Comment on Proposed Cybersecurity General Terms and Conditions for Vendor Products and Services

Submitted by: **Gary Michor,** CEO, Screaming Power Inc.

Introduction

Screaming Power Inc. appreciates the continued efforts of NIST, NAESB, utilities, vendors, cybersecurity professionals, regulators, and standards organisations to strengthen cybersecurity expectations across the North American energy sector.

The proposed Cybersecurity General Terms and Conditions represent an important step toward improving vendor accountability, software supply chain transparency, vulnerability disclosure, secure development practices, incident reporting, and product security assurance. The draft establishes significant obligations for vendors, including cybersecurity policies, product vulnerability notices, remediation plans, secure-by-design attestations, audit rights, product support disclosures, known vulnerability reporting, and Software Bill of Materials (SBOM) information.

Screaming Power supports the objective of improving cybersecurity across the industry. However, we believe the proposed framework should be expanded and strengthened to address the full operating environment in which these vendor obligations will apply. Cybersecurity risk is not limited to vendors. It also exists within utility-operated systems, legacy infrastructure, utility affiliates, proprietary data environments, emerging AI-enabled systems, and inconsistent regulatory or procurement frameworks.

For these reasons, the proposed requirements should be advanced as part of a broader industry-wide framework that includes vendor accountability, utility accountability, open data, interoperability, Canadian standards alignment, AI readiness, and continuous enforcement.

1. Utility Accountability Should Accompany Vendor Accountability

The proposed terms place significant obligations on vendors. These include maintaining cybersecurity policies, notifying product users of exploitable vulnerabilities, providing remediation plans, supporting product trust verification, allowing vulnerability audits or inspections, and providing product-level attestations and disclosure information such as SBOMs, known vulnerability reports, product support status, and supplier information.

These obligations are appropriate and increasingly necessary. However, comparable attention should also be given to utility-operated systems, utility-developed software, internal applications, legacy operational technology, and ageing infrastructure.

Public reporting indicates that utilities continue to face material cybersecurity risk from legacy and unpatched environments. One 2026 utilities cybersecurity report found that 77% of utilities organisations experienced attacks involving outdated software or unavailable patches on legacy equipment during the previous 12 months. The same report also found that 76% experienced phishing or business email compromise, 74% experienced malware, and more than 70% experienced unauthorised system access. [intelligentciso.com]

These statistics reinforce an important point: cybersecurity is a shared responsibility. Vendor requirements are necessary, but they are not sufficient if the utility environments into which vendor products are deployed do not meet comparable standards of governance, security monitoring, vulnerability management, access control, patch management, and incident response.

The industry should avoid creating an environment in which vendors are held to stricter cybersecurity standards than the utility-owned systems, internally developed platforms, and operational environments with which those vendor products must integrate.

2. Utility Affiliates, Competitive Neutrality, and Non-Public Utility Data

A further consideration is the growing role of utility affiliates, utility-controlled platforms, and utility-developed commercial services that may compete with independent vendors.

Where utility affiliates or utility-operated business functions participate in competitive markets, they should be subject to cybersecurity obligations comparable to those imposed on independent vendors. Cybersecurity requirements should be technology-neutral, ownership-neutral, and competitively neutral.

This issue is not merely theoretical. Public reporting from a proceeding in Ohio indicates that market participants asked regulators to prohibit affiliate preferences arising from non-public utility data unless that data is made available on a non-discriminatory basis. The same reporting noted concerns that regulated utility functions or affiliates may gain competitive advantages through access to non-public utility information.

This reinforces the need for cybersecurity frameworks to address not only vendor obligations, but also the broader market structure in which utility data, utility affiliates, and third-party vendors operate.

If a utility affiliate, utility-developed platform, or utility-controlled service competes with vendors, it should be subject to the same disclosure, audit, vulnerability management, incident reporting, and data access expectations. The ownership structure of the technology should not determine the level of cybersecurity scrutiny applied.

3. Canadian Standards and Self-Assessment Pathways Should Be Considered

The draft appropriately references several U.S.-based frameworks and authorities, including NIST, CISA, NERC, ISO/IEC, IEC, CVE, CWE, CVSS, and related vulnerability disclosure practices.

However, the draft does not appear to provide a clear pathway for Canadian cybersecurity frameworks, Canadian self-assessment approaches, or Canadian standards alignment. This is important because the North American energy sector is integrated across the United States and Canada, and many vendors and utilities operate in both countries.

In Canada, the Canadian Centre for Cyber Security is described as the single unified source of expert advice, guidance, services, and support on cybersecurity for Canadians. In addition, the Government of Canada's Canadian Program for Cyber Security Certification, or CPCSC, includes a Level 1 self-assessment approach for certain federal suppliers and refers to 13 security requirements and controls based on ITSP.10.171.

Screaming Power recommends that NIST, NAESB, and related standards stakeholders consider how Canadian cybersecurity programmes, Canadian Centre for Cyber Security guidance, CSA-related standards where applicable, and Canadian self-assessment or certification approaches can be recognised as complementary evidence of cybersecurity maturity.

This would help avoid unnecessary duplication and would support cross-border consistency for Canadian utilities, U.S. utilities, and vendors serving both markets.

4. Ontario GO-ITS as a Useful Public-Sector Comparator

Ontario's Government of Ontario Information and Technology Standards, or GO-ITS, should also be considered as a useful comparator for security governance, even where it may not be mandatory for utilities.

Ontario states that GO-ITS are the official publications concerning standards, guidelines, technical reports, and preferred practices adopted by the Government of Ontario. GO-ITS 25.0 defines general security requirements for protecting the integrity, confidentiality, and availability of Government of Ontario networks and computer systems.

However, many municipal and regulated utilities are not generally required to adopt GO-ITS unless such requirements are imposed through contract, procurement, policy, legislation, or regulatory obligation. As a result, cybersecurity governance practices can vary considerably among organisations operating within the same province or sector.

For this reason, NIST and other standards bodies should consider how public-sector security frameworks such as GO-ITS can be used as reference points when evaluating utility cybersecurity readiness, vendor requirements, cloud-hosted systems, customer data platforms, and third-party integrations.

The goal should not be to impose duplicative requirements, but to improve consistency, transparency, and comparability across public-sector, utility-sector, and vendor security expectations.

5. Cybersecurity Must Advance Alongside Open Data and Interoperability

Cybersecurity cannot be viewed in isolation from data governance, interoperability, and market competition.

For many years, utilities and customers have faced challenges associated with vendor lock-in. Proprietary systems, proprietary interfaces, closed data structures, and restricted access to customer or operational data can make it difficult and expensive to replace underperforming or non-compliant technology providers.

The proposed cybersecurity framework should therefore be developed alongside open data standards, standardised communications frameworks, and interoperability requirements.

Green Button provides an important example of how secure data access and interoperability can support innovation. The U.S. Department of Energy states that the Green Button initiative was designed to give utility customers easy and secure access to energy usage information in a consumer-friendly and computer-friendly format. Adoption of a consensus standard can also enable developers and entrepreneurs to build applications and services that help consumers manage energy use. However, the current standard is ageing, and implementation can vary by utility. This limits consistency and creates practical barriers for customers, vendors, and regulators seeking reliable, interoperable access to data.

NAESB states that its Energy Services Provider Interface, or ESPI, model business practices define a data exchange protocol for transferring energy usage information between a utility and a third party with customer authorisation. ESPI also serves as the basis for Green Button implementations throughout North America. The Green Button Alliance describes Green Button Connect My Data as an open-data standard intended to unlock access to utility interval usage and billing data while enabling secure, customer-authorised sharing with third-party solutions. In practice, however,

implementation can still vary across utilities. Without stronger consistency, accountability, and migration requirements, customers and third-party vendors may face high costs, operational disruption, and inconsistent access to data.

This is highly relevant to cybersecurity standards because a secure system that cannot be replaced, audited, integrated, or migrated away from remains a long-term operational risk.

Screaming Power's experience with utility data platforms, Green Button, EBT, CIS, EMS, customer data systems, and energy management platforms reinforces the importance of combining cybersecurity requirements with data portability and interoperability requirements. Public-sector utility data requirements increasingly refer to open, non-proprietary database formats, Green Button integration, secure data exchange, and vendor transition planning. However, the transition from legacy systems can still create barriers that favour incumbents, increase switching costs, and delay movement to more secure technology.

The proposed framework should therefore recognise that cybersecurity resilience includes the ability to replace vendors, platforms, and systems that fail to meet evolving security expectations. That requires more than security policies. It requires open data models, clear communication standards, exportable data, migration rights, auditable interfaces, and non-proprietary integration pathways.

6. Vendor Replacement Should Be a Security Principle

If a vendor fails to meet cybersecurity expectations, the utility or customer should be able to replace that vendor without excessive cost, disruption, or loss of access to data.

Likewise, if a utility-developed platform, utility affiliate, or incumbent system fails to meet evolving cybersecurity expectations, customers and regulators should have a practical path to transition to better alternatives.

This is why cybersecurity and interoperability must be treated as connected policy objectives.

A security framework that strengthens disclosure obligations but does not address data portability may unintentionally reinforce dependence on the very systems or vendors that create long-term risk.

The industry should therefore consider adding language that encourages:

- open data standards;
- standardised application programming interfaces;
- customer-authorised data sharing;
- documented data export rights;
- non-proprietary data migration formats;
- interoperability between utility and third-party systems;
- equal treatment of utility-owned platforms and independent vendors;

- transition rights where systems fail to meet cybersecurity requirements.

7. Artificial Intelligence is Changing the Cybersecurity Threat Landscape

Artificial intelligence is changing both offensive and defensive cybersecurity capabilities.

NIST has recognised that AI systems can be subject to adversarial attacks, including attempts to confuse or poison AI systems, and has stated that there is no foolproof defence against such attacks. NIST's AI Risk Management Framework also includes work related to generative AI and a concept note for trustworthy AI in critical infrastructure.

The implications for the energy sector are significant. AI can accelerate vulnerability discovery, code analysis, reconnaissance, phishing, exploit development, malware generation, system monitoring, anomaly detection, and remediation. This means cybersecurity standards must be designed to evolve continuously.

Recent reporting also indicates that NIST is exploring how AI can support modernisation of the National Vulnerability Database, including the vulnerability management lifecycle, risk assessment, remediation, and handling of emerging threats. The proposed vendor terms should therefore include a mechanism for continuous review and revision as AI-enabled threats and AI-enabled defensive systems evolve.

Future versions should explicitly consider:

- AI-assisted vulnerability discovery;
- AI-generated software risk;
- AI supply chain risk;
- adversarial machine learning;
- model poisoning;
- AI-enabled phishing and social engineering;
- AI-supported incident response;
- AI governance for critical infrastructure;
- security expectations for AI-enabled vendor products.

Without explicit consideration of AI, standards developed today may become incomplete before they are widely implemented.

8. Evidence Shows the Pace of Risk is Increasing

The need for an adaptive framework is supported by recent cybersecurity reporting across the energy and critical infrastructure sectors.

DNV reported that, in a survey of 375 energy professionals, 65% said their leadership views cybersecurity as the greatest current risk to their business. Dragos reported that ransomware activity affecting industrial organisations increased by more than 87% year over year, and that it tracks 23 OT cyber threat groups, with 9 active in OT operations in 2024. Cyble reported 187 ransomware incidents, 37 unauthorised network access listings, and 57 data breach and leak incidents affecting energy and utility organisations worldwide in 2025.

These statistics demonstrate that cybersecurity frameworks cannot remain static. The energy sector is facing a rapidly changing threat environment involving ransomware, supply chain risk, ageing infrastructure, operational technology exposure, AI-enabled threats, and increasingly complex vendor ecosystems.

The proposed requirements should therefore include mechanisms for continuous updating, measurable accountability, and practical enforcement.

9. Standards Development and Enforcement Must Advance Faster

Historically, standards development has often progressed over multi-year cycles. That pace is increasingly misaligned with the speed of change in cloud computing, AI, operational technology, distributed energy resources, customer data platforms, and cyber threats.

A highly prescriptive cybersecurity framework may be valuable when published, but without rapid update mechanisms it may become outdated before broad industry implementation occurs. The industry should therefore focus on:

- cybersecurity maturity for utilities and vendors;
- utility affiliate accountability and independence;
- software supply chain transparency;
- SBOM expectations;
- vulnerability disclosure and remediation timelines;
- AI-specific risk management;
- open data and interoperability;
- vendor replacement rights;
- data portability;
- regulatory alignment;
- continuous review and enforcement mechanisms.

Cybersecurity should not be treated only as a contractual obligation imposed on vendors. It should be treated as a continuously evolving industry governance model.

10. Recommended Additions to the Proposed Framework

Screaming Power recommends that NIST, NAESB, and relevant standards stakeholders consider adding the following principles to the proposed framework:

1. **Utility accountability -** Utilities should assess their own cybersecurity maturity against comparable standards applied to vendors.
2. **Affiliate neutrality -** Utility affiliates and utility-developed commercial platforms should meet the same cybersecurity and transparency expectations as independent vendors.
3. **Canadian alignment -** Canadian cybersecurity guidance, Canadian Centre for Cyber Security materials, CSA-related standards where applicable, and Canadian self-assessment or certification programmes should be considered complementary pathways for demonstrating cybersecurity maturity.
4. **GO-ITS comparability -** Public-sector frameworks such as Ontario GO-ITS should be considered useful reference points for utility procurement, governance, and information security expectations, particularly as utility systems become more interconnected with public-sector, customer, cloud, and third-party platforms.
5. **Open data and interoperability -** Security frameworks should be developed alongside open data, communications, and interoperability frameworks so systems can be replaced, audited, integrated, and migrated without unnecessary cost or disruption.
6. **Vendor replacement rights -** Utilities and customers should be able to replace systems that fail to meet cybersecurity expectations without being constrained by proprietary data formats or restricted access.
7. **AI readiness -** Future standards should explicitly address AI-enabled threats, AI-enabled defence, AI-generated software, AI supply chain risk, and AI governance in critical infrastructure.
8. **Continuous updating -** Standards should include mechanisms for rapid review, revision, and enforcement as threats and technologies evolve.

Conclusion

Screaming Power supports the development of stronger cybersecurity requirements for vendors serving the energy sector. The proposed Cybersecurity General Terms and Conditions are a meaningful step forward and correctly recognise the importance of vulnerability disclosure, product security, secure development practices, SBOMs, and software supply chain transparency.

However, the long-term success of this framework will depend on whether it is applied within a broader and more balanced industry model. Cybersecurity risk does not reside only with vendors. It

also exists within utility-operated systems, legacy infrastructure, utility-developed platforms, utility affiliates, proprietary data environments, and emerging AI-enabled technologies.

The energy sector should therefore use this opportunity to advance an integrated framework that supports cybersecurity, interoperability, open data, competitive neutrality, Canadian alignment, AI readiness, utility accountability, and vendor accountability together.

The most resilient future will be one in which standards bodies, regulators, utilities, vendors, cybersecurity experts, technology providers, and customers collaborate to create systems that are secure, auditable, interoperable, replaceable, and adaptable.

By advancing cybersecurity and open data together, the industry can create a stronger foundation for innovation, consumer access, critical infrastructure protection, and long-term energy sector resilience.

Respectfully submitted,

Gary Michor
CEO
Screaming Power Inc.

Appendix: Supporting Evidence

- The draft vendor terms require cybersecurity policies, vulnerability notices, remediation plans, product attestations, trust verification, audit rights, SBOM information, known vulnerability reporting, product support status, and supplier disclosures.
- Public reporting indicates that 77% of utilities organisations experienced attacks involving outdated software or unavailable patches on legacy equipment during the previous 12 months. [intelligentciso.com]
- DNV reported that 65% of surveyed energy professionals said leadership views cybersecurity as the greatest current risk to the business. [dnv.com]
- Dragos reported industrial ransomware activity increased by more than 87% year over year and that it tracks 23 OT cyber threat groups. [dragos.com]
- Cyble reported 187 ransomware incidents impacting energy and utility organisations worldwide in 2025. [cyble.com]
- CISA states that SBOMs are an “ingredients list” for software and a key building block of software security and supply chain risk management. [cisa.gov]
- Green Button and NAESB ESPI provide established examples of secure, customer-authorised, machine-readable energy data access and data exchange. However, implementation consistency, accountability, and replacement planning remain important considerations for cybersecurity and interoperability policy. [energy.gov], [naesb.org]

- Ontario states that GO-ITS are the official technology standards, guidelines, technical reports, and preferred practices adopted by the Government of Ontario, and GO-ITS 25.0 defines general security requirements for Government of Ontario networks and systems. [ontario.ca], [ontario.ca]
- The Government of Canada's CPCSC Level 1 self-assessment refers to 13 security requirements and controls for certain suppliers handling specified information. [canada.ca]
- NIST has recognised adversarial machine learning risks and has stated that there is no foolproof defence against AI attacks. [nist.gov]