NORTHFLEET

GUIDE

Seven questions about the software

For buyers and accreditors of classified or disconnected systems

NOVEMBER 2026 VERSION 1.0 · TLP:CLEAR northfleetsecurity.ca

SUMMARY

Software for a classified or disconnected system keeps arriving for decades after the contract is awarded. These are seven questions to put to whoever supplies it, each with what a good answer looks like and the evidence to ask for. They fit in a contract's terms, a statement of work or an intake rule.

CONTENTS

03 Why these seven

03 What's in it and who ships each piece?

03 What's each release checked against?

04 Does the check still work with the cable out?

04 Would you hear if the builder changed?

05 What record stays with the operator?

05 What happens the day the deliveries stop?

05 What do these checks miss?

06 The seven on one page

07 Where they fit

07 Sources

Why these seven

Plenty of what National Defence buys has software in it. In February 2026 Canada's Defence Industrial Strategy warned that foreign control can restrict a buyer's access to "the needed IP, schematics and software updates". It promised that "Procurement decisions by the DIA [the Defence Investment Agency] will include steps to mitigate these risks to sovereign control."

We went looking for those steps in the federal budget and in Bill C-40, which would make the agency a Crown corporation, and didn't find them. If the agency asks what its "steps to mitigate" should look like for software, this is the list we'd hand over.

They're for anyone buying, accrediting or building software that goes into a classified or disconnected system. Each comes with the answer we'd hope to hear and the evidence to ask for.

What's in it and who ships each piece?

Ask for a list of every software component the system needs to keep running, with who builds each one, who signs it, where its updates come from and which country's law could restrict it.

The supplier should already have it as a document, with a date on it, and every component in the bill of materials shipped with the last release should be on it. Most lines will sit outside Canada. Base images, libraries and build tools mostly do, and nobody's going to move them. You're reading it to see whether the supplier knows which country's law could restrict each line, and which lines a buyer could check without asking whoever owns them.

The Canadian Centre for Cyber Security's Medium impact profile, which replaced its Protected B profile in April 2026, asks for an assessment of the injury from external legal compulsion (control SA-400). For software, we'd start that assessment from this list.

What's each release checked against?

The operator should check the supplier's signature before anything's installed, against a key or signing identity that the operator pinned ahead of time and got by some route other than the release itself. The release should also come with provenance, a record that names the source it was built from and the build that produced it.

A hash read off the supplier's portal comes from the same place as the release, so it's no help if someone has tampered with the portal itself. If the supplier ships its own checking tool, the tool needs the same treatment or it's vouching for itself.

Ask to see the record of the last release that came in. It should show what the release was checked against, who did the check and where the key came from.

Does the check still work with the cable out?

The Medium impact profile puts administrative work on a workstation with no internet access (control SI-400), which is where a release gets applied. The profile says it doesn't address the capabilities of sophisticated state actors, so treat it as a floor. For critical infrastructure, the Cyber Centre asks operators to "be prepared to isolate systems for up to 3 months" and to plan a rebuild from "trusted offline copies and immutable backups". A check that calls out to a verification service, a licence server or an online log fails in both places.

The supplier should be able to list what has to be on the shelf for the check to finish: the release itself, its provenance, the root certificates and keys it's checked against, and a dated revocation list. It should also know what happens when a signing certificate expires in week six. A good answer is that the signature is judged as of a signed timestamp that travels with the release.

For evidence, ask for a demonstration. Pull the cable, rebuild one system from the shelf and write down everything that reaches for the network.

Would you hear if the builder changed?

A supplier's own signature verifies just as well after the supplier's been compromised or compelled. Provenance signed by a build service the supplier doesn't run covers one case: a release that carries the supplier's signature but was built somewhere else. Its provenance names a different builder, so a check pinned to the builder and the source repository fails. It doesn't cover a change pushed through the usual source and build, which the last question comes back to. Ask which build service signs the provenance, and which country's law that service sits under.

Then ask whether the contract requires the supplier to tell you when the company is sold, when a signing key or the build platform changes, or when a dependency changes hands. If the answer's yes, ask which clause. Whatever the contract already says about a change of

ownership, check that it reaches the key, the build platform and the dependencies. The power in Bill C-40 to exclude a bidder from a competition would apply to what's proposed when the bid comes in, and software keeps arriving for decades after award.

What record stays with the operator?

Each release that comes in should leave a dated entry on the operator's own systems with what arrived, what it was checked against, who approved it and where it went in. Without phoning the supplier or logging in to its portal, the operator should be able to produce a list of every release that's ever come in.

An accreditor will want the record anyway. When a bad release turns up later, it's also how you find out where that release went. Ask for last quarter's entries.

What happens the day the deliveries stop?

Suppliers get sold and products get dropped. Does the software need a licence renewed to keep running, and what does it do the day after the licence lapses? Is the last good release sitting with the operator? How long was the system designed and tested to run with no new patches, and on what assumptions?

Escrow is a common answer for the long run, and the terms are worth reading. Check whether the source is released when support stops, and whether the deposit is kept up to date. Check too whether the deposit holds everything a rebuild would need, toolchain and libraries included, and whether anyone on the buyer's side could run the rebuild.

What do these checks miss?

A release that was bad when the supplier built it passes everything above. So does a backdoor written into the source, or a release from a new owner who kept the key and the build service and changed the code.

Rebuilding from source and comparing catches a release that doesn't match its source, but only for software whose build comes out the same twice, and it trusts the tools used for the rebuild. A backdoor in the source builds clean either way. That one takes somebody reading the code. With closed-source software the buyer gets to do either only if the contract says so.

Good answers to the first six questions give the operator a say over when a release goes in and a record of where it went. Trust a supplier more if it tells you what its checks miss before you ask.

The seven on one page

#	QUESTION	A GOOD ANSWER	ASK TO SEE
1	**What's in it and who ships each piece?**	A dated list of every component: who builds it, who signs it, where its updates come from and whose law could restrict it.	The list, beside the bill of materials from the last release.
2	**What's each release checked against?**	The supplier's signature, checked against a key or signing identity the operator pinned ahead of time and got by another route. Provenance that names the source and the build.	The record of the last release that came in.
3	**Does the check still work with the cable out?**	A list of what has to be on the shelf, and a signature judged as of a signed timestamp, so a certificate can expire while the system is isolated.	One system rebuilt from the shelf with the cable pulled, and the list of everything that reached for the network.
4	**Would you hear if the builder changed?**	Provenance signed by a build service the supplier doesn't run, checked against a pinned builder and source repository, and a contract that requires notice of a sale or a change of key, build platform or dependency owner.	The name of the build service, the law it sits under, and the clause.
5	**What record stays with the operator?**	A dated entry for each release on the operator's own systems.	Last quarter's entries, produced without the supplier.
6	**What happens the day the deliveries stop?**	Known behaviour when the licence lapses, the last good release held by the operator, a tested period the system can run unpatched, and escrow that releases the source when support stops and holds everything a rebuild needs.	The escrow terms, and the last good release on the operator's shelf.
7	**What do these checks miss?**	A supplier that names what its checks don't catch.	For closed-source software, the contract terms that let the buyer rebuild from source or read the code.

Where they fit

We don't think any of the seven needs Bill C-40 to change. They fit in a contract's terms, a statement of work or an intake rule, and a supplier can have its answers ready before anyone asks.

About Northfleet. Northfleet is a Canadian-incorporated vendor building the sovereign supply chain that wraps a customer-operated classified cluster: a deploy-time bundle protocol, attestation chain, and tamper-evident audit trail. The design has the customer's cleared engineering teams operate the cluster under their own keys. Northfleet holds no customer data and no customer signing keys. Every release Northfleet ships carries provenance binding it to the source it was built from, which the customer can check without Northfleet's participation. The architecture assumes the vendor can be compromised or compelled, so compelling Northfleet doesn't produce a silent backdoor, though catching one depends on someone actually checking releases against their source and reading that source.

Corrections are welcome at corrections@northfleetsecurity.ca. To talk through the questions, or your own answers to them, write to us at northfleetsecurity.ca/contact.

Sources

National Defence, Security, Sovereignty and Prosperity: Canada's Defence Industrial Strategy, February 17, 2026. Pillar II, under "BUY: Acquire from Others with Domestic Reinvestment and Sovereign Control".

Canadian Centre for Cyber Security, Suggested organizational security and privacy control and activity profile, Medium impact (ITSP.10.033-01), April 2026. Controls SA-400 and SI-400.

Bill C-40, Strengthening Canada's Defence Sector Act, first reading, October 6, 2026. Amendments to the Defence Production Act, s. 29.

Canadian Centre for Cyber Security, Critical Infrastructure Resilience and Escalated Threat Navigation (CIREN) initiative, last modified September 18, 2026.

Northfleet field notes, at northfleetsecurity.ca/field-notes. Each carries its own sources.

- Who holds the switch, August 26, 2026. The operator's record.
- Already in the rulebook, September 18, 2026. The Protected B profile's control text.
- How far down the supply chain, October 28, 2026. The component list.
- What Europe will ask Canada to prove, November 3, 2026. The component list.
- Federal budget: masters of our destiny, software updates sold separately, November 5, 2026. The budget and Bill C-40.
- Three months offline, November 10, 2026. What reaches for the network.
- Palantir at DND: who checks the updates?, November 11, 2026. Keys, hashes and portals.
- Buy Canadian: owned here, built where?, November 16, 2026. Builders, sales and escrow.

- Defence industry at committee: seven questions about the software, November 19, 2026. The note this guide is drawn from.

© 2026 Northfleet Security Ltd. This guide may be copied and shared whole. It describes public guidance as of its date and is not advice on any particular system.