AMPLIFY Act: Resident Security Protocols and Interoperability

Legislating Drafter Working Package — 33-bill modular AMPLIFY build

Legislating drafter file. This chapter draft is designed to stand on its own and to support modular insertion into broader AMPLIFY stacks.

Bill 8. AMPLIFY Act: Resident Security Protocols and Interoperability

Single subject. Resident-side security protocols, operator honor duties, and system interoperability.

Purpose. Replace vague black-box concepts with functional, defensible security protocol language.

Draft structure

Section	Core draft direction
1. Short title	This act shall be known and may be cited as the "AMPLIFY Act: Resident Security Protocols and Interoperability".
2. Legislative declaration	The general assembly finds and declares that replace vague black-box concepts with functional, defensible security protocol language.
3. Definitions	Definitions should be alphabetized, lowercase, and drafted in singular form unless a term of art requires otherwise.
4. Operative sections	Substantive rights, duties, approvals, or restrictions listed below.
5. Administration	Rulemaking, designation of administering authority, records, notices, and implementation mechanics.
6. Construction	Independent operation, severability, no implied repeal, and other necessary construction clauses.
7. Effective date	Effective date and any conditional clause required by filing strategy.

Draft definitions

resident security protocol. a software, hardware, network, managed-service, or hybrid protective layer approved by rule.

interoperability. the ability of authorized systems to exchange recognized verification, routing, or audit information in a compatible manner.

qualified interface. an interface, api, credential layer, or gateway recognized by rule.

Draft operative provisions

Section 4. Resident rights
- A resident may deploy or use a qualified resident security protocol to authenticate, route, inspect, restrict, revoke, or log covered interactions.
- A covered operator shall not intentionally defeat a qualified interface or recognized verification signal without lawful justification.

Section 5. Functional compliance
- A resident security protocol may be satisfied through existing commercially available firewall, router, credential, filtering, managed-service, vpn, api, or equivalent technologies recognized by rule.
- Nothing in this act mandates universal distribution of a single physical device.

Section 6. Interoperability standards

- The administering authority may approve interoperable protocol classes and data-exchange standards by rule.

Required construction clauses

- Independent operation. This act operates independently and remains effective whether or not any related measure or companion act is adopted.
- Severability. If any provision of this act or its application is held invalid, the invalidity does not affect other provisions or applications that can be given effect without the invalid provision or application.
- Single-subject construction. This act shall be construed to embrace only the single subject described in its title and no separate subject shall be inferred from a remedy, definition, recordkeeping duty, funding mechanism, or construction clause that is necessarily and properly connected to that subject.