Cyber Risk Meets Regulation: What Energy Companies Need to Know Now

By: Jason T. Seay, AIGP, CIPP-US

June 6, 2026

Cybersecurity and privacy are no longer back-office concerns for the energy sector; they are front-line legal and operational risks. With expanding federal directives, evolving threat tactics, and an increasingly aggressive privacy litigation landscape, some energy companies are rethinking how they manage cyber and data risk. This Alert highlights the latest developments and what they mean for your business.

Key Takeaways

1. Federal Cybersecurity Mandates Are Expanding Rapidly

- The **Transportation Security Administration (TSA) continues to roll out mandatory cybersecurity directives** for critical pipeline infrastructure.
- These apply to designated pipeline owners and operators and are evolving annually.
- Expect more assets to be classified as "critical infrastructure," increasing regulatory reach.

2. Compliance Now Requires a Structured, Documented Cyber Program

- TSA directives establish a two-layer framework:
    - **Governance and Reporting (01 Series):**
        - Designated cybersecurity coordinator (24/7 availability)
        - Mandatory incident reporting to the Cybersecurity and Infrastructure Security Agency (CISA)
        - Formal risk assessments and governance structures
    - **Mitigation and Testing (02 Series):**

        - Cybersecurity Implementation Plans
        - Incident response and recovery planning
        - Ongoing testing, validation, and documentation
- **Key shift:** Regulators now expect audit-ready evidence of compliance, not just policies.

3. 2025–2026 Updates Signal a Move Toward Continuous Oversight

- Recent TSA updates emphasize:
    - Performance-based compliance
    - Real-time monitoring and detection capabilities
    - Stricter reporting timelines and remediation tracking
- **Implication:** Cybersecurity is now an ongoing operational obligation, not a periodic exercise.

4. Threat Actors Are Targeting Identity, Not Just Systems

- Attack strategies are evolving quickly:
    - Help desk impersonation and social engineering
    - Multi-factor authentication (MFA) fatigue ("push-bombing")
    - Identity provider (IdP) compromise (e.g., centralized access systems)
    - Exploitation of non-human identities (API keys, service accounts)
- Generative AI is accelerating:
    - Phishing sophistication
    - Malware development
    - Attack scale and speed
- **Takeaway:** Traditional perimeter defense is becoming obsolete.

5. Privacy Litigation Is Expanding Beyond Traditional Targets

- The California Invasion of Privacy Act (CIPA) is being applied to:
    - Website tracking technologies (cookies, pixels)
    - Chatbots and AI tools
    - Session replay and user interaction tracking
- Plaintiffs argue that third-party tools "intercept" user communications—triggering potential liability under California state law.
- **Risk exposure:** Up to $5,000 per violation, with broad applicability to any site accessible in California.

6. New Privacy Laws Add Another Layer of Compliance

- The Oklahoma Privacy Act (effective 2027) introduces:
    - Enforcement by the Attorney General
    - Penalties up to $7,500 per violation
- At the same time, updated California Consumer Privacy Act regulations require:
    - Risk assessments for high-risk data processing
    - Cybersecurity audits for covered businesses
- **Notably:** Sensitive data like precise geolocation is a key focus.

7. Proactive Risk Management Is Now a Business Imperative

- Leading practices include:
    - Comprehensive data and AI tool inventory (chatbots, analytics, tracking tools)
    - Vendor contract scrutiny (data use, model training, reuse rights)
    - Regular audits (at least every 6 months)
    - Stronger consent frameworks (clear disclosures and enforceable terms)

The Bottom Line

Legal, IT, and operations teams must work in lockstep as cybersecurity and privacy risks in the energy industry are converging and intensifying. Federal mandates, sophisticated cyber threats, and expanding privacy litigation, are creating a complex, high-stakes environment.

Companies that treat cybersecurity and data governance as core business functions, not just compliance exercises, will be best positioned to manage risk, maintain operational resilience, and avoid costly enforcement actions.

This series covers topics featured during GableGotwals' Annual Energy Market Drivers and Current Legal Issues Seminar. To receive Alerts and information on future Firm events, subscribe to our mailing list.

Jason T. Seay, AIGP, CIPP-US

918-595-4832

jseay@gablelaw.com