Department of Legislative Services

Maryland General Assembly
2020 Session

FISCAL AND POLICY NOTE
First Reader

House Bill 996 (Delegate Lisanti)
Health and Government Operations

Department of Information Technology - Cybersecurity Response Team

This bill requires the Department of Information Technology (DoIT) to establish a Cybersecurity Response Team (CRT). CRT must work with local jurisdictions to ensure that, by December 31, 2021, each local jurisdiction (1) has developed an emergency response strategy for cybersecurity attacks and incidents and (2) enters into a related mutual aid agreement. The bill authorizes the 9-1-1 Trust Fund to be used to fund the development of the response strategies and *requires* the Comptroller to disburse the funds for that purpose. By January 1 of each year, DoIT must report to the Governor and the General Assembly on CRT's activities.

Fiscal Summary

State Effect: General and special fund expenditures and special fund revenues increase significantly in FY 2021 and 2022 as DoIT hires consultants to staff CRT and is reimbursed by local governments, as discussed below. Special fund expenditures from the 9-1-1 Trust Fund increase significantly beginning in FY 2021 to reimburse local governments for costs associated with implementing the bill; the total is likely to exceed $500,000 in FY 2021 and $1.0 million in FY 2022, as discussed below.

Local Effect: Local government expenditures and revenues increase significantly and correspondingly beginning in FY 2021 as local governments pay DoIT for services provided by CRT and are, in turn, reimbursed from the 9-1-1 Trust Fund. Local expenditures further increase, likely significantly, to cover larger funding gaps in the 9-1-1 system.

Small Business Effect: Minimal.

Analysis

Bill Summary: CRT must work with local jurisdictions to ensure that each local jurisdiction (1) has an emergency response strategy to protect vital technology infrastructure against cybersecurity attacks and incidents and (2) develops and enters into mutual aid agreements for reciprocal emergency aid and assistance in the event of a cybersecurity attack or incident.

Current Law/Background:

9-1-1 Trust Fund

The State's 9-1-1 system is funded through the 9-1-1 Trust Fund. The fund is administered by the Department of Public Safety and Correctional Services and includes revenue from a State fee, a local fee, and a fee on prepaid wireless services (as well as investment earnings on the fund). Historically, county expenditures for 9-1-1 systems have consistently exceeded available fee revenues. Across all counties, in fiscal 2018, fee revenues covered only 36.3% of operating costs. Chapters 301 and 302 of 2019 increased the fees that accrue to the 9-1-1 Trust Fund, but it is not yet clear whether these additional revenues are sufficient to account for the chronic deficit in 9-1-1 system funding.

For more information on the 9-1-1 fee, as well as the State's current 9-1-1 system and recent legislation to modernize the system, please see the **Appendix 1 – 9-1-1 Funding and Modernization.**

Department of Information Technology and Cybersecurity

DoIT and the Secretary of Information Technology are responsible for, among other things, (1) developing and enforcing information technology (IT) policies, procedures, and standards; (2) providing technical assistance, advice, and recommendations to any unit of State government; and (3) developing and maintaining a statewide IT master plan. Certain agencies, such as the Maryland Stadium Authority and University System of Maryland, are exempt from DoIT's direct oversight.

The fiscal 2020 operating budget for DoIT included $5 million in general funds for DoIT to enhance cybersecurity in the State, and DoIT advises that the Governor's proposed budget for fiscal 2021 includes $10 million in general funds for the same purpose. DoIT plans to use these funds primarily to conduct cybersecurity assessments of State agencies and work to rectify any problems discovered.

For more information on cybersecurity issues in the State and across the nation, please see the **Appendix 2 – Cybersecurity.**

State Fiscal Effect:

Department of Information Technology

DoIT advises that it currently has a contract for cybersecurity incident response experts to assist and advise the State; the hourly rate for an expert is $300 per hour. Moreover, DoIT does not currently have the staff necessary to assist every local jurisdiction with developing and implementing cybersecurity response strategies in the timeline allotted. As such, this analysis assumes that DoIT employs a team of experts under its contract to staff CRT and assist local jurisdictions. DoIT estimates that four experts, each working full time for one year are necessary to ensure each local jurisdiction meets the timeline established by the bill, but actual timing may vary from this estimate.

Therefore, general and special fund expenditures increase significantly in fiscal 2021 and 2022 for DoIT to employ the experts to staff CRT. A precise estimate of the total cost depends on how long the experts must be employed and, therefore, cannot be reliably estimated at this time. Since the bill takes effect October 1, 2020, and the response strategies must be in place by December 1, 2021, the maximum number of months the experts must be employed is 15 months. *For illustrative purposes*, expenditures increase by (1) $48,000 for each week the team of four is employed; (2) $2.5 million if the team is employed for a full year; and (3) $3.1 million if the team is employed for a full 15 months.

Since DoIT operates on a fee-for-service basis, any expense it incurs to hire the experts for CRT will be billed to local governments and paid for as special funds; nevertheless, some portion of this cost may need to be covered with general funds, at least initially. As discussed in the following sections, local government expenditures for this purpose are to be reimbursed from the 9-1-1 Trust Fund.

9-1-1 Trust Fund

Special fund expenditures from the 9-1-1 Trust Fund increase significantly to reimburse local governments for the costs they incur to develop cybersecurity response strategies under the bill. The total impact depends on numerous unknown factors, including the length of time during which the CRT experts discussed above are employed (and, thus, how much counties are billed by DoIT for their work) and whether local governments must upgrade any existing technology or hire new staff as part of the cybersecurity response strategy. Therefore, a reliable estimate is not feasible. Even so, expenditures are likely to total millions of dollars in fiscal 2021 and 2022 so that local governments can reimburse DoIT for CRT staff. Expenditures could total hundreds of thousands of dollars in future years if additional staff are needed on a permanent basis by local governments.

Local Fiscal Effect:

Emergency Cybersecurity Response Strategy Development

Some local governments advise they already comply with the bill as they have an emergency response strategy for cybersecurity incidents and attacks in place. Others advise that complying with the bill requires additional time and resources to be spent on technology upgrades and/or staff to develop and implement such a strategy, and doing so could cost hundreds of thousands of dollars.

As CRT reviews existing plans and assists local governments in developing new plans, if necessary, local government expenditures increase significantly. The total cost for each local government depends on how long the CRT team is needed and likely varies significantly from local government to local government. For example, for a local government that believes it is currently in compliance with the bill, CRT may only require a few days to review and approve the existing strategy. Conversely, CRT may need weeks or even months to help a local government without a strategy develop and implement one.

Since the bill requires local governments to be reimbursed for any costs related to development of the cybersecurity strategy from the 9-1-1 Trust Fund, local government revenues increase correspondingly.

9-1-1 System Funding

Total local revenues from the 9-1-1 Trust Fund are not changed, but under the bill a portion of those revenues goes to cover the cost of the CRT instead of to the 9-1-1 system. As discussed below in Appendix 1, the 9-1-1 system is underfunded and local governments cover funding gaps for their 9-1-1 systems. Moreover, it is not yet clear whether the additional revenues from Chapters 301 and 302 of 2019 are sufficient to close the chronic deficit in 9-1-1 system funding. To the extent that the bill exacerbates current funding deficits for the 9-1-1 Trust Fund by using funds for cybersecurity response strategies, local expenditures for 9-1-1 system operations may increase and/or 9-1-1 system upgrades and improvements may be delayed.

Additional Comments: The Department of Legislative Services notes that the bill requires annual reports on the activities of the CRT, but the CRT's work appears to conclude year-end 2021.

Additional Information

Prior Introductions: None.

Designated Cross File: None.

Information Source(s): Department of Information Technology; Baltimore City; Montgomery and Prince George's counties; Maryland Association of Counties; City of Bowie; Maryland Municipal League; Comptroller's Office; Department of Legislative Services

Fiscal Note History: First Reader - March 6, 2020
rh/mcr

Analysis by: Richard L. Duncan

Direct Inquiries to:
(410) 946-5510
(301) 970-5510

Appendix 1 – 9-1-1 Funding and Modernization

Maryland's 9-1-1 System

Chapter 730 of 1979 established a statewide 9-1-1 system, as well as the Emergency Number Systems Board (ENSB) to oversee the new system. The legacy 9-1-1 model, which is based on a landline phone system, consists of local public safety access points (PSAPs) connected to an analog wireline phone network to deliver emergency calls via a circuit-switched architecture. However, 70% of 9-1-1 calls are now made from cell phones, and an increasing number are made via Voice over Internet Protocol networks, presenting a challenge as to how to process and obtain accurate caller location and phone number information.

As analog landline communication is phased out completely, state and local governments are preparing for "next generation" technology that will allow 9-1-1 centers to access not only more accurate information about caller location, but also other information that will assist emergency personnel in communicating with callers and responding more efficiently. This Next Generation 9-1-1 (NG 9-1-1) technology will allow PSAPs to receive text, chat, video, location, and various other types of data from a single 9-1-1 call. However, local governments face challenges both in maintaining existing 9-1-1 systems and in transitioning to NG 9-1-1 systems, primarily due to a lack of funding.

9-1-1 System Funding

The 9-1-1 system is funded through the 9-1-1 Trust Fund. The fund is administered by the Department of Public Safety and Correctional Services and includes revenue from a State fee, local fee, and fee on prepaid wireless services (as well as investment earnings on the fund).

Telephone companies, wireless carriers, and other 9-1-1 accessible service providers collect and remit monthly the State 9-1-1 fee and the county additional charge to the Comptroller for deposit into the fund. The State 9-1-1 fee is distributed to counties at the discretion of ENSB in response to county 9-1-1 system enhancement requests. The county additional charge, the prepaid wireless 9-1-1 fee remittances, and any investment earnings of the fund are all distributed quarterly to each county in prorated amounts according to the level of fees collected in each jurisdiction. The State 9-1-1 fee and 25% of all collected prepaid wireless 9-1-1 fees may be used to reimburse counties for the cost of enhancing the 9-1-1 system. The county additional charge and the remaining 75% of all collected prepaid wireless 9-1-1 fees may be spent on maintenance and operating costs of 9-1-1 systems.

Commission to Advance NG 9-1-1 Across Maryland

Chapters 301 and 302 of 2018 established the Commission to Advance Next Generation 9-1-1 Across Maryland to study and make recommendations regarding next generation 9-1-1 emergency communication services. The commission's preliminary report, released in November 2018, makes 23 recommendations regarding numerous issues, including, among other things, technology standards, cybersecurity, NG 9-1-1 implementation, staffing, and fees. The report emphasizes the importance of adjusting the State's 9-1-1 fee structure, concluding that, "current 9-1-1 funding is grossly insufficient to support the current 9-1-1 system, let alone the updated NG 9-1-1 technology." The commission's final report is expected to be released during the 2020 legislative session.

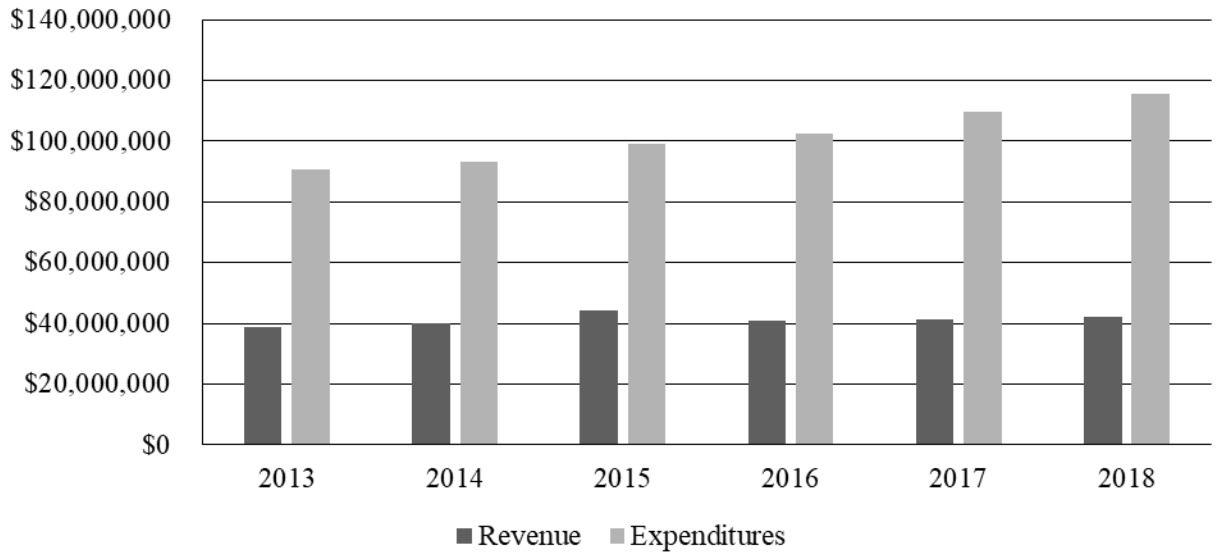
Recent Legislation to Modernize and Enhance the 9-1-1 System

Many of the commission's recommendations were addressed through Chapters 301 and 302 of 2019. Among other things, the Acts expanded the responsibilities of ENSB to include additional oversight and training for PSAPs, increased the 9-1-1 fees, and applied the fees to each separate outbound call voice channel capacity instead of each account.

Historically, county expenditures for 9-1-1 systems have consistently exceeded available fee revenues. **Exhibit 1** shows total 9-1-1 fee revenues and total 9-1-1 operating expenditures per fiscal year from fiscal 2013 to 2018 (the most recent publicly available data). Across all counties, in fiscal 2018, fee revenues covered 36.3% of operating costs. However, the percentage of costs offset by revenues varied significantly by county in that year, as shown in **Exhibit 2**. For example, only 9.7% of Dorchester County's costs were offset by fee revenues, while in Anne Arundel County, 55.7% of costs were offset. To address this shortfall, Chapters 301 and 302 modified the fees in the following manner:

- the State 9-1-1 fee and local 9-1-1 fee now both apply to each separate outbound call voice channel capacity (*i.e.*, lines), instead of each account, as specified;
- the State 9-1-1 fee was increased from $0.25 per month to $0.50 per month; and
- a local government is authorized to temporarily increase its local 9-1-1 fee under specified circumstances; combined with the existing local 9-1-1 fee, the maximum amount a local government may charge is increased from $0.75 per month to $1.50 per month.

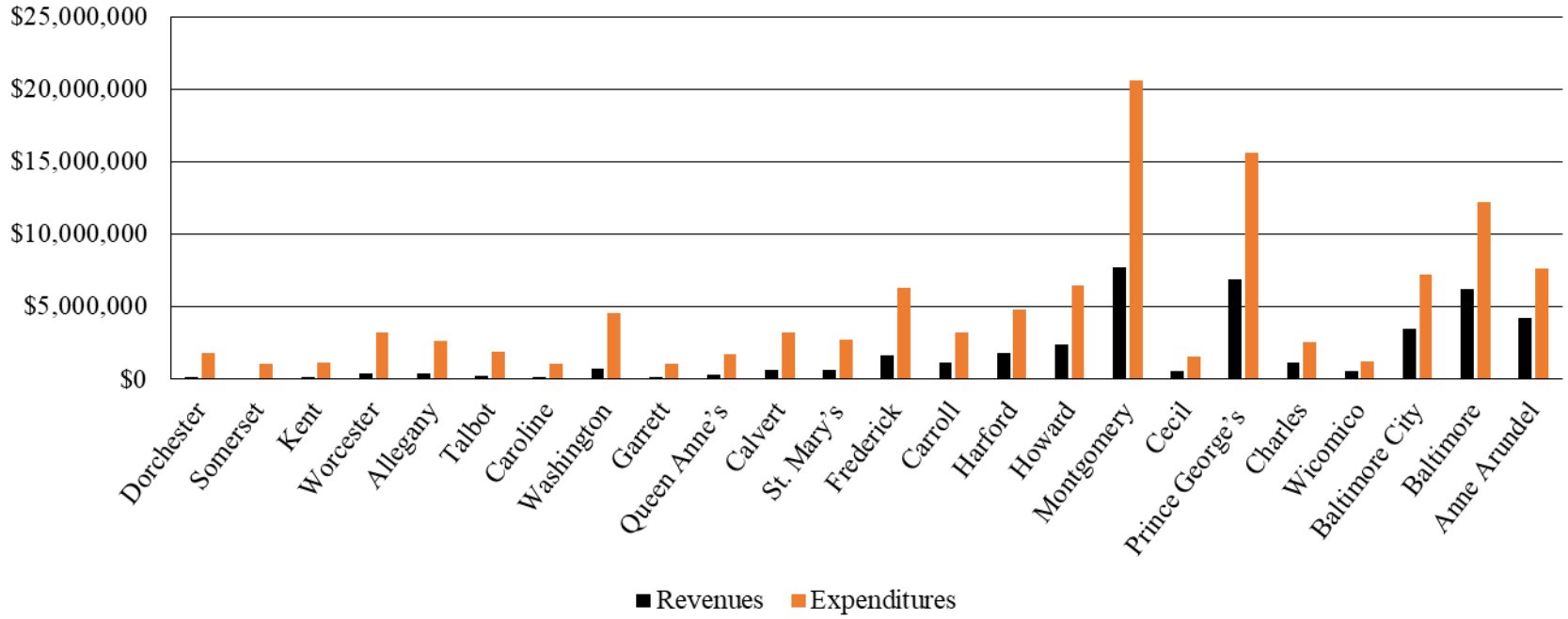
Exhibit 1
Total County 9-1-1 Fee Revenue and Operational Expenditures
Fiscal 2013-2018



Note: Prepaid wireless 9-1-1 fee revenues were first collected in fiscal 2014. County operating expenditures are costs as reported by county-selected independent auditors and typically include 9-1-1-related personnel salaries and benefits, recurring maintenance and service fees, mapping maintenance and updates, network associated fees, and capital expenditures not covered by the Emergency Number Systems Board.

Source: Emergency Number Systems Board annual reports (FY 2013-2019)

Exhibit 2
9-1-1 Fee Revenues and Operating Expenditures by County
Fiscal 2018



Source: Emergency Number Systems Board, 2018 annual report

Appendix 2 – Cybersecurity

Cybersecurity Issues

In recent years, cybersecurity and privacy issues have received significant attention from the general public and policymakers as a result of the many ransomware attacks, data breaches, and other cyber attacks that have taken place in the nation and the State. Globally, and in 2019 alone, the Center for Strategic & International Studies identified nearly 100 known cyber attacks (many of which involved the United States) involving (1) government agencies; (2) defense and high tech companies; or (3) economic crimes with losses of more than $1 million.

Also in 2019, governments in the State experienced numerous cyber attacks and breaches. Most notably, Baltimore City government's computer systems were infected with ransomware that made the systems inaccessible to government officials and employees. The systems remained unavailable for weeks, and recovery is still ongoing. Similarly, the Maryland Department of Labor's licensing database was breached, and the personally identifiable information (PII) of as many as 78,000 licensees may have been accessed by the hackers.

Recent State Action

In June 2019, the Governor signed Executive Order 01.01.2019.07, which creates the Maryland Cyber Defense Initiative to strengthen the State's ability to manage the effects of a cybersecurity incident. The initiative creates the Office for Security Management within the Department of Information Technology (DoIT) and charges the office with responsibility for the direction, coordination, and implementation of an overall cybersecurity strategy for all Executive Branch information technology (IT) systems. The office is led by a newly created State Chief Information Security Officer (SCISO), who is appointed by the Governor. The order also established the Maryland Cybersecurity Coordinating Council to assist the SCISO and office in its duties.

In that same month, DoIT released the State of Maryland Information Technology Security Manual. The manual currently serves as the primary policy for establishing and defining the State's IT security practices and requirements; all State agencies are required to adhere to the manual.

Audits of State Agency Cybersecurity Discover PII Vulnerabilities

Over the 2019 interim, the Office of Legislative Audits (OLA) summarized its recent audit findings related to cybersecurity and PII and reported those findings to the Joint Audit and Evaluation Committee in December 2019. OLA found that, from July 2013 through December 2019, approximately 37.9 million PII records existed in State and local government agencies that were not adequately protected with data security controls. Over that same period, 77 of OLA's audits contained findings related to PII.

OLA also emphasized the financial cost associated with data breaches by citing the Ponemon Institute, an independent research organization focused on data protection, and IBM, one of the largest computer manufacturers in the world. The two organizations annually publish a report on global data breaches and their economic impacts. The 2019 Cost of a Data Breach Report found:

- during an average data breach, 25,575 records are accessed;
- the average total cost of a data breach is $8.2 million; and
- the average cost per lost record is $242.

These costs include detection of the breach, escalation, notifications, response, and lost business.

Cybersecurity Legislation in Other States

The National Conference of State Legislatures advises that 43 states and Puerto Rico introduced or considered about 300 bills or resolutions that dealt significantly with cybersecurity in 2019. Some of the key cybersecurity issues considered included:

- appropriating funds for improved security in government;
- addressing cybersecurity threats to elections;
- requiring government agencies to implement training and security policies and practices;
- creating cybersecurity task forces, commissions, or studies;
- targeting cyber threats such as ransomware or other computer crimes;
- addressing cybersecurity within the insurance industry or cybersecurity insurance for government;
- providing for the confidentiality of government cybersecurity information and plans by exempting it from public records laws;
- encouraging cybersecurity training, education, and workforce development;

- studying the use of blockchain for cybersecurity;
- requiring the private sector to improve security practices; and
- addressing the security of connected devices.

Moreover, 31 states adopted or enacted significant cybersecurity-related legislation in 2019. Most notably, (1) New York City enacted the Stop Hacks and Improve Electronic Data Security Act, which amended the state's data breach notification law and imposed more expansive data security requirements on companies; (2) Alabama, Delaware, Mississippi, and New Hampshire passed legislation establishing a comprehensive security framework that insurance companies must implement; and (3) Oregon enacted legislation requiring manufacturers of "connected devices" to equip those devices with reasonable security features.