JOINT STATE GOVERNMENT COMMISSION

General Assembly of the Commonwealth of Pennsylvania

CYBERSECURITY IN PENNSYLVANIA

A STAFF STUDY

September 2015

Serving the General Assembly of the Commonwealth of Pennsylvania Since 1937

REPORT

Cybersecurity in Pennsylvania

Project Manager:	Michael Dirckx, Staff Attorney
Staff:	Wendy L. Baker, Executive Assistant

JOINT STATE GOVERNMENT COMMISSION

Room 108 Finance Building
613 North Street
Harrisburg, PA 17120-0018

Telephone: 717-787-4397
Fax: 717-783-9380
E-mail: jntst02@legis.state.pa.us
Website: http://jsg.legis.state.pa.us

The Joint State Government Commission was created in 1937 as the primary and central non-partisan, bicameral research and policy development agency for the General Assembly of Pennsylvania.[1]

A fourteen-member Executive Committee comprised of the leadership of both the House of Representatives and the Senate oversees the Commission. The seven Executive Committee members from the House of Representatives are the Speaker, the Majority and Minority Leaders, the Majority and Minority Whips, and the Majority and Minority Caucus Chairs. The seven Executive Committee members from the Senate are the President Pro Tempore, the Majority and Minority Leaders, the Majority and Minority Whips, and the Majority and Minority Caucus Chairs. By statute, the Executive Committee selects a chairman of the Commission from among the members of the General Assembly. Historically, the Executive Committee has also selected a Vice-Chair or Treasurer, or both, for the Commission.

The studies conducted by the Commission are authorized by statute or by a simple or joint resolution. In general, the Commission has the power to conduct investigations, study issues, and gather information as directed by the General Assembly. The Commission provides in-depth research on a variety of topics, crafts recommendations to improve public policy and statutory law, and works closely with legislators and their staff.

A Commission study may involve the appointment of a legislative task force, composed of a specified number of legislators from the House of Representatives or the Senate, or both, as set forth in the enabling statute or resolution. In addition to following the progress of a particular study, the principal role of a task force is to determine whether to authorize the publication of any report resulting from the study and the introduction of any proposed legislation contained in the report. However, task force authorization does not necessarily reflect endorsement of all the findings and recommendations contained in a report.

Some studies involve an appointed advisory committee of professionals or interested parties from across the Commonwealth with expertise in a particular topic; others are managed exclusively by Commission staff with the informal involvement of representatives of those entities that can provide insight and information regarding the particular topic. When a study involves an advisory committee, the Commission seeks consensus among the members.[2] Although an advisory committee member may represent a particular department, agency, association, or group, such representation does not necessarily reflect the endorsement of the department, agency, association, or group of all the findings and recommendations contained in a study report.

---

[1] Act of July 1, 1937 (P.L.2460, No.459) (46 P.S. § 65), amended by the act of June 26, 1939 (P.L.1084, No.380); the act of March 8, 1943 (P.L.13, No.4); the act of May 15, 1956 (1955 P.L.1605, No.535); the act of December 8, 1959 (P.L.1740, No.646); and the act of November 20, 1969 (P.L.301, No.128).

[2] Consensus does not necessarily reflect unanimity among the advisory committee members on each individual policy or legislative recommendation. However, it does, at a minimum, reflect the views of a substantial majority of the advisory committee, gained after lengthy review and discussion.

Over the years, nearly one thousand individuals from across the Commonwealth have served as members of the Commission's numerous advisory committees or have assisted the Commission with its studies. Members of advisory committees bring a wide range of knowledge and experience to deliberations involving a particular study. Individuals from countless backgrounds have contributed to the work of the Commission, such as attorneys, judges, professors and other educators, state and local officials, physicians and other health care professionals, business and community leaders, service providers, administrators and other professionals, law enforcement personnel, and concerned citizens. In addition, members of advisory committees donate their time to serve the public good; they are not compensated for their service as members. Consequently, the Commonwealth of Pennsylvania receives the financial benefit of such volunteerism, along with the expertise in developing statutory language and public policy recommendations to improve the law in Pennsylvania.

The Commission periodically reports its findings and recommendations, along with any proposed legislation, to the General Assembly. Certain studies have specific timelines for the publication of a report, as in the case of a discrete or timely topic; other studies, given their complex or considerable nature, are ongoing and involve the publication of periodic reports. Completion of a study, or a particular aspect of an ongoing study, generally results in the publication of a report setting forth background material, policy recommendations, and proposed legislation. However, the release of a report by the Commission does not necessarily reflect the endorsement by the members of the Executive Committee, or the Chair or Vice-Chair of the Commission, of all the findings, recommendations, or conclusions contained in the report. A report containing proposed legislation may also contain official comments, which may be used in determining the intent of the General Assembly.[3]

Since its inception, the Commission has published more than 350 reports on a sweeping range of topics, including administrative law and procedure; agriculture; athletics and sports; banks and banking; commerce and trade; the commercial code; crimes and offenses; decedents, estates, and fiduciaries; detectives and private police; domestic relations; education; elections; eminent domain; environmental resources; escheats; fish; forests, waters, and state parks; game; health and safety; historical sites and museums; insolvency and assignments; insurance; the judiciary and judicial procedure; labor; law and justice; the legislature; liquor; mechanics' liens; mental health; military affairs; mines and mining; municipalities; prisons and parole; procurement; state-licensed professions and occupations; public utilities; public welfare; real and personal property; state government; taxation and fiscal affairs; transportation; vehicles; and workers' compensation.

Following the completion of a report, subsequent action on the part of the Commission may be required, and, as necessary, the Commission will draft legislation and statutory amendments, update research, track legislation through the legislative process, attend hearings, and answer questions from legislators, legislative staff, interest groups, and constituents.

[3] 1 Pa.C.S. § 1939 ("The comments or report of the commission . . . which drafted a statute may be consulted in the construction or application of the original provisions of the statute if such comments or report were published or otherwise generally available prior to the consideration of the statute by the General Assembly").

General Assembly of the Commonwealth of Pennsylvania
JOINT STATE GOVERNMENT COMMISSION
Room 108 – Finance Building
Harrisburg, Pa 17120

717-787-4397
Fax 717-783-9380

September 22, 2015

Dear Members of the General Assembly of Pennsylvania:

2014 House Resolution 778 directed the Joint State Government Commission to conduct a comprehensive study of the cybersecurity measures and protocols that Pennsylvania's state government established to protect residents' personal and private information stored in commonwealth computer databases.

The report, ***Cybersecurity in Pennsylvania***, presents a broad review of the cybersecurity efforts undertaken by state agencies. Because of the risk of breaches of the commonwealth's cybersecurity infrastructure and the potential for extraordinary damage, detailed analyses were not made available during the course of the study. Nonetheless, IT professionals from a number of Pennsylvania agencies cooperated in providing information to the fullest extent possible.

The report is available on our website, http://jsg.legis.state.pa.us/.

Sincerely,

Glenn Pasewicz
Executive Director

CONTENTS

INTRODUCTION

On December 19, 2013 national retail chain Target revealed that it had suffered a cyberattack that resulted in the unauthorized access to payment card data of customers making credit and debit card purchases in its U.S. stores.[4] Initially, Target estimated that approximately 40 million credit and debit card accounts may have been impacted between November 27 and December 15, 2013.[5] Upon further investigation, Target discovered that names, mailing addresses, phone numbers, or email addresses for up to 70 million individuals were also stolen.[6]

Eventually, it was determined that the hackers gained access to Target's data using network credentials stolen from an HVAC company based in Sharpsburg, Pennsylvania.[7] The credentials were stolen using an email malware attack on the HVAC company that began at least two months before hackers started stealing data from thousands of Target cash registers.[8]

The Target incident is just one of several recent high-profile instances of personal data theft. It should come as no surprise, then, that cybersecurity is becoming a growing concern for governments, which possess personal information about their citizens, as well as sensitive government data. As a result, the Pennsylvania House of Representatives adopted 2014 House Resolution 778, directing the Joint State Government Commission (JSGC) to conduct a comprehensive study of the Commonwealth's cybersecurity efforts and protocols to protect private information of its citizens.[9]

It is important to note that certain specific information about networks and security measures cannot be published in order to protect the systems in place and to avoid revealing vulnerabilities. In fact, Pennsylvania's Right-to-Know Law[10] provides a specific exception for records that, if released, would create "a reasonable likelihood of endangering the safety or the physical security of a building, public utility, resource, infrastructure, facility or information storage system...."[11]

[4] Target Brands, Inc., "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores," Dec. 19, 2013, http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores.
[5] *Id.*
[6] Target Brands, Inc., "Target Provides Update on Data Breach and Financial Performance," Jan. 10, 2014, http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance.
[7] Brian Krebs, "Target Hackers Broke in Via HVAC Company," Feb. 14, 2014, http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.
[8] Brian Krebs, "Email Attack on Vendor Set Up Breach at Target," Feb. 14, 2014, http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.
[9] 2014 H.R.778.
[10] Act of Feb 14, 2008 (P.L.6, No.3), 65 P.S. § 67.101 *et seq.*
[11] *Id.* at § 708(b)(3).

Records "regarding computer hardware, software and networks, including administrative or technical records, which, if disclosed, would be reasonably likely to jeopardize computer security" are also excepted.[12] Therefore, this report, the result of JSGC's comprehensive study, provides only an overview of the cybersecurity policies in place throughout the Commonwealth government.

Although Pennsylvania has not yet suffered a major breach, state offices and agencies are under constant threat. The question is not *whether* a breach will occur, but *when* a breach will occur. To address these concerns, JSGC staff determined that there are areas where improvements could be made. For example, centralization of cybersecurity efforts will enhance cybersecurity efforts. The Governor's Office of Administration has set a good example for centralized cybersecurity, and would be a good model for the legislature and the courts to follow. Greater cooperation between the branches will also enhance cybersecurity efforts.

The other improvement JSGC staff identified is the modernization of Pennsylvania's security breach notification law, the act of December 22, 2005, (P.L.474, No.94). This act has not been amended in the 10 years since its enactment, despite the fact that technology has rapidly changed, often in ways that could not have been foreseen, and continues to do so. This report includes suggested amendments.

[12] *Id*. at § 708(b)(4).

Each branch of Pennsylvania's government addresses cybersecurity separately. All branches of the Commonwealth government implement cybersecurity efforts and protocols directed at safeguarding the personal information of residents of the Commonwealth. However, Pennsylvania's cybersecurity standards and protocols differ between the branches of government, and to an extent, within branches of the government. Nevertheless, all branches of the Commonwealth government employ dedicated, hard-working, and well-qualified individuals who routinely examine the capabilities of the cybersecurity systems to protect against cyberattacks, and remain vigilant against evolving threats.

The Executive Branch

Pursuant to Executive Order No. 2011-05, dated July 27, 2011,[13] and as embodied in the Pennsylvania Code at Title 4, Chapter 7a, Subchapter F, the Governor's Office of Administration (OA), Office for Information Technology (OIT), is responsible for:

- Developing and recommending to the Secretary of Administration priorities and strategic plans;
- Consolidating infrastructure and support services; and
- Directing IT investments, procurement, and policy.

OIT's authority extends to all agencies under the governor's jurisdiction. OIT also provides network services to several independent agencies that are not under the governor's executive jurisdiction.

[13] 41 Pa.B. 5345.

The agencies and offices that are on OIT's network include the following:

- The Department of Aging;
- The Department of Agriculture;
- The Department of Banking & Securities;
- The Department of Community & Economic Development;
- The Department of Conservation & Natural Resources;
- The Department of Corrections;
- The Department of Drug and Alcohol Programs;
- The Department of Education;
- The Department of Environmental Protection;
- The Department of General Services;
- The Department of Health;
- The Department of Human Services (formerly The Department of Public Welfare);
- The Department of Labor & Industry;
- The Department of Military & Veterans' Affairs;
- The Department of Revenue;
- The Department of State;
- The Department of Transportation;
- The Executive Offices;
- The Milk Marketing Board;
- The Office of the Lieutenant Governor;
- The Pennsylvania Board of Probation & Parole;
- The Pennsylvania Emergency Management Agency;
- The Pennsylvania Environmental Hearing Board;
- The Pennsylvania Fish & Boat Commission;
- The Pennsylvania Game Commission;
- The Pennsylvania Gaming Control Board;
- The Pennsylvania Historical & Museum Commission;
- The Pennsylvania Infrastructure Investment Authority (PENNVEST);
- The Pennsylvania Insurance Department;
- The Pennsylvania Liquor Control Board;
- The Pennsylvania Municipal Retirement Board;
- The Pennsylvania Public Utility Commission;
- The Pennsylvania State Civil Service Commission;
- The Pennsylvania State Employees' Retirement System;
- The Pennsylvania State Ethics Commission;
- The Pennsylvania State Police;
- The Pennsylvania Treasury; and
- The Public School Employees' Retirement System.

OIT has numerous written policies on the subject of cybersecurity, and these policies are publicly available on its website.[14] These policies address everything from security auditing and monitoring, to contractor background checks, encryption standards, and incident reporting.[15] In addition, OIT's website provides a wealth of general information regarding cybersecurity that is applicable to government offices and the Commonwealth's residents alike.[16]

According to information provided to JSGC staff for the purposes of this report, OIT conducts compliance checks on agencies and works with outside vendors to perform risk assessments. OIT is aligning its policies with the recently-released National Institute of Standards and Technology (NIST) Cybersecurity Framework, as well as the National Governors Association's (NGA) call to action.[17]

OIT is actively engaged in improving Pennsylvania's cybersecurity. One example of OIT's efforts is a grant from NIST as part of the National Strategy for Trusted Identities in Cyberspace (NSTIC), a public-private initiative to identify ways to create an identity ecosystem that allows individuals to choose from an array of credentials in order to transact business online.[18] Specifically, the pilot program will enable Pennsylvanians to obtain one secure credential to conduct online transactions with participating agencies.[19] If the pilot program is successful, Pennsylvanians would register just once to access a variety of services, eliminating the need to create multiple accounts.[20]

OIT is also implementing security scorecards, which indicate how well the offices and agencies under its authority are managing risks.[21] The scorecards will allow agency executives to see what security risks each agency is facing, compare risks among agencies, and see how quickly issues are addressed.[22]

---

[14] *See* Pa. Office of Admin., Records and Directives, http://www.portal.state.pa.us/portal/server.pt?open=514&objID=210791&mode=2.

[15] *Id.*

[16] *See* Pa. Office of Admin., Chief Info. Sec. Office, http://www.portal.state.pa.us/portal/server.pt/community/cyber_security/337; http://www.portal.state.pa.us/portal/server.pt/community/security_awareness/494; http://www.portal.state.pa.us/portal/server.pt/community/cyber_security_for_kids/496; http://www.portal.state.pa.us/portal/server.pt/community/best_practices/495.

[17] NIST, "Cybersecurity Framework," http://www.nist.gov/cyberframework/; Nat'l Governors Ass'n, "Act and Adjust: A Call to Action for Governors for Cybersecurity," Sept. 2013, http://www.nga.org/files/live/sites/NGA/files/pdf/2013/1309_Act_and_Adjust_Paper.pdf; Elaine Pittman, "Pennsylvania CISO Erik Avakian is Developing Strategies to Improve Security for All States," *Government Technology*, June 4, 2014, http://www.govtech.com/security/Pennsylvania-CISO-Erik-Avakian-is-Developing-Strategies-to-Improve-Security-for-All-States.html.

[18] Eric Chabrow, "State Launches Single Identity Pilot," Nov. 1, 2013, http://www.bankinfosecurity.com/identity-project-eyes-fraud-reduction-a-6296/op-1.

[19] Eric Chabrow, "States Test New Credentialing Approaches," Sept. 25, 2013, http://www.govinfosecurity.com/states-test-new-credentialing-approaches-a-6091/op-1.

[20] *Id.*

[21] Nicole Blake Johnson, "Pennsylvania Adopts Cyber Scorecards," June 3, 2014, http://www.statetechmagazine.com/article/2014/06/pennsylvania-adopts-cyber-scorecards.

[22] *Id.*

The Judicial Branch

The judicial power of the Commonwealth is vested in a unified judicial system headed by the Supreme Court, and the Supreme Court is granted general supervisory and administrative authority over the unified judicial system.[23]

Under its authority to adopt administrative and procedural rules, the Supreme Court adopted Chapter 5 of Title 201 of the Pennsylvania Code, which describes the powers and duties the Administrative Office of Pennsylvania Courts (AOPC).[24]

Rule 501, therein, provides that the Court Administrator of Pennsylvania shall be responsible for the prompt and proper disposition of the business of all courts and justices of the peace.[25] It is under this authority that AOPC provides for the cybersecurity of all courts and justices of the peace of the Commonwealth and utilizes funds in the Judicial Computer System Augmentation Account for the initial startup and the ongoing operations of the statewide judicial computer system.[26]

According to information provided to JSGC staff for the purposes of this report, AOPC maintains multiple data centers connecting to approximately 700 remote sites throughout Pennsylvania. Information is continuously synchronized between data centers over a dedicated private circuit using SAN technology.[27] However, all services and systems can operate from any one data center location. These data centers provide the needed infrastructure, business continuity solutions, and disaster recovery scenarios for AOPC's systems and services.

AOPC's security measures include the following:

- Antivirus, spam, and malware protection;
- The use of secure protocols such as SSL,[28] TLS,[29] and SFTP;[30]

[23] 42 Pa.C.S. §§ 301, 1701.
[24] 42 Pa.C.S. §§ 1722, 1901, & 1902.
[25] 201 Pa. Code Ch. 5.
[26] AOPC does not provide for the cybersecurity of certain municipal and county courts; 42 Pa.C.S. § 3732.
[27] Storage Area Network - "A SAN is a network of storage devices that can be accessed by multiple computers. Each computer on the network can access hard drives in the SAN as if they were local disks connected directly to the computer. This allows individual hard drives to be used by multiple computers, making it easy to share information between different machines." The Tech Terms Computer Dictionary, http://techterms.com/definition/san.
[28] Secure Sockets Layer - "SSL is a secure protocol developed for sending information securely over the Internet. Many websites use SSL for secure areas of their sites, such as user account pages and online checkout.... SSL encrypts the data being transmitted so that a third party cannot "eavesdrop" on the transmission and view the data being transmitted." The Tech Terms Computer Dictionary, http://techterms.com/definition/ssl.
[29] Transport Layer Security - TLS "is a protocol that provides communication security between client/server applications that communicate with each other over the Internet. It enables privacy, integrity and protection for the data that's transmitted between different nodes on the Internet. TLS is a successor to the secure socket layer (SSL) protocol." Techopedia, https://www.techopedia.com/definition/4143/transport-layer-security-tls.
[30] Secure File Transfer Protocol - SFTP "is a secure version of File Transfer Protocol (FTP), which facilitates data access and data transfer over a Secure Shell (SSH) data stream.... Both the commands and data are encrypted in order

- Regularly scheduled tests, scans, and penetration tests;
- Multiple firewalls;
- Intrusion protection systems;
- Proxies to intercept and filter HTTP[31] and FTP traffic;
- Device encryption;
- Application delivery via CITRIX technology;[32]
- Applications confined to servers within protected data centers;
- Encrypted communication protocols;
- Session hijacking protection; and
- DoS attack monitoring.[33]

AOPC contracts with US Bank, a private vendor, for all eCommerce services, including storage of payment information.

AOPC uses the Pennsylvania Justice Network (JNET) infrastructure to securely pass data from its case management systems to municipal, county, and state users. JNET is a statewide network that allows information to be shared among federal, state, county, and municipal agencies. Information is shared with the end user by two methods: a secure, web-based interface; and XML-based messaging.[34]

AOPC also provides information to agencies, such as those that are outside of the JNET infrastructure, or those departments that cannot participate in a messaging solution, as well as public access clients, through FTP and secure FTP sites.

AOPC's Judicial Automation department is currently engaged in a contract with the CERT Division of the Software Engineering Institute at Carnegie Mellon University to assess the policies, security, and network infrastructure of its automation efforts. AOPC also works with other third-party security vendors to implement industry best practices.

---

to prevent passwords and other sensitive information from being transferred over the network." Techopedia, https://www.techopedia.com/definition/1879/secure-file-transfer-protocol-sftp.

[31] Hyper Text Transfer Protocol - "HTTP is the protocol used to transfer data over the web." The Tech Terms Computer Dictionary, http://techterms.com/definition/http.

[32] CITRIX - "Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud." Citrix Systems, Inc., "About Us," https://www.citrix.com/about.html.

[33] Denial-of-Service Attack - A DoS attack "is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy." Techopedia, https://www.techopedia.com/definition/24841/denial-of-service-attack-dos.

[34] Extensible Markup Language - XML "is a universal format maintained by the W3C used for representation and transfer of structured data on the web or between different applications." Techopedia, https://www.techopedia.com/definition/24387/extensible-markup-language-xml.

The Legislative Branch

The legislative branch of Pennsylvania's government is less centralized than the judicial and executive branches. Consequently, the cybersecurity policies are less consistent.

The Legislative Data Processing Center (LDPC) is a legislative service agency of the Pennsylvania General Assembly. It was created by the act of December 10, 1968 (P.L.1158, No. 365), to establish and operate computer systems capable of storing and retrieving all of the financial, factual, procedural, and legal information necessary to serve all of the committees, officers, and agencies of the Pennsylvania General Assembly.[35]

According to information provided to JSGC staff for the purposes of this report, LDPC provides support for the following offices and agencies:

- Capitol Preservation Committee;
- Center for Rural Pennsylvania;
- Independent Fiscal Office;
- Independent Regulatory Review Commission;
- Joint Legislative Conservation Committee;
- Joint State Government Commission;
- Legislative Budget and Finance Committee;
- Legislative Data Processing Center;
- Local Government Commission; and
- Commission on Sentencing (Harrisburg office only).

LDPC provides limited support to the following offices and agencies:

- House Chamber;
- Senate Chamber;
- House Appropriations Committee Democrats;
- Chief Clerk of the Senate;
- Secretary of the Senate;
- Senate Democratic Caucus; and
- Senate Republican Caucus.

LDPC does not provide support to the following offices and agencies, which have independent IT systems and policies:

- House Republican Caucus;
- House Democratic Caucus;

[35] Pa. Legislative Data Processing Ctr., "About LDPC," http://www.paldpc.us/.

- Chief Clerk of the House;
- House Comptroller; and
- Legislative Reference Bureau.

Most of LDPC's systems do not contain personal information. However, while the Legislative Payroll System (LPS) and the Legislative Financial System (LFS) do contain personal information, they are only accessible to legislative offices, and are secured from public access by multiple firewalls.

Communications are encrypted using industry standard protocols, such as HTTPS.[36] In addition, multiple levels of user security exist for gaining access to the systems. The ability to change each level of user security is limited to a small number of staff, and requires multiple levels of approval. Protocols are in place requiring routine password changes, specifying password complexity, and limiting password reuse.

The systems are accessed through in-house developed software programs, and changes to the software programs require multiple levels of approval and are restricted so that only a limited number of staff have the capability of modifying program code. System and user security is monitored internally. Prior to 2009, LDPC's computer security was evaluated annually by the certified public accountant retained by the Legislative Audit Advisory Commission, which is responsible for auditing the financial affairs of the General Assembly; however, LDPC has not been contacted for the security review since 2009.

As mentioned previously, several legislative branch offices and agencies have independent IT systems and policies. Legislative Reference Bureau (LRB) is one such agency. The primary purpose of LRB is to prepare legislation for introduction in the General Assembly. As a result, LRB does not handle personal information. LDPC provides payroll services to LRB, so LRB does not handle employee personal information, either.

The caucuses, which also have independent IT systems and policies, handle limited personal information. They possess databases of Pennsylvania residents that allow General Assembly members to communicate with their constituents and to follow issues of interest to their constituents. These databases are protected by firewalls and passwords, and members cannot access constituent information of other members. Access to these databases is limited to those individuals who need access for legitimate purposes. The caucus IT departments work with vendors to conduct reviews of their networks and security protocols, and they conduct internal reviews as well. LDPC provides payroll services for the caucuses, so they do not handle employee personal information.

[36] Secure Hyper Text Transfer Protocol - HTTPS "is a variant of the standard web transfer protocol (HTTP) that adds a layer of security on the data in transit through a secure socket layer (SSL) or transport layer security (TLS) protocol connection. HTTPS enables encrypted communication and secure connection between a remote user and the primary web server." Techopedia, https://www.techopedia.com/definition/5361/hypertext-transport-protocol-secure-https.

The Framework for Improving Critical Infrastructure Cybersecurity

The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) was published by the National Institute of Standards and Technology (NIST) on February 12, 2014, as directed by President Obama in Executive Order 13636.[37] The Framework, based on existing standards, guidelines, and best practices, provides guidance for reducing cybersecurity risk for public and private organizations that choose to implement it as part of their IT systems.[38] The Framework was developed in a yearlong, collaborative process in which NIST served as a convener for industry, academic, and government stakeholders.[39] The Framework was designed to be a "living" document that evolves based on user feedback and experiences.[40]

Executive Order 13636 directed NIST to identify areas for improvement in the Framework.[41] NIST identified a number of "high-priority areas for development, alignment, and collaboration...."[42] These areas included:

- Authentication;
- Automated indicator sharing;
- Conformity assessment;
- Cybersecurity workforce;
- Data analytics;
- Federal agency cybersecurity alignment;
- International aspects, impacts, and alignment;
- Supply chain risk management; and
- Technical privacy standards.[43]

[37] NIST, "Update on the Cybersecurity Framework," Dec. 5, 2014, http://www.nist.gov/cyberframework/upload/nist-cybersecurity-framework-update-120514.pdf at p. 1.
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] NIST, "NIST Roadmap for Improving Critical Infrastructure Cybersecurity," Feb. 12, 2014, http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf at p. 2.
[42] *Id.*
[43] *Id.* at pp. 3-8.

The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers.[44] The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors.[45] The Core consists of five functions (identify, protect, detect, respond, and recover) that "provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk."[46] The Core provides detailed guidance for developing individual organizational Profiles.[47] In an appendix to the Framework, NIST provided an example Core that presents a common set of cybersecurity risk management activities.[48]

The Profiles help organizations align their cybersecurity activities with their business requirements, risk tolerances, and resources.[49] An organization can compare its current Profile with a target Profile in order to identify opportunities for improving its cybersecurity posture.[50] The Profiles also allow the organization to prioritize and measure progress toward its target.[51]

The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risks.[52] The Tiers reflect a spectrum of cybersecurity approaches, progressing from informal, reactive responses to agile and risk-informed responses.[53] Although an organization identified as Tier 1 (Partial) is encouraged to move toward Tier 2 or greater, the Tiers do not represent maturity levels.[54] Moving to a higher Tier is encouraged only where such a move would reduce cybersecurity risk and be cost effective.[55]

As required by the executive order, the Framework allows for methods to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities by assisting organizations in incorporating them as part of a comprehensive cybersecurity program.[56]

However, the Framework was not designed to create additional regulation.[57] Instead, the Framework was designed as "an organizing construct for aligning and communicating requirements."[58]

---

[44] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," Feb. 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf at p. 1.
[45] *Id.*
[46] *Id.* at p. 4.
[47] *Id.* at p. 1.
[48] *Id.* at p. 18.
[49] *Id.* at p. 1.
[50] *Id.* at p. 5.
[51] *Id.*
[52] *Id.* at p. 1.
[53] *Id.* at p. 5.
[54] *Id.* at p. 9.
[55] *Id.*
[56] *Id.* at p. 1.
[57] *Supra* note 37, at p. 4.
[58] *Id.*

The National Governors Association's Call to Action

The National Governors Association (NGA) issued a call to action in September 2013.[59] The NGA and the call to action were guided by the following core principles:

- Support governors;
- Be actionable;
- Reduce complexity;
- Protect privacy;
- Employ technologically neutral solutions;
- Focus on the state as enterprise;
- Promote flexible federalism;
- Rely on evidence-based practices;
- Use and generate metrics; and
- Promote the use of incentives.[60]

Based on these principles, the NGA called for policies and practices that would make state systems and data more secure.[61] The policies and practices included:

- Establishing a governance and authority structure for cybersecurity;
- Conducting risk assessments and allocating resources accordingly;
- Implementing continuous vulnerability assessments and threat mitigation practices;
- Ensuring that the state complies with current security methodologies and business disciplines in cybersecurity; and
- Creating a culture of risk awareness.[62]

[59] Nat'l Governors Ass'n, "Act and Adjust: A Call to Action for Governors for Cybersecurity," Sept. 2013, http://www.nga.org/files/live/sites/NGA/files/pdf/2013/1309_Act_and_Adjust_Paper.pdf
[60] *Id.* at p. 1-2.
[61] *Id.* at p. 1.
[62] *Id.*

Establishing a governance and authority structure for cybersecurity

According to the NGA, because state systems and networks are interconnected, developing a robust cybersecurity governance structure would require an enterprise-wide approach.[63] Therefore, the NGA suggests that governors need to ensure that they have a strong statewide governance structure with some degree of central authority that provides a framework to prepare for, respond to, and prevent cyberattacks.[64]

The NGA noted that in many states, chief information security officers (CISOs), who are responsible for developing and carrying out IT security policies, have only limited authority over statewide networks, and often operate in decentralized environments.[65]

Additionally, because of the interconnectedness of government and private-sector IT assets, collaboration at all levels of government and with the private sector could be a useful tool in establishing a comprehensive cybersecurity plan.[66]

Conducting risk assessments and allocating resources accordingly

The NGA advises that states need a comprehensive understanding of the risks and threats to make accurate and timely decisions when allocating resources.[67] Without a comprehensive understanding, states are vulnerable to interruptions in operations, as well as financial and data losses.[68] To gain this awareness, states should develop security strategies and business practices by conducting risk assessments that identify assets, simulating threats to those assets, and planning to protect against those threats.[69]

In addition to establishing best practices and using existing resources, states should also conduct hands-on activities and exercises for their IT personnel as a part of the security assessments, including regular penetration testing and vulnerability scanning, and should be included in security policies.[70] Based on the results of these assessments, states can make decisions regarding resource allocation and can implement plans to improve for future assessments.[71]

Finally, appropriate state officials who have applicable security clearances should receive regular classified cybersecurity briefings.[72] The Department of Homeland Security (DHS) can assist states in planning these briefings.[73]

---

[63] *Id.* at p. 2.
[64] *Id.*
[65] *Id.*
[66] *Id.* at p. 3.
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.*
[73] *Id.*

Implementing continuous vulnerability assessments and threat mitigation practices

States are exposed to phishing scams, malware, denial of service (DOS) attacks, and other cyberthreats on a daily basis.[74] Consistent monitoring of threats and vulnerabilities can help states proactively defend their networks against these threats.[75] Technologies and business practices that identify potential threats, track cyberattacks in real time, and offer mitigation techniques are essential for all mission-critical systems.[76]

One key resource for cyberthreat prevention, protection, response, and recovery for state governments is the Multi-State Information Sharing and Analysis Center (MS-ISAC).[77] The MS-ISAC is a division of a division of the Center for Internet Security, a nonprofit organization whose mission is enhancing the security readiness and response of public and private entities, and is a voluntary and collaborative effort based on a strong partnership with the Office of Cybersecurity and Communications within the US Department of Homeland Security.[78] MS-ISAC serves as a central resource for situational awareness and incident response, and provides states with managed security services that include ongoing monitoring of networks and firewalls.[79]

Another key resource available to states is DHS's Continuous Diagnostics and Mitigation (CDM) program.[80] The CDM program expands deployment of automated network sensors that feed data about an agency's cybersecurity vulnerabilities into a continuously updated dashboard.[81] The program also has a blanket purchasing program, allowing states to reduce costs associated with purchasing tools and services that enhance their cybersecurity.[82]

Ensuring that the state complies with current security methodologies and business disciplines in cybersecurity

The NGA suggests that states turn to two industry standards for guidance in establishing effective cybersecurity practices.[83] The first, the Council on CyberSecurity's "Critical Controls for Effective Cyber Defense," is an industry standard that provides a framework that can strengthen cyberdefenses and protect information, infrastructure, and critical assets.[84] The framework is based on five guiding principles: using evidence-based practices to build effective defenses, assigning priorities to risk reduction and protection actions, establishing a common language that measures the effectiveness of security, continuous monitoring, and automating defenses.[85]

---

[74] *Id.* at p. 4.
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *See* MS-ISAC Charter, March 2013, https://msisac.cisecurity.org/about/charter/documents/MS-ISACCharter2013-03.pdf; Ctr. for Internet Sec., "2014 Annual Report," http://www.cisecurity.org/about/documents/2014ANNUALREPORT.pdf; *and* MS-ISAC Membership Overview, https://msisac.cisecurity.org/about/documents/MS-ISACMembershipOverview2015.pdf.
[79] *Supra* note 59, at p. 4.
[80] *Id.*
[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] *Id.*
[85] *Id.*, *citing* SANS, "CSIS: 20 Critical Security Controls," http://www.sans.org/critical-security-controls/guidelines.

The second industry standard advocated by the NGA is the Information Technology Infrastructure Library (ITIL).[86] According to the NGA, "ITIL is a set of practices for information technology service management (ITSM) that are designed to align information technology with core business requirements."[87] ITIL was designed by AXELOS, "[a] joint venture company, created by the Cabinet Office on behalf of Her Majesty's Government (HMG) in the United Kingdom and Capita plc to run the Global Best Practice portfolio."[88] Axelos claims that "ITIL has been adopted by thousands of organizations worldwide,..." and that "ITIL best practices underpin the foundations of ISO/IEC 20000 (previously BS15000), the international Service Management standard."[89]

Creating a culture of risk awareness

According to the NGA, the best firewalls and the most advanced antivirus software cannot prevent cyberattacks if the network users are careless or inattentive to basic security practices.[90] To develop a strong cybersecurity culture, the NGA suggests that focus should be put on increasing awareness, setting appropriate expectations, and influencing day-to-day security practices of network users.[91]

[86] *Id.*
[87] *Id.* at pp. 4-5; *see also* Valerie Arraj, "ITIL®: The Basics," July 2013, http://www.best-management-practice.com/gempdf/itil_the_basics.pdf.
[88] AXELOS, "About AXELOS," https://www.axelos.com/about-axelos.
[89] AXELOS, "What is ITIL®?," https://www.axelos.com/best-practice-solutions/itil/what-is-itil.
[90] *Supra* note 59, at p. 5.
[91] *Id.* at p. 5.

In 2002, a cyberattack on California's Stephen P. Teale Data Center resulted in a breach that compromised the personal information of 265,000 state employees.[92] In response, California enacted the first state security breach notification law in July 2003.[93] Since then, 47 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted similar laws.[94] Appendix B of this report contains a table that includes citations to the other jurisdictions' breach notification laws. Act 94 of 2005, known as the Breach of Personal Information Notification Act, is Pennsylvania's security breach notification law. It provides for the notification of residents whose personal information was, or may have been, disclosed due to a security system breach.[95]

Act 94

Under Act 94, an entity that maintains, stores, or manages computerized data that includes personal information must provide notice of any breach of the security of the system, following discovery of the breach, to any resident of the Commonwealth whose unencrypted and unredacted personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.[96] An entity must provide notice of a breach if encrypted information is accessed and acquired in an unencrypted form, if the breach is linked to a breach of the security of the encryption, or if the breach involves a person with access to the encryption key.[97]

A breach is defined as the unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth.[98]

An entity is defined by the act as a state agency, a political subdivision of the Commonwealth, or an individual or business doing business in the Commonwealth.[99]

---

[92] Univ. Cal.-Berkeley Sch. of Law, Samuelson Law, Tech., & Pub. Policy Clinic, "Security Breach Notification Laws: Views from Chief Security Officers," Dec. 2007, https://www.law.berkeley.edu/files/cso_study.pdf at p. 40.

[93] Jill Joerling, *Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data*, 32 Wash. U. J.L. & Pol'y 467, 471 (2010).

[94] Nat'l Conf. of State Legislatures, "Security Breach Notification Laws," June 6, 2015, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[95] Act of Dec. 2, 2005 (P.L.474, No.94), 73 P.S. § 2301 *et seq.*

[96] *Id.* at § 3(a).

[97] *Id.* at § 3(b).

[98] *Id.* at § 2.

[99] *Id.*

Personal information is defined as "[a]n individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted: Social Security number; driver's license number or a state identification card number; or financial account number, credit, or debit card number, in combination with any required security code, access code or password."[100] Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.[101]

Notice under the act may be written, telephonic, emailed, a conspicuous posting on the entity's website, or notification to major statewide media, depending on the circumstances of the breach, the number of individuals affected, the cost to notify the individuals, and the contact information available to the entity.[102]

A vendor that maintains, stores, or manages computerized data on behalf of another entity must provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores, or manages the data, and the entity is then responsible for making the determinations and discharging any remaining duties under the act.[103]

The notification required by the act may be delayed if a law enforcement agency determines and advises the entity that the notification will impede a criminal or civil investigation.[104] The notification required by the act must then be made after the law enforcement agency determines that it will not compromise the investigation or national or homeland security.[105]

When an entity provides notification to more than 1,000 people at one time, the entity must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in Section 603 of the Fair Credit Reporting Act,[106] of the timing, distribution, and number of notices.[107]

However, an entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and is consistent with the notice requirements of the act is deemed to be in compliance with the notification requirements of the act if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.[108] Furthermore, a financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with the act.[109] Any other entity that complies with the notification requirements or procedures pursuant to the rules,

---

[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] *Id.* at § 3(c).
[104] *Id.* at § 4.
[105] *Id.*
[106] Public Law 91-508, 15 U.S.C. § 1681a.
[107] *Supra* note 95, at § 5.
[108] *Id.* at § 7(a).
[109] *Id.* at § 7(b)(1); *see* 12 C.F.R. Pt. 570, App. B, Supp. A.

regulations, procedures, or guidelines established by the entity's primary or functional Federal regulator is also deemed to be in compliance with the act.[110]

A violation of the act is deemed to be an unfair or deceptive act or practice in violation of Pennsylvania's Unfair Trade Practices and Consumer Protection Law,[111] and the Office of Attorney General has exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of the act.[112] The Unfair Trade Practices and Consumer Protection Law provides for injunctive relief and civil penalties.[113]

Other States

Although 47 states, the District of Columbia, Guam, Puerto Rico, and the US Virgin Islands have enacted breach notification laws based on California's law, variations exist in several key areas, including the following: covered entities, the definition of personal information, who must be notified, the timeline of notification, and the consequences of non-compliance.[114]

Common Themes

While variations exist between the numerous state notification laws, common themes exist as well. Most of the state laws, including Pennsylvania's, apply only to information stored electronically, although some statutes apply to paper records too.[115]

Most states provide for an "encrypted data safe harbor," meaning that covered entities do not have to provide notification of a breach if the information was encrypted unless the encryption key was also compromised.[116] Furthermore, many states provide a "risk of harm" exemption, which exempts a covered entity from the notification requirement if, after appropriate investigation, the covered entity reasonably determines that the breach did not result or is unlikely to result in harm to the individuals whose personal information was compromised.[117] While Act 94 does not provide for an explicit safe harbor or exemption, its definition of breach incorporates these concepts.

---

[110] *Id.* at § 7(b)(2).
[111] Act of Dec. 17, 1968 (P.L.1224, No.387), 73 P.S. § 201-1 *et seq.*
[112] *Supra* note 95, at § 8.
[113] *Supra* note 111, at §§ 4, 8.
[114] *Supra* note 94.
[115] *Supra* note 93, at pp. 473-4.
[116] Rachael M. Peters, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 Ariz. L. Rev. 1171, 1182 (2014).
[117] *Supra* note 93, at p. 475.

Differences

Covered Entities

Act 94, like most of the other laws, covers entities very broadly. However, a few jurisdictions have more limited statutes. For example, Georgia limits the covered entities to "[a]ny *information broker* or *data collector* that maintains computerized data that includes personal information of individuals...."[118] While data collector is defined as "any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity," information broker is defined as "any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties."[119]

Iowa and Oregon define covered entities based on how the data is normally used, so that their statutes only apply to a person who owns, maintains, licenses, or otherwise possesses data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities.[120]

Maryland's statute only applies to businesses, and the definition of "business" does not include government agencies.[121] New York provides an exception for the judiciary and "all cities, counties, municipalities, villages, towns, and other local agencies" from its statute.[122]

Definition of Personal Information

Some states define personal information more broadly than Pennsylvania. California's law includes an individual's username or email address in combination with a password or security question answer that would permit access to an online account, as well as medical and health insurance information.[123]

Iowa's law includes biometric data, such as fingerprints.[124]

Kansas's law does not require an account number or credit or debit card number to be accompanied by a security code, access code, or password to qualify for notification.[125]

[118] Ga. Code § 10-1-912, emphasis added.
[119] Ga. Code § 10-1-911.
[120] Iowa Code § 715C.2; ORS § 646A.604.
[121] Md. Code, Commercial Law §§ 14-3504, 14-3501.
[122] State Tech., § 208(1)(c)(2).
[123] Ca. Civ. Code §§ 1280.15, 1798.29, 1798.80-84.
[124] Iowa Code § 715C.1(11).
[125] Kan. Stat. Ann. § 50-7a01(g).

New Jersey's law includes dissociated data if the means to link the dissociated data were also accessed during the breach.[126]

North Dakota's law includes date of birth, mother's maiden name, employee number, and digitized signature in its definition of personal information.[127]

Wisconsin's law includes DNA profiles.[128]

Who Must be Notified

Although Pennsylvania does not require the attorney general, a state agency, or the General Assembly to be notified of breaches, many states do.[129] Some states require a minimum number of affected individuals before notification of their attorneys general or legislatures is required, while others limit the requirement to breaches at state agencies.[130] Some states, including Pennsylvania, also require notification of consumer reporting agencies.[131]

Notification Timeline

Like Pennsylvania, most states do not prescribe a specific timeframe for notification. The typical proscribed timeframe is simply some form of the phrase "without unreasonable delay."[132]

However, Connecticut provides for a five-day notification period for incidents reportable to the Department of Insurance.[133]

Florida provides for a 30-day notification period.[134] Additionally, entities that hold personal information for other entities must notify the entities within 10 days.[135] Entities have 30 days to notify the attorney general if they determine, after consultation with law enforcement agencies, that the breach will not result in harm to consumers.[136]

---

[126] N.J. Stat. § 56:8-161.
[127] N.D. Cent. Code. § 51-30-01(4).
[128] Wis. Stat. § 134.98(1)(b).
[129] Attorney general or other state agency: AK, CA, CT, FL, HI, ID, IN, IA, LA, ME, MD, MA, MO, NH, NJ, NY, NC, PR, SC, VT, VA. General assembly: IL.
[130] Minimum number of affected individuals: CA, FL, HI, IA, MO, SC, VA. Breaches at state agencies: ID, IL.
[131] AK, CO, DC, FL, GA, HI, IN, KS, KY, ME, MD, MA, MI, MN, MO, NV, NH, NJ, NY, NC, OH, OR, SC, TN, TX, VT, VA, WV, WI.
[132] *Supra* note 95, at § 3(a).
[133] State of Conn., Ins. Dep't, "Bulletin IC-25," Aug. 18, 2010, http://www.ct.gov/cid/lib/cid/Bulletin_IC_25_Data_Breach_Notification.pdf.
[134] Fla. Stat. §§ 501.171(3)-(6).
[135] Fla. Stat. §§ 501.171(3)-(6).
[136] Fla. Stat. §§ 501.171(3)-(6).

Maine requires entities to provide notice within seven business days after a law enforcement agency has determined that notification will not interfere with a criminal investigation.[137]

Ohio specifies that notification must occur no later than 45 days following the discovery of the breach, unless disclosure impedes a law enforcement investigation.[138]

Similarly, Wisconsin requires notification no later than 45 days after discovery of the breach, unless disclosure impedes a law enforcement investigation.[139]

Vermont requires notification of its attorney general within 14 business days, and notification of the affected individuals no later than 45 days after the discovery of the breach, unless disclosure impedes a law enforcement investigation.[140]

Puerto Rico provides that within 10 days after the detection of a breach, the entity must notify the Department of Consumer Affairs, which then has 24 hours to notify the public.[141]

Consequences of Non-Compliance

Some jurisdictions provide for a private cause of action against covered entities, allowing affected individuals to recover damages.[142] However, some jurisdictions limit the cause of action to non-government entities.[143] Pennsylvania does not provide for a private cause of action.

Additionally, some jurisdictions provide for civil or even criminal penalties in the event of a violation, ranging from injunctions to fines, and even prison sentences.[144] Pennsylvania provides for civil penalties in the event of a violation.

[137] 10 Me. Rev. Stat. §1348, sub-§3.
[138] Ohio Rev. Code, Title XIII, Ch. 1349, § 19(B)(2).
[139] Wis. Stat. § 134.98(3)(a).
[140] Vt. Stat. tit. 9, § 2435.
[141] P.R. Laws tit. 10. Subtit. 3. Ch. 310 § 4052.
[142] AK, CA, DE, LA, MD, MA, MN, NH, NC, OR, RI, SC, TN, VA, WA, WY, DC, PR, VI.
[143] AK.
[144] AK, AZ, AR, CT, DE, FL, HI, ID, IL, IN, IA, KS, LA, ME, MD, MA, MI, MS, MO, MT, NH, NY, NC, ND, OH, OK, OR, PA, RI, SC, TN, TX, UT, VT, VA, WA, WV, WY, DC, PR, VI.

CYBERSECURITY IN OTHER STATES

Like Pennsylvania, other states are protective of the details of their cybersecurity practices. However, the NGA discussed steps taken by a few states in its Call to Action.[145]

Other States

MICHIGAN | Michigan has created a centralized security department run by a chief security officer (CSO).[146] The centralized security department coordinates physical security and cybersecurity directors, managers, and employees of various agencies.[147] Michigan provides security awareness training to all state employees, and has posted guides online.[148] Additionally, Michigan "recently launched a research, test, training, and evaluation facility for cybersecurity and cyberdefense."[149] In 2014, the counties of Livingston, Monroe, Oakland, Washtenaw, and Wayne, and the state of Michigan were recognized by the Center for Digital Government for the Cyber Security Assessment for Everyone (CySAFE) tool, which helps governments assess, plan, and implement cybersecurity measures.[150]

MINNESOTA | Minnesota has also adopted an emphasis on communication and collaboration between a central organization and other stakeholders.[151] The state's chief information officer (CIO) works with the governor, a Technology Advisory Committee, and other agency leaders.[152] Several governmental entities also have their own CIOs, allowing for a direct link between the state CIO and decisions made at different levels of government.[153]

CALIFORNIA | California created the California Cybersecurity Task Force to facilitate collaboration between all levels of government and with the private sector.[154] The primary purpose of the task force is to share information.[155]

---

[145] *Supra* note 59.
[146] *Id.* at p. 2.
[147] *Id.* at pp. 2-3.
[148] *Id.* at p. 5.
[149] *Id.*
[150] Janet Grenslitt, "Winners Announced - Cybersecurity Leadership and Innovation Awards 2014," Oct. 28, 2014, http://www.govtech.com/cdg/cybersecurity/Winners-Announced-Cybersecurity-Leadership-and-Innovation-Awards-2014.html.
[151] *Supra* note 59, at p. 3.
[152] *Id.*
[153] *Id.*
[154] *Id.*
[155] *Id.*

MARYLAND | Maryland uses the Maryland Air National Guard 175th Network Warfare Squadron to help support its cybersecurity efforts.[156] These efforts include penetration training exercises, which feature "simulated attacks from malicious outsiders or insidious insiders."[157] The Guard also provides network vulnerability assessments of various state agencies.[158] The arrangement has the added benefit of providing training to the squadron's members.[159] Additionally, the Maryland Emergency Management Administration facilitated a cabinet-level tabletop exercise that assessed cybersecurity.[160]

DELAWARE | To foster a culture of risk awareness, state employees in Delaware provide cybersecurity presentations to elementary school students that emphasize the importance of internet safety.[161] To encourage the public to create materials that promote cybersecurity awareness, the state also hosts video and poster contests.[162]

SOUTH CAROLINA | Unfortunately, not all states have made cybersecurity news for good reasons. In 2002, hackers breached South Carolina's Department of Revenue database, stealing nearly 3.6 million Social Security numbers and 400,000 payment card numbers.[163] In 2014, the state responded by enacting the South Carolina Restructuring Act of 2014, which gave the governor's office more executive power and created a new cabinet-level agency.[164] The new agency, the Department of Administration, is charged with managing and protecting the state's technology, although the legislature retained the power to evaluate the new agency's allocation and expenditure of funds, including for its oversight of technology policy creation and implementation.[165]

HAWAII | Several other states have also recently taken steps to enhance their cybersecurity. For example, in June 2014, Hawaii created a full-time "cybersecurity, economic, education, and infrastructure security coordinator to oversee cybersecurity and cyber resiliency matters" within the state's department of defense.[166]

TEXAS | In May 2013, Texas created a cybersecurity coordinator within the Department of Information Resources.[167] The cybersecurity coordinator is authorized to "establish a council that includes public and private sector leaders and cybersecurity practitioners to collaborate on matters of cybersecurity...."[168]

---

[156] *Id.* at p. 4.
[157] *Id.*
[158] *Id.*
[159] *Id.*
[160] *Id.* at p. 5.
[161] *Id.*
[162] *Id.*
[163] Nat'l Conf. of State Legislatures, "Trends and Transitions: July/August 2013," http://www.ncsl.org/bookstore/state-legislatures-magazine/trends-and-transitions-sl-magazine-july-2013.aspx#Pay Now or Pay Later.
[164] Brian Heaton, "South Carolina Centralizes IT Oversight," Sept. 15, 2014, http://www.govtech.com/security/South-Carolina-Centralizes-IT-Oversight.html.
[165] *Id.*
[166] Haw. Rev. Stat. § 128B-1.
[167] Gov't Code, Title 10, Subtitle B, Ch. 2054, Subch. O, § 2054.551.
[168] *Id.* at § 2054.552.

FLORIDA | Through the Information Technology Security Act, Florida created the Agency for State Technology, which "is responsible for establishing standards and processes consistent with generally accepted best practices for information technology security and adopting rules that safeguard an agency's data, information, and information technology resources to ensure availability, confidentiality, and integrity."[169] Under the act, the agency is required to develop and annually update a statewide information technology security strategic plan, develop and publish for use by state agencies an information technology security framework, assist state agencies in complying with data security laws, collaborate with the Cybercrime Office of the Department of Law Enforcement to provide training for state agency information security managers, and annually review the strategic and operational information technology security plans of executive branch agencies.[170]

Florida's act also requires each state agency head to do the following:

- Designate an information security manager to administer the information technology security program of the state agency;
- Submit the agency's strategic operational information technology security plans to the Agency for State Technology annually;
- Conduct, and update every 3 years, a comprehensive risk assessment to determine the security threats to the data, information, and information technology resources of the agency;
- Develop and periodically update written internal policies and procedures;
- Implement managerial, operational, and technical safeguards established by the Agency for State Technology to address identified risks to the data, information, and information technology resources of the agency;
- Ensure that periodic internal audits and evaluations of the agency's information technology security program for the data, information, and information technology resources of the agency are conducted;
- Include appropriate information technology security requirements in the written specifications for the solicitation of information technology and information technology resources and services;
- Provide information technology security awareness training to all state agency employees concerning information technology security risks and the responsibility of employees to comply with policies, standards, guidelines, and operating procedures adopted by the state agency to reduce those risks; and
- Develop a process for detecting, reporting, and responding to threats, breaches, or information technology security incidents that are consistent with the security rules, guidelines, and processes established by the Agency for State Technology.[171]

[169] Fla. Stat. § 282.318.
[170] Fla. Stat. § 282.318
[171] Fla. Stat. § 282.318

Other State Identity and Privacy Protections

In addition to breach notification statutes, many states and the federal government provide other identity and privacy protections by statute. For example, "at least 32 states and Puerto Rico have enacted laws that require entities to destroy, dispose, or otherwise make personal information unreadable or undecipherable."[172] Fifty states and the District of Columbia have enacted laws that allow consumers to place a "security freeze" on their credit reports, which limits a consumer reporting agency from releasing a credit report or any information from the report without authorization from the consumer, if a person suspects that he or she has been victimized by identity theft.[173] Furthermore, every state has enacted laws regarding identity theft or impersonation.[174]

Federal Statutes

At the federal level, laws relating to data privacy and breaches include: the Computer Fraud and Abuse Act (CFAA); the Electronic Communications Privacy Act (ECPA); healthcare privacy laws, including the Health Insurance Portability and Accountability Act (HIPAA), as enhanced by the Health Information Technology for Economic and Clinical Health Act (HITECH) and the Patient Protection and Affordable Care Act (ACA); financial data laws including the Gramm-Leach-Bliley Act of 1999 (GLBA), Red Flags Rules of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), the Fair Credit Reporting Act, and the Bank Secrecy Act; the Family Educational Rights and Privacy Act (FERPA); and the Children's Online Privacy Protection Act.[175]

Pennsylvania's Status Nationwide

Although Pennsylvania does not have a broad data security law like Florida's, it is a leader in many other ways. According to the Center for Digital Government's 2014 Digital States Survey, Pennsylvania was among five states that earned an A-.[176] Only Missouri, Michigan, and Utah earned higher grades.[177] Pennsylvania received the Center for Digital Government's 2014 Cybersecurity Leadership and Innovation Award for its implementation of the Commonwealth Application Certification and Accreditation (CA^2) process.[178] The CA^2 process identifies and eliminates potential vulnerabilities from applications before they are deployed.[179]

---

[172] Nat'l Conf. of State Legislatures, "Data Disposal Laws," Jan. 21, 2015, http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.
[173] Nat'l Conf. of State Legislatures, "Consumer Report Security Freeze State Laws," July 17, 2015, http://www.ncsl.org/research/financial-services-and-commerce/consumer-report-security-freeze-state-statutes.aspx.
[174] Nat'l Conf. of State Legislatures, "Identity Theft," http://www.ncsl.org/research/financial-services-and-commerce/identity-theft-state-statutes.aspx.
[175] Rachael M. Peters, *So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws*, 56 Ariz. L. Rev. 1171, 1177 (2014).
[176] Janet Grenslitt, "Digital States Survey 2014 Results," Sept. 3, 2014, http://www.govtech.com/cdg/digital-states/Digital-States-Survey-2014-Results.html.
[177] *Id.*
[178] *Supra* note 150.
[179] *Supra* note 176.

Centralize

As described previously in this report, several states have moved towards a more centralized model for cybersecurity policy and implementation. Although this model is not without risks, it reduces the likelihood of hardware and software incompatibility, poor communication of threats, inconsistent policies, and lack of oversight that can result from a fragmented model of cybersecurity. In addition, larger central agencies often allow for greater efficiency and reduced costs by eliminating redundancies. For these reasons, it is the recommendation of JSGC staff that Pennsylvania adopt a more centralized approach to cybersecurity.

The Governor's Office of Administration (OA) has the expertise of managing cybersecurity for all Executive Branch agencies, and has published, publicly-available policies in place. OA strives to implement industry best practices, and has been recognized for its efforts. Therefore, OA is an excellent example for AOPC (the courts) and LDPC (the legislature) to follow. AOPC should continue its efforts to extend its services to all courts in the Commonwealth. Furthermore, legislative branch offices and agencies should work to centralize cybersecurity and IT services under LDPC rather than maintaining separate systems.

As the branches centralize and look to OA for guidance, they should also continue to work together, and with state officials such as the Governor, Speaker of the House, President Pro Temp of the Senate, and the Chief Justice of the Supreme Court.

The branches should also consider implementing measures taken by other states that have proven effective, such as increased auditing. By looking to their counterparts in other states and to industry best practices, Pennsylvania's cybersecurity officials can continue to provide protection to the offices, agencies, and citizens of Pennsylvania. However, implementing best practices, conducting system audits, and ensuring that IT staff are aware of current threats requires resources. For this reason, continued support of the Commonwealth's cybersecurity efforts is critical in protecting the state and its citizens.

Modernize

Act 94 was enacted in 2005, and has not been amended in the ten years since its enactment. In the mean time, technology has changed and advanced; for example, the iPhone was introduced in 2007.[180] While legislation can never keep pace with rapidly evolving technologies, Act 94

[180] Apple Inc., "Apple Reinvents the Phone with iPhone," Jan. 9, 2007, http://www.apple.com/pr/library/2007/01/09Apple-Reinvents-the-Phone-with-iPhone.html.

should be amended to reflect a more modern understanding of cybersecurity. One such amendment should be to the definition of personal information.

Act 94 defines personal information as "[a]n individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted: Social Security number; driver's license number or a state identification card number; or financial account number, credit, or debit card number, in combination with any required security code, access code or password."[181] Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.[182]

However, many other states and the federal government define personal information more broadly. NIST released a special publication specifically relating to personal information.[183] In that report, NIST defined personal information as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[184]

NIST also provided a list of examples of information that could be personal information, which included:

- Name, such as full name, maiden name, mother's maiden name, or alias;
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number;
- Address information, such as street address or email address;
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people;
- Telephone numbers, including mobile, business, and personal numbers;
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry);

[181] *Supra* note 95, at § 2.
[182] *Id.*
[183] NIST, "Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information," April 2010, http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.
[184] *Id.* at 2-1, *quoting* GAO, "Report 08-536 - Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information," May 2008, http://www.gao.gov/new.items/d08536.pdf.

- Information identifying personally owned property, such as vehicle registration number or title number and related information; and

- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).[185]

NIST's definition and list of examples is quite broad, but it better accounts for the modern understanding of personal information and how it can be used in harmful ways.

Furthermore, the "risk of harm" exemption in Act 94, which exempts a covered entity from the notification requirement if, after appropriate investigation, the covered entity reasonably determines that the breach did not result or is unlikely to result in harm to the individuals whose personal information was compromised, creates uncertainty and places a burden on Commonwealth offices and agencies to determine whether there was a risk of harm.[186] Act 94 should be amended to remove the risk of uncertainty and the burden of analysis.

Additionally, Act 94 does not provide for a specific timeframe for notification. Instead, it uses the generic phrase "without unreasonable delay."[187] While this provides Commonwealth offices and agencies with flexibility, it again creates the risk for uncertainty. Requiring notification no later than 45 days after discovery of the breach, unless disclosure impedes a law enforcement investigation, would provide clarity, and would also provide agencies ample time to perform any necessary investigations or consultations.

Finally, Act 94 does not require the notification of any central authority, such as the Attorney General. Pennsylvania should join the 22 other states that require notification of a central authority. This will aid in tracking security breaches, especially small ones. Because the Office of Attorney General has exclusive authority to bring an action under Act 94, it is the logical central authority to which notice of breaches should be given.[188]

Appendix A of this report includes proposed legislation that incorporates the recommended amendments to Act 94.

[185] *Id.* at 2-2.
[186] *Supra* note 95, at § 2.
[187] *Id.* at § 3(a).
[188] *Id.* at § 8.

APPENDIX A

Breach of Personal Information Notification Act

Amending the act of December 22, 2005 (P.L.474, No.90), entitled "Breach of Personal Information Notification Act," further providing for definitions and notification of breach.

The General Assembly of the Commonwealth of Pennsylvania hereby enacts as follows:

Section 1. Section 2 of the act of December 22, 2005 (P.L.474, No.90), entitled "Breach of Personal Information Notification Act," is amended to read:

Section 2. Definitions.

***

"Breach of the security of the system." The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals [and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth]. Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.

***

"Personal information."

(1) An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when <u>either the name or</u> the data elements are not encrypted or redacted:

(i) [Social Security number.]<u>Identification numbers, such as:</u>

<u>(a) Social Security number.</u>

<u>(b) Driver's license number.</u>

<u>(c) State identification card number issued in lieu of a driver's license.</u>

<u>(d) Passport number.</u>

<u>(e) Taxpayer identification number.</u>

<u>(f) Patient identification number.</u>

(g) Insurance member number.

(h) Employee identification number.

(ii) [Driver's license number or a State identification card number issued in lieu of a driver's license.] Other associated names, such as:

(a) Maiden name.

(b) Mother's maiden name.

(c) Alias.

(iii) Financial account number, credit or debit card number, alone or in combination with any required expiration date, security code, access code or password that would permit access to an individual's financial account.

(iv) Electronic identifier or routing code, in combination with any required security code, access code or password that would permit access to an individual's financial account.

(v) Electronic account information, such as account name or user name.

(vi) Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular individual or small, well-defined group of individuals.

(vii) Biometric data, such as genetic information, a fingerprint, facial scan, retina or iris image, voice signature, x-ray image, or other unique physical representation or digital representation of biometric data.

(viii) Date of birth.

(ix) Place of birth.

(x) Insurance information.

(xi) Employment information.

(xii) Educational information.

(xiii) Vehicle information, such as:

(a) Registration number.

(b) Title number.

(xiv) Contact information, such as:

(a) Telephone number.

(b) Address.

(c) Email address.

(xv) Digitized or other electronic signature.

(2) The term does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records.

***

Section 2. Section 3 of the act is amended to read:

Section 3. Notification of breach.

(a) General rule.--An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Notice must also be provided to the Office of the Attorney General. Except as provided in section 4 or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made [without unreasonable delay] no later than 45 days after discovery of the breach. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.

(b) Encrypted information.--An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.

(c) Vendor notification.--A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.

Section 3. This act shall take effect immediately.

APPENDIX B

Security Breach Notification Laws	
STATE	**CITATION**
Alaska	Alaska Stat. § 45.48.010 *et seq.*
Arizona	Ariz. Rev. Stat. § 44-7501
Arkansas	Ark. Code § 4-110-101 *et seq.*
California	Cal. Civ. Code §§ 1798.29, 1798.80 *et seq.*
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen. Stat. § 36a-701b
Delaware	Del. Code tit. 6, § 12B-101 *et seq.*
Florida	Fla. Stat. § 501.171
Georgia	Ga. Code §§ 10-1-910 *et seq.*, 46-5-214
Hawaii	Haw. Rev. Stat. § 487N-1 *et seq.*
Idaho	Idaho Stat. § 28-51-104 *et seq.*
Illinois	815 Ill. Comp. Stat. § 530/1 *et seq.*
Indiana	Ind. Code §§ 4-1-11 *et seq.*, 24-4.9 *et seq.*
Iowa	Iowa Code § 715C.1 *et seq.*
Kansas	Kan. Stat. § 50-7a01 *et seq.*
Kentucky	KY Rev. Stat. §§ 365.732, 61.931 *et seq.*
Louisiana	La. Rev. Stat. § 51:3071 *et seq.*
Maine	Me. Rev. Stat. tit. 10 § 1347 *et seq.*
Maryland	Md. Code Com. Law § 14-3501 *et seq.*, Md. State Gov't Code § 10-1301 *et seq.*
Massachusetts	Mass. Gen. Laws § 93H-1 *et seq.*
Michigan	Mich. Comp. Laws § 445.72
Minnesota	Minn. Stat. §§ 325E.61, 325E.64
Mississippi	Miss. Code § 75-24-29
Missouri	Mo. Rev. Stat. § 407.1500
Montana	Mont. Code §§ 2-6-504, 30-14-1701 *et seq.*
Nebraska	Neb. Rev. Stat. § 87-801 *et seq.*
Nevada	Nev. Rev. Stat. §§ 603A.010 *et seq.*, 242.183
New Hampshire	N.H. Rev. Stat. § 359-C:19 *et seq.*
New Jersey	N.J. Stat. § 56:8-163
New York	N.Y. Gen. Bus. Law § 899-aa, N.Y. State Tech. Law 208
North Carolina	N.C. Gen. Stat § 75-65
North Dakota	N.D. Cent. Code § 51-30-01 *et seq.*
Ohio	Ohio Rev. Code §§ 1347.12, 1349.19 *et seq.*

Security Breach Notification Laws

STATE	CITATION
Oklahoma	Okla. Stat. §§ 74-3113.1, 24-161 *et seq.*
Oregon	Oregon Rev. Stat. § 646A.600 *et seq.*
Pennsylvania	73 Pa. Stat. § 2301 *et seq.* (Act of Dec. 22, 2005, P.L. 474, No. 94)
Rhode Island	R.I. Gen. Laws § 11-49.2-1 *et seq.*
South Carolina	S.C. Code § 39-1-90
Tennessee	Tenn. Code § 47-18-2107
Texas	Tex. Bus. & Com. Code § 521.053
Utah	Utah Code § 13-44-101 *et seq.*
Vermont	Vt. Stat. tit. 9, § 2435
Virginia	Va. Code § 18.2-186.6
Washington	Wash. Rev. Code §§ 19.255.010 *et seq.*, 42.56.590
West Virginia	W.V. Code § 46A-2A-101 *et seq.*
Wisconsin	Wis. Stat. § 134.98
Wyoming	Wyo. Stat. § 40-12-501 *et seq.*
District of Columbia	D.C. Code § 28- 3851 *et seq.*
Guam	9 GCA § 48-10 *et seq.*
Puerto Rico	10 L.P.R. § 4051 *et seq.*
Virgin Islands	14 V.I.C. § 2208

Source: Compiled by JSGC from Nat'l Conf. of State Legislatures, "Security Breach Notification Laws," June 11, 2015, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

PRIOR PRINTER'S NO. 3346 PRINTER'S NO. 3830

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE RESOLUTION

No. 778 Session of 2014

INTRODUCED BY THOMAS, MILLARD, COHEN, V. BROWN, BISHOP, READSHAW, SWANGER, D. COSTA, BROWNLEE, KINSEY, QUINN, DERMODY, DENLINGER AND DAVIDSON, APRIL 9, 2014

AS REPORTED FROM COMMITTEE ON COMMERCE, HOUSE OF REPRESENTATIVES, AS AMENDED, JUNE 24, 2014

A RESOLUTION

Directing the Joint State Government Commission to conduct a comprehensive study on the Commonwealth's cyber security efforts and protocols to protect private information of our citizens.

WHEREAS, The Commonwealth collects and possesses sensitive personal information about the residents of this Commonwealth through various State programs and routine administrative activities that are conducted by Commonwealth agencies and their contractors; and

WHEREAS, Recent headlines in the news about third parties hacking into retail and private corporate computer systems and the resulting compromise of personal information about customers is a grave concern; and

WHEREAS, It is necessary for the Commonwealth to be vigilant in protecting the personal information of its residents through adequate cyber security measures; and

WHEREAS, The level of cyber security efforts and protocols in this Commonwealth needs to be determined to assess risk and to

implement the best available safeguards of personal information; therefore be it

RESOLVED, That the House of Representatives direct the Joint State Government Commission to conduct a comprehensive study on the extent to which all branches of the Commonwealth government, including their contractors and subcontractors, implement cyber security efforts and protocols directed at safeguarding the personal information of residents of this Commonwealth; and be it further

RESOLVED, That the study review Statewide standards and protocols that serve as the framework for cyber security protection to determine:

(1) whether or not these standards and protocols are in place for the myriad of State offices that exist throughout this Commonwealth; and

(2) if funding and resources are sufficient to maintain and enhance security hardware, software, personnel and training to remain vigilant against evolving threats; and be it further

RESOLVED, That the study review the coordination of State information technology personnel involved in cyber security, including:

(1) whether or not they routinely examine the capabilities of the security systems to protect against cyber attacks;

(2) safeguards and restrictions placed on inter-agency sharing of State data and information;

(3) safeguards and restrictions placed on data and information sharing between State and local government agencies; and

(4) if there are resources available for continuing education of the information technology personnel;

and be it further

RESOLVED, That the study review the Commonwealth's standards and protocols as they apply to private entities that contract with the State; and be it further

RESOLVED, That the study review best practices in cyber security protection, including those used by Federal and other states' government; and be it further

RESOLVED, That the study determine if the Commonwealth would benefit from routine peer reviews of its cyber security protections, including input solicited from academic and private sector experts; and be it further

RESOLVED, That the study determine if current laws are adequate regarding public notification of data breaches, including privacy rights for residents of the Commonwealth, and the Commonwealth's strategic plan for cyber security and contingencies if a data breach occurs; and be it further

RESOLVED, That the commission consult with the Governor's Office ~~for Information Technology~~ OF ADMINISTRATION in preparing <-- the study; and be it further

RESOLVED, That the commission report its findings from the study to the General Assembly within one year of the adoption of this resolution.