH A UNIT IN SUBSECTION (C) OF THIS SECTION.**

**(B) A UNIT THAT COMPLIES WITH THE REQUIREMENTS FOR NOTIFICATION PROCEDURES, THE PROTECTION OR SECURITY OF PERSONAL OR PRIVATE INFORMATION, OR THE DESTRUCTION OF PERSONAL OR PRIVATE INFORMATION UNDER THE RULES, REGULATIONS, PROCEDURES, OR GUIDELINES ESTABLISHED BY THE PRIMARY OR FUNCTIONAL FEDERAL OR STATE REGULATOR OF THE UNIT SHALL BE DEEMED TO BE IN COMPLIANCE WITH THIS SUBTITLE.**

**(C) AN AFFILIATE THAT COMPLIES WITH § 501(B) OF THE FEDERAL GRAMM–LEACH–BLILEY ACT; 15 U.S.C. § 6801, § 216 OF THE FEDERAL FAIR AND ACCURATE TRANSACTIONS ACT; 15 U.S.C. § 1681W DISPOSAL OF RECORDS; THE FEDERAL INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS; AND THE FEDERAL INTERAGENCY GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE; AND ANY REVISIONS, ADDITIONS, OR SUBSTITUTIONS OF THOSE ENACTMENTS, SHALL BE DEEMED TO BE IN COMPLIANCE WITH THIS SUBTITLE.**

**10–1308.**

**(A) IF A UNIT VIOLATES THE PROVISIONS OF THIS SUBTITLE, A RESIDENT MAY FILE A CIVIL ACTION FOR DAMAGES UNDER THE APPLICABLE PROVISIONS OF:**

**(1) THE MARYLAND TORT CLAIMS ACT, AS SET FORTH IN TITLE 12 OF THIS ARTICLE; OR**

**(2) THE LOCAL GOVERNMENT TORT CLAIMS ACT, AS SET FORTH IN TITLE 5, SUBTITLE 3 OF THE COURTS ARTICLE.**

**(B) A CIVIL ACTION UNDER THIS SECTION SHALL BE FILED IN THE COUNTY IN WHICH THE RESIDENT RESIDES.**

**10–1309.**

**THE SECRETARY OF INFORMATION TECHNOLOGY, IN CONSULTATION WITH THE DEPARTMENT OF BUDGET AND MANAGEMENT AND THE DIVISION OF**

**CONSUMER PROTECTION IN THE OFFICE OF THE ATTORNEY GENERAL, SHALL ADOPT REGULATIONS TO CARRY OUT THE PROVISIONS OF THIS SUBTITLE FOR THE GOVERNMENT AGENCIES SPECIFIED IN § 10–1301(H)(1) OF THIS SUBTITLE.**

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2013.