Joint Committee on Cybersecurity, Information Technology, and Biotechnology 2017 Interim Membership Roster

Senator James C. Rosapepe, Co-chair
Delegate C. William Frick, Co-chair

Senators

Senator Brian J. Feldman
Senator Bill Ferguson
Senator Stephen S. Hershey, Jr.
Senator J. B. Jennings
Senator Susan C. Lee

Delegates

Delegate Benjamin F. Kramer
Delegate Aruna Miller
Delegate Warren E. Miller
Delegate Dan K. Morhaim
Delegate C. T. Wilson

Committee Staff

Tami D. Burt
Richard L. Duncan
Jody J. Sprinkle

Joint Committee on Cybersecurity, Information Technology, and Biotechnology

December 18, 2017

The Honorable Thomas V. Mike Miller, Jr., Co-chair
The Honorable Michael E. Busch, Co-chair
Members of the Legislative Policy Committee

Ladies and Gentlemen:

The Joint Committee on Cybersecurity, Information Technology, and Biotechnology respectfully submits this summary report of its 2017 interim activities. The committee's statutory charge is to "work to broaden the support, knowledge, and awareness of advances in cybersecurity, information technology, and biotechnology to benefit the people of Maryland, evaluate State cybersecurity systems and the adequacy of economic development and job skills training programs to advance cybersecurity in the State, and make recommendations regarding actions to promote cybersecurity, information technology, and biotechnology industries in the State." The committee met twice during the interim: October 26 and December 5, 2017.

At the first meeting, the committee was briefed on the need for technology infrastructure to support smart-medicine solutions and the status of providing public school digital (broadband) equity in connecting all K-12 students. At the second meeting, the committee was briefed on the status of the Department of Human Services' efforts to modernize its systems to that it may use big data to assist in providing government services, several examples of smart-medicine solutions developed by Johns Hopkins, the challenges and concerns with the cybersecurity of the Internet of Things, and the status of the federal Internet consumer privacy policy.

On behalf of the committee, we wish to thank those individuals who contributed their time and effort during the 2017 interim in assisting the committee with its work.

Respectfully submitted,

James C. Rosapepe
William Frick

James C. Rosapepe
Senate Chair

C. William Frick
House Chair

JCR:CWF/TDB/nac

cc: Ms. Carol L. Swan
Mr. Ryan Bishop

Joint Committee on Cybersecurity, Information Technology, and Biotechnology 2017 Interim Report

Need for Technology Infrastructure to Support Smart-Medicine Solutions

On October 26, 2017, the committee heard from David Sharp, Ph.D., Director, Center for Health Information Technology and Innovative Care Delivery, Maryland Health Care Commission (MHCC). Mr. Sharp presented the following information on the need for technology infrastructure to support smart-medicine solutions.

- *Electronic Health Records (EHRs):* EHR adoption in hospitals is widespread, with Maryland at 100% and the nation at 96%. Maryland has received over $300.0 million to use for implementing EHR. Maryland has distributed $223.0 million to Medicare (with an average of $4.8 million received per hospital) and $83.0 million to Medicaid (with an average of $1.8 million received per hospital). The hospitals are building upon meaningful use achievements as they prepare to meet new metrics that aim to link optimization of EHR data and quality. Remaining ahead of the national average, State EHR incentives influenced earlier adoption among Maryland physicians (over $9.0 million paid to practices since 2011). Office-based physicians in hospital-owned practices are more likely to have adopted EHRs than those in independent practices. EHR adoption among long term care (or comprehensive care) facilities has steadily increased over the past four years. About half of the adopters report using at least basic features of the EHR.

- *Health Information Exchange (HIE):* The continued diffusion of HIE is essential to achieving the HIE goal of providing the right information to the right place at the right time. HIE is a critical component to support the shifting business model in health care from volume to value. Accelerating availability of electronic information to guide decision making and promote care coordination is a priority for Maryland and the nation. Nine HIEs have registered with MHCC. As a State-designated HIE, the Chesapeake Regional Information System for Our Patients (CRISP) is tasked with building the technical infrastructure to support a statewide HIE. Eight other regional HIEs facilitate local exchange activities (six are owned and operated by acute care hospitals). Registered entities must meet the statutory definition of HIE and adopt privacy security protections above the minimum required by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). As technology continues to evolve, stakeholders have expressed concerns that the HIE definition in statute is too narrowly defined.

- *Telehealth:* About 77% of Maryland hospitals have adopted telehealth, as compared to 71% nationwide. Of the total Maryland hospitals, a higher percent of the health systems hospitals have adopted telehealth than community-based hospitals. The adoption among the hospitals is in various phases from exploratory discussions to deploying telehealth projects in specific specialties and identifying ways to sustain these projects over time. All hospitals report that improving quality of care is the leading reason for adopting telehealth. Adoption among office-based physicians in Maryland is about 7%, much lower than the national average of 49%. Of the total Maryland physicians, adoption is highest among psychiatrists followed by dermatologists.

- *Telehealth and Mobile Health Grants:* Since 2014, MHCC has awarded 5 rounds of telehealth grants to 12 organizations totaling $525,000. These grantees implemented diverse use cases to test the effectiveness of telehealth with various technology, patients, providers, clinical protocols, and care settings. Examples include (1) enhancing care coordination between comprehensive care facilities and acute care hospitals; (2) reducing hospital admissions and readmissions through remote patient monitoring; and (3) supporting chronic care management of high risk patients. In 2016, MHCC awarded an mHealth grant to one organization totaling $100,000. This grantee implemented a unique use case to test the effectiveness of an mHealth application in managing pediatric patients with asthma. The objectives of mHealth are to increase consumer access to health care services, information, and education; and enable consumers to take more responsibility in managing their health.

- *Breaches*: Significant hacking incidents have occurred in the last few years, causing breaches of individual health records. Over 114 million records were compromised in 2015, compared to 41 million records between 2010 and 2014. In relation to other states, Maryland ranks above the 50th percentile for number of breaches between 2010 and 2016. Maryland remains midway in number of breaches occurring between 2010 and 2016 in comparison to states with similar characteristics. Breaches involving a hacking/IT incident and unauthorized access/disclosure account for at least a third of all breaches in Maryland and in comparative states. To reduce the risk of breaches, additional protections and awareness are needed. Incident response plans need to include specific cybersecurity procedures. The human element needs to be managed through robust security education and awareness programs. There needs to be appropriate oversight of business associates that handle protected heath information.

The committee is interested in hearing at a future meeting from several grantees to learn about how they are using grant funds and how the grant funds are beneficial to promoting the acceleration of technology. The committee plans to further discuss whether the health care community can come together to develop best practices to prevent breaches. Possible additional funding, legislation, or other actions may be needed to assist in moving the industry toward implementing protections.

Status of Providing Public School Digital (Broadband) Equity in Connecting All K-12 Students

Also on October 26, the committee heard from Kristy Michel, Deputy Superintendent for Finance and Administration, Maryland State Department of Education (MSDE); and Antonio Herrera, Chief Information Officer, MSDE. The speakers presented the following information on the status of providing public school digital (broadband) equity in connecting all K-12 students.

- *Maryland Takes Action to Close Fiber Gap:* MSDE conducted a statewide survey of local school systems in mid-2016 to determine internet speed, capacity, type of connection, and where there might be a lack of capacity. With the Governor's Office and the Education Superhighwy, MSDE engaged 12 CIO's to offer technical assistance and support for e-Rate applications. The federal E-rate program, established by the Federal Communications Commission (FCC), is designed to assist schools in implementing Internet access to the schools and within the schools. MSDE also worked with the Board of Public Works and the Public School Construction Program to modify COMAR to allow local education agencies (LEAs) to access existing school construction funds for e-Rate eligible broadband construction.

- *Maryland Broadband Fiber Initiative:* In late 2015, the State had over 200 schools that were without a direct fiber connection; all the schools without fiber connection had broadband speed connections through other means, such as microwave. The State decided to move all schools to fiber connections to allow for flexibility in upgrading or downgrading service levels to meet demand. In early 2016, Maryland was among seven states accepted into the National Governors Association's "Educational Broadband Policy Academy." For this intensive year-long effort, the policy academy partnered with the nonprofit Education SuperHighway (ESH) for its technical and policy expertise. The mission of the policy academy is to help connect as many K-12 as possible to fiber optic Internet by assessing existing educational fiber infrastructure, identifying challenges, and providing technical and policy guidance to close any gap. MSDE worked collaboratively with the Governor's Administration, the Department of Information Technology (DoIT), and local school system on this initiative. MSDE's Chief Information Officer (CIO) and the e-Rate policy subject matter expert worked with the K-12 District CIOs to provide improved tracking on connectivity, capacity, and schools without fiber connection. As of October 2017, more than 99% of Maryland's public schools have fiber optic broadband-only 12 out of 1,434 schools lack fiber connections, and of these, 5 have fiber projects under way. The remaining have broadband via cable, microwave, or other technology.

- *Limited Time for LEAs to Save up to 90% on Broadband Construction:* In October 2017, Maryland received the final Universal Service Administration Company (USAC) approval of its state-matching eligibility. School systems are now able to apply for the matching funds. Next school year is the final e-Rate cycle for the federal government to match state funds for up to 10% of approved broadband construction projects on top of a district's existing e-Rate discount. By acting now, school systems may be reimbursed up to 90% of their eligible broadband construction. E-rate will continue, but the federal match will not.

- *Internet Bandwidth:* All schools have reported having adequate Internet bandwidth. In the past 2 years, 12 districts made significant improvements to their Internet bandwidth. Many more districts made improvements to internal infrastructure and Wide-Area Networking (WAN). In less than 2 years, Maryland has improved its broadband bandwidth by 20% across the State.

The committee expressed concern that there are 12 schools (mostly elementary schools) without fiber connectivity (although they do have broadband Internet using other means). The committee requested MSDE to provide the committee with the projected timeline for each school to be connected. The committee also requested MSDE to provide information related to the adequacy of bandwidth in each school, the devices used in each school, and the cost to eliminate any shortage of bandwidth in each school.

Status of the Department of Human Services' Efforts to Modernize its Systems so that it May Use Big Data to Assist in Providing Government Services.

On December 5, the committee heard from Secretary Lourdes Padilla, Department of Human Services (DHS); Subi Muniasamy, Chief Technology Officer, DHS; and Michael Leahy, Secretary, Department of Information Technology (DoIT). The speakers presented the following information on its MD THINK system, a modernized system that will allow it to use big data to assist in providing government services.

- *MD THINK Vision:* MD THINK envisions establishing a modernized technology platform for enhanced service delivery to Maryland residents. The database system will provide a shared technology platform hosted on the Cloud, as well as a shared data repository for health and human services applications across the State. DHS is working with DoIT to develop the system which can be used by multiple administrations within DHS (such as the Child Support Administration, the Social Services Administration, and the Financial Assistance Administration) and also multiple agencies, thereby creating efficiencies in managing data. Since multiple agencies need similar data, sharing data means entering the data at a single input and eliminates duplicate verification of data efforts.

- *Timeline:* Completed in phases through September 2020, the system will be used for eligibility and exchange on long term care services (effective June 2018), for child welfare and juvenile services (effective March 2019), and child support replacement services (May 2020). By having one system with significant data fields across multiple agencies, there will be more opportunities for "big data" analysis aimed at improving services. A MD THINK team in DHS is responsible for technical delivery and performance, as well as coordination across vendor and agencies. A Steering Committee was established comprised of the agencies that are anticipated to use the system (including the Department of Human Services, the Department of Juvenile Services, the Department of Health, the Department of Information Technology, the Department of Budget and Management, and the Maryland Health Benefit Exchange). For its cybersecurity strategy, MD THINK will adhere to National Institute of Standards and Technology (NIST) and Federal Information Security Management Act (FISMA) standards. Other agencies (including the Department of Labor, Licensing, and Regulation; and Department of Public Safety and Correctional Services) will be integrated into the system in the next phase. The system will be designed so other agencies can easily be connected.

The committee expressed support for the implementation of MD THINK and requested DHS to let the committee know if there are any actions the legislature should take to assist with moving the process forward. The committee would like an update in about a year on the progress. Also, the committee requested DHS to provide information that specifies the benefits of the system for each involved agency. Specifically, how will the system help each agency and with the new system, how can each agency do a better job providing government services to consumers?

Several Examples of Smart-Medicine Solutions

Also, on December 5, the committee heard from Dwight Raum, Vice President and Chief Technology Officer, Johns Hopkins University and Johns Hopkins Health System; Gregory Krauss, Professor of Neurology, Johns Hopkins University School of Medicine; and Sezin Palmer, Mission Area Executive for National Health, Johns Hopkins University Applied Physics Laboratory. The presenters presented the following information on several examples of smart-medicine solutions.

- *InHealth:* In transforming research and patient care, there is a digital shift of medicine. Johns Hopkins *in*Health is a vision that each health decision is fully informed by scientific knowledge. Researchers combine clinical, genetic, lifestyle, and other data sources to create innovative health analysis tools intended to improve decision making in the prevention and treatment of a range of conditions, including cancer, cardiovascular disease, autoimmune disorders, and infectious disease. In all of Johns Hopkins scientific endeavors, it seeks to provide the right care to the right person at the right time. Its goals are to capture clinically-relevant and biologically-anchored subgroups more intentionally at scale, use such subgroups to diagnose and treat more efficiently and to discover mechanisms, and integrate discovery and deliver. Hopkins' Technology Innovation Center has a team of 27 technology professionals. The center partners with faculty and health IT start-ups to intersect medicine and technology.

- *Examples:* The center has a partnership with Multiple Sclerosis (MS) Centers of Excellence. Current optical coherence tomography (OCT) scans exist as standalone reports and are not easily available for longitudinal or cohort analysis. OCT scans are used to view retinal thinning since that condition correlates with the disability of progression for MS patients. The solution is a prognosis health analysis tool to rapidly extract structured data from OCT scans for comparison. Another example is the IVC Filter Alert System which catches blood clots. A third example is the EpiWatch, a highly successful research App. The watch collects seizure biosensor and labelling data for non-electroencephalogram (EGG) seizure detection and helps persons with epilepsy manage their disease. In revolutionizing care for patients of epilepsy, the watch monitors seizures and alerts caregivers and helps to improve medication dosage and adherence which results in preventing seizures.

The committee requested Johns Hopkins to let the committee know if there are any actions the legislature can do to assist with maximizing their efforts. The committee would like a briefing next year from Johns Hopkins on their strategy for coming up with innovative health analysis tools.

Challenges and Concerns with Cybersecurity of the Internet of Things

Additionally, on December 5, the committee heard from Charles Ames, Director, Statewide Security Services, Department of Information Technology (DoIT). Mr. Ames presented the following information on the challenges and concerns with cybersecurity of the Internet of Things (IoT).

- *Privacy Concerns:* A growing IoT, or the Network of Everything, brings with it an enormous burden on the social contract governing citizens, businesses, and governments. Although able to solve or inform an unending variety of individual or business problems, the IoT challenges the basic concepts of privacy, or at least intensifies privacy concerns. From the beginning of U.S. telephony, the data the phone companies used to route calls were mandated to be held so that the calls existence could be a matter for law enforcement to collect and for courts to consider. Today, there are cases where both companies and law enforcement reach into a user's cell phone location history and browsing data history to establish behavioral patterns either to improve marketing, in the first case, or as evidence in the latter case. The enormous amount of private and descriptive data made available by the common use of the IoT (*e.g.,* smart phones and Internet browsers) places the burden of maintaining privacy on the user.

- *Traditional Devices:* The Pew Research Center indicates that the median household in 2016 had at least 5 Internet-connected devices. Further, 20% of households had more than 10 connected devices. Approximately 8.4 billion connected "things" will be in use in 2017, up 31% from 2016. Predictions are that more than 20 billion devices are anticipated to be connected to the Internet in the next few years. These IoT devices are mostly the traditional items that are meant to be connected to the internet for full functionality. Their protections against exploitation varies widely by device and user. In most cases, these items (*e.g.*, PCs, smartphones, printers, and tablets) have security features, though they may not be completely understood by their users. Other IoT devices include TV sets, appliances, traffic scanners, assistance devices such as Alexa and Siri, and modern vehicles.

- *Other Devices:* A second group of IoT devices are those that are: obsolete, no longer actively maintained or monitored, possibly no longer securable, or ones where the method of connection was not securely designed. In the workplace, these items should be included in a traditional security strategy. They include: truck scales, medical devices, manufacturing equipment, and kiosks. A third group of IoT devices are those that were never designed to be connected to the Internet or a part of the IoT. In the workplace, these devices often remain unknown to security and network professionals, and there are few, if any, means to secure the devices. These include: generations of industrial controls (gas valves and water systems); and formerly manually-controlled devices that now have modern electronic controls (*e.g.,* thermostats, retrofitted older vehicle controller access networks, and telco switching centers).

- *Russian Electric Grid Hack:* In 2015, Russian hackers socially engineered, or fooled, key electrical grid operators in the Ukraine into betraying their own network credentials. Using those credentials, the hackers were able to remotely turn off the power to vast regions of the Ukraine. Importantly, the power was able to be restored within hours only because the physical switches had yet to be replaced, and the engineers who knew how to operate the switches were still available. Otherwise, the IoT, which eliminates much of the physical switching requirements, as well as the engineers required to operate the physical switches, would have been exploited as a weapon.

- *Federal Legislation and Awareness Campaign:* In response to security lapses and breaches, the IoT Cybersecurity Improvement Act was introduced in Congress in 2017 to require security standards for U.S. Government purchased IoT devices. There are generally ways to control how devices communicate on the networks they are connected to. However, this is not a readily available capability for many small businesses and residential homes. *Via* an awareness campaign, information could be disseminated to residents and businesses, while also including instructions on common techniques that can improve security on many of these devices, such as setting up passwords and ensuring devices communicate over encrypted connections.

Status of the Federal Internet Consumer Privacy Policy

Lastly, on December 5, the committee heard from Laura M. Moy, Deputy Director, Center on Privacy & Technology, Georgetown University Law Center. Ms. Moy presented the following information on the status of the federal Internet consumer privacy policy.

- *Consumers Feel They Lost Control of Their Privacy:* Ms. Moy, a consumer and privacy advocate, indicated that consumers feel that they have lost control of their private information, and consistently are asking for greater control. About 91% agree or strongly agree that consumers have lost control of how personal information is collected and used by companies, and 68% believe current laws are not good enough in protecting consumers' privacy online. Policymakers should consider how to give consumers greater control over the personal information they share in many different contexts. However, there is no one-size-fits-all approach for privacy. Rather, privacy laws and regulations should be context-specific, carefully tailored based on the avoid-ability of the information sharing, the sensitivity of the information shared, and the expectations of consumers. Consumers are in the greatest need of greater control when they do not have a choice about whether to share the information in the first place. There are a variety of laws that protect consumer information in specific contexts in which sharing is unavoidable – such as the information shared by students in an educational context, by consumers in a financial context, by customers in a telecommunications context, and by patients in a medical context.

- *Credit Reporting Agencies and ISPs:* Consumers do not get to choose whether or not their information is shared with credit reporting agencies (CRAs), and, therefore, that information should be afforded strong protection by default. Further, consumers need strong default privacy rules for Internet service providers (ISPs). In the modern era, it is difficult or even impossible to get an education, apply for a job, run a business, or conduct banking without an Internet connection through an ISP. Not only are consumers unable to avoid sharing information with ISPs, but the information consumers share may be deeply private. As the consumer's gateway to the Internet, ISPs have broad, unfettered access into nearly everything the consumer does online. A complete record of the websites a consumer visits and the applications they use, especially in combination with details about the timing, duration, and volume of traffic, can be used to determine their medical conditions, employment status, family status, political leanings, romantic and sexual preferences, and sleep habits.

- *ISP Options:* Consumers' personal data does not belong to ISPs; it rightfully belongs to consumers. While consumers pay their bills for their Internet connections, they do not also need to pay through their personal data. They only share private information with ISPs so that their Internet traffic can be routed to the right place. They do not expect ISPs to collect, retain, and use that information to make money off of them. In areas where consumers have only one option for high-speed broadband, consumers cannot switch providers if they dislike the privacy practices of their ISP. In areas where there are two or three possible providers, switching costs, contract termination fees, installation fees, and the time investment necessary to research and adopt an alternative make it difficult for a subscriber of one provider to switch to another.

- *No Federal Privacy Rules:* There is not much that the average consumer can do to hide their online activities from their ISP. The few things consumers can do to protect their own privacy from their ISPs add up to a handful of weak tools. In recognition of the need for strong broadband privacy protections, in October 2016 the Federal Communications Commission (FCC) issued rules that would have required ISPs to provide their customers with meaningful choices about their personal information, and to keep customer data secure. However, in March 2017, Congress used the Congressional Review Act to eliminate those rules. As a result, there are no federal rules that currently govern the privacy obligations of ISPs.

Note: Senate Bill 1200 of 2017 (did not pass) would have prohibited an ISP from selling or transferring consumer's personally identifying information to a person without the consumer's express and affirmative permission. Likewise, an ISP would not have been allowed to send or display to a consumer an advertisement that has been selected to be sent or displayed because of the consumer's browsing history without the consumer's express and affirmative permission.

The committee understands that about 20 states have attempted to pass Internet privacy legislation. The committee requested Ms. Moy to provide the committee with information about what other states have done.