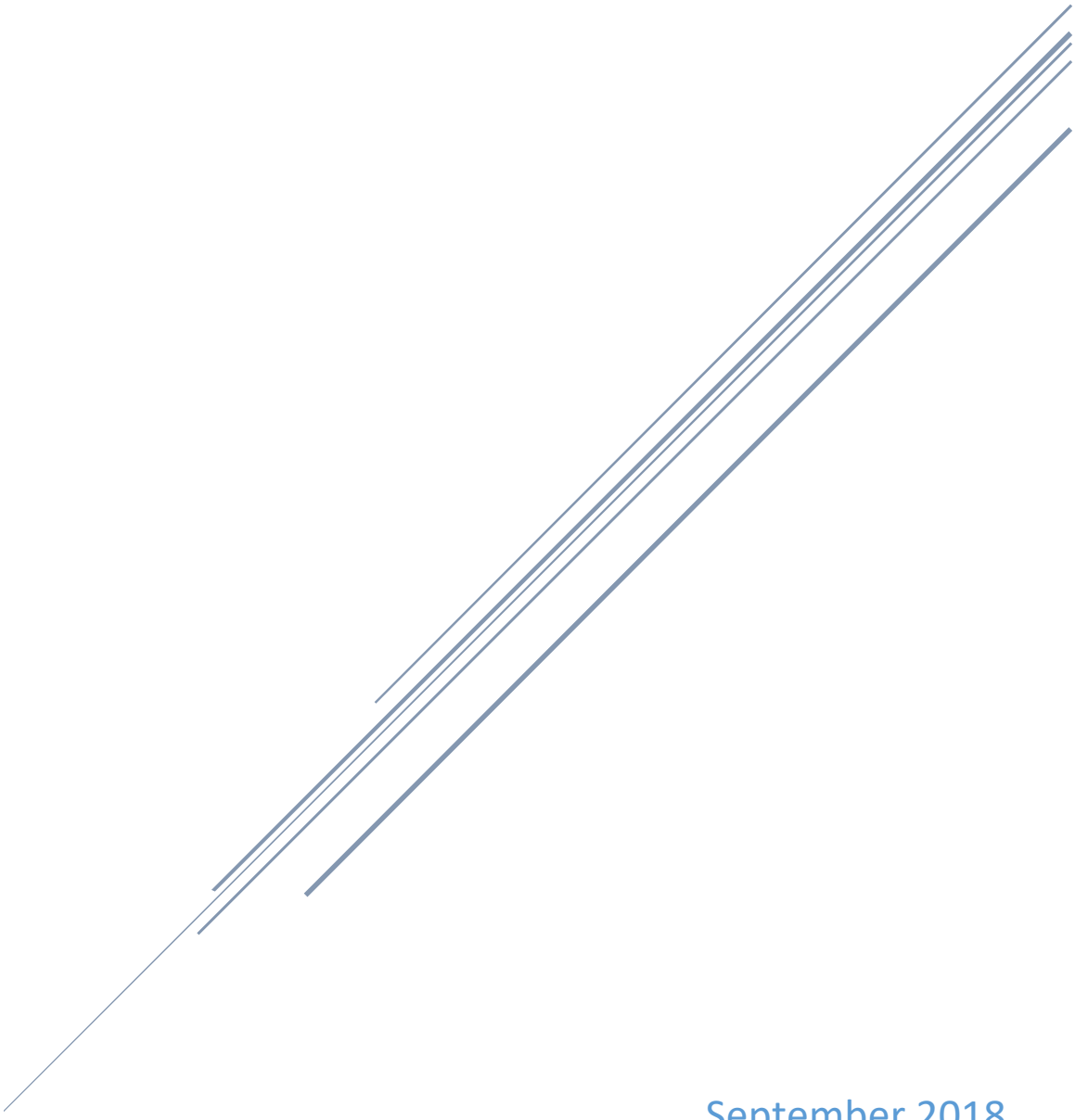
LEGAL AND INSURANCE WORKING GROUP STRATEGIC PLAN

Chair: Curtis Hill | Co-Chair: Stephen Reynolds



September 2018
Indiana Executive Council on Cybersecurity

Legal and Insurance Working Group Plan

Contents

Committee Members

Committee Members

Name	Organization	Working Group Position	IECC Membership Type
Curtis Hill	Indiana Attorney General	Chair	Voting
Stephen Reynolds	Ice Miller	Co-Chair	Advisory
Douglas Swetnam	Indiana Attorney General	Chair Proxy	Voting Proxy
Jan Campbell	Leeuw Oberlies & Campbell, P.C.	Full Time	Advisory
Jim Ehrenberg	Indiana Office of Technology	Full Time	Advisory
George Lyle	Purdue University	As Needed	Advisory
Frank Nevers	Eskenazi Health	As Needed	Advisory
William Russell	Cummins, Inc	Full Time	Advisory
Mark Swearingen	Hall, Render, Killian, Heath & Lyman, P.C.	Full Time	Advisory
Amy Beard	Indiana Department of Insurance	Full Time	Advisory
Adam Krupp	Indiana Department of Revenue	As Needed	Voting
Brian Mcginnis	Barnes & Thornburg	Full Time	Advisory
Scott Miller	Citizens Energy Group	As Needed	Advisory
Leon Ravenna	KAR Auction Services	Full Time	Advisory
Nicholas Reuhs	Ice Miller	Full Time	Advisory
Alejandro Valle	Citizens Energy Group	Full Time	Advisory
Todd Vare	Barnes & Thornburg	Full Time	Advisory
Von Welch	Indiana University	As Needed	Advisory

Introduction

Introduction

With the signing of Executive Order 17-11 by Governor Eric J. Holcomb, the Indiana Executive Council on Cybersecurity (IECC) and its mission was continued. With the ever-growing threat of cyberattacks, the IECC has been tasked with developing and maintaining a strategic framework to establish goals, plans, and best practices for cybersecurity to protect Indiana's critical infrastructure. The IECC is comprised of twenty committees and working groups who worked together to develop a comprehensive strategic plan and implementation plans. This implementation plan is one of the twenty specific plans that make up the complete 2018 Indiana Cybersecurity Strategic Plan.

Executive Summary

Executive Summary

- **Research Conducted**
  - General Liability insurance exclusions
  - Cybersecurity-related insurance products
  - National Association of Insurance Commissioners Standards
  - OHIO Safe Harbor Bill
  - New Jersey Cybersecurity Bill
  - New York (NY) Financial Services
  - New York Shield law
  - United Kingdom (UK) Cybersecurity Policy
  - Wisconsin (WI) Broadband Bill
  - Indiana Office of Technology (IOT) Consumer TIPS ACT of 2017
  - Washington (WA) Biometric Bill
  - Small Business Cybersecurity Act 2017
  - New York Shield Law & NY Financial Services
  - Virginia HB 679 personal information
  - Verizon 2017 Data Breach report
  - Washington (HB 1493)
  - Cybersecurity insurance presentation by CHUBB
  - Cybersecurity insurance presentation by Travelers
  - Cybersecurity insurance presentation by Evolve MGA
  - State UDAP statutes, state Personal Information Protection Acts, state Data Breach of Security Acts for all 50 states plus District of Columbia
  - Federal statutes
  - General Data Protection Regulation (GDPR)

- **Research Findings**
  - Cybersecurity incidents are generally excluded from General Liability coverage.
  - A variety of companies are currently competing to serve the burgeoning market for insurance products covering cybersecurity-related services and risks.
  - There is no consistency between the cybersecurity policies currently offered in the marketplace.
  - There are approximately 12 different types of cybersecurity-related coverages.
  - There is no central collection of applicable state, federal and international laws with which Indiana businesses and local governments comply.

- **Working Group Deliverables**
  - Insurance Guide defining the different types of service and coverage
  - Relevant statutes and regulations
  - Cyber Insurance Survey

Additional Notes
  - None at this time.

Research

Research

1. **What has your area done in the last five years to educate, train, and prepare for cybersecurity?**
    a. **Department of Revenue (DOR)**
        i. Provided security awareness training to all full-time employees (FTEs), contractors, temps, and vendors at on-boarding and annually thereafter. This training apprises employees of the data they must protect, and the methods by which they must be protected.
        ii. Led a Continuity of Operations plan exercise in 2014—next one projected for 2018
        iii. Trained and exercised the DOR Incident Response team and plan annually
        iv. Sent periodic e-mails and published articles in agency publications apprising all DOR employees of security issues and best security practices
        v. Sent e-mails to all DOR employees apprising them of urgent real-world security issues, and how to address them (e.g., phishing messages and phone-based social engineering attacks)
    b. **Cummins**
        i. Cummins has undertaken a multi-year effort to raise the level of cybersecurity preparedness within the company. Among the investments is a 300% increase in the number of employees working on cybersecurity and a commensurate increase in budget. We have adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework on which to base our cybersecurity programs. We have initiated an employee awareness program with regular communications and annual events during Cybersecurity Awareness Month (October). We have partnered with Ivy Tech to provide cybersecurity students hands-on experience within Cummins cybersecurity operations center in conjunction with their classroom studies in cybersecurity. This has resulted in several hires of local students upon graduation and the program now includes students from Franklin University and IUPUI/IUPUC.
    c. **Gregory Appel**
        i. Law firms, insurance brokers, and insurance carriers semi-frequently hold client (public) educational sessions geared toward clients/insureds to better grasp the exposure, threat, responsibility, and legal/insurance protection for privacy and network security liability. These sessions are generally offered from a knowledge leadership perspective, but because of their nature can be geared to an entry level of understanding of cyber liability concerns. Certain industries, such as healthcare, have moved beyond a 101 level of education/training because of their risk and regulatory environment. Many risk-oriented firms offer tabletop breach exercise simulations to test and evaluate a client/insured's incident response program's communication effectiveness.

d. **Indiana Office of Technology (IOT)**
    i. The Indiana Office of Technology instituted a computer-based cybersecurity training program that is intended to make State employees aware of common types of cyber threats and the value of basic cyber hygiene. The name of the product that was used in 2017 is Security Mentor. We also instituted a phishing simulation. Essentially, we sent spam emails to state employees with links in them. Employees who clicked on the links where directed to a webpage which explained that they had been phished and that they would be enrolled in a phishing prevention training program.

2. What (or who) are the most significant cyber vulnerabilities in your area?

a. **DOR**
    i. External threats (State and non-state cyber actors, cybercriminals, cyberterrorists, etc.)
    ii. Malicious insiders
    iii. Employees who fall for social engineering schemes
    iv. Servers containing sensitive data that reside outside of the state's protected zone (PZ)

b. **Gregory Appel**
    i. Insurance industry statistics point to healthcare, financial and retail sectors as having the most severity. While main street, mom n' pop, and small business account for the frequency comprising approximately two-third of breaches.

c. **Cummins**
    i. Skill gaps for employees in general related to cybersecurity and safe use of computing and network resources. In addition, as a manufacturing company, we rely on a number of legacy systems in our manufacturing processes which are difficult to patch and maintain, retiring these systems is a priority.

d. **IOT**
    i. There are approximately 40K state employees. There are multiple layers to our cybersecurity safeguards. That said, in theory, a malicious actor could gain access to our systems if just one of those 40K employees makes a mistake. Another challenge that we have is keeping up with software updates and patches.

3. What is your area's greatest cybersecurity need and/or gap?

a. **DOR**
    i. Funding and manpower to support security assessments and implementation of security enhancements

b. **Gregory Appel**
    i. Understanding of their legal and regulatory responsibilities for privacy and network security liability and how to best structure an insurance program to work with and support a meaningful incident response plan (IRP).

c. **Cummins**
    i. Our greatest challenges are in synchronization of global operations in a complex regulatory environment. Differing requirements and technology limitations make the operation of a global cybersecurity infrastructure very complex and difficult.
d. **IOT**
    i. Our biggest need is in manpower. There are just 11 employees on the IOT Security Team.

4. **What federal, state, or local cyber regulations is your area beholden to currently**?
    a. **DOR**
        i. Internal Revenue Service (IRS) Publication 1075
        ii. NIST Special Publication 800-53: Using Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) for detailed security assessments
        iii. Indiana Code and policies
        iv. IOT policies and standards
        v. DOR policies and procedures
    b. **Cummins**
        i. Sarbanes Oxley, Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), Defense Federal Acquisition Regulation Supplement (DFARS), China Cybersecurity Law, Data residency rules in India and European Union, GDPR.
        ii. US China Commission studies on cyber capabilities of the Peoples Liberation Army.
    c. **Gregory Appel**
        i. All of them. With approximately 48 different State Breach Statutes and a potential myriad of Federal and International regulatory frameworks, educating a client on how to navigate them from a legal or insurance perspective is at best challenging.
    d. **IOT**
        i. We maintain various types of confidential information for state agencies; including personal health information, personally identifiable information, data from the Social Security Administration, federal tax information, etc. We are required to abide by HIPAA, IRS Publication 1075, and other state and federal laws calling for the protection of such information.

5. **What case studies and or programs are out there that this Council can learn from as we proceed with the Planning Phase?**
    a. **IOT**
        i. The Information Security Research and Education (INSuRE) program researches and seeks solutions to hard security problems. INSuRE members are the US Intelligence Community, US National Laboratories, US universities and colleges which include Purdue, and State government organizations such as IOT.

b. **Gregory & Appel**
    i. Most Insurance carriers offering cyber liability (and technology errors & omissions) have pre-packaged claim scenarios, actual paid claim losses with detail scrubbed of the names of the innocent. Indiana Security & Privacy Network (INSPN) for example regularly highlights recent breaches during its quarterly update.

6. What research is out there to validate your group's preliminary deliverables? This could be surveys, whitepapers, articles, books, etc. Please collect and document.
    i. [No response]

7. What are other people in your sector in other states doing to educate, train, prepare, etc. in cybersecurity?
a. All other state departments of revenue/taxation that receive Federal Tax Information (FTI) are required by IRS to provide:
    i. Security awareness training for all employees
    ii. Role-based training to personnel based on assigned security roles and responsibilities
    iii. Contingency training for personnel responsible for recovering backup copies of FTI
    iv. Incident response training to personnel responsible for handling and reporting security events.
b. Other Attorney General offices enforce their state data privacy, security, and data breach laws.

8. What does success look like for your area in one year, three years, and five years?
a. **DOR**
    i. Year 1
        1. Conduct security assessments
        2. Implement security controls, address severe and significant vulnerabilities and threats
    i. Year 3
        1. DOR, its vendors, partners, and e-filing tax community comply with DOR security requirements
        2. Work towards the following goals
            a. All sensitive DOR servers reside in the state's PZ
            b. DOR servers reside within appropriate network segments
            c. All sensitive DOR data within the state network is encrypted at rest and in motion
            d. DOR users have least privileged access
            e. Security patching is done immediately
            f. Continuity of Operations (COOP) and Disaster Recovery (DR) plans are developed, appropriately resourced, and successfully tested
    i. Year 5: Achieve the following goals
        1. All sensitive DOR servers reside in the state's PZ

2. DOR servers reside within appropriate network segment
3. All sensitive DOR data within the state network is encrypted at rest and in motion
4. DOR users have least privileged access
5. Security patching is done immediately
6. COOP and DR plans are developed, appropriately resourced, and successfully tested

b. **Cummins**
   i. A modernized IT infrastructure, operated and maintained by a trained IT and cybersecurity workforce that is able to quickly detect and respond to malicious activity to maintain business operations.

c. **IOT**
   i. In the short term, we would like to develop a formal cybersecurity incident response plan that will allow us to respond to incidents timely, effectively, and appropriately. In the long run, we would generally like to increase our cybersecurity protections and preparedness.

d. **Gregory & Appel**
   i. A public better informed about their responsibilities in a breach and what or how a cyber liability product can risk transfer the monetary cost of implementing an IRP. More insureds purchase cyber today than three years ago and more will purchase it three years from now than purchase today and at higher limits. It very much should become a part of most Commercial Insured Risk Transfer/Insurance program.

9. What is the education, public awareness, and training needed to increase the State's and your area's cybersecurity?

a. **DOR**
   i. The public should be apprised that DOR continuously implements tools and processes to bolster cybersecurity to protect their information, which may appear inconvenient to them. For example, we may require taxpayers logging into our applications to increase the length and complexity of their passwords.

b. **Cummins**
   i. Better user training beginning in K-12 so we have a well-informed workforce able to safely operate their IT resources.

c. **Gregory & Appel**
   i. There should be more industry-focused cyber liability workshops or tabletop breach exercises geared towards educating a particular industry group about their key exposures, the cost, and how to think about cyber insurance effectively.

10. What is the total workforce in your area in Indiana? How much of that workforce is cybersecurity related? How much of that cybersecurity-related workforce is not met?

a. **DOR**
   i. Total DOR Workforce as of December 2017: 751. 659 FTEs and 92 contractors.
   ii. Total DOR Cybersecurity Staff: 6

iii. Total DOR Cybersecurity Staff shortfall: 0

b. **Cummins**
   i. We have approximately 1000 total IT employees within Cummins. Cybersecurity is currently at 45 employees and we have 2-4 vacancies at any given time.

c. **Gregory & Appel**
   i. Most of the insurance carrier resources dedicated to cyber liability reside outside of Indiana with Chicago comprising the most concentrated hub of underwriting talent. Many larger insurance brokers purport to have experienced cyber brokers on staff or available (any licensed insurance agent can sell a cyber policy, but not all of them are comfortable with the nuances). Most law firms in the city have a cyber practice.

d. **IOT**
   i. There are approximately 40K state employees. There are approximately 440 IOT employees and contractors. The IOT Security Team has 11 employees. Other agencies have security personnel as well. However, their focus is not entirely on security.

11. What do we need to do to attract cyber companies to Indiana?

a. There is already some very good IT security and forensics firms such as Pondurance and Rook located in Indiana.
b. Attracting cyber talent is what is needed.

12. What are your communication protocols in a cyber emergency?

a. **DOR**
   i. DOR employee, IOT, or anyone else identifies and reports suspicious activities to DOR Security Team
   ii. DOR Security Team assesses and analyzes the situation, and determines if there is an emergency
   iii. DOR Security Team, upon DOR Chief Information Officer (CIO) approval, takes immediate action as necessary to stop the perpetuation of damage
   iv. DOR Security Team develops multiple courses of action (COA) to address remaining security concerns and to recover from the event, then presents them to other members of the DOR Incident Response Team comprising DOR Chief Operating Officer, DOR Chief Information Officer, DOR Inspector General, DOR Legal Team, DOR Communications Team, and IOT Chief Information Security Officer
   v. DOR Incident Response Team decides on a single course of action
   vi. DOR Incident Response Team briefs DOR Commissioner on the situation, actions taken, and proposed COA
   vii. DOR Commissioner approves COA
   viii. DOR Incident Response Team works with IOT to execute the approved COA

b. **Cummins**
   i. We manage crisis communication centrally with a cross-functional working group made up of decision makers from legal, finance, IT, business

operations, HR and Global Security. Cummins does not publicly discuss details of malicious activity unless required by regulation or law.

c. **IOT**
    i. Notice of a cyber event typically comes to the Security Operations Center. The SOC handles the situation if it is a relatively minor event – e.g., a virus protection situation. If the situation requires a higher level of expertise, such as a spam email with malicious links or attachments to multiple state employees, it is escalated to the IOT Security Team which considers if other teams inside and outside of IOT should be alerted. If the IOT Security Team determines that it cannot contain the event on its own, it contacts the IOT Chief Information Security Officer (CISO) and CIO.

13. What best practices should be used across the sectors in Indiana? Please collect and document.

a. Defense-in-depth: an information assurance concept in which multiple layers of security controls are placed throughout an information technology system
b. Initial and annual security awareness training
c. Phishing testing

Deliverable: Insurance Guide

Deliverable: Insurance Guide

General Information

1. **What is the deliverable?**
    a. Document describing various types of coverages available in existing cybersecurity insurance policies.

2. **What is the status of this deliverable?**
    a. Version 1 Complete 100%

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns.**
   See Executive Order 17-11 for further context.
   ☐ Establish an effective governing structure and strategic direction.
   ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
   ☒ Strengthen best practices to protect information technology infrastructure.
   ☐ Build and maintain robust statewide cyber-incident response capabilities.
   ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
   ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
   ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
   ☐ Research – Surveys, Datasets, Whitepapers, etc.
   ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
   ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
   ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
   ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
   ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. A guide for Indiana residents describing the different types of coverages and services available in “cybersecurity policies”

6. **What metric or measurement will be used to define success?**
    a. Completed documents made publicly available through state websites.

7. **What year will the deliverable be completed?**
    a. Initial version was completed in 2018. Subsequent versions will be released yearly.

8. **Who or what entities will benefit from the deliverable?**
    a. All Indiana businesses.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

---

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Strategic resource and Public Awareness Training

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. We are meeting with the leading cybersecurity insurance companies to gather the different coverages and services offered under a cyber risk policy.

12. **Who should be main lead of this deliverable?**
    Reid Putnam (with assistance from Nick Reuhs and Jan Campbell)

13. **What are the expected challenges to completing this deliverable?**
    a. Cyber risk and liability insurance is a new and fast-changing marketplace, so the information will likely change each year for the next five to ten years.

Implementation Plan

---

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. This will require periodic updates, at least annually.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Meeting and discussion with representatives from leading cybersecurity policy providers	Reid Putnam	100%	Completed May 2018	
Publicize availability of Insurance and resources	Needs to be assigned to communication committee	0%	December 2018	
Conduct survey of businesses for insurance coverage and cybersecurity insurance coverage	Cybersecurity Council (perhaps working with Secretary of State to be done with annual corporate reports)	0%	2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
¼ FTE	¼ FTE	cybersecurity insurance broker	Cybersecurity Council office	Indiana General Assembly appropriation	
¼ FTE	1/16 FTE	Communications	Cybersecurity Council office	Indiana General Assembly	
¼ FTE	¼ FTE	Survey	Cybersecurity Council office	Indiana General Assembly	Secretary of State should be involved

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Website space	Making documents available for review or download	May be within scope of current IN website maintenance	unknown	Cybersecurity Council office	Indiana Legislature	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. By publishing details on types of services and insurance coverages commercially available, Indiana businesses and local governments will increase awareness and understanding of cyber risks and the products available to manage those risks.
b. By increasing the number of businesses protected against cybersecurity loss, Indiana's economy will be more resilient in the face of increasing cyber threats.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. It has been estimated up to 60% of small and medium-sized businesses fail within 6 months of a cybersecurity attack. By encouraging small and medium-sized businesses to protect against cybersecurity risk, Indiana companies and local governments will be better protected.

19. What is the risk or cost of not completing this deliverable?

a. Up to 60% of small and medium-sized businesses fail within 6 months of a cybersecurity attack, and the risk of being targeted by an attack is rising exponentially. Indiana's economy could be damaged as the result of cyber attacks against Indiana businesses and local government.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Completed list of currently available cybersecurity coverages and services.
b. There is no current survey of Indiana businesses on this subject. Cybersecurity council could work with 1) Indiana Chamber of Commerce, or 2) Secretary of State's office to conduct a survey of Indiana businesses, and use the increase of businesses covered by cybersecurity policies as a measure of success.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No
b. **If Yes, please list states/jurisdictions**
    i. Other states or jurisdictions are likely analyzing similar information, but we are not currently aware of concrete examples.
    ii. We are not aware of initiatives in other states.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No
b. **If Yes, please list states/jurisdictions**
    i. We are not aware of similar initiatives in other states, but cybersecurity is a hot topic and there has been a flurry of activity at the state level.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Availability of committee members.
b. Scheduling conflicts among committee members.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. Yes
b. **If Yes, what is the change and what could be the fiscal impact if the change is made?**
    i. Making insurance coverage and specifically cybersecurity insurance coverage part of a corporation's annual or semi-annual filing with Secretary of State would require legislative and administrative change.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. The list of applicable laws will require continual updating.
b. The types of coverages available under cybersecurity insurance policies are changing as cybersecurity risks change and will require continuous updating.
c. Surveys of businesses will require annual surveys or coordination with Indiana Chamber of Commerce or Secretary of State.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Insurance policy coverages:
    i. American International Group (AIG)
    ii. Chubb
    iii. Travelers Insurance
    iv. CNA insurance

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All sectors

Communications

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All stakeholders would benefit from this information.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. Indiana cybersecurity office could coordinate with Chris Profitt, Director of Communications for Office of Indiana Attorney General, and Mary Allen, Director of Outreach for Office of Indiana Attorney General.
b. Indiana Chamber of Commerce could help promote.

Evaluation Methodology

Objective 1: IECC Legal and Insurance Working Group develop a Cyber Insurance Guide to be provided to government and businesses by September 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Policy Review

Deliverable: Policy Review

General Information

1. **What is the deliverable?**
    a. List of cybersecurity laws and regulations for Indiana businesses and residents

2. **What is the status of this deliverable?**
    a. Version 1 is 100% complete.

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☒ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☐ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☐ Research – Surveys, Datasets, Whitepapers, etc.
    ☒ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. Companies, local governments and individuals will be better able to comply with relevant laws.

6. **What metric or measurement will be used to define success?**
    a. A completed document that captures all current, applicable laws.

7. **What year will the deliverable be completed?**
    a. Initial version was completed in 2018. Subsequent versions will be released as needed.

8. **Who or what entities will benefit from the deliverable?**
    a. The document will educate Indiana businesses and local government about their responsibilities under existing cyber laws.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. None.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Public Awareness and Training.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Attorney General offices across the United States and data privacy and security attorneys on Legal and Insurance Working Group.

12. **Who should be main lead of this deliverable?**
    a. Doug Swetnam/Stephen Reynolds

13. **What are the expected challenges to completing this deliverable?**
    a. Availability of committee members.
    b. Scheduling committee members.

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Cybersecurity laws are rapidly changing and new lists will need to be compiled at least annually, if not more frequently.

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Review and revise list of laws applicable to Indiana businesses and residents under current landscape	Doug Swetnam/Stephen Reynolds	Version 1 100% complete	August 2018	Federal and State legislation should be monitored for changes in existing laws.

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
¼ FTE	¼ FTE	Legal – legislative – Track legislative updates to cyber laws in all jurisdictions affecting IN	Cybersecurity Council office or Indiana Attorney General	Indiana General Assembly appropriation	
¼ FTE	1/16 FTE	Communications	Cybersecurity Council office	Indiana General Assembly	

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Website space	Making documents available for review or download	May be within scope of current IN website maintenance	unknown	Cybersecurity Council office	Indiana legislature	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. Businesses and local governments will have a legal reference to identify the current patchwork of cybersecurity laws, regulations and requirements.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. It has been estimated up to 60% of small and medium sized businesses fail within 6 months of a cybersecurity attack. By making companies more aware of the legal requirements expected of them, and the potential penalties and liability for non-compliance, they will be better motivated to plan and prepare for a cyber emergency.

19. What is the risk or cost of not completing this deliverable?

a. Up to 60% of small and medium sized businesses fail within 6 months of a cybersecurity attack, and the risk of being targeted by an attack is rising exponentially. Indiana's economy could be damaged as the result of cyber attacks against Indiana businesses who are not prepared to respond to an incident.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. Version 1 Survey of Cybersecurity laws and regulations completed.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No
b. **If Yes, please list states/jurisdictions**
    i. Other states or jurisdictions are likely looking at these statistics, but we are not currently aware of concrete examples.
    ii. We are not aware of initiatives in other states, but there may be.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. Yes
b. **If Yes, please list states/jurisdictions**
    i. There is a possibility other states have comparable initiatives, though we are not aware of any at this time.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. Availability of legal resources to review and verify applicable laws and regulation.
b. With the fast pace of cybersecurity rules and regulations over the past several years it is possible to omit some.

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. The list of applicable laws will require continual updating.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. Applicable laws – Legal and Insurance working group

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All sectors

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All stakeholders would benefit from this information.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. Indiana cybersecurity office could coordinate with Office of Indiana Attorney General communications.

Evaluation Methodology

Objective 1: Legal and Insurance Working Group develop a list of cyber laws applicable to Indiana businesses and residents under the current landscape by August 2018.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Deliverable: Cyber Insurance Survey

Deliverable: Cyber Insurance Survey

General Information

1. **What is the deliverable?**
    a. Survey of Indiana businesses who have cybersecurity insurance coverage.

2. **What is the status of this deliverable?**
    a. Not Started

3. **Which of the following IECC goals does this deliverable meet? Check ONE that most closely aligns. See Executive Order 17-11 for further context.**
    ☐ Establish an effective governing structure and strategic direction.
    ☐ Formalize strategic cybersecurity partnerships across the public and private sectors.
    ☐ Strengthen best practices to protect information technology infrastructure.
    ☐ Build and maintain robust statewide cyber-incident response capabilities.
    ☐ Establish processes, technology, and facilities to improve cybersecurity statewide.
    ☒ Leverage business and economic opportunities related to information, critical infrastructure, and network security.
    ☐ Ensure a robust workforce and talent pipeline in fields involving cybersecurity.

4. **Which of the following categories most closely aligns with this deliverable (check ONE)?**
    ☒ Research – Surveys, Datasets, Whitepapers, etc.
    ☐ Informational Product – Definitions, Glossary, Guidelines, Inventory, Best Practices, etc.
    ☐ Operational Product – Programs, Processes, etc. (generally can be produced within the group or with current resources)
    ☐ Operational Proposal – Programs, Processes, etc. (generally requires additional resources)
    ☐ Templates/Toolkits – Actionable Resource Kits, Turnkey Templates
    ☐ Policy Recommendation – Recommended Changes to Law

Objective Breakout of the Deliverable

5. **What is the resulting action or modified behavior of this deliverable?**
    a. The initial objective is to create a baseline measurement of cybersecurity risk management analyses undertaken by Indiana businesses.

6. **What metric or measurement will be used to define success?**
    a. A steadily increasing number of Indiana businesses who have gone through a process to assess their cybersecurity risks and make an informed business decision as a result of that review. (Whether they choose to insure, or not.)

7. **What year will the deliverable be completed?**
    a. Annually starting 2019

8. **Who or what entities will benefit from the deliverable?**
    a. Individual Indiana businesses will benefit from making informed cyber risk assessments, and the Indiana economy as a whole will benefit by being better prepared for cyber risks.

9. **Which state or federal resources or programs overlap with this deliverable?**
    a. The Indiana Department of Insurance gathers annual information on admitted carriers, but we do not believe any entity is currently conducting the survey we are suggesting.

Additional Questions

10. **What other committees and/or working groups will your team be working with to complete or plan this deliverable?**
    a. Policy working group and possibly Strategic Resources working group.

11. **Which state agencies, federal agencies, associations, private organizations, non-profit organizations, etc. will need to be involved to complete or plan this deliverable?**
    a. Indiana Secretary of State

12. **Who should be main lead of this deliverable?**
    Cybersecurity Council office

13. **What are the expected challenges to completing this deliverable?**
    a. No Response

Implementation Plan

14. **Is this a one-time deliverable or one that will require sustainability?**
    a. Ongoing surveys (annually)

Tactic Timeline

Tactic	Owner	% Complete	Deadline	Notes
Conduct a survey of businesses for insurance coverage and cybersecurity insurance coverage.	Cybersecurity Council (perhaps working with Secretary of State to be done with annual corporate reports)	0%	December 2019	

Resources and Budget

15. Will staff be required to complete this deliverable?

a. Yes

b. **If Yes, please complete the following**

Estimated Initial FTE	Estimated Continued FTE	Skillset/Role	Primary Source of Funding	Alternate Source of Funding	Notes
¼ FTE	¼ FTE	Survey	Cybersecurity Council office	Indiana General Assembly	Secretary of State should be involved.

16. What other resources are required to complete this deliverable? (Examples include software, hardware, supplies, materials, equipment, services, facilities, etc.)

Resource	Justification/Need for Resource	Estimated Initial Cost	Estimated Continued Cost, if Applicable	Primary Source of Funding	Alternate Source of Funding	Notes
Website space	Making documents available for review or download	May be within scope of current IN website maintenance	Unknown	Unknown	Unknown	

Benefits and Risks

17. What is the greatest benefit of this deliverable? (Please provide qualitative and/or quantitative support.)

a. By publishing details on types of services and insurance coverages available, Indiana will increase awareness and understanding of the need for cyber risk coverage.

b. By increasing the number of businesses protected against cybersecurity loss, Indiana's economy will be more resilient in the face of increasing cyber threats.

18. How will this deliverable reduce the cybersecurity risk or impact? What is the estimated costs associated with that risk reduction?

a. It has been estimated that up to 60% of small and medium sized businesses fail within six (6) months of a cybersecurity attack. By encouraging small and medium sized businesses to protect against cybersecurity risks, Indiana companies will be better protected.

19. What is the risk or cost of not completing this deliverable?

a. Up to 60% of small and medium sized businesses fail within six (6) months of a cybersecurity attack and the risk of being targeted by an attack is rising exponentially. Indiana's economy could be damaged as the result of cyberattacks against Indiana businesses.

20. What defines success and/or what metrics will be used to measure success? What is the baseline for your metrics?

a. There is no current survey of Indiana businesses on this subject. The Cybersecurity Council could work with (1) the Indiana Chamber of Commerce or (2) the Office of the Indiana Secretary of State to conduct a survey of Indiana businesses and use the increase of businesses covered by cybersecurity policies as a measure of success.

21. Are there comparable jurisdictions (e.g. other states) that have similar projects that we can compare this project to using the same metrics?

a. No
b. **If Yes, please list states/jurisdictions**
    i. Other states or jurisdictions are likely looking at these statistics but we are not currently aware of concrete examples.

22. Are there comparable jurisdictions (e.g. other states) that does not have a comparable project that we can use as a control to show what happens if Indiana does not complete the deliverable?

a. No
b. **If Yes, please list states/jurisdictions**
    i. We are not aware of initiatives in other states. But there may be.

Other Implementation Factors

---

23. List factors that may negatively impact the resources, timeline, or budget of this deliverable?

a. None known

24. Does this deliverable require a change from a regulatory/policy standpoint?

a. No
b. **If Yes, what is the change and what could be the fiscal impact if the change is made**?
    i. N/A.

25. What will it take to support this deliverable if it requires ongoing sustainability?

a. Surveys of Indiana businesses will require annual surveys or coordination with the Indiana Chamber of Commerce or the Office of the Indiana Secretary of State.

26. Who has the committee/working group contacted regarding implementing this deliverable?

a. No one outside of working group as of yet.

27. Can this deliverable be used by other sectors?

a. Yes
b. **If Yes, please list sectors**
    i. All sectors

Communications

---

28. Once completed, which stakeholders need to be informed about the deliverable?

a. All stakeholders would benefit from this information.

29. Would it be appropriate for this deliverable to be made available on Indiana's cybersecurity website (www.in.gov/cybersecurity)?

a. Yes

30. What are other public relations and/or marketing considerations to be noted?

a. The Indiana Cybersecurity Office could coordinate with Office of the Indiana Attorney General's communications team.

Evaluation Methodology

Objective 1: Legal and Insurance Working Group conduct a survey of businesses for insurance coverage and cybersecurity insurance coverage by August 2019.

Type: ☒ Output ☐ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Objective 2: Legal and Insurance Working Group provide a report of the findings of the cyber insurance survey to the IECC by December 2019.

Type: ☐ Output ☒ Outcome

Evaluative Method:

☒ Completion
☐ Award/Recognition
☐ Survey - Convenient
☐ Survey – Scientific
☐ Assessment Comparison
☐ Scorecard Comparison
☐ Focus Group
☐ Peer Evaluation/Review
☐ Testing/Quizzing
☐ Benchmark Comparison
☐ Qualitative Analysis
☐ Quantifiable Measurement
☐ Other

Supporting Documentation

Supporting Documentation

This section contains all of the associated documents that are referenced in this strategic plan and can be used for reference, clarification, and implementation details.

- Cyber & Technology Insurance Guide - Version 1
- Survey of Cyber Laws

IECC Legal and Insurance Working Group

Cyber & Technology Insurance Guide Version 1

August 2018

CYBER & TECHNOLOGY INSURANCE COVERAGE

Today, consumers, businesses, and government agencies use internet-capable devices every day. These high tech devices – from laptops to security systems to medical devices – increase efficiency in the collection and exchange of data, and revolutionize industries. Cyber technology also brings new risks. Large companies subject to data breaches have made headlines, but small and mid-size companies that collect data and private information may also be vulnerable. Businesses may be obligated to protect private information by governing laws and regulations – such as Personally Identifiable Information, Personal Health Information and Confidential Corporate Information. Smaller businesses may not be able to survive the costs associated with a data breach. One of the largest growing financial risks a business must face is a cyber breach. Insurance is a necessary component of a business's risk management and disaster recovery plan. Inadequately insured businesses are unlikely to survive major incidents.

Until recently, most businesses have insured only computer equipment and mobile devices against physical risks such as damage, theft, or fire loss. Electronic equipment was insured on the same basis as furniture and automobiles, with no coverage for lost, stolen or disrupted data. Some organizations may have had wider, more extensive policies that also include coverage for equipment breakdown and limited expenses for reinstatement of data, but most cyber risks are now excluded under traditional commercial general liability policies.

Insurers and businesses have recognized that traditional insurance is inadequate, and there is a need for tailored cyber liability insurance to cover a wide variety of exposures that can result from technology-related activities -- from misplaced company cell phones to cyberattacks. Cyber liability insurance is intended to address an insured's obligation to protect private information from inappropriate access undergoing significant changes and likely will continue to do so as it is linked to the ever-changing world of technology. Therefore, it is important to know the terminology, to review your risks, and to determine your coverage needs. Cyber liability insurance is increasingly becoming an important consideration for conducting business in a high-tech marketplace.

FREQUENTLY ASKED QUESTIONS

Q What is cyber liability?

A Cyber liability is the risk of a data breach as a result of online activities and the use of electronic storage technology.

Q What is cyber liability insurance?

A While policies vary, cyber liability insurance is designed to protect a business or organization from:

- Liability claims involving the unauthorized release of information for which the organization has a legal obligation to keep private or confidential, such as employee, patient or customer records.

- Liability claims alleging invasion of privacy.
- Liability claims alleging failure of computer security that results in alterations of data and defense costs.

- Data Response Services, including legal, computer forensics, notification services, credit and identity monitoring products and crisis management expertise, and the reimbursement to the insured for certain out-of-pocket expenses.

Q What is a data breach?

A A data breach occurs when secured information is released to or accessed by unauthorized individuals. The lost data may be employee personnel records, customer financial accounts, or business trade secrets. The incidents pose serious risks for organizations as well as the individuals whose data has been lost or disseminated.

Q How do data breaches happen?

A Data breaches can occur by accident, such as an employee sends out an unsecured email, or by crime, such as a malicious hacker.

Q What data or information do businesses need to secure?

A Most businesses generate vast amounts of data which is available and stored on their electronic storage network systems, which may be subject to certain privacy laws:

- Personal information:
  - Personally identifiable information (PII): name, address, date of birth, telephone number, email address, Social Security number, zip code, biometric data.
  - Protected health information (PHI): healthcare-based treatment information, medical history, health insurance information, including member identification numbers.

- Corporate information: intellectual property, business, contracts, attorney-client privileged information:
  - Payment cardholder information (PCI): credit/debit card data, including account numbers, security codes, insurance account information, etc.

- Cyber-based data: web browser history, cookie information, metadata, and IP addresses.

Q Why consider cyber liability insurance?

A

There are various reasons why a company may want to consider cyber liability insurance as a way to protect confidential data and insure the risk against financial exposure:

- Frequency of privacy breaches are on the rise;
- Threats are getting dramatically worse;
- Almost all 50 states have enacted privacy laws in response to privacy breaches;
- Consumers expect that their confidential information will be protected.
- Class action litigation is becoming more active as a result of privacy breaches.
- Many business contracts now require cyber insurance.
- Cyber liability insurance products are becoming more widely available.

GLOSSARY OF CYBER INSURANCE TERMS

Breach Response – Investigation. Costs incurred to investigate data breach; investigate potential indemnity.

Breach Response – Notification. Costs incurred to notify individuals of breach.

Breach Response – Public Relations. Costs incurred to hire public relations firm.

Breach Response – Remediation. Costs incurred to remediate data breach (e.g., credit monitoring, call center, etc.).

Business Income (or Business Interruption Income Loss) is defined as net profit or loss before income taxes, as well as the continuing normal operating and payroll expenses.

Claim Expenses include reasonable and necessary legal fees, costs, and expenses incurred in the investigation, adjustment, defense, or appeal of a claim. They also typically include the cost of any bond or appeal bond required in any defended suit.

Computer System means computer hardware and software, and the electronic data stored thereon, as well as associated input and output devices, terminal devices, data storage devices, networking equipment, components, software, and electronic backup facilities, including systems accessible through the internet, intranets, extranets, or virtual private networks.

Cyber Attack (Denial of Service Attack) is action preventing an information system from functioning in accordance with its intended purpose; the inability of an authorized third party to access the company's Computer System; and the inability of an authorized third party to access his or her Computer System, where such inability is directly cause by the company's Computer System.

Cyber Extortion. Losses and expenses arising out of a criminal threat to release sensitive information or bring down a system/network.

Damages/Loss includes the amounts the business is legally obligated to pay as a result of a covered judgment, award, or settlement; costs charged against the business in any suit; or pre-

judgment and post-judgment interest and defense costs. It also includes punitive or exemplary damages where insurable by law.

Data Restoration – Security Failure. Costs to restore lost data caused by security failure.

Data Restoration – System Failure. Costs to restore lost data caused by system failure.

Denial of Service Attack is action preventing an information system from functioning in accordance with its intended purpose (see Cyber Attack).

Extra Expense means any reasonable and necessary expenses in excess of the business's normal operating expenses that the business incurs during the Period of Restoration associated with restoring and resuming operations, including securing temporary third-party Internet Service Provider services, temporary website and/or email hosting services, rental of temporary networks, or other temporary equipment or service contracts.

First Party Claim. A first party claim is brought by an insured under the insured's cyber policy for a loss that occurs because of loss or damage to the insured's business.

Funds Transfer and Computer Fraud – Social Engineering. Loss of money or property arising from *bona fide* wire instructions induced through social engineering.

Funds Transfer and Computer Fraud – Traditional Coverage. Loss of money or property arising from fraudulent wire instructions or fraudulent entries into a computer system.

Identity Restoration Services typically means consultation and assistance to an individual receiving notification services to determine whether identity theft has occurred, and, if so, to restore the individual's identity to pre-theft status.

Media or Electronic Publishing Incident means the actual or alleged unintentional libel, slander, trade libel, or disparagement resulting from the insured electronic publishing. It also includes plagiarism, violation of privacy, infringement of a copyright or trademark, or unauthorized use of titles formats, plots, or other protected material resulting from the insured's electronic or media publishing.

Media Liability. Claim by third party in connection with the insured's media content, which may include claim for trademark infringement, defamation, libel, product disparagement, copyright violation, or invasion of privacy.

Network/Computer System typically includes the computer hardware, software, and electronic data, as well as associated input and output devices, terminal devices, data storage devices, networking equipment, components, software, and electronic backup facilities, including systems accessible through the Internet, intranets, extranets, or virtual private networks.

Network Interruption – Contingent BI. Loss of income arising from business interruption caused by third-party service failure (including mitigation expenses).

Network Interruption – Security Failure. Loss of income arising from business interruption caused by security failure (including mitigation expenses).

Network Interruption – System Failure. Loss of income arising from business interruption caused by system failure (including mitigation expenses).

Network Security Liability. Claim by third party arising from the insured's failure of network security.

Network Security/Cyber Incident typically means any Unauthorized Access/Use of, or introduction of malicious code into, or Denial of Service Attack upon, the company's Computer System, that directly results in an interruption in services; or the corruption of deletion of digital assets.

Notification Services typically mean the preparation and distribution of notice letters from the insured advising individuals of the network security event and the availability of related resources if such notices are required by applicable law, as well as call center support services.

Period of Restoration is the period from which the business first suffered an interruption in service to the date and time it was restored (or could have been restored) with reasonable speed to substantially return to the level of operation that existed prior to the interruption. There is typically a limit on the policy that the period of restoration cannot exceed thirty days.

Personal Identifiable Information (PII) is information not available to the general public from which a person can be identified. This definition should be broad enough to include a person's name, telephone number, Social Security number, medical or healthcare data, driver's license number or state identification number, account number, credit and debit card number, or password.

Privacy Incident is the unintentional and unauthorized disclosure of Personal Identifiable Information or confidential information in the care, custody, or control of the business or service provider; a violation of a Privacy Regulation; or failure to comply with the term's own privacy policies.

Privacy Liability – Business Records Claim. Claim by third party arising from the insured's failure to protect trade secrets or other confidential business information.

Privacy Liability – Privacy Claim. Claim by third party arising from the insured's failure to protect personal information (including PII, PHI and FAI).

Privacy Liability – Regulatory Claims. Third party liability coverage that generally is designed to protect an insured business in connection with certain requests for information, investigative demands and/or civil proceedings often brought by or on behalf of a governmental agency arising from the insured's failure to protect personal information. The coverage often includes civil fines and penalties imposed on the insured, to the extent such fines and penalties are insurable by law.

Privacy Notification Costs are reasonable and necessary costs to hire a security expert to determine the existence and cause of a breach; costs to notify consumers under a breach notification law; or fees incurred to determine the actions necessary to comply with a breach notification law.

Privacy Regulation means statutes associate with the control and use of personally identifiable financial, medical, or other sensitive information.

Public Relations Expense typically means the hiring of a public relations firm or crisis management firm for communication services to explain the nature of the network security/cyber event and any corrective actions taken.

Regulatory Fines includes civil money penalties imposed by a federal, state, local, or foreign government entity pursuant to a regulatory proceeding.

Regulatory Proceeding is an investigation of an insured by an administrative, regulatory, or government agency concerning a Privacy Incident; or an administrative adjudicative proceeding for a privacy Wrongful Act or network security Wrongful Act.

Regulatory Injury means injury sustained by a person due to actual or alleged disparagement of an organization's products or services; libel or slander of natural person; or violation of such person's rights of privacy or publicity result from cyber activities.

Retroactive Date means the date in the declarations section of the policy. If no date is set forth in the declarations page, then the retroactive date is the date of the inception of the policy.

Reward Payment/Expenses/Cyber Extortion Costs means the reasonable amount paid by the business, with prior approval of the insurer, to an informant for information not otherwise available, which leads to the arrest and conviction of persons responsible for a cyber attack or threat covered under the policy.

Service Provider means a business the business does not own, operate or control, but that the insured hires and contracts to perform services related to the business' computer systems, including maintaining the computer system; hosting the business' internet website; handling, storing or destroying information and confidential materials; or providing other IT-related services.

Technology Errors & Omissions. Claim by third party for financial loss arising from errors or omissions in the technology-facing component of the insured's business (tech services or products).

Third Party Claim. A third party claim is a demand against the business for monetary damages or non-monetary relief; a written demand for arbitration; or a civil proceeding brought by the service of a complaint or similar pleading.

Unauthorized Access/Use is the use of, or access to, a computer system by a person unauthorized by the insured to do so, or the authorized use of, or access to, a Computer System in a manner not authorized by the insured.

Wrongful Act typically means the actual or alleged act, unintentional error, omission, neglect, or breach of duty by an insured business or Service Provider that directly results in a breach of the insured's network.

IECC Legal and Insurance Working Group

Survey of Cyber Laws

July 2018

Survey of Indiana Cyber Laws

Title or Description	Standard Type	Reference	Synopsis	Penalty	Statute of Limitations	Enforcement
IN Senate Bill 221 - E-Prescription Bill	State	SB 221	The bill requires prescribers to have access to and utilize INSPECT, a state-sponsored website database that allows practitioners to check a patient's controlled substance prescription history	https://iga.in.gov/legislative/2018/bills/senate/221		https://iga.in.gov/legislative/2018/bills/senate/221
IN Telephone Solicitation of Consumers ("Do Not Call Law")	State	IC art. 24-4.7	" A telephone solicitor may not make or cause to be made a telephone sales call to a telephone number if that telephone number appears in the most current quarterly listing published by the division." IC § 24-4.7-4-2.	$10,000 for the first call; $25,000 for subsequent calls. IC § 24-4.7-5-2(a)(2).	2 years after the call is made. IC § 24-4.7-5-4.	Attorney General: IC § 24-4.7-5-1.
IN Do Not Text Law	State	IC art. 24-4.7	"A telephone solicitor may not make or cause to be made a telephone sales call to a telephone number if that telephone number appears in the most current quarterly listing published by the division." IC § 24-4.7-4-2. A Telephone sales call can be defined as the "transmission of: a text message . . ." IC § 24-4.7-2-9(b)	$10,000 for the first call; $25,000 for subsequent calls. IC § 24-4.7-5-2(a)(2).	2 years after the call is made. IC § 24-4.7-5-4.	Attorney General: IC § 24-4.7-5-1.
IN Prohibited Spyware	State	IC art. 24-4.8	A person who is not the owner or operator of the computer may not knowingly or intentionally: (1) transmit computer software to the computer; and (2) by means of the computer software transmitted under subdivision (1), do any of the following" including deceptively modify computer settings or collect personally identifying information among other things. IC § 24-4.8-2-2.	Damages or $100,000: IC § 24-4.8-3-1(2).	Undefined by statute.	Private right of action: IC § 24-4.8-3-1.
IN Disclosure of Security Breach Act	State	IC art. 24-4.9	After a data security breach involving "personal information," a "data base owner" may need to alert (1) affected Indiana residents, (2) the attorney general, (3) consumer reporting agencies, and (4) the data base owner (if the breached party is not the data base owner). Must notify without unreasonable delay (likely within 30 days of the breach discovery). IC § 24-4.9.-3-1; IC § 24-4.9.-3-2.	$150,000 per notification type: IC § 24-4.9.-4-2(2)	Likely 2 years from notification of Attorney General. Undefined by the statute.	Attorney General: IC § 24-4.9-4-2
IN Protection of Personal Information	State	IC § 24-4.9-3-3.5(c)	"A data base owner shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner." "A person that knowingly or intentionally fails to comply with any provision of this section commits a deceptive act . . ."	$5,000 per deceptive act: IC § 24-4.9-3-3.5(c).	Likely 2 years from notification of Attorney General. Undefined by the statute.	Attorney General: IC § 24-4.9-3-3.5(f)
IN Disposal of Personal Information	State	IC § 24-4.9-3-3.5(d)	" A data base owner shall not dispose of or abandon records or documents containing unencrypted and unredacted personal information of Indiana residents without shredding, incinerating, mutilating, erasing, or otherwise rendering the personal information illegible or unusable."	$5,000 per deceptive act: IC § 24-4.9-3-3.5(c).	Likely 2 years from notification of Attorney General. Undefined by the statute.	Attorney General: IC § 24-4.9-3-3.5(f)
IN Disposal of Personal Information	State	IC § 24-4-14-8	"A person who disposes of the unencrypted, unredacted personal information of a customer without shredding, incinerating, mutilating, erasing, or otherwise rendering the information illegible or unusable commits a Class C infraction."	Class C or Class A infraction: IC § 24-4-14-8; 34-28-5-4	2 years: IC § 34-28-5-1(c)(2)	Prosecuting Attorney: IC § 34-28-5-1
IN Disposal of Electronic Waste	State	IC § 13-20.5-10-1	Covered entities cannot dispose of electronic in a landfill or through incineration	None: IC § 13-20.5-10-2	NA	NA
IN Deceptive Consumer Sales Act	State	IC ch. 24-5-0.5	"A supplier may not commit an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction. Such an act, omission, or practice by a supplier is a violation of this chapter whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations." IC § 24-5-0.5-3(a)	$5,000 per knowingly deceptive act: IC § 24-5-0.5-4(g)	2 years after the occurrence of the deceptive act: IC § 24-5-0.5-5.	Private Right of action and Attorney General: IC § 24-5-0.5-4(c)
IN Regulation of Automatic Dialing Machines	State	IC ch. 24-5-14	Indiana's Auto Dialer law prohibits most prerecorded calls, commonly known as "robo-calls," made via an automatic dialing-announcing device ("ADAD") regardless of the subject matter of the message. IC § 24-5-14-5(b).	$5,000 per knowingly deceptive act: IC § 24-5-0.5-4(g)	2 years after the occurrence of the deceptive act: IC § 24-5-0.5-5.	Attorney General: IC § 24-5-14-13.
IN Do Not Fax Law	State	IC § 24-5-0.5-3(b)(19).	Prohibition on sending unsolicited facsimile ("fax") advertisements . The law applies to advertisements sent to residential and business fax numbers. Unlike the Do Not Call law, the Do Not Fax law does not require people to register their fax numbers.	$5,000 per knowingly deceptive act: IC § 24-5-0.5-4(g)	2 years after the occurrence of the deceptive act: IC § 24-5-0.5-5.	Attorney General: IC § 24-5-14-13.

IN Deceptive Commercial Electronic Mail	State	IC ch. 24-5-22	Prohibition on sending unsolicited commercial electronic mail, when failing to comply with statutory sending standards. IC § 24-5-22-8.	Damages or $500 per email: IC § 24-5-22-10(d)(2).	Undefined by statute.	Private right of action: IC § 24-5-22-10(a).
IN Health Records and Identifying Information Protection	State	IC ch. 4-6-14	Provision relates to the Indiana Attorney General's responsibility related to abandoned health records and other records that contain personal information.	NA	NA	NA
IN Notice of Security Breach Act for State Agencies	State	IC ch. 4-1-11	"Any state agency that owns or licenses computerized data that includes personal information shall disclose a breach of the security of the system following discovery or notification of the breach to any state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person." IC § 4-1-11-5.	NA	NA	NA
IN Release of Social Security Numbers by State Agencies	State	IC § 4-1-10, et seq.	Details the scope of permissible disclosures of Social Security numbers as well as the consequences for violations of the statute.	Level 6 felony: IC § 4-1-10-8; Class A infraction: IC § 4-1-10-10.		Attorney General: IC §§ 4-1-10-11; 4-1-10-12.
IN Release of Social Security Numbers by State Agencies, Notice to Attorney General: Rules	Rule	10 IAC § 5-4-1	"When a state agency becomes aware of a release of Social Security numbers or other personal identifying information, the state agency or employee shall, within two (2) business days of the disclosure, notify the office of attorney general for the state in writing . . ."	NA	NA	NA
IN Driver's Privacy Protection Act ("DPPA")	State	IC § 9-14-13-2	Prohibits the disclosure of personal information associated with motor vehicle records by the Indiana Bureau of Motor Vehicles.	Class C misdemeanor: IC § 9-14-13-11	2 years: IC § 34-28-5-1(c)(2)	Prosecuting Attorney: IC § 33-39-1-5
IN Criminal Law - Wiretap Statute	State	IC art. 35-33.5	Provision outlines the requirements for the state to obtain a warrant to intercept the telephonic or telegraphic communications of an individual.	Suppression of Evidence: IC § 35-33.5-4-4.	NA	NA
IN Rights of Victims of Identity Deception: Civil	State	IC § 24-5-26-2	Provision outlines the duties of those that conduct trade or commerce concerning the protections for victims of identity theft.	$5,000: IC § 24-5-26-3	2 years from the mistreatment date: IC § 24-5-26-3	Attorney General: IC § 24-5-26-3
IN Rights of Victims of Identity Deception: Criminal	State	IC ch. 35-40-14	Provision outlines the duty of law enforcement agencies concerning identity theft and the protections for victims of identity theft.	NA	NA	NA
IN Criminal Law - Offense Against Intellectual Property	State	IC § 35-43-1-7	A person who knowingly or intentionally and who without authorization: (1) modifies data, a computer program, or supporting documentation; (2) destroys data, a computer program, or supporting documentation; or (3) discloses or takes data, a computer program, or supporting documentation that is: (A) a trade secret (as defined in IC 24-2-3-2); or (B) otherwise confidential as provided by law; and that resides or exists internally or externally on a computer, computer system, or computer network, commits an offense against intellectual property, a Level 6 felony.	Level 6 Felony: IC § 35-50-2-7	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-5
IN Criminal Law - Offense Against Computer Users	State	IC § 35-43-1-8	(a) A person who knowingly or intentionally and who without authorization: (1) disrupts, denies, or causes the disruption or denial of computer system services to an authorized user of the computer system services that are: (A) owned by; (B) under contract to; or (C) operated for, on behalf of, or in conjunction with; another person in whole or part; (2) destroys, takes, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; (3) destroys or damages a computer, computer system, or computer network; or (4) introduces a computer contaminant into a computer, computer system, or computer network; commits an offense against computer users, a Level 6 felony.	Level 6 Felony: IC § 35-50-2-7	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-6
IN Criminal Law - Identity Deception	State	IC § 35-43-5-3.5	(a) Except as provided in subsection (c), a person who knowingly or intentionally obtains, possesses, transfers, or uses the identifying information of another person, including the identifying information of a person who is deceased: (1) without the other person's consent; and (2) with intent to: (A) harm or defraud another person; (B) assume another person's identity; or (C) profess to be another person; commits identity deception, a Level 6 felony.	Level 6 Felony: IC § 35-50-2-7	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-7

IN Criminal Law - Synthetic Identity Deception	State	IC § 35-43-5-3.8	(a) A person who knowingly or intentionally obtains, possesses, transfers, or uses the synthetic identifying information: (1) with intent to harm or defraud another person; (2) with intent to assume another person's identity; or (3) with intent to profess to be another person; commits synthetic identity deception, a Level 6 felony.	Level 6 Felony: IC § 35-50-2-7	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-8
IN Criminal Law - Fraud	State	IC § 35-43-5-4	Encompasses different types of fraud including obtaining property by use of another's credit card unlawfully.	NA	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-9
IN Criminal Law - Unlawful Possession of a Card Skimming Device	State	IC § 35-43-5-4.3	A person who possesses a card skimming device with intent to commit: (1) identity deception (IC 35-43-5-3.5); (2) synthetic identity deception (IC 35-43-5-3.8); (3) fraud (IC 35-43-5-4); or (4) terroristic deception (IC 35-43-5-3.6); commits unlawful possession of a card skimming device. Unlawful possession of a card skimming device under subdivision (1), (2), or (3) is a Level 6 felony. Unlawful possession of a card skimming device under subdivision (4) is a Level 5 felony.	Level 5 Felony: IC § 35-50-2-6	5 years: IC § 35-41-4-2(a)(1)	Prosecuting Attorney: IC § 33-39-1-10
IN Unlawful Recording	State	IC § 35-46-8-4	"A person who knowingly or intentionally uses an audiovisual recording device in a motion picture exhibition facility with the intent to transmit or record a motion picture commits unlawful recording, a Class B misdemeanor."	Class B misdemeanor: IC § 35-50-3-3	2 years: IC § 35-41-4-2(a)(2)	Prosecuting Attorney: IC § 33-39-1-11
IN Unlawful Photography and Surveillance of Private Property	State	IC § 35-46-8.5-1	"A person who knowingly or intentionally places a camera or electronic surveillance equipment that records images or data of any kind while unattended on the private property of another person without the consent of the owner or tenant of the private property commits a Class A misdemeanor." Note: Numerous exceptions enumerated within the statute.	Class A misdemeanor: IC § 35-50-3-2	2 years: IC § 35-41-4-2(a)(2)	Prosecuting Attorney: IC § 33-39-1-12
IN State Insurance Commissioners **Navigators and Application Organizations**	State	760 IAC § 4-5-2	"Navigators and application organizations shall comply with the following safeguards to maintain and protect the confidentiality of personal information:"	Up to $10,000 per violation: 760 IAC § 4-7-1(d)	NA	If a navigator or application organization does not comply with the requirements of this rule, the commissioner may initiate an enforcement action against the navigator or application organization under 760 IAC 4-7.
IN Department of Financial Institutions ("DFI")	State		Enforces FFIEC standards.			

Survey of Federal Cyber Laws

Date	Title	Subtitle	Reference	Information
1914	Executive Order 13571		15 U.S.C. § 45, et seq.	Gave the FTC the authority to enforce rules prohibiting “unfair or deceptive acts or practices in or affecting commerce."
		FTC Section 5 Authority	15 U.S.C. § 45(a)(1), et seq.	The basic consumer protection statute enforced by the Commission is Section 5(a) of the FTC Act, which provides that "unfair or deceptive acts or practices in or affecting commerce...are...declared unlawful."
1966	Freedom of Information Act (FOIA) of 1966		5 U.S.C. § 552, et seq.	Under FOIA, “any person” may request “records” maintained by an executive agency. People or entities requesting records need not state a reason for requesting records. Today, all fifty states have freedom of information laws, many of which are based upon the FOIA.
1968	Wiretap Act of 1968		8 U.S.C. § 2511, et seq.	Broadly prohibits the intentional interception, use, or disclosure of wire and electronic communications unless a statutory exception applies. In general, these prohibitions bar unauthorized third parties (including the government) from wiretapping telephones and installing electronic "sniffers" that read Internet traffic.
1968	Omnibus Crime and Control and Safe Streets Act of 1968		18 U.S.C. §§ 2510–22, et seq.	Extended the reach of wiretap regulations to state officials as well as to private parties. Despite its profound increase in the extent of protection, Title III had important limitations. It applied to the interception of “aural” communications; it did not apply to visual surveillance or other forms of electronic communication.
1970	Fair Credit Reporting Act of 1970		15 U.S.C. § 1681, et seq.	The Fair Credit Reporting Act (FCRA) provides limited protections for individuals. It enables people to access their records, and restricts the manner in which records are disclosed. Individuals can challenge inaccuracies on their reports and can sue to collect damages for violations of the Act. However, FCRA immunizes creditors and credit reporting agencies from lawsuits for “defamation, invasion of privacy, or negligence” except when the information is “furnished with malice or willful intent to injure such consumer.” Although the FCRA allows people to sue for negligent violations of the Act, there is a two-year statute of limitations “from the date on which the liability arises."
1970	Racketeer Influenced and Corrupt Organization (RICO) Act of 1970		118 U.S.C. ch. 96	Passed in 1970, the Racketeer Influenced and Corrupt Organizations Act (RICO) is a federal law designed to combat organized crime in the United States. It allows prosecution and civil penalties for racketeering activity performed as part of an ongoing criminal enterprise. Such activity may include illegal gambling, bribery, kidnapping, murder, money laundering, counterfeiting, embezzlement, drug trafficking, slavery, and a host of other unsavory business practices.

1970	Bank Secrecy Act of 1970		Pub. L. No. 91-508 12 U.S.C. §§ 1730(d), 1829b, 1951-59, et seq. 31 U.S.C. H9 1051-1122, et seq.	The Bank Secrecy Act, enacted in 1970, requires banks to retain records and create reports to help law enforcement investigations. The Act was passed due to concerns that the computerization of records would make white collar crime more difficult to detect. Federally insured banks must record the identities of account holders and maintain copies of each financial instrument. International transactions exceeding $5,000 are subject to reporting, as well as domestic transactions exceeding $10,000. In *California Bankers Ass'n v. Shultz* , 416 U.S. 21 (1974), the Supreme Court upheld the Act against a Fourth Amendment challenge by a group of bankers and account holders. The Court concluded that the bankers lacked Fourth Amendment rights in the data because "corporations can claim no equality with individuals in the enjoyment of a right to privacy." *Id* at 65. The account holders failed to allege that they engaged in transactions exceeding $10,000, and as a result, lacked standing.
1974	Privacy Act of 1974		5 U.S.C. § 552a, et seq.	The Act responded to many of the concerns raised by the United States Department of Health Education and Welfare (HEW) report, "Records, Computers, and the Rights of Citizens." It regulates the collection and use of records by federal agencies, and affords individuals right to access and correct their personal information.
1974	Family Educational Rights and Privacy Act of 1974		20 U.S.C. § 1232g, et seq.	The Family Educational Rights and Privacy Act of 1974 (FERPA), otherwise known as the "Buckley Amendment," regulates the accessibility of student records. FERPA does not apply to records maintained by school law enforcement officials or health and psychological records.
1978	Protection of Pupil Rights Amendment ("PPRA") of 1978		20 U.S.C. § 1232h, et seq.; 34 C.F.R. part 98, et seq.	PPRA is a federal law that affords certain rights to parents of minor students with regard to surveys that ask questions of a personal nature. Briefly, the law requires that schools obtain written consent from parents before minor students are required to participate in any U.S. Department of Education funded survey, analysis, or evaluation that reveals information certain topics.
1978	Foreign Intelligence Surveillance Act of 1978		50 U.S.C. §§ 1801–11, et seq.	The Foreign Intelligence Surveillance Act (FISA) of 1978, created a distinct regime for electronic surveillance to gather foreign intelligence. Whereas Title III regulated electronic surveillance for domestic law enforcement purposes, FISA applied when foreign intelligence gathering was "the purpose" of the investigation. FISA permits electronic surveillance and covert searches pursuant to court orders, which are reviewed ex parte by a special court of seven federal judges.
1978	Right to Financial Privacy Act of 1978		29 U.S.C. § 3407, et seq.	The Right to Financial Privacy Act (RFPA) provided limited protection of financial records to fill the gap left by *United States v. Miller* , 425 U.S. 435, 435 (1976). Pursuant to the RFPA, government officials must use a warrant or subpoena to obtain financial information. There must be "reason to believe that the records sought are relevant to a legitimate law enforcement inquiry." Subject to certain exceptions, the customer must receive prior notice of the subpoena.
1978	Airline Deregulation Act - Preemption of authority over prices, routes, and service		49 U.S.C.A. § 41713, et seq.	"[A] State, political subdivision of a State, or political authority of at least 2 States may not enact or enforce a law, regulation, or other provision having the force and effect of law related to a price, route, or service of an air carrier that may provide air transportation under this subpart."

1979	Drug Abuse Prevention, Treatment, and Rehabilitation Act of 1979		42 C.F.R. part 2, et seq.	Drug Abuse Prevention, Treatment, and Rehabilitation Act (Act) is a federal statute designed to be a practical resource for governments, policy planners, service commissioners and treatment providers against drug abuse. The Act makes provision for federal drug abuse programs and activities. The Act also provides for education, treatment, rehabilitation, research, training, and law enforcement efforts to prevent drug abuse.
1980	Privacy Protection Act of 1980		42 U.S.C. § 2000aa, et seq.	Dissatisfaction over *Zurcher v. Stanford Daily* , 436 U.S. 547 (1978) led Congress to pass the Privacy Protection Act in 1980. The Act restricts the search or seizure of "any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." As a result of the Act, a subpoena is needed to obtain work product materials, which permits the party to challenge the request in court and to produce the documents without having law enforcement officials intrude on the premises.
1984	Cable Communications Policy Act of 1984		42 U.S.C. § 551, et seq.	The Cable Communications Policy Act (CCPA) of 1984 protects the privacy of cable records. Cable companies must notify subscribers about the collection and use of personal information. Companies cannot disclose a subscriber 's viewing habits. The Act is enforced with a private right of action.
1986	Computer Fraud and Abuse Act of 1986		18 U.S.C. § 1030, et seq.	A United States cybersecurity bill that was enacted in 1986 as an amendment to existing computer fraud law (18 U.S.C. § 1030), which had been included in the Comprehensive Crime Control Act of 1984. The law prohibits accessing a computer without authorization, or in excess of authorization. The original 1984 bill was enacted in response to concern that computer-related crimes might go unpunished. The House Committee Report to the original computer crime bill characterized the 1983 techno-thriller film WarGames—in which a young Matthew Broderick breaks into a U.S. military supercomputer programmed to predict possible outcomes of nuclear war and unwittingly almost starts World War III—as "a realistic representation of the automatic dialing and access capabilities of the personal computer."
1988	Computer Matching and Privacy Protection Act of 1988		5 U.S.C. § 552a(a)(8)–(13), (e)(12), (o)–(r), (u)), et seq.	A major loophole in the Privacy Act of 1974 has been the "routine use" exception. Under this exception, to detect fraud, the federal government in 1977 began running computer comparisons of employee records with the records of people receiving benefits. In 1988, Congress addressed this practice, known as "computer matching" by passing the Computer Matching and Privacy Protection Act. The law established procedures for computer matchings, but did not halt the practice.
1988	Employee Polygraph Protection Act of 1988		29 U.S.C. §§ 2001-09, et seq.	In 1988, Congress passed the Employee Polygraph Protection Act (EPPA). The EPPA prohibits private sector employers from using polygraph examinations on employees and prospective employees. The Act does not apply to public sector employers. Employers can, however, use polygraphs "in connection with an ongoing investigation involving economic loss or injury to the employer's business, such as theft, embezzlement, misappropriation, or an act of unlawful industrial espionage or sabotage" when "the employer has a reasonable suspicion that the employee was involved in the incident or activity under investigation." Private sector employers who provide security services are exempt.

1988	Video Privacy Protection Act of 1988		18 U.S.C. § 2710(b), et seq.	The confirmation hearings of Supreme Court Justice nominee Robert Bork sparked a law to protect videocassette rental data. Reporters attempted to obtain a list of the videos Bork had rented from his video store. Incensed at this practice, Congress passed the Video Privacy Protection Act (VPPA) of 1988.251 The VPPA forbids videotape service providers from disclosing customer video rental or purchase information.
1986	Electronic Communications Privacy Act of 1986		18 U.S.C. §§ 2510-22, 2701-11, 3121-27, et seq.	In 1986, Congress revisited its wiretapping law by substantially reworking Title III of 1968. The Electronic Communications Privacy Act (ECPA) expanded Title III to new forms of communications, with a particular focus on computers. The ECPA restricts the interception of transmitted communications and the searching of stored communications. Title I of the ECPA, known as the "Wiretap Act," regulates the interception of communications. Title II, referred to as the "Stored Communications Act," governs access to stored communications and records held by communications service providers (such as ISPs). Title III, called the "Pen Register Act," provides limited regulation of pen registers and trap and trace devices.
1991	Telephone Consumer Protection Act of 1991		47 U.S.C. § 227, et seq.	In 1991, Congress enacted the Telephone Consumer Protection Act (TCPA), which permits people to request that telemarketers not call them again. If the telemarketer continues to call, people can sue for damages of up to $500 for each call.
1993	Government Performance and Results Act of 1993		Pub. L. No. 103-62	Requires executive agency heads to submit to the Director of the Office of Management and Budget (OMB) and the Congress a strategic plan for performance goals of their agency's program activities. Requires such plan to cover at least a five-year period and to be updated at least every three years. See: https://www.congress.gov/bill/103rd-congress/senate-bill/20
1994	Driver's Privacy Protection Act of 1994		18 U.S.C. §§ 2721-25, et seq.	In 1994, Congress passed the Driver 's Privacy Protection Act (DPPA), which requires that states first obtain a person's consent before disclosing her motor vehicle record information to marketers.
1995	Paperwork Reduction Act (PRA) of 2005		44 U.S.C. § 3501, et seq.	Designed to reduce the public's burden of answering unnecessary, duplicative, and burdensome government surveys.
1996	Health Insurance Portability and Accountability Act (HIPAA) of 1996		Pub. L. No. 104-191, 110 Stat. 1936	The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is the first federal statute to directly address health privacy. HIPPA required the Department of Health and Human Services (HHS) to draft regulations to protect the privacy of medical records. HHS's regulations, among other things, require that people authorize all uses and disclosures of their health information that are not for treatment, payment, or health care operation (such as for marketing purposes).

		HIPAA Privacy Rule	45 C.F.R. part 160, et seq. and 45 C.F.R. part 164, subparts A and E, et seq.	The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
		HIPAA Security Rule	45 C.F.R. part 160 and 45 C.F.R. part 164, subparts A and C, et seq.	The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
		HIPAA Breach Notification Rule	45 CFR part 164, subpart D, et seq.	Requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.
		Uses and disclosures for which an authorization or opportunity to agree or object is not required.	45 C.F.R. § 164.512, et seq.	Provides when covered entities or business associates are nor required to obtain valid authorization to use or disclose protected health information. General exceptions exist for public health activities.
		Uses and disclosures to carry out treatment, payment, or health care operations.	45 C.F.R. § 164.506, et seq.	Provides when covered entities or business associates are nor required to obtain valid authorization to use or disclose protected health information. General exceptions exist for collection of payments for medical services.
		Imposition of Civil Money Penalties	45 CFR, part 160, subpart D, et seq.	Provides guidelines for determining what amount an entity should be penalized for violating HIPAA.
1996	Economic Espionage Act of 1996		8 U.S.C. §§ 1831-39, et seq.	This regulation is intended to protect from disclosure outside the government proprietary information that is provided to the government during a bidding process. Exemption 4 of the Freedom of Information Act exempts from mandatory disclosure information such as trade secrets and commercial or financial information obtained by the government from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or protect the government's interest in compliance with program effectiveness. The law on Disclosure of Confidential Information (18 U.S.C. § 1905) makes it a crime for a federal employee to disclose such information.

1997	No Electronic Theft Act of 1997		Pub. L. No. 105-147	Provides for criminal prosecution of individuals who engage in copyright infringement under certain circumstances, even when there is no monetary profit or commercial benefit from the infringement.
1998	Children's Online Privacy Protection Act of 1998		15 U.S.C. §§ 6501-06, et seq.	The Children's Online Privacy Protection Act (COPPA) of 1998 governs the collection of children's personal information on the Internet. The law only applies to children under the age of thirteen. Children's websites must post privacy policies and obtain "parental consent for the collection, use, or disclosure of personal information from "children." COPPA applies only to websites "directed to children" or where the operator of the website "has actual knowledge that it is collecting personal information from a child."
1998	Digital Millennium Copyright Act (DMCA) of 1998		Pub. L. No. 105-304; 17 U.S.C. §§ 101, 104, 104A, 108, 112, 114, 117, 701, et seq.; 17 U.S.C. §§ 512, 1201–1205, 1301–1332, et seq.; 28 U.S.C. § 4001, et seq.	A U.S. copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO). It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works (commonly known as digital rights management or DRM). It also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself. In addition, the DMCA heightens the penalties for copyright infringement on the Internet.
1999	U.S. Uniform Computer Information Transactions Act (UCITA) of 1999 (Last Amended or Revised in 2002)		Uniform Laws Annotated. Uniform Computer Information Transactions Act (Last Amended or Revised in 2002)	UCITA provides a comprehensive set of rules for licensing computer information, whether computer software or other clearly identified forms of computer information. Computerized databases and computerized music are other examples of computer information that would be subject to UCITA. It would also govern access contracts to sites containing computer information, whether on or off the Internet. UCITA would also apply to storage devices, such as disks and CDs that exist only to hold computer information. Professional services by a member of a regulated profession (doctor, lawyer, accountant, for example) are not within UCITA even though communications about the transaction will be in the form of computer information.
1999	The Gramm-Leach-Bliley Act of 1999		15 U.S.C. § 6802(a)-(b), et seq.	In 1999, Congress passed the Gramm-Leach-Bliley (GLB) Act, which allows financial institutions with different branches or affiliates engaging in different services to share the "nonpublic personal information" among each branch of the company. Affiliates must inform customers of the information sharing, but people have no right to stop the companies from sharing it. However, when financial institutions desire to share customer data with third parties, people have a right to opt-out.

2000	Security and Exchange Commission ("SEC") Privacy of Consumer Financial Information Regulations of 2000		17 C.F.R. part 248, subpart A, et seq.	The SEC adopted Regulation S-P, privacy rules promulgated under section 504 of the Gramm-Leach-Bliley Act. Section 504 of GLBA required the Commission to adopt rules implementing notice requirements and restrictions on a financial institution's ability to disclose nonpublic personal information about consumers. The Regulation implements these requirements of the GLBA with respect to investment advisers registered with the Commission, brokers, dealers, and investment companies, which are the financial institutions subject to the Commission's jurisdiction under that Act.
2000	U.S. Congress Electronic Signatures in Global National ("ESIGN") Commerce Act of 2000		Pub. L. No. 106–229	The ESIGN Act is a landmark federal law in the United States. Passed in 2000, it granted legal recognition to electronic signatures and records in the USA based on the understanding that if all parties to a contract choose to use electronic documents and to sign them electronically, they are legal. The ESIGN Act (along with its precursor UETA) provided the legal foundation for use of electronic records and electronic signatures in commerce. It confirmed that electronic records and signatures carry the same weight and have the same legal effect as traditional paper documents and wet ink signatures.
2001	The U.S. Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001		Pub. L. No. 107-56	In a very short time after the September 11 terrorist attack, Congress passed the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" (USA PATRIOT Act) of 2001. The Act made several significant changes to the ECPA and FISA, among other statutes. In one amendment, the USA PATRIOT Act enlarged the definition of pen registers and trap and trace devices to apply to addressing information on emails and to "IP addresses." The Act also provided for new justifications for delayed notice of search warrants, increasing the types of subscriber records that could be obtained from ISPs and communications providers, and allowing for a nationwide scope for pen register orders and search warrants for email. The Act also provided for roving wiretaps under FISA as well as increased sharing of foreign intelligence information between law enforcement entities.
2002	Confidential Information Protection and Statistical Efficiency Act (CIPSEA) of 2002		44 U.S.C. § 101	CIPSEA establishes uniform confidentiality protections for information collected for statistical purposes by U.S. statistical agencies, and it allows some data sharing between the Bureau of Labor Statistics, Bureau of Economic Analysis, and Census Bureau. The agencies report to OMB on particular actions related to confidentiality and data sharing. The law give the agencies standardized approaches to protecting information from respondents so that it will not be exposed in ways that lead to inappropriate or surprising identification of the respondent. By default the respondent's data is used for statistical purposes only. If the respondent gives informed consent, the data can be put to some other use.
2002	Sarbanes-Oxley Act ("SOX") of 2002		15 U.S.C. ch. 2A, 98, et seq.	SOX protects shareholders and the general public from accounting errors and fraudulent practices of organizations. It was also tailored to improve the accuracy of corporate disclosures. SOX compliance has recently shifted to include cybersecurity.

2002	E-Government Act of 2002		44 U.S.C. § 3601, et seq.	Established procedures to ensure the privacy of personal information in electronic records. Section 208 of the E-Government Act of 2002 requires agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. PIAs must be made publicly available, unless the agency determines not to make the PIA publicly available if such publication would raise security concerns, reveal classified (i.e., national security), or reveal sensitive information (e.g., potentially damaging to a national interest, law enforcement effort, or competitive business interest).
2002	The Homeland Security Act of 2002		6 U.S.C. § 222, et seq.	In 2002, Congress passed the Homeland Security Act, which created the Department of Homeland Security (DHS), consisting of twenty-two federal agencies. The Act created a Privacy Office for ensuring compliance with privacy laws.
2002	Federal Information Security Management Act ("FISMA") of 2002		44 U.S.C. § 3551, et seq.	FISMA is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA assigns responsibilities to various agencies to ensure the security of data in the federal government. The act requires program officials, and the head of each agency, to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely and efficient manner.
2003	Do-Not-Call Implementation Act (National Do-Not-Call Registery) of 2003		15 U.S.C. ch. 87-87A, et seq.	In an effort to address unwanted telemarketing calls, the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) created a do-not-call registry. People can voluntarily register their telephone numbers, and commercial telemarketers are prohibited from calling the numbers. Telemarketers challenged the do-not-call registry as a violation of their First Amendment rights. In 2004, a federal circuit court concluded in *Mainstream Marketing Services, Inc. v. Federal Trade Commission* , 358 F.3d 1228 (10th Cir. 2004) that the do-not-call registry satisfied the *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York* , 447 U.S. 557 (1980) balancing test for commercial speech and therefore did not run afoul of the First Amendment.
2003	The CAN-SPAM Act of 2003		15 U.S.C. § 7701, et seq.	The Act establishes requirements for those who send unsolicited commercial email. The Act bans false or misleading header information and prohibits deceptive subject lines. It also requires that unsolicited commercial email be identified as advertising and provide recipients with a method for opting out of receiving any such email in the future. In addition, the Act directs the FTC to issue rules requiring the labeling of sexually explicit commercial email as such and establishing the criteria for determining the primary purpose of a commercial email.
2003	The Fair and Accurate Credit Transactions Act of 2003		Pub. L. No. 108-159	In 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACTA), which amended the Fair Credit Reporting Act and extended its preemption on certain state law provisions addressing identity theft and credit reporting. Among other things, the FACTA provided some limited protections against identity theft. For example, FACTA requires credit reporting agencies to provide people with a free credit report each year. It requires credit reporting agencies to disclose to a consumer her credit score, and it allows victims of fraud to alert just one credit reporting agency, which then must notify the others. These provisions and others were criticized by many as not going far enough to address the problem of identity theft.

2004	The Intelligence Reform and Terrorism Prevention Act of 2004		Pub. L. No. 108-458	In 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act to facilitate greater information sharing between federal agencies. The Act requires that intelligence be “provided in its most shareable form” and it aims to “promote a culture of information sharing.
2005	The Real ID Act of 2005		Pub. L. No. 109-13	Attached to a military spending bill, and passed without debate, the Real ID Act of 2005 mandated that state driver ’s licenses meet federal standards set forth by the DHS. Critics claimed that it would establish a de facto national identification card and that it would be extremely costly for the states to implement.
2006	U.S. SAFE WEB Act of 2006		15 U.S.C. §§ 45-58, et seq.	This Act, amending the FTC Act of 1914, provides the FTC with a number of tools to improve enforcement regarding consumer protection matters, particularly those with an international dimension, including increased cooperation with foreign law enforcement authorities through confidential information sharing and provision of investigative assistance. The Act also allows enhanced staff exchanges and other international cooperative efforts.
2007	Open Government Act of 2007		Public Law No. 110-175; 5 U.S.C. § 552, et seq.	Promotes accessibility, accountability, and openness in Government by strengthening 5 U.S.C. § 552 and codifies several provisions of Executive Order 13,392, "Improving Agency Disclosure of Information."
2007	The Freedom of Information Act (FOIA) of 2007		5 U.S.C. § 552, et seq.	Amended Freedom of Information Act (FOIA) of 1966. Provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that such records (or portions of them) are protected from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions.
2008	Genetic Information Nondiscrimination Act ("GINA") of 2008		15 U.S.C. §§ 2000ff - 2000ff(11), et seq.	GINA protects individuals against discrimination based on their genetic information in health coverage and in employment. GINA is divided into two sections, or Titles. Title I of GINA prohibits discrimination based on genetic information in health coverage. Title II of GINA prohibits discrimination based on genetic information in employment.
2009	Health Information Technology for Economic and Clinical Health Act ("HITECH Act")		42 C.F.R. parts 412, 413, 422, and 495, et seq.	Promotes the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.
		Access to systems and records.	42 C.F.R. § 495.346, et seq.	"The State agency must allow HHS access to all records and systems operated by the State in support of this program, including cost records associated with approved administrative funding and incentive payments to Medicaid providers. State records related to contractors employed for the purpose of assisting with implementation or oversight activities or providing assistance, at such intervals as are deemed necessary by the Department to determine whether the conditions for approval are being met and to determine the efficiency, economy, and effectiveness of the program."

		Combating fraud and abuse.	42 C.F.R. § 495.368, et seq.	"(a) General rule. (1) The State must comply with Federal requirements to— (i) Ensure the qualifications of the providers who request Medicaid EHR incentive payments; (ii) Detect improper payments; and (iii) In accordance with § 455.15 and § 455.21 of this chapter, refer suspected cases of fraud and abuse to the Medicaid Fraud Control Unit. (2) The State must take corrective action in the case of improper EHR payment incentives to Medicaid providers."
2010	Government Performance and Results Modernization (GPRM) Act of 2010 (Amends the Government Performance and Results Act of 1993)		Pub. L. No. 111-352 (Amends the Government Performance and Results Act of 1993)	Amends the Government Performance and Results Act of 1993 to require each executive agency to make its strategic plan available on its public website on the first Monday in February of any year following that in which the term of the President commences and to notify the President and Congress. Requires such plan to cover at least a four-year period and to include a description of how the agency is working with other agencies to achieve its goals and objectives, as well as relevant federal government priority goals. Requires the Director of the Office of Management and Budget (OMB) to coordinate with agencies to develop a federal government performance plan, which shall be submitted with the annual federal budget and concurrently made available on an OMB website of agency programs. Requires such plan to: (1) establish government performance goals for the current and next fiscal years; (2) identify activities, entities, and policies contributing to each goal; (3) identify a lead government official responsible for coordinating efforts to achieve the goal; (4) establish common federal government performance indicators with quarterly targets; (5) establish clearly defined quarterly milestones; and (6) identify major management
2014	Federal Information Security Modernization Act of 2014		44 U.S.C. § 3541, et seq.	This Act amends the Federal Information Security Management Act of 2002, 44 U.S.C. § 3541, and requires agencies to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of an agency.
2017	Social Security Number Fraud Prevention Act of 2017		Pub. L. No. 115-59	This Act: (1) prohibits federal agencies from including any individual's Social Security account number on any document sent by mail unless the agency head determines that such inclusion is necessary; and (2) requires agencies that have Chief Financial Officers to issue regulations, within five years of this bill's enactment, that specify the circumstances under which such inclusion is necessary.
2017	The Protecting Patient Access to Emergency Medications Act of 2017		21 U.S.C. § 823, et seq.	In 1970, the Controlled Substances Act (CSA) was created to regulate substances that have the potential to be abused. At the time, the CSA lacked instructions for the maintenance and use of these substances by emergency medical services (EMS). States, therefore, created their own EMS-related controlled substances requirements. In 2017, the Protecting Patient Access to Emergency Medications Act (PPAEMA) was introduced in the United States Congress to amend the CSA to include EMS requirements and end confusion among states and EMS agencies. The PPAEMA was signed into law on November 17, 2017.

2018	Defense Federal Acquisition Regulation Supplement ("DFARS")		48 C.F.R. § 201.104, et seq.	DFARS Safeguarding riles and clauses, for the basic safeguarding of contractor information systems that process, store or transmit Federal contract information. DFARS provides a set of “basic” security controls for contractor information systems upon which this information resides. These security controls must be implemented at both the contractor and subcontractor levels based on the information security guidance in NIST Special Publication 800-171 “Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations.”

FEDERAL AGENCY POLICIES

Date	Title	Subtitle	Reference	Information
1973	Organization of Economic Cooperation and Development (OECD) Fair Information Practices		U.S. Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Comm. On Automated Personal Data Systems 29 (1973)	The OCED Fair Information Practices were articulated by the United States Department of Health Education and Welfare (HEW) in 1973. HEW investigated the issues with increasing computerization of information and growing depositories of personal data. The report recommended the page of a code of Fair Information Practices, which were later codified in the Privacy Act of 1974. The recommended practices included the following: 1. There must be no personal data record-keeping systems whose very existence is secret. 2. There must be a way for an individual to find out what information about him is in a record and how it is used. 3. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent. 4. There must be a way for an individual to correct or amend a record of identifiable information about him. 5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

1980	Organization of Economic Cooperation and Development (OECD) Privacy Guidelines		Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available in Marc Rotenburg, Privacy Law Sourcebook (2002)	The OECD Privacy Guidelines built upon the Fair Information Practices articulated by the United States Department of Health Education and Welfare (HEW). The OECD Guidelines contain eight principles: (1) collection limitation—data should be collected lawfully with the individual's consent; (2) data quality—data should be relevant to a particular purpose and be accurate; (3) purpose specification—the purpose for data collection should be stated at the time of the data collection and the use of the data should be limited to this purpose; (4) use limitation—data should not be disclosed for different purposes without the consent of the individual; (5) security safeguards—data should be protected by reasonable safeguards; (6) openness principle—individuals should be informed about the practices and polices of those handling their personal information; (7) individual participation—people should be able to learn about the data that an entity possesses about them and to rectify errors or problems in that data; (8) accountability—the entities that control personal information should be held accountable for carrying out these principles.

Survey of Other States Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement
Alabama Breach Notification Law	Ala. Code § 8-38-5	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 people • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 10,000 residents or $500,000 • Credit Monitoring: No	$500,000 and $5,000 per day: Ala. Code § 8-38-9	Attorney General: Ala. Code § 8-38-9
Alabama Personal Information Protection Act	Ala. Code § 8-38-3	"Each covered entity and third-party agent shall implement and maintain reasonable security measures to protect sensitive personally identifying information against a breach of security."	Most likely, this would be considered a deceptive practice under Ala. Code § 8-19-5.	None
Alabama Unfair, Deceptive, or Abusive Acts and Practices	Ala. Code § 8-19-5	"The following deceptive acts or practices in the conduct of any trade or commerce are hereby declared to be unlawful: . . . (27) Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce."	Up to $2,000 per violation: Ala. Code § 8-19-11	Attorney General: Ala. Code § 8-19-4
Alaska Breach Notification Law	Alaska Stat. § 45.48.010	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if not disclosing to residents • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Unclear • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 300,000 residents or $150,000 • Credit Monitoring: No	Up to $50,000: Alaska Stat. § 45.48.080(b)(1)	Attorney General: Alaska Stat. § 44.23.020(b)(4)
Alaska Personal Information Protection Act	Alaska Stat. § 45.48.430	"A person doing business, including the business of government, may not disclose an individual's social security number to a third party."	Up to $3,000: Alaska Stat. § 45.48.480	Attorney General: Alaska Stat. § 44.23.020(b)(4)
Alaska Unfair, Deceptive, or Abusive Acts and Practices	Alaska Stat. § 45.50.471	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce are declared to be unlawful."	Between $1,000 and $25,000 per violation: Alaska Stat. § 45.50.537	Attorney General: Alaska Stat. § 45.50.501
Arizona Breach Notification Law	Ariz. Rev. Stat. § 18-545	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 100,000 people or $50,000 • Credit Monitoring: No	$10,000 per breach: Ariz. Rev. Stat. § 18-545(H)	Attorney General: Ariz. Rev. Stat. § 18-545(H)
Arizona Unfair, Deceptive, or Abusive Acts and Practices	Rev. Stat. § 44-1522	"The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice."	Up to $10,000 per violation: Ariz. Rev. Stat. § 44-1531	Attorney General: Ariz. Rev. Stat. § 44-1524
Arkansas Breach Notification Law	Ark. Code § 4-110-105	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 500,000 residents or $250,000 • Credit Monitoring: No •	Up to $10,000 per violation: Ark. Code §§ 4-110-108; 4-88-113	Attorney General: Ark. Code Ark. Code §§ 4-110-108;§ 4-88-104

Arkansas Personal Information Protection Act	Ark. Code § 4-110-104(b)	"A person or business that acquires, owns, or licenses personal information about an Arkansas resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure"	Up to $10,000 per violation: Ark. Code §§ 4-110-108; 4-88-113	Attorney General: Ark. Code Ark. Code §§ 4-110-108;§ 4-88-104
Arkansas Unfair, Deceptive, or Abusive Acts and Practices	Ark. Code § 4-88-108	"When utilized in connection with the sale or advertisement of any goods, services, or charitable solicitation, the following shall be unlawful: (1) The act, use, or employment by any person of any deception, fraud, or false pretense; or (2) The concealment, suppression, or omission of any material fact with intent that others rely upon the concealment, suppression, or omission."	Up to $10,000 per violation: Ark. Code § 4-88-113	Attorney General: Ark. Code § 4-88-104
California Breach Notification Law	Cal. Civ. Code § 1798.82	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: • Credit Monitoring: • Other:	Up to $3,000 per transaction: Cal. Civ. Code § 1798.84	Private right of action: Cal. Civ. Code § 1798.84
California Personal Information Protection Act	Cal. Civ. Code § 1798.81.5	"A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."	Up to $3,000 per transaction: Cal. Civ. Code § 1798.84	Private right of action: Cal. Civ. Code § 1798.84
California Unfair, Deceptive, or Abusive Acts and Practices	Cal. Bus. & Prof. Code § 17200	"As used in this chapter, unfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by Chapter 1 (commencing with Section 17500) of Part 3 of Division 7 of the Business and Professions Code."	$2,500 per violation: Cal. Bus. & Prof. Code § 17206	Attorney General: Cal. Bus. & Prof. Code § 17206
Colorado Breach Notification Law	Colo. Rev. Stat. § 6-1-716	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 250,000 residents or $250,000 • Credit Monitoring: No	"The attorney general may bring an action in law or equity to address violations of this section and for other relief that may be appropriate to ensure compliance with this section or to recover direct economic damages resulting from a violation, or both. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law." Colo. Rev. Stat. § 6-1-716(4)	Attorney General: Colo. Rev. Stat. § 6-1-716(4)
Colorado Unfair, Deceptive, or Abusive Acts and Practices	Colo. Rev. Stat. § 6-1-105	"A person engages in a deceptive trade practice when, in the course of the person's business, vocation, or occupation, the person:"	Up to $2,000 per violation: Colo. Rev. Stat. § 6-1-112	Attorney General: Colo. Rev. Stat. § 6-1-103.
Connecticut Breach Notification Law	Conn. Gen. Stat. § 36a-701b	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 500,000 residents or $250,000 • Credit Monitoring: Yes, 12 months • Other:	Up to $5,000 per violation: Conn. Gen. Stat. §§ 36a-701b(g), 42-110o	Attorney General: Conn. Gen. Stat. §§ 36a-701b(g), 42-110o

Connecticut Personal Information Protection Act	Conn. Gen. Stat. § 42-471	"Any person who collects Social Security numbers in the course of business shall create a privacy protection policy which shall be published or publicly displayed. For purposes of this subsection, "publicly displayed" includes, but is not limited to, posting on an Internet web page. Such policy shall: (1) Protect the confidentiality of Social Security numbers, (2) prohibit unlawful disclosure of Social Security numbers, and (3) limit access to Social Security numbers."	Up to $5,000 per violation: Conn. Gen. Stat. §§ 42-471(h), 36a-701b(g), 42-110o,	Attorney General: Conn. Gen. Stat. §§ 42-471(h), 36a-701b(g), 42-110o,
Connecticut Unfair, Deceptive, or Abusive Acts and Practices	Conn. Gen. Stat. § 42-110b	"No person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."	Up to $5,000 per violation: Conn. Gen. Stat. § 42-110o	Attorney General: Conn. Gen. Stat. § 42-110o
Delaware Breach Notification Law	Del. Code tit. 6, § 12B-102	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 500 residents • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay, but no more than 60 days • Substitute Notice: Yes, if over 100,000 residents or $75,000 • Credit Monitoring: Yes, if SSN breached, 12 months • Other:	"an action in law or equity to address the violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both." 6 Del. C. § 12B-104	Director of Consumer Protection of the Department of Justice: 6 Del. C. § 12B-104
Delaware Personal Information Protection Act	Del. Code tit. 6, § 12B-100	"Any person who conducts business in this State and owns, licenses, or maintains personal information shall implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business."	"an action in law or equity to address the violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both." 6 Del. C. § 12B-104	Director of Consumer Protection of the Department of Justice: 6 Del. C. § 12B-104
Delaware Unfair, Deceptive, or Abusive Acts and Practices	Del. Code tit. 6, § 2532	"A person engages in a deceptive trade practice when, in the course of a business, vocation, or occupation, that person:. . ."	Up to $10,000 per willful violation: Del. Code tit. 6, § 2533	Attorney General: Del. Code tit. 6, § 2533
Florida Breach Notification Law	Fla. Stat. § 501.171(4)(a)	• Notify Affected Residents: Yes • Notify Department of Legal Affairs: Yes, if over 500 • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 500,000 residents or $250,000 • Credit Monitoring: • Other:	Up to $500,000 and more penalties: Fla. Stat. § 501.171(9)	Department of Legal Affairs: Fla. Stat. § 501.171(9)
Personal Information Protection Act	Fla. Stat. § 501.171(2)	"Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information."	Up to $500,000 and more penalties: Fla. Stat. § 501.171(9)	Department of Legal Affairs: Fla. Stat. § 501.171(9)
Unfair, Deceptive, or Abusive Acts and Practices	Fla. Stat. § 501.204	"Unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful"	Up to $10,000 per violation: Fla. Stat. § 501.2075	Department of Legal Affairs: Fla. Stat. § 501.2075
Georgia Breach Notification Law	Ga. Code § 10-1-912	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 10,000 residents • If not data owner, notify data owner: Yes, within 24 hours • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 100,000 residents or $50,000 • Credit Monitoring: No	None	None
Unfair, Deceptive, or Abusive Acts and Practices	Ga. Code § 10-1-393	"Unfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce are declared unlawful."	Up to $5,000 per violation: Ga. Code § 10-1-397(a)(2)(B)	Attorney General: Ga. Code § 10-1-397

Hawaii Breach Notification Law	Haw. Rev. Stat. § 487N-2	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 200,000 residents or $100,000 • Credit Monitoring: No	Up to $2,500 per violation: Haw. Rev. Stat. § 487N-3	Attorney General: Haw. Rev. Stat. § 487N-3
Unfair, Deceptive, or Abusive Acts and Practices	Haw. Rev. Stat. § 480-2	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are unlawful."	Up to $10,000 per violation: Haw. Rev. Stat. § 480-3.1	Attorney General or Director of the Office of Consumer Protections: :Haw. Rev. Stat. § 480-3.1
Idaho Breach Notification Law	Idaho Code § 28-51-105	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 50,000 residents or $25,000 • Credit Monitoring: No	Up to $25,000 per breach: Idaho Code § 28-51-107	Attorney General: Idaho Code § 28-51-107
Unfair, Deceptive, or Abusive Acts and Practices	Idaho Code § 48-603	"The following unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared to be unlawful, where a person knows, or in the exercise of due care should know, that he has in the past, or is:"	Up to $10,000 per violation: Idaho Code § 48-606(1)(e)	Attorney General: Idaho Code § 48-606
Illinois Breach Notification Law	815 Ill. Comp. Stat. § 530/10	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	Up to $50,000: 815 ILCS §§ 530/20; 505/7	Attorney General: 815 ILCS §§ 530/20; 505/7
Personal Information Protection Act	815 Ill. Comp. Stat. § 530/45	"A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."	Up to $50,000: 815 ILCS §§ 530/20; 505/7	Attorney General: 815 ILCS §§ 530/20; 505/7
Unfair, Deceptive, or Abusive Acts and Practices	815 Ill. Comp. Stat. § 505/2	"Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in Section 2 of the "Uniform Deceptive Trade Practices Act", approved August 5, 1965,1 in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby. In construing this section consideration shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a) of the Federal Trade Commission Act.2"	Up to $50,000: 815 Ill. Comp. Stat. § 505/7	Attorney General: 815 Ill. Comp. Stat. § 505/7
Iowa Breach Notification Law	Iowa Code § 715C.2	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 500 residents • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 350,000 residents or $250,000 • Credit Monitoring: No	Up to $40,000 per violation: Iowa Code §§ 715C.2(9), 714.16(7)	Attorney General: Iowa Code §§ 715C.2(9), 714.16(7)

Unfair, Deceptive, or Abusive Acts and Practices	Iowa Code § 714.16	"The act, use or employment by a person of an unfair practice, deception, fraud, false pretense, false promise, or misrepresentation, or the concealment, suppression, or omission of a material fact with intent that others rely upon the concealment, suppression, or omission, in connection with the lease, sale, or advertisement of any merchandise or the solicitation of contributions for charitable purposes, whether or not a person has in fact been misled, deceived, or damaged, is an unlawful practice."	Up to $40,000 per violation: Iowa Code § 714.16(7)	Attorney General: Iowa Code § 714.16(7)
Kansas Breach Notification Law	Kan. Stat. § 50-7a02	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 5,000 residents or $100,000 • Credit Monitoring: No	"an action in law or equity to address violations of this section and for other relief that may be appropriate": Kan. Stat. § 50-7a02(g)	Attorney General: Kan. Stat. § 50-7a02(g)
Personal Information Protection Act	Kan. Stat. § 50-6,139b(b)(1)	" A holder of personal information shall: (1) Implement and maintain reasonable procedures and practices appropriate to the nature of the information, and exercise reasonable care to protect the personal information from unauthorized access, use, modification or disclosure. If federal or state law or regulation governs the procedures and practices of the holder of personal information for such protection of personal information, then compliance with such federal or state law or regulation shall be deemed compliance with this paragraph and failure to comply with such federal or state law or regulation shall be prima facie evidence of a violation of this paragraph; . . ."	Up to $10,000 per violation or $20,000 per willful violation: Kan. Stat. §§ 50-6139b(d, e), 50-636	Attorney General: Kan. Stat. § 50-636
Unfair, Deceptive, or Abusive Acts and Practices	Kan. Stat. § 50-626	"No supplier shall engage in any deceptive act or practice in connection with a consumer transaction."	Up to $10,000 per violation or $20,000 per willful violation: Kan. Stat. § 50-636	Attorney General: Kan. Stat. § 50-636
Kentucky Breach Notification Law	Ky. Rev. Stat. § 365.732	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 500,000 residents or $250,000 • Credit Monitoring: • Other:	None	Private Right of Action: Ky. Rev. Stat. § 365.730
Unfair, Deceptive, or Abusive Acts and Practices	Ky. Rev. Stat. § 367.170	"Unfair, false, misleading, or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $2,000 per violation: Ky. Rev. Stat. § 367.990(2)	Attorney General: Ky. Rev. Stat. § 367.990(2)
Louisiana Breach Notification Law	La. Rev. Stat. § 51:3074	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 50,000 residents or $250,000 • Credit Monitoring: No • Other:	"a fine not to exceed $5,000 per violation. Notice to the attorney general shall be timely if received within 10 days of distribution of notice to Louisiana citizens. Each day notice is not received by the attorney general shall be deemed a separate violation." 16 La. Admin. Code Pt III, 701	Attorney General: 16 La. Admin. Code Pt III, 701
Unfair, Deceptive, or Abusive Acts and Practices	La. Stat. § 51:1405	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $5,000 per violation: La. Rev. Stat. § 51:1407(B)	Attorney General: La. Rev. Stat. § 51:1407(A)

Maine Breach Notification Law	Me. Rev. Stat. tit. 10 § 1348	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 1,000 people or $5,000 • Credit Monitoring: No	"[M]aximum of $2,500 for each day the person is in violation:" Me. Rev. Stat. tit. 10 § 1349	Attorney General: Me. Rev. Stat. tit. 10 § 1349
Unfair, Deceptive, or Abusive Acts and Practices	Me. Rev. Stat. tit. 5 § 207	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are declared unlawful."	$5,000 penalty for non-compliance with § 211: Me. Rev. Stat. tit. 5 § 212	Attorney General: Me. Rev. Stat. tit. 5 § 212
Maryland Breach Notification Law	Md. Code, Com. Law § 14-3504	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, over 1000 • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay and several day requirements • Substitute Notice: Yes, if over 175,000 residents or $100,000 • Credit Monitoring: No • Other:	$1,000 per violation: Md. Code, Com. Law §§ 14-3508, 13-410	Division of Consumer Protection: Md. Code Comm . Law §§ 13-403 and 13-410
Personal Information Protection Act	Md. Code, Com. Law § 14-3503	"To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations."	$1,000 per violation: Md. Code, Com. Law §§ 14-3508, 13-410	Division of Consumer Protection: Md. Code Comm . Law §§ 13-403 and 13-410
Unfair, Deceptive, or Abusive Acts and Practices	Md. Code Comm . Law §13-303	"A person may not engage in any unfair or deceptive trade practice, as defined in this subtitle or as further defined by the Division, in:. . ."	$1,000 per violation: Md. Code, Com. Law § 13-410	Division of Consumer Protection: Md. Code Comm . Law §§ 13-403 and 13-410
Massachusetts Breach Notification Law	Mass. Gen. Laws Ch. 93H § 1	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Attorney General • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,00 residents or $250,000 • Credit Monitoring: 2 years	Up to $5,000 per violation: Mass. Gen. Laws Ch. 93A § 4	Attorney General: Mass. Gen. Laws § 93H § 1
Unfair, Deceptive, or Abusive Acts and Practices	Mass. Gen. Laws Ch. 93A § 2	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $5,000 per violation: Mass. Gen. Laws Ch. 93A § 4	Attorney General: Mass. Gen. Laws Ch. 93A § 4
Michigan Breach Notification Law	Mich. Comp. Laws § 445.72	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	$250 per notice failure, or up to $750,000 per breach: Mich. Comp. Laws § 445.72(13)	Attorney General: Mich. Comp. Laws § 445.72(13)
Unfair, Deceptive, or Abusive Acts and Practices	Mich. Comp. Laws § 445.903	"Unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce are unlawful and are defined as follows:. . ."	Up to $25,000: Mich. Comp. Laws § 445.905	Attorney General: Mich. Comp. Laws § 445.905

Minnesota Breach Notification Law	Minn. Stat. § 325E.61,	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 500 residents. Notification in 48 hours. • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	Unclear: Minn. Stat. §§ 325E.61(6), 8.31	Attorney General: Minn. Stat. §§ 325E.61(6), 8.31
Unfair, Deceptive, or Abusive Acts and Practices	Minn. Stat. § 325F.69	"Fraud, misrepresentation, deceptive practices. The act, use, or employment by any person of any fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the intent that others rely thereon in connection with the sale of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby, is enjoinable as provided in section 325F.70."	Unclear: Minn. Stat. § 8.31	Attorney General: Minn. Stat. § 8.31
Mississippi Breach Notification Law	Miss. Code § 75-24-29	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 5,000 residents or $5,000 • Credit Monitoring: • Other:	$10,000 per violation: Miss. Code § 75-24-19	Attorney General: Miss. Code § 75-24-29(8)
Unfair, Deceptive, or Abusive Acts and Practices	Miss. Code § 75-24-5	"Unfair methods of competition affecting commerce and unfair or deceptive trade practices in or affecting commerce are prohibited. Action may be brought under Section 75-24-5(1) only under the provisions of Section 75-24-9."	$10,000 per violation: Miss. Code § 75-24-19	Attorney General: Miss. Code § 75-24-9
Missouri Breach Notification Law	Mo. Rev. Stat. § 407.1500	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 150,000 residents or $150,000 • Credit Monitoring: • Other:	Up to $150,000: Mo. Rev. Stat. § 407.1500(3)	Attorney General: Mo. Rev. Stat. § 407.1500(3)
Unfair, Deceptive, or Abusive Acts and Practices	Mo. Rev. Stat. § 407.020	"he act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce or the solicitation of any funds for any charitable purpose, as defined in section 407.453, in or from the state of Missouri, is declared to be an unlawful practice."	Up to $1000 per violation: Mo. Rev. Stat. § 407.100(6)	Attorney General: Mo. Rev. Stat. § 407.100
Montana Breach Notification Law	Mont. Code § 30-14-1704	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, coordination provision • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: • Other:	Up to $10,000 per willful violation: Mont. Code §§ 30-14-1705; 30-14-142(2)	Department of Justice (Attorney General): Mont. Code § 30-14-1705
Unfair, Deceptive, or Abusive Acts and Practices	Mont. Code § 30-14-103	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are unlawful."	Up to $10,000 per willful violation: Mont. Code § 30-14-142(2)	Department of Justice (Attorney General): Mont. Code § 30-14-1705

Nebraska Breach Notification Law	Nebraska Neb. Rev. Stat. § 87-803	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 residents or $75,000 • Credit Monitoring: No	Direct economic damage: Neb. Rev. Stat. § 87-806	Attorney General: Neb. Rev. Stat. § 87-806
Unfair, Deceptive, or Abusive Acts and Practices	Neb. Rev. Stat. § 59-1602	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce shall be unlawful."	Up to $2,000 per violation: Neb. Rev. Stat. § 59-1614	Attorney General: Neb. Rev. Stat. § 59-1614
Nevada Breach Notification Law	Nev. Rev. Stat. § 603A.220	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	Injunction: Nev. Rev. Stat. § 603A.290	Attorney General: Nev. Rev. Stat. § 603A.290
Personal Information Protection Act	Nev. Rev. Stat. § 603A.210	"A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."	Injunction: Nev. Rev. Stat. § 603A.290	Attorney General: Nev. Rev. Stat. § 603A.290
Unfair, Deceptive, or Abusive Acts and Practices	Neb. Rev. Stat. § 59-1602	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce shall be unlawful."	Up to $2,000 per violation: Neb. Rev. Stat. § 59-1614	Attorney General: Neb. Rev. Stat. § 59-1608
New Hampshire Breach Notification Law	N.H. Rev. Stat. § 359-C:20	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if subject to N.H. Rev. Stat. § 358-A:3(I) • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: As soon as possible • Substitute Notice: Yes, if over 1,000 residents or $5,000 • Credit Monitoring: No	Up to $10,000 per violation: N.H. Rev. Stat. §§ 359-C:20; 358-A:4(III)(b)	Attorney General: N.H. Rev. Stat. §§ 359-C:20; 358-A:4
Unfair, Deceptive, or Abusive Acts and Practices	N.H. Rev. Stat. § 358-A:2	"It shall be unlawful for any person to use any unfair method of competition or any unfair or deceptive act or practice in the conduct of any trade or commerce within this state. Such unfair method of competition or unfair or deceptive act or practice shall include, but is not limited to, the following:"	Up to $10,000 per violation: N.H. Rev. Stat. § 358-A:4(III)(b)	Consumer Protection and Antitrust Bureau, Department of Justice: N.H. Rev. Stat. § 358-A:4
New Jersey Breach Notification Law	N.J. Stat. § 56:8-163	• Notify Affected Residents: Yes • Notify Attorney General: Yes, prior to notification to customers • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No • Other:	Up to $10,000 for the first offense, and $20,000 for subsequent offenses: N.J. Stat. § 56:8-13	Attorney General: N.J. Stat. § 56:8-3.1

Unfair, Deceptive, or Abusive Acts and Practices	N.J. Stat. § 56:8-2	"The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice; provided, however, that nothing herein contained shall apply to the owner or publisher of newspapers, magazines, publications or printed matter wherein such advertisement appears, or to the owner or operator of a radio or television station which disseminates such advertisement when the owner, publisher, or operator has no knowledge of the intent, design or purpose of the advertiser."	Up to $10,000 for the first offense, and $20,000 for subsequent offenses: N.J. Stat. § 56:8-13	Attorney General: N.J. Stat. § 56:8-3.1
New Mexico Breach Notification Law	N.M. Stat. § 57-12c-6	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: No later than 45 days after the breach discovery date • Substitute Notice: Yes, if over 50,000 residents or $100,000 • Credit Monitoring: No	Up to $150,000: N.M. Stat. § 57-12c-11	Attorney General: N.M. Stat. § 57-12c-11
Personal Information Protection Act	N.M. Stat. § 57-12c-4	"A person that owns or licenses personal identifying information of a New Mexico resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal identifying information from unauthorized access, destruction, use, modification or disclosure."	Up to $25,000: N.M. Stat. § 57-12c-11	Attorney General: N.M. Stat. § 57-12c-11
Unfair, Deceptive, or Abusive Acts and Practices	N.M. Stat. § 57-12-3	"Unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce are unlawful."	Up to $5,000 per violation: N.M. Stat. § 57-12-11	Attorney General: N.M. Stat. § 57-12-11
New York Breach Notification Law	N.Y. Gen. Bus. Law § 899-AA, N.Y. State Tech. Law 208	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 5000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	Up to $150,000: N.Y. Gen. Bus. Law § 899-AA(6)	Attorney General: N.Y. Gen. Bus. Law § 899-AA(6)
Unfair, Deceptive, or Abusive Acts and Practices	N.Y. Gen. Bus. Law § 349	"Deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."	Up to $5,000 per violation: N.Y. Gen. Bus. Law § 350-d	Attorney General: N.Y. Gen. Bus. Law § 349(f)
North Carolina Breach Notification Law	N.C. Gen. Stat § 75-65	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 or $250,000 • Credit Monitoring: No • Other:	Up to $5,000 per violation: N.C. Gen. Stat. §§ 75-65(i), 75-15.2	Attorney General: N.C. Gen. Stat. §§ 75-65(i), 75-15
Unfair, Deceptive, or Abusive Acts and Practices	N.C. Gen. Stat. § 75-1.1	"Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful."	Up to $5,000 per violation: N.C. Gen. Stat. § 75-15.2	Attorney General: N.C. Gen. Stat. § 75-15

North Dakota Breach Notification Law	N.D. Cent. Code § 51-30-02	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 250 people • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 or $250,000 • Credit Monitoring: No	Up to $5,000 per violation: N.D. Cent. Code §§ 51-30-07, 51-15-11	Attorney General: N.D. Cent. Code § 51-30-07
Unfair, Deceptive, or Abusive Acts and Practices	N.D. Century Code § 51-15-02	"The act, use, or employment by any person of any deceptive act or practice, fraud, false pretense, false promise, or misrepresentation, with the intent that others rely thereon in connection with the sale or advertisement of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby, is declared to be an unlawful practice. The act, use, or employment by any person of any act or practice, in connection with the sale or advertisement of any merchandise, which is unconscionable or which causes or is likely to cause substantial injury to a person which is not reasonably avoidable by the injured person and not outweighed by countervailing benefits to consumers or to competition, is declared to be an unlawful practice."	Up to $5,000 per violation: N.D. Cent. Code § 51-15-11	Attorney General: N.D. Cent. Code § 51-15-07
Ohio Breach Notification Law	Ohio Rev. Code § 1349.19	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: No longer than 45 days following the breach discovery date • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No • Other: Substitute notice exception for small businesses.	Cascading penalties based on delay: Ohio Rev. Code § 1349.192	Attorney General: Ohio Rev. Code § 1349.19(i)
Unfair, Deceptive, or Abusive Acts and Practices	Ohio Rev. Code § 1345.02	"No supplier shall commit an unfair or deceptive act or practice in connection with a consumer transaction. Such an unfair or deceptive act or practice by a supplier violates this section whether it occurs before, during, or after the transaction."	Up to $25,000: Ohio Rev. Code § 1345.07	Attorney General: Ohio Rev. Code § 1345.02(E)(3)
Oklahoma Breach Notification Law	Okla. Stat. tit. 24, § 163	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 residents or $50,000 • Credit Monitoring: No	Up to $150,000: Okla. Stat. § 24-165	Attorney General: Okla. Stat. § 24-165
Unfair, Deceptive, or Abusive Acts and Practices	Okla. Stat. tit. 15, § 753	"A person engages in a practice which is declared to be unlawful under the Oklahoma Consumer Protection Act when, in the course of the person's business, the person . . ."	Up to $2,000 per violation or up to $10,000 per willful violation: Okla. Stat. tit. 15, § 761.1	Attorney General: Okla. Stat. tit. 15, § 761.
Oregon Breach Notification Law	Oregon Rev. Stat. § 646A.604	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 250 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 350,000 residents and $250,000 • Credit Monitoring: Yes	Or. Rev. Stat. §§ 646A.604(9)(a), 646.642(3)	Director of the Department of Consumer and Business Services: Or. Rev. Stat. § 646A.624
Personal Information Protection Act	Or. Rev. Stat. § 646A.622	"A person that owns, maintains or otherwise possesses, or has control over or access to, data that includes personal information that the person uses in the course of the person's business, vocation, occupation or volunteer activities shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including safeguards that protect the personal information when the person disposes of the personal information."	Up to $1000 per violation: Or. Rev. Stat. § 646A.624	Director of the Department of Consumer and Business Services: Or. Rev. Stat. § 646A.624

Unfair, Deceptive, or Abusive Acts and Practices	Or. Rev. Stat. § 646.607	"A person engages in an unlawful trade practice if in the course of the person's business, vocation or occupation the person. . ."	Up to $250,000 per violation: Or. Rev. Stat. § 646.642(3)	Prosecuting attorney: Or. Rev. Stat. § 646.642(3)
Pennsylvania Breach Notification Law	73 Pa. Stat. § 2303	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 175,000 people or $100,000 • Credit Monitoring: No	Up to $1,000 per violation: 73 Pa. Stat. §§ 2308, 201-8	Attorney General: 73 Pa. Stat. § 2308
Unfair, Deceptive, or Abusive Acts and Practices	73 Pa. Stat. § 201-3	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce as defined by subclauses (i) through (xxi) of clause (4) of section 21 of this act and regulations promulgated under section 3.12 of this act are hereby declared unlawful. The provisions of this act shall not apply to any owner, agent or employee of any radio or television station, or to any owner, publisher, printer, agent or employee of an Internet service provider or a newspaper or other publication, periodical or circular, who, in good faith and without knowledge of the falsity or deceptive character thereof, publishes, causes to be published or takes part in the publication of such advertisement."	Up to $1,000 per violation: 73 Pa. Stat. § 201-8	Attorney General: 73 Pa. Stat. § 201-8
Rhode Island Breach Notification Law	R.I. Gen. Laws § 11-49.3-4	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over • Credit Monitoring: • Other:	$100 per reckless violation, $200 per knowing/willful violation: R.I. Gen. Laws § 11-49.3-5	Attorney General: R.I. Gen. Laws § 11-49.3-5
Personal Information Protection Act	R.I. Gen. Laws § 11-49.3-2	"A municipal agency, state agency or person that stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about a Rhode Island resident shall implement and maintain a risk-based information security program that contains reasonable security procedures and practices appropriate to the size and scope of the organization; the nature of the information; and the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction, or disclosure and to preserve the confidentiality, integrity, and availability of such information. A municipal agency, state agency, or person shall not retain personal information for a period longer than is reasonably required to provide the services requested; to meet the purpose for which it was collected; or in accordance with a written retention policy or as may be required by law. A municipal agency, state agency, or person shall destroy all personal information, regardless of the medium that such information is in, in a secure manner, including, but not limited to, shredding, pulverization, incineration, or erasure."	$100 per reckless violation, $200 per knowing/willful violation: R.I. Gen. Laws § 11-49.3-5	Attorney General: R.I. Gen. Laws § 11-49.3-5
Unfair, Deceptive, or Abusive Acts and Practices	R.I. Gen. Laws § 6-13.1-2	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are declared unlawful."	Up to $10,000 per violation: R.I. Gen. Laws § 6-13.1-8	Attorney General: R.I. Gen. Laws § 6-13.1-8
South Carolina Breach Notification Law	S.C. Code § 39-1-90	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over • Credit Monitoring: • Other:	$1,000 per resident for knowing or willful violation: S.C. Code § 39-1-90(H)	Attorney General: S.C. Code § 39-1-90(H)
Unfair, Deceptive, or Abusive Acts and Practices	S.C. Code § 39-5-20	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $5,000 per violation: S.C. Code § 39-5-110	Attorney General: S.C. Code § 39-5-110

South Dakota Breach Notification Law	SD SB62	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 250 residents • Notify Credit Reporting Agencies: Yes • If not data owner, notify data owner: Yes • How many days to Notify: Within 60 days of breach discovery date. • Substitute Notice: Yes, if over 500,000 people or $250,000 • Credit Monitoring: • Other:	Enacted on 3/21/2018, effective July 1, 2018	http://sdlegislature.gov/docs/legsession/2018/Bills/SB62ENR.pdf
Unfair, Deceptive, or Abusive Acts and Practices	S.D. Codified Laws § 37-24-6	"It is a deceptive act or practice for any person to: (1) Knowingly act, use, or employ any deceptive act or practice, fraud, false pretense, false promises, or misrepresentation or to conceal, suppress, or omit any material fact in connection with the sale or advertisement of any merchandise, regardless of whether any person has in fact been misled, deceived, or damaged thereby. . . "	Up to $2,000 per violation: S.D. Codified Laws § 37-24-27	Attorney General: S.D. Codified Laws § 37-24-23
Tennessee Breach Notification Law	Tenn. Code § 47-18-2107	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes, within 45 of breach discovery date • How many days to Notify: Within 45 of breach discovery date • Substitute Notice: Yes, if over 500,000 people or $250,000 • Credit Monitoring: No	"civil penalty of whichever of the following is greater: ten thousand dollars ($10,000), five thousand dollars ($5,000) per day for each day that a person's identity has been assumed or ten (10) times the amount obtained or attempted to be obtained by the person using the identity theft.": Tenn. Code § 47-18-2105	Division of Consumer Affairs of the Department of Commerce and Insurance: Tenn. Code § 47-18-2105
Personal Information Protection Act	Tenn. Code § 47-18-2110	"On and after January 1, 2008, any person, nonprofit or for profit business entity in this state, including, but not limited to, any sole proprietorship, partnership, limited liability company, or corporation, engaged in any business, including, but not limited to, health care, that has obtained a federal social security number for a legitimate business or governmental purpose shall make reasonable efforts to protect that social security number from disclosure to the public."	"civil penalty of whichever of the following is greater: ten thousand dollars ($10,000), five thousand dollars ($5,000) per day for each day that a person's identity has been assumed or ten (10) times the amount obtained or attempted to be obtained by the person using the identity theft.": Tenn. Code § 47-18-2105	Division of Consumer Affairs of the Department of Commerce and Insurance: Tenn. Code § 47-18-2105
Unfair, Deceptive, or Abusive Acts and Practices	Tenn. Code § 47-18-104	The following unfair or deceptive acts or practices affecting the conduct of any trade or commerce are declared to be unlawful and in violation of this part:	Up to $1,000 per violation: Tenn. Code § 47-18-108(b)(3)	Division of Consumer Affairs of the Department of Commerce and Insurance: Tenn. Code § 47-18-108
Texas Breach Notification Law	Tex. Bus. & Com. Code § 521.053	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 10,000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 500,000 people or $250,000 • Credit Monitoring: No	Between $2,000 and $50,000 per violation and up to $150,000 in additional penalties: Tex. Bus. & Com. Code § 521.151	Attorney General: Tex. Bus. & Com. Code § 521.151
Personal Information Protection Act	Tex. Bus. & Com. Code § 521.052	"A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business."	Between $2,000 and $50,000 per violation: Tex. Bus. & Com. Code § 521.151	Attorney General: Tex. Bus. & Com. Code § 521.151
Unfair, Deceptive, or Abusive Acts and Practices	Tex. Bus. & Com. Code § 17.45	"False, misleading, or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful and are subject to action by the consumer protection division. . ."	Up to $20,000 per violation: Tex. Bus. & Com. Code § 17.47	Consumer Protection Division, Attorney General: Tex. Bus. & Com. Code § 17.47

Utah Breach Notification Law	Utah Code § 13-44-202	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Not allowed • Credit Monitoring: No	Up to $100,000: Utah Code § 13-44-301	Attorney General: Utah Code § 13-44-301
Personal Information Protection Act	Utah Code § 13-44-201	"Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to: (a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and (b) destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person."	Up to $100,000: Utah Code § 13-44-301	Attorney General: Utah Code § 13-44-301
Unfair, Deceptive, or Abusive Acts and Practices	Utah Code § 13-11-5	"An unconscionable act or practice by a supplier in connection with a consumer transaction violates this act1 whether it occurs before, during, or after the transaction."	Up to $2,500 per violation (administrative fine): Utah Code § 13-11-17	Division of Consumer Protections: Utah Code § 13-11-17
Vermont Breach Notification Law	Vt. Stat. tit. 9 § 2435	• Notify Affected Residents: Yes • Notify Attorney General: Yes, within 14 business days of breach discovery • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 5,000 residents or $5,000 • Credit Monitoring: • Other:	Unclear from statute	Attorney General: Vt. Stat. tit. 9 § 2435(g)
Unfair, Deceptive, or Abusive Acts and Practices	Vt. Stat. tit. 9, § 2453	"Unfair methods of competition in commerce and unfair or deceptive acts or practices in commerce are hereby declared unlawful."	Up to $10,000 per violation: Vt. Stat. tit. 9, § 2461	Attorney General: Vt. Stat. tit. 9, § 2461
Virginia Breach Notification Law	Va. Code § 18.2-186.6	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 residents or $50,000 • Credit Monitoring: • Other: Special provisions for income tax data	Up to $150,000 per breach: Va. Code § 18.2-186.6(I)	Attorney General: Va. Code § 18.2-186.6(I)
Unfair, Deceptive, or Abusive Acts and Practices	Va. Code § 59.1-200	"The following fraudulent acts or practices committed by a supplier in connection with a consumer transaction are hereby declared unlawful . . ."	Up to $2,500 per violation: Va. Code § 59.1-206	Attorney General: Va. Code § 59.1-206
Washington Breach Notification Law	Wash. Rev. Code § 19.255.010	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 500 residents • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: No more than 45 days after the breach discovery • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: • Other: Reimbursement from businesses to financial institutions provision	Up to $25,000: Wash. Rev. Code §§ 19.255.010(17), 19.86.140	Attorney General: Wash. Rev. Code § 19.255.010(17)
Unfair, Deceptive, or Abusive Acts and Practices	Wash. Rev. Code § 19.86.020	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $25,000: Wash. Rev. Code § 19.86.140	Attorney General: Wash. Rev. Code § 19.86.080

West Virginia Breach Notification Law	W.Va. Code § 46A-2A-102	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 residents or $50,000 • Credit Monitoring: No • Other:	Up to $5,000 per violation: W.Va. Code §§ 46A-2A-104, 46A-7-111	Attorney General: W.Va. Code § 46A-2A-104
Unfair, Deceptive, or Abusive Acts and Practices	W. Va. Code § 46A-6-104	Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $5,000 per violation: W.Va. Code § 46A-7-111	Attorney General: W.Va. Code § 46A-7-111
Wisconsin Breach Notification Law	Wis. Stat. § 134.98	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Within 45 days of the breach discovery date • Substitute Notice: Yes, see statute • Credit Monitoring:	None	No one
Unfair, Deceptive, or Abusive Acts and Practices	Wis. Stat. § 100.20	"Methods of competition in business and trade practices in business shall be fair. Unfair methods of competition in business and unfair trade practices in business are hereby prohibited."	From $100 to $10,000 per violation: Wis. Stat. § 100.26(6)	The Department of Agriculture, trade, and consumer protection: Wis. Stat. § 100.20
Wyoming Breach Notification Law	Wyo. Stat. § 40-12-502	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, see statute • Credit Monitoring: No	Damages: Wyo. Stat. § 40-12-502	Attorney General: Wyo. Stat. § 40-12-502(f)
Unfair, Deceptive, or Abusive Acts and Practices	Wyo. Stat. § 40-12-105	"A person engages in a deceptive trade practice unlawful under this act when, in the course of his business and in connection with a consumer transaction, he knowingly. . ."	Up to $5,000 per violation: Wyo. Stat. § 40-12-113	Attorney General: Wyo. Stat. § 40-12-113
District of Columbia Breach Notification Law	D.C. Code § 28- 3852	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 or $50,000 • Credit Monitoring: No	$100 per Affected Resident: D.C. Code § 28- 3853	US Attorney General: D.C. Code § 28- 3853
Unfair, Deceptive, or Abusive Acts and Practices	D.C. Code § 28-3904	"It shall be a violation of this chapter, whether or not any consumer is in fact misled, deceived or damaged thereby, for any person to: . . ."	Up to $1000 per violation: D.C. Code § 28-3909	Corporation Counsel: D.C. Code § 28-3909
Guam Breach Notification Law	9 GCA § 48.30	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 5,000 residents or $10,000 • Credit Monitoring: No • Other:	Up to $150,000 per breach: 9 GCA § 48.50	The Attorney General: 9 GCA § 48.50

Unfair, Deceptive, or Abusive Acts and Practices	5 GCA § 32201	"False, misleading, or deceptive acts or practices, including, but not limited to those listed in this chapter, are hereby declared unlawful and are subject to action by the Attorney General or any person as permitted pursuant to this chapter or other provisions of Guam law. A violation consisting of any act prohibited by this title is in itself actionable, and may be the basis for damages, rescission, or equitable relief. The provisions of this chapter are to be liberally construed in favor of the consumer, balanced with substantial justice, and violation of such provisions may be raised as a claim, defense, crossclaim or counterclaim."	Up to $5,000 per violation: 5 GCA § 32127	Attorney General: 5 GCA § 32116
Puerto Rico Breach Notification Law	10 Laws of Puerto Rico § 4051	• Notify Affected Residents: Yes • Notify the Secretary of Consumer Affairs: Yes, within 10 days • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 people or $100,000 • Credit Monitoring: No	Up to $5,000 per violation of the provisions of this chapter: 10 Laws of Puerto Rico § 4055	The Secretary: 10 Laws of Puerto Rico § 4055
Unfair, Deceptive, or Abusive Acts and Practices	10 Laws of Puerto Rico § 259	"Unfair methods of competition, and unfair or deceptive acts or practices in trade or commerce are hereby declared unlawful."	"a civil penalty imposed by the Department of Consumer Affairs up to a maximum of five thousand dollars ($5,000). Each separate violation of said decision shall be considered as continuous noncompliance therewith, in which case, each day the decision is not complied with shall be considered as a separate violation." 10 Laws of Puerto Rico § 259	The Office of Monopolistic Affairs: 10 Laws of Puerto Rico § 259
Virgin Islands Breach Notification Law	V.I. Code tit. 14, § 2208	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 50,000 residents or $100,000 • Credit Monitoring: No • Other:	Actual damages: V.I. Code tit. 14, § 2211	Private right of action: V.I. Code tit. 14, § 2211
Unfair, Deceptive, or Abusive Acts and Practices	V.I. Code tit. 12, § 101	"No person shall engage in any deceptive or unconscionable trade practice in the sale, lease, rental or loan or in the offering for sale, lease, rental, or loan of any consumer goods or services, or in the collection of consumer debts."	Up to $5,000 per violation: V.I. Code tit. 12, § 104	The Commissioner: V.I. Code tit. 12, § 104

Survey of International Cyber Laws

Title	Country	Information	Applies to	Notes
China Cybersecurity Law (CSL)	CHINA	CSL regulates the construction, operation, maintenance and use of networks, as well as network security supervision and management within mainland China. The Cyberspace Administration of China (CAC) is the primary governmental authority supervising and enforcing the CSL.		
General Data Privacy Regulation (GDPR)	EUROPEAN UNION	The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.	Countries that belong to the EEA include EU + 3. Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom. Non-EU countries in the EEA Norway, Iceland, Liechtenstein	While GDPR is In place as law there is not yet specific country by country adoption of laws to align or go stricter than GDPR. It should be expected that Germany, France and Spain will go above and beyond the standard GDPR language and add more provisions.
International Traffic in Arms Regulations (ITAR)	UNITED STATES	A United States regulatory regime to restrict and control the export of defense and military related technologies to safeguard U.S. national security and further U.S. foreign policy objectives ITAR is the International Traffic in Arms Regulations and requires, in part, that defense-related articles and technical data listed on the United States Munitions List USML only be shared with U.S. citizens absent special authorization or exemption. Furthermore, ITAR is a set of standards that deals with information security involving any parties that handle technical data related to the manufacturing, the exporting and a general involvement with defense articles or services.		
Encryption and Export Administration Regulation (EAR)		The Export Administration Regulations (EAR) is a set of US government regulations on the export and import of most commercial items. The U.S. Department of Commerce is responsible for implementing and enforcing EAR. Specifically, working with items deemed dual-use and having both commercial and military applications. In particular, encryption or Cryptographic Information Security		
Australia		The Privacy Act includes thirteen Australian Privacy Principles (APPs). The APPs set out standards, rights and obligations for the handling, holding, use, accessing and correction of personal information (including sensitive information).		
India	India	India is not a part of any convention on protection of personal data that is equvalent to the GDPR. India has adopted other international declarations and conventions including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, these acts recognise the right to privacy.		
Japan		European Union (EU)-Japan Economic Partnership Agreement (EPA) is a reciprocal adequacy arrangement that established the equivalence of the EU's General Data Protection Regulation (GDPR) and Japan's Act on the Protection of Personal Information (APPI) and enabling cross-border data transfers between the two. Japan was previously not included in the EU's whitelist of countries considered as having adequate levels of personal data protection.		

Russia		In 2014, Russia adopted personal data localisation rules. These rules required all operators that collect and process Russian citizens personal data to use databases located in Russia. These requirements apply to the personal data of all Russian citizens, regardless of their relation with the company. The new rules do not cross-border transfer of personal data. However, the requirement for primary data processing via Russian databases is considered to be onerous.		
Canada		Canada has adequacy with the EU and GDPR (as of the launch of GDPR) based on the PIPDEA law that covers data privacy in Canada. In general, Canada privacy is not that bad. However, organizations in British Columbia and Nova Scotia that do business with quasi-governmental entities such as banks & transportation are subject to FIPPA. In particualr, article 30. is critical to understand as it prohibits transfer of data outside of Canada.		

Survey of Institutions

Title	Information	URL
Cloud Security Alliance	Offers a number of certifications including: CSA Security, Trust & Assurance Registry (STAR) Certificate of Cloud Security Knowledge (CCSK) Certified Cloud Security Professional (CCSP) Global Consultancy Program	https://cloudsecurityalliance.org/
Commission on Accreditation for Law Enforcement Agencies ("CALEA")	CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance while protecting the privacy of information outside the scope of the investigation. It requires that telecommunications carriers and manufacturers of telecommunications equipment design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities to comply with legal requests for information.	http://www.calea.org/
Control Objectives for Information and Related Technologies ("COBIT")	COBIT 5 is the only business framework for the governance and management of enterprise IT. COBIT 5 integrates other major frameworks, standards and resources, including ISACA's Val IT and Risk IT, Information Technology Infrastructure Library (ITIL®) and related standards from the International Organization for Standardization (ISO).	http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
Federal Energy Regulatory Commission (FERC) Revised Critical Infrastructure Protection (CIP) Reliability Standards	NERC, which FERC has certified as the nation's Electric Reliability Organization, developed Critical Infrastructure Protection (CIP) cyber security reliability standards. On January 18, 2008, the Commission issued Order No. 706, the Final Rule approving the CIP reliability standards, while concurrently directing NERC to develop significant modifications addressing specific concerns. In January 2016, FERC issued a Final Rule revising the CIP reliability standards. Docket No. RM15-14-000. As of December 2017, FERC release a Notice of Proposed Rulemaking to direct NERC to develop and submit modifications to improve mandatory reporting of Cyber Security Incidents. [Docket Nos. RM18-2-000 and AD17-9-000.	https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp
Federal Financial Institutions Examination Councils ("FFIEC")	The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) and to make recommendations to promote uniformity in the supervision of financial institutions. Guidance includes: Online Banking: https://www.ffiec.gov/pdf/authentication_guidance.pdf FFIEC Cybersecurity Assessment Tool: https://www.ffiec.gov/cyberassessmenttool.htm	https://www.ffiec.gov/
Health Insurance Trust Alliance (HITRUST) CSF	HITRUST CSF is a certifiable framework that provides organizations with a comprehensive, flexible and efficient approach to regulatory compliance and risk management.	https://hitrustalliance.net/hitrust-csf/

Indiana Department of Financial Institutions (DFI)	Enforces FFIEC standards.	https://www.in.gov/dfi/
Indiana State Insurance Commissioners Navigators and Application Organizations		https://www.in.gov/idoi/
International Organization for Standardization ("ISO")	ISO creates documents that provide requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose.	https://www.iso.org/home.html
ISA/IEC 62443 (ISA99)	The ISA-99/IEC 62443 standard is the worldwide standard for security of the Industrial Control Systems in the Operational Technology (OT) domain of organizations. The standard was created by the International Society of Automation, a leading worldwide nonprofit organization. The standard offers organizations handles to improve the digital security and safety of their process and SCADA environments.	https://www.isa.org/isa99/
National Institute of Standards and Technology ("NIST")	NIST is a measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce.	https://www.nist.gov/
North American Electric Reliability Corporation ("NERC")	The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel.	https://www.nerc.com/Pages/default.aspx
PCI Security Standards Council	Helps merchants and financial institutions understand and implement standards for security policies, technologies and ongoing processes that protect their payment systems from breaches and theft of cardholder data. Also helps vendors understand and implement standards for creating secure payment solutions.	https://www.pcisecuritystandards.org/
SSAE-18/ ISAE 3402	ISAE 3402 was developed to provide an international assurance standard for allowing public accountants to issue a report for use by user organizations and their auditors (user auditors) on the controls at a service organization that are likely to impact or be a part of the user organization's system of internal control over financial reporting.	https://www.ssae-16.com/soc-1-report/the-ssae-18-audit-standard/