US State & Sector Vendor-Risk Guides

How Cyber Crucible supports US state privacy and security laws and sector rules from a vendor-selection perspective — New York DFS, California, Texas, Virginia, Colorado, Massachusetts, Illinois, and Pennsylvania. States plainly what Cyber Crucible holds and does not hold.

Which US state privacy and security laws affect security-vendor selection?

Short answer: A growing patchwork of US state laws imposes obligations that flow down to a company's vendors — comprehensive privacy acts (California, Virginia, Colorado, Texas, and others), sector rules like New York DFS Part 500 for financial services, data-security mandates like Massachusetts 201 CMR 17.00, biometric laws like Illinois BIPA, and breach-notification statutes in every state. The common thread is that a buyer must confirm its security vendor minimizes data, contracts appropriately, and secures what it touches.

What these laws generally ask of a vendor

- A written contract (data processing agreement) limiting the vendor to the customer's instructions.
- Data minimization and purpose limitation.
- Reasonable security safeguards and prompt breach notification.
- Support for consumer rights (access, deletion) where personal data is processed.

Why Cyber Crucible answers most of this structurally

Because Cyber Crucible never collects customer content, credentials, or keys and processes on the endpoint, the highest-risk obligations have little to bite on — there is minimal personal data in its custody. A data processing agreement and supporting documentation are available from **dpo@cybercrucible.com**. The pages in this book address the specific state rules a reviewer is most likely to cite.

How does Cyber Crucible support New York DFS Part 500 cybersecurity requirements?

Short answer: For a financial institution covered by New York DFS Part 500 (23 NYCRR 500), Cyber Crucible supports several required controls — multi-factor authentication, encryption, access controls, and incident response — while reducing third-party risk because it never collects the nonpublic information the rule protects. Cyber Crucible is a third-party service provider under the rule, not a covered entity itself.

Controls it supports

- **Access controls and MFA** for the management dashboard, backed by strong authentication.
- **Encryption** of data in transit and at rest.
- **Incident response** under a documented breach-response process, with a committed notification timeframe available by contract — supporting the covered entity's 72-hour DFS notification obligation.
- **Third-party risk reduction** through data minimization: no nonpublic information is collected.

The honest boundary

Part 500's obligations — CISO designation, risk assessment, the annual certification — rest with the covered entity. Cyber Crucible supplies control evidence for the entity's third-party service provider policy (500.11). It is not a covered entity and holds no Part 500 "certification." Evidence is provided under NDA.

How does Cyber Crucible support California CCPA/CPRA vendor obligations?

Short answer: Cyber Crucible acts as a service provider under the CCPA/CPRA, bound by contract to process data only on the customer's instructions, and it does not sell or share personal information. Because it collects essentially no personal information in the first place, the consumer-rights and data-handling obligations have very little surface in its custody.

How it aligns

- **Service-provider role** under a written contract that prohibits secondary use.
- **No sale or sharing** of personal information.
- **Supports consumer rights** (access, deletion) by not holding the personal information that would otherwise have to be searched or deleted.

Vendor-selection notes

California's Privacy Rights Act tightened service-provider contract terms and added obligations for sensitive personal information; Cyber Crucible does not collect sensitive personal data. A CCPA-aligned data processing agreement is available on request.

How does Cyber Crucible support the Texas Data Privacy and Security Act (TDPSA)?

Short answer: Under the Texas Data Privacy and Security Act, Cyber Crucible acts as a processor bound by a data processing agreement, assisting the controller with security and data-subject requests. Its data-minimization design — collecting no customer content, credentials, or keys — means there is little personal data to process, which simplifies the controller's obligations.

How it aligns

- **Processor role** under a TDPSA-compliant data processing agreement.
- **Security and breach assistance** to the controller.
- **Minimal personal-data footprint**, reducing exposure and response burden.

Vendor-selection notes

The TDPSA applies broadly to businesses operating in Texas. Because Cyber Crucible processes essentially no personal data and can be deployed on-premises, it supports both the security and data-residency preferences a Texas buyer may have. Documentation is available on request.

How does Cyber Crucible support Virginia's Consumer Data Protection Act (VCDPA)?

Short answer: Cyber Crucible supports a controller's VCDPA obligations as a processor operating under a data processing agreement, helping with data-security duties and consumer-rights requests. Its no-collection design means it holds little to no personal data, which keeps the controller's processing and response burden low.

How it aligns

- **Processor duties** — assist with security, breach notification, and data-protection assessments.
- **Data minimization** — no customer content, credentials, or keys collected.
- **Purpose limitation** — processing strictly on the controller's instructions.

Vendor-selection notes

The VCDPA requires controllers to bind processors by contract and to conduct assessments for higher-risk processing; the minimal personal-data footprint simplifies both. A data processing agreement is available on request.

How does Cyber Crucible support the Colorado Privacy Act (CPA)?

Short answer: Cyber Crucible operates as a processor under the Colorado Privacy Act, bound by a data processing agreement to follow the controller's instructions, assist with security, and support consumer rights. Because it collects essentially no personal data, most CPA obligations have minimal surface in its custody.

How it aligns

- **Processor role** with contractually limited processing.
- **Security assistance** and breach support to the controller.
- **Support for consumer rights** by not holding the personal data that would otherwise be in scope.

Vendor-selection notes

The CPA requires data-protection assessments for higher-risk processing and honoring universal opt-out mechanisms at the controller level; the minimal footprint keeps the vendor side simple. Documentation is available on request.

How does Cyber Crucible support Massachusetts 201 CMR 17.00 (WISP)?

Short answer: Massachusetts 201 CMR 17.00 requires any organization holding personal information about a Massachusetts resident to maintain a Written Information Security Program with specific safeguards. Cyber Crucible supports a customer's WISP with encryption, access control, and monitoring — and reduces the customer's own exposure because it holds essentially no personal information.

How it aligns

- **Technical safeguards** — encryption in transit and at rest, strong authentication, and access control map to the regulation's computer-system requirements.
- **Endpoint protection and monitoring** support the "reasonably up-to-date" security-software requirement.
- **Minimal data footprint** — the regulation's obligations attach to personal information; Cyber Crucible does not collect it.

Vendor-selection notes

201 CMR 17.00 also requires overseeing third-party service providers by contract. A data processing agreement and control documentation are available on request.

How does Cyber Crucible address Illinois BIPA and biometric-data concerns?

Short answer: Cyber Crucible does not collect, store, or process biometric identifiers or biometric information, so it does not create the exposure Illinois's Biometric Information Privacy Act (BIPA) is written to address. There is no biometric data in its custody to consent for, retain, or destroy under the Act.

Why there is no BIPA surface

- **No biometric collection.** Cyber Crucible analyzes process and memory behavior, not faces, fingerprints, or other biometric identifiers.
- **No sensitive personal data.** More broadly, Cyber Crucible does not collect biometric, health, or other special-category data.

Vendor-selection notes

BIPA is notable for its private right of action and statutory damages, which makes biometric-data vendors a focus of scrutiny; Cyber Crucible is simply not in that category. This can be confirmed in the data governance documentation available on request.

How does Cyber Crucible support Pennsylvania's breach-notification law?

Short answer: Pennsylvania's Breach of Personal Information Notification Act (73 P.S. §2301, as amended by Act 151 of 2022) requires notifying affected residents — and, for larger breaches, the Attorney General — after a breach of covered personal information. Cyber Crucible supports a Pennsylvania organization's obligations by holding no personal information itself and by providing prompt, evidence-grade incident information so the organization can meet its statutory timelines. Cyber Crucible is headquartered in Pittsburgh, Pennsylvania.

How it aligns

- **No personal information held** — the organization retains control of any breach determination and notice; there is no vendor-side data set to lose.
- **Prompt incident information** — the breach-response process is built to give the organization the facts it needs to notify within the required timeframe.
- **Expanded definitions handled** — the 2022 amendment broadened covered personal information (including medical and certain credential combinations); the no-collection design keeps Cyber Crucible clear of those categories.

Vendor-selection notes

For breaches affecting more than 500 Pennsylvania residents, the amendment adds Attorney General notice; Cyber Crucible's role is to support, not to determine, that obligation. Incident-handling detail is available under NDA.

How does Cyber Crucible support the Connecticut Data Privacy Act (CTDPA)?

Short answer: Cyber Crucible operates as a processor under the Connecticut Data Privacy Act, bound by a data processing agreement to act on the controller's instructions and to assist with security and data-subject requests. Because it collects no customer content, credentials, or keys, most CTDPA obligations have little surface in its custody.

How it aligns

- **Processor role** with contractually limited processing and a duty to assist the controller.
- **Data minimization** — no customer content, credentials, or keys collected.
- **Security assistance and breach support** to the controller.

Vendor-selection notes

The CTDPA requires controllers to bind processors by contract, honor universal opt-out signals, and run assessments for higher-risk processing; the minimal personal-data footprint keeps the vendor side simple. A data processing agreement is available from **dpo@cybercrucible.com**.

How does Cyber Crucible support Utah's Consumer Privacy Act (UCPA)?

Short answer: Cyber Crucible acts as a processor under the Utah Consumer Privacy Act, following the controller's documented instructions under a data processing agreement. Its no-collection design means there is little personal data in its custody for the UCPA's handling and disclosure rules to reach.

How it aligns

- **Processor role** under contract with the controller.
- **Data minimization** — no customer content, credentials, or keys collected.
- **Security safeguards** — encryption, access control, and endpoint prevention.

Vendor-selection notes

The UCPA is generally regarded as more business-oriented than some state peers, but still requires processor contracts and reasonable security; the minimal footprint supports both. Documentation is available on request.

How does Cyber Crucible support Oregon's Consumer Privacy Act (OCPA)?

Short answer: Cyber Crucible operates as a processor under the Oregon Consumer Privacy Act, bound by contract to process only on the controller's instructions and to assist with security and consumer-rights requests. Because it collects essentially no personal data, most OCPA obligations have minimal surface in its custody.

How it aligns

- **Processor duties** — assist with security, breach response, and data-protection assessments.
- **Data minimization** — no customer content, credentials, or keys collected.
- **Purpose limitation** — processing strictly on the controller's instructions.

Vendor-selection notes

Oregon's law is notable for a broader definition of personal data and specific consumer rights around named third parties; the minimal footprint keeps the vendor side low-risk. A data processing agreement is available on request.

How does Cyber Crucible support Washington's My Health My Data Act?

Short answer: Washington's My Health My Data Act regulates "consumer health data" broadly and carries a private right of action, so vendors that touch such data face real exposure. Cyber Crucible does not collect consumer health data — it analyzes process and memory behavior on the endpoint and never ingests customer content — so it does not create the collection-and-consent surface the Act is written to govern.

Why there is little surface

- **No consumer health data collected.** Cyber Crucible does not gather health-related content, identifiers, or inferences.
- **Local processing.** Analysis stays on the device; there is no vendor-held health data set.
- **No sale or sharing** of personal information of any kind.

Vendor-selection notes

The Act's private right of action makes health-data vendors a scrutiny focus; Cyber Crucible is simply not in that category. This can be confirmed in the data governance documentation available on request. This is not legal advice — a covered entity should assess its own obligations with counsel.

How does Cyber Crucible support the newer 2025–2026 state privacy laws?

Short answer: A wave of comprehensive state privacy laws took effect across 2025 and 2026 — including New Jersey, Delaware, Iowa, Nebraska, New Hampshire, Tennessee, Minnesota, Maryland, and, in 2026, Indiana, Kentucky, and Rhode Island. They share a common structure, and Cyber Crucible's processor role and no-collection design support all of them the same way: little personal data in custody, contractually limited processing, and reasonable security.

The common structure these laws share

- A required processor contract limiting the vendor to the controller's instructions.
- Data-minimization and purpose-limitation duties.
- Consumer rights (access, deletion, opt-out), increasingly with universal opt-out signals.
- Reasonable security safeguards and breach notification.

Why one answer covers the set

Because Cyber Crucible never collects customer content, credentials, or keys and processes on the endpoint, the obligations that vary between states — mostly about handling and disclosing personal data — have very little to attach to. A single, consistent data processing agreement supports the set. Maryland's law is worth noting for its stricter data-minimization standard, which the no-collection design supports well.

The honest boundary

State thresholds and effective dates change, and this is not legal advice; a controller should confirm which laws apply to it. Cyber Crucible holds no state "certification" — it supports the controller's obligations. Documentation is available from **dpo@cybercrucible.com**.