HOUSE BILL 996

P1 0lr1211

By: **Delegate Lisanti**
Introduced and read first time: February 5, 2020
Assigned to: Health and Government Operations

A BILL ENTITLED

AN ACT concerning

Department of Information Technology – Cybersecurity Response Team

FOR the purpose of requiring the Department of Information Technology, in consultation with the Maryland Cybersecurity Council, to establish a Cybersecurity Response Team; setting forth the duties of the Cybersecurity Response Team; requiring the Department to report annually to certain persons on the activities of the Cybersecurity Response Team; altering the purposes of the 9–1–1 Trust Fund; requiring the Comptroller to disperse certain funds from the 9–1–1 Trust Fund to certain local jurisdictions for a certain purpose; and generally relating to the Cybersecurity Response Team in the Department of Information Technology.

BY repealing and reenacting, with amendments,
Article – Public Safety
Section 1–308(b)(2)
Annotated Code of Maryland
(2018 Replacement Volume and 2019 Supplement)

BY adding to
Article – Public Safety
Section 1–309(b)(5)
Annotated Code of Maryland
(2018 Replacement Volume and 2019 Supplement)

BY adding to
Article – State Finance and Procurement
Section 3A–315
Annotated Code of Maryland
(2015 Replacement Volume and 2019 Supplement)

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

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

Article – Public Safety

1–308.

(b) (2) Subject to paragraph (3) of this subsection and beginning January 1, 2020, in addition to the purposes described under paragraph (1) of this subsection, the purposes of the 9–1–1 Trust Fund include:

(i) funding the operation and maintenance of 9–1–1 systems, enhanced 9–1–1 systems, and Next Generation 9–1–1 services, including:

1. equipment and software utilized directly for providing 9–1–1 services by a public safety answering point;

2. protocol systems and software utilized directly for providing 9–1–1 services by a public safety answering point;

3. interpretation services provided for a public safety answering point;

4. services provided for a public safety answering point to ensure improved access to individuals with disabilities and other individuals who use assistive technology; and

5. voice, data, and call log recorders utilized to capture information from 9–1–1 systems, enhanced 9–1–1 systems, and Next Generation 9–1–1 services;

(ii) funding the operation and maintenance of 9–1–1 systems, enhanced 9–1–1 systems, and Next Generation 9–1–1 services connectivity and infrastructure equipment, including:

1. automatic number and location identification; and

2. Primary Rate Interface and Session Initiation Protocol trunking for 10–digit emergency and nonemergency lines;

(iii) funding geographical information systems hardware, software, data development, and data management costs incurred for the effective operation of 9–1–1 systems, enhanced 9–1–1 systems, and Next Generation 9–1–1 services, including:

1. mapping equipment;

2. interfaces to computer–aided dispatch; and

3. geographical information systems base layer development

and management;

(iv) funding public safety answering point facilities costs, including access control, security systems, and standby power;

(v) funding costs for public education materials;

(vi) funding the training of county personnel working in or directly supporting a public safety answering point;

(vii) funding the provision of tuition reimbursement for 9–1–1 specialists for educational programs related to the 9–1–1 specialist career field; **[**and**]**

(viii) funding costs to maintain the cybersecurity of 9–1–1 systems, enhanced 9–1–1 systems, and Next Generation 9–1–1 services**; AND**

(IX) FUNDING THE DEVELOPMENT OF CYBERSECURITY EMERGENCY RESPONSE STRATEGIES BY LOCAL JURISDICTIONS IN ACCORDANCE WITH § 3A–315 OF THE STATE FINANCE AND PROCUREMENT ARTICLE.

1–309.

(b) **(5) NOTWITHSTANDING ANY OTHER LAW, THE COMPTROLLER SHALL DISPERSE FUNDS FROM THE 9–1–1 TRUST FUND TO LOCAL JURISDICTIONS FOR THE DEVELOPMENT OF EMERGENCY RESPONSE STRATEGIES UNDER § 3A–315 OF THE STATE FINANCE AND PROCUREMENT ARTICLE.**

Article – State Finance and Procurement

3A–315.

(A) THE DEPARTMENT, IN CONSULTATION WITH THE MARYLAND CYBERSECURITY COUNCIL, SHALL ESTABLISH A CYBERSECURITY RESPONSE TEAM.

(B) THE CYBERSECURITY RESPONSE TEAM SHALL WORK WITH LOCAL JURISDICTIONS TO ENSURE THAT:

(1) BY DECEMBER 31, 2021, EACH LOCAL JURISDICTION HAS AN EMERGENCY RESPONSE STRATEGY TO PROTECT VITAL TECHNOLOGY INFRASTRUCTURE AGAINST CYBERSECURITY ATTACKS OR OTHER CYBERSECURITY INCIDENTS; AND

(2) EACH LOCAL JURISDICTION DEVELOPS AND ENTERS INTO MUTUAL AID AGREEMENTS FOR RECIPROCAL EMERGENCY AID AND ASSISTANCE IN

THE EVENT OF A CYBERSECURITY ATTACK OR OTHER CYBERSECURITY INCIDENT.

(C) ON OR BEFORE JANUARY 1 EACH YEAR, THE DEPARTMENT SHALL REPORT TO THE GOVERNOR AND, IN ACCORDANCE WITH § 2–1257 OF THE STATE GOVERNMENT ARTICLE, THE GENERAL ASSEMBLY ON THE ACTIVITIES OF THE CYBERSECURITY RESPONSE TEAM.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect October 1, 2020.