OVERVIEW OF STATE CYBERSECURITY LAWS & LEGISLATION

PAM GREENBERG, NCSL | NASS 2019 SUMMER CONFERENCE | JULY 2019
Serves 7,383 legislators and 25,000 legislative staff.

Provides nonpartisan research and analysis

Links legislators with each other and with experts

Speaks on behalf of state legislatures in D.C.
Mission:

- Educate and engage task force members in cybersecurity policy discussions.
- Extend networking opportunities among legislative leaders on cybersecurity issues.
- Engage with strategic partners and extend networks to develop and maintain security programs.
- Provide well-defined programs on key and critical cyber policy issues.
Cybersecurity Laws & 2019 Legislation/Trends

- Private sector
- Government

Public Records Laws & Cybersecurity

- Current laws
- 2019 legislation/trends
Cybersecurity: Defending against attacks to various networks, computers and data.

Data security: Protecting information from unauthorized access.

Privacy: Controlling who has access to personal information.
State Cybersecurity Laws & Legislation

Cybersecurity/Data Security Laws

Private sector
- Breach notification laws = 50 states
- Data security laws = 25 states
Government

Data security laws = 29 states

- Statewide authority, oversight
- “Reasonable security” practices
- Specific security requirements
Data Disposal Laws

- For private sector = 34 states
- For government = 14 states
Key cybersecurity enactments—Private sector:

- Connected devices/IoT (OR, WA)
- Insurance (AL, CT, KS, MS)
- Security practices/requirements (Ø)
Top 3 cybersecurity enactments—Government:
- Security requirements for government
- Elections security
- Public records exemptions for cybersecurity
Cybersecurity enactments—
Government:

- Centralizing cybersecurity authority (ND, NV, VT, WV)
- Security requirements (NV, OK, WV)
- Emergency preparedness (MT, NV)
- Req. govt. employee training (TX)
- Explore blockchain for security (FL)
Cybersecurity enactments—Elections:

- Security practices (IA, IN, NV, OK, TX, VA)
State Laws: Confidentiality of Cybersecurity Information

- *Expressly* refer to cyber threats, cybersecurity systems = 23 states
- Refers only to systems or technology in the context of anti-terrorism or homeland security threats = 5 states
- Refers to “security systems,” plans, etc., *without* specific reference to information systems or technology = 5 states
Public Records & Cybersecurity 2019 Enactments

- Exemption of cybersecurity information from disclosure (IN, MS, ND, NV, WV)
STATE LEGISLATIVE UPDATE
TRENDS IN CYBERSECURITY LEGISLATION 2018

NCSL Web Resources: www.ncsl.org
- Security Breach Laws and Legislation
- Cybersecurity Legislation 2016-2018
- Data Security Laws – Private Sector
- Data Security Laws – Government
- Data Disposal Statutes
- Computer Crime Statutes
- Election Security: State Policies

Questions?

Additional Information
Pam Greenberg, NCSL Denver Office
pam.greenberg@ncsl.org