MEMO OF SUPPORT

S1961 (Gonzalez) / A5739 (Solages)

Secure Our Data Act

April 4, 2025

TITLE OF BILL
Secure Our Data Act.

STATEMENT OF SUPPORT
Our groups strongly support this bill because it will protect sensitive state data.

As hackers become more sophisticated, state information systems have been subject to a number of security breaches, including:

- April 2024: The State Legislature's bill drafting system was hacked, leading to state employees' credit card and social security numbers being accessed.
- June 2021: Hackers associated with China breached the MTA's computer systems.
- January 2020: Hacker infiltrated New York State's computer network, leading to an FBI investigation.

The State Comptroller has also detailed how New York ranks third for ransomware attacks nationwide, and agencies with sensitive personal information, such as healthcare and financial services, are among the most vulnerable.

Since future attacks are inevitable, the state must do everything it can to ensure sensitive personal data is secure. By requiring state agencies to develop plans for preventing cyberattacks and rigorously testing state systems, this legislation will help keep New Yorkers' personal information safe.

We urge the Legislature to pass the bill, and the Governor to sign it.

SUMMARY OF PROVISIONS
Section 1 states the bill's title.

Section 2 states the legislative intent, which is that cyberattacks and breaches on state data have exposed sensitive personal information, and that the state must act to ensure that this data is protected in the future.

Section 3 adds a new §210 to State Technology Law providing definitions in subdivision 1 for "breach of the security of the system," "data subject," "data violation," "immutable," "mission critical," "segmented storage," "state entity-maintained personal information," and "state entity."

Subdivision 2 provides that within one year of the bill's effective date, the director of the Office of Information Technology Services (ITS) shall promulgate regulations designing and developing standards for:

- Protection of personal data and critical information systems against breaches
- Data backup, including:
    - Immutable backups of personal data
    - Exclusion of unwanted data (such as malware) from immutable backups, except for stress testing
    - Storage of immutable backups in segmented storage
- Recovery of data
- Data retention and deletion policies
- Annual workforce training for protecting data and what to do in case of a breach.

Subdivision 3 provides that from January 1st, 2026 and annually thereafter, each state entity shall perform at least one vulnerability test of a mission critical system per year. From December 1st of that year, each state entity's entire system shall undergo vulnerability testing. A report on the findings shall be submitted to ITS no later than 45 days after the test is complete.

Subdivision 4 requires that within one year of the bill's effective date, each state entity inventory its data to develop a list of information systems. The list will provide the purpose of each information system, and mark which are mission critical, use personal information, and are backed up in segmented storage. If an inventory has already been completed, the entity shall update that inventory. This information shall not be made available via Freedom of Information Law (FOIL) requests unless in response to a subpoena or other court order.

Subdivision 5 that within 18 months of the bill's effective date, each state entity must create an incident response plan to deal with breaches that includes procedures for protecting personal information and mission critical systems. Beginning January 1, 2028, each state entity shall annually conduct a simulation of its response plan.

Section 4 is a severability clause.

Section 2 states that the bill takes effect immediately.