

BRIAN E. FROSH
Attorney General



ELIZABETH F. HARRIS
Chief Deputy Attorney General

CAROLYN QUATTROCKI
Deputy Attorney General

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL

FACSIMILE NO.

WRITER'S DIRECT DIAL NO.

410-576-6584

February 2, 2021

TO: The Honorable Shane E. Pendergrass
Chairwoman, Health and Government Operations Committee

FROM: The Office of the Attorney General

RE: Letter of Information for HB 38 – State Government – Department of
Information Technology – Cybersecurity

The Maryland Cybersecurity Council was established July 1, 2015, through Senate Bill 542.¹ Senate Bill 542 set-forth the membership of the Council, including that the Council be chaired by the Attorney General. The membership was revised by Senate Bill 281, effective October 1, 2018. Pursuant to SB 542, the council must work with the National Institute of Standards and Technology, and other federal agencies, private sector businesses, and private cybersecurity experts to improve cybersecurity in Maryland. Beginning July 1, 2017, the council must submit a report of its activities every two years thereafter.

In its Biennial Activities Report², published July 1, 2019, the Council recommended the following:

2019 Recommendation 2. North Dakota Senate Bill 2110 should be considered in conjunction with all interested stakeholders to understand to what extent it could serve as a model for Maryland by enlarging DoIT's role with respect to the other branches of State government as well as local governments and the public university system.

HB 38 implements this recommendation by incorporating key provisions of North Dakota Bill 2110³. Specifically, HB 38:

¹ Md. Ann. Code, St. Gov't Art. §9-2901

² Maryland Cybersecurity Council Activities Report (2017 – 2019), p 26, at <https://www.umgc.edu/documents/upload/maryland-cybersecurity-council-activities-report-2017-2019.pdf>

³ North Dakota Century Code, § 54-59-01 and § 54-59-05 at <https://www.legis.nd.gov/assembly/66-2019/documents/19-8091-04000.pdf>

1. Borrows key definitions from the North Dakota bill:⁴

"Cybersecurity" means processes or capabilities, wherein, systems, communications, and information are protected and defended against damage, unauthorized use or modification, and exploitation.

"Cybersecurity strategy" means a vision, plan of action, or guiding principles.

2. Invests in DoIT key responsibilities described in the North Dakota bill:⁵

Shall advise and oversee cybersecurity strategy for all executive branch state agencies, including institutions under the control of the state board of higher education, counties, cities, school districts, or other political subdivisions. For purposes of this subsection, the department shall consult with the attorney general on cybersecurity strategy.

Shall advise and consult with the legislative and judicial branches regarding cybersecurity strategy

We hope that this background helps inform your consideration of HB 38.

Thank you.

cc: Health and Government Operations Committee

⁴ *Id.*, § 54-59-01, Definitions 2 and 3

⁵ *Id.*, § 54-59-05, Section 2