STATEMENT TO

SENATE COMMITTEE SUBSTITUTE FOR
SENATE, No. 647

with Senate Floor Amendments
(Proposed by Senator GREENSTEIN)

ADOPTED: JUNE 15, 2020

These Senate floor amendments would:

(1) require each water purveyor in the State to obtain a cybersecurity insurance policy, and define the term "cybersecurity insurance policy";

(2) require a water purveyor to identify in its cybersecurity program the individual chiefly responsible for ensuring that the water purveyor's cybersecurity policies, plans, processes, and procedures are executed in a timely manner;

(3) require a water purveyor to submit a copy of its cybersecurity program to the Board of Public Utilities (BPU) and the Department of Environmental Protection (DEP), in addition to the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC);

(4) require a water purveyor to submit a copy of any revised cybersecurity program to the BPU, the DEP, and the NJCCIC;

(5) require a water purveyor to submit a copy of the cybersecurity certification required pursuant to subsection c. of section 3 of the bill to the BPU, in addition to the DEP and the NJCCIC;

(6) require that a water purveyor's cybersecurity certification be signed by the responsible corporate officer of the public water system, if privately held, executive director, if an authority, or mayor or chief executive officer of the municipality, if municipally owned;

(7) provide that the NJCCIC will audit, for compliance with the cybersecurity provisions of the "Water Quality Accountability Act (WQAA)," P.L.2017, c.133 (C.58:31-1 et seq.), any public water system that fails to submit its cybersecurity program, any updates to the program, or its cybersecurity certification;

(8) provide that a water purveyor must report certain cybersecurity incidents to the BPU, the DEP, and the NJCCIC immediately after an employee is made aware of the cybersecurity incident;

(9) require the NJCCIC, no later than 30 days after receiving a report of a cybersecurity incident from a water purveyor under the bill, to audit the water purveyor's cybersecurity program and any actions the water purveyor took in response to the cybersecurity incident;

(10) require the DEP to audit any public water system that fails to submit the certification required under section 6 of the WQAA in a timely manner;

(11) provide that, if the DEP finds that a water purveyor has made a false or misleading statement in a certification submitted pursuant to the "Water Quality Accountability Act" or this bill, the DEP shall

forward the matter to the Attorney General for further investigation and, if appropriate, criminal prosecution or other relief;

(12) provide that the DEP shall annually audit for compliance with the requirements of the "Water Quality Accountability Act" a random selection of at least 10 percent of all public water systems in the State;

(13) provide that a cybersecurity program would not be considered a government record pursuant to P.L.1963, c.73 (C.47:1A-1 et seq.) and would not be available for public inspection; and

(14) make technical corrections to the bill.