Contract clauses or statutory duties: where cybersecurity obligations come from for defence suppliers

For companies that supply goods or services to defence departments, cybersecurity is not optional. The real question is where the obligation comes from. Is it a contractual requirement written into a specific agreement, or does it flow from a statute or regulation that applies whether the contract mentions it or not? The answer matters because it determines what you must do, who enforces it, and what happens if you fall short.

Understanding the source of your cybersecurity duties helps you plan compliance spending, allocate staff time, and avoid surprises during audits or after an incident. This article compares the two main sources of obligation, contract requirements and statutory duties, and explains when each one applies, how they interact, and what defence suppliers should watch for.

Contract requirements: obligations you agree to

Most defence suppliers first encounter cybersecurity through a contract. A request for proposals or a supply agreement will include clauses that set out security standards, data handling rules, and reporting duties. These clauses are negotiated (or more often accepted as-is) and become legally binding once the contract is signed.

Contract requirements are specific. They might reference a standard such as NIST SP 800-171 or the Canadian government's ITSG-33, or they might set out bespoke rules about encryption, access controls, and breach notification. Because they are written into a particular agreement, they apply only to the work covered by that contract. A supplier might have one contract with strict security measures and another with looser ones, depending on what each customer demands.

The advantage of contract-based obligations is clarity. The contract says what you must do, by when, and often how to prove you have done it. Non-compliance is a breach of contract, which can lead to financial penalties, loss of the contract, or being barred from future bids. For many suppliers, the immediate risk of losing revenue concentrates the mind.

The downside is inconsistency. A supplier juggling multiple defence contracts may face different security regimes for each one, creating administrative overhead and the danger of missing a requirement buried in a schedule. Contract requirements also change only when the contract is renegotiated, so they may lag behind evolving threats or updated standards.

Statutory duties: obligations the law imposes

Statutory duties come from legislation or regulation, not from any agreement between parties. In Canada, several laws impose cybersecurity obligations on organisations that handle personal information, operate critical infrastructure, or supply the government. Examples include the Personal Information Protection and Electronic Documents Act (PIPEDA), which requires safeguards for personal data, and the Security of Canada Information Sharing Act, which relates to threats to national security.

For defence suppliers, the most relevant statutory duties often flow from sector-specific regulations. The Canadian government's Industrial Security Program, for instance, sets baseline security requirements for companies that handle classified information. These are not optional: they apply regardless of what any individual contract says.

Statutory duties tend to be broader and less prescriptive than contract clauses. They set a standard (for example, "appropriate safeguards") rather than a checklist. This gives organisations flexibility in how they comply, but it also creates uncertainty. What counts as "appropriate" can depend on the context, and regulators may interpret it differently after an incident.

Enforcement also differs. Breaching a statutory duty can result in regulatory fines, orders to change practices, or even criminal liability for senior officers. The reputational damage can be severe. Unlike a contract dispute, which stays between the supplier and its customer, a regulatory action is often public.

How they interact: overlapping and reinforcing

For most defence suppliers, contract requirements and statutory duties are not alternatives. They coexist, and often the stricter of the two sets the floor. A contract may reference a statutory standard, making compliance with that law a contractual obligation as well. Or a statute may require measures that go beyond what the contract demands, meaning the supplier must meet the higher bar regardless.

This layering can create confusion. A supplier might believe it is compliant because it has passed a contractual audit, only to discover that a regulator expects additional controls under a separate law. The reverse also happens: a supplier that meets statutory requirements may still be in breach of a contract that demands more.

The practical takeaway is that defence suppliers should map both sets of obligations for each contract and for their general operations. That means reviewing not only the security clauses in current agreements but also the statutes and regulations that apply to the type of data handled, the industry sector, and the relationship with the government. One resource that can help suppliers navigate this overlap is Infosec Hub Canada Canadian cybersecurity compliance

guidance, which provides plain-language explanations of the frameworks and duties that typically apply to defence work.



When contract requirements dominate

Contract requirements are the main source of obligation when the work does not involve personal information or classified data, and when no sector-specific regulation applies. For example, a supplier that manufactures metal components for a defence vehicle may handle no sensitive data beyond basic contact information. In that case, the contract itself is likely the only source of cybersecurity duties.

Contract requirements also dominate when the customer is a private prime contractor rather than a government entity. Private primes can impose their own security standards, but those standards are not backed by statute unless they reference one. The supplier's duty runs to the prime, not to a regulator.

In these situations, the supplier should focus on negotiating clear, achievable security clauses and on documenting compliance for each contract. The risk of a statutory penalty is low, but the risk of losing the contract for non-compliance is real.

When statutory duties dominate

Statutory duties take centre stage whenever the work involves personal information, classified information, or systems that are part of Canada's critical infrastructure. Defence suppliers that

handle employee data, subcontractor records, or technical data subject to export controls will find that statutes set the baseline.

Government contracts almost always trigger statutory duties because they incorporate standards such as the ITSG guidance or the Contract Security Program. Even if the contract language is vague, the supplier is still bound by the underlying regulations. In practice, this means a supplier cannot rely on a contract that says nothing about cybersecurity to avoid compliance: the law may still require it.

When statutory duties dominate, the supplier should invest in a compliance program that meets the highest applicable standard, rather than tailoring controls to each contract. This approach reduces administrative burden and lowers the risk of missing a regulatory requirement.

Practical steps for defence suppliers

Start by listing every contract you hold that involves defence work. For each one, pull out the cybersecurity clauses and note which standards they reference. Then identify the statutes and regulations that apply to your organisation based on the data you handle, your industry classification, and your relationship with the government.

Compare the two sets of obligations. Where they conflict, the stricter one generally prevails. Where one is silent and the other is not, the explicit requirement fills the gap. Document your reasoning so that an auditor or regulator can see you have considered both sources.

Build a compliance framework that can adapt. Contract requirements change when contracts are renewed; statutory duties change when laws are amended. A framework that tracks both sources and flags updates will save time and prevent oversights. The plain-language resources available through Infosec Hub Canada Canadian cybersecurity compliance can help suppliers understand what each framework requires and how they fit together.

Finally, do not treat compliance as a one-time exercise. Both contract requirements and statutory duties evolve. A supplier that reviews its obligations annually, and after every major contract change, will stay ahead of the curve and avoid the scramble that follows an incident or an audit.