China's New GB Standards: Complying with GB 44495-2024 & GB 44496-2024

China's new mandatory cybersecurity standards for connected vehicles don't require a specific SBOM format *(at least for now).* However, they do require a Cybersecurity Management System (CSMS) and a Software Update Management System (SUMS) that, in practice, are impossible to run without high-fidelity SBOMs across all ECUs/software variants.

What's New:

- **GB 44496-2024** *(software update)* enforced for new type approvals from Jan 1, 2026, and for existing types by Jan 1, 2028
- **GB 44495-2024** *(vehicle cybersecurity)* defines the overarching CSMS controls these SBOM workflows sit inside

SBOM-Driven Compliance: What You Need to Implement

Software Inventory & Traceability per Vehicle Type

- Maintain SBOMs per ECU and software version (firmware, middleware, apps, bootloaders).
- Link SBOMs to "same type identification" configuration used in GB 44495/44496 testing and documentation.
- Expect auditors to sample versions against your declared type/config list.

Embed SBOMs into CSMS & SUMS Workflows

- CSMS (GB 44495): Show policies and evidence that SBOMs drive vulnerability monitoring, risk assessment, and incident response across the lifecycle.
- SUMS (GB 44496): Demonstrate that update planning/validation, rollback, authenticity/integrity checks, and post-deployment monitoring use SBOMs to determine impact and coverage.
- Audits include OTA/offline update security tests; you'll need component/version lineage to pass.

Map Vuln Intel to China's Vulnerability Databases (Not Just CVE/NVD)

- Correlate SBOM components with CNNVD/CNVD entries (in addition to CVE/NVD/EPSS) and keep evidence of triage decisions.
- Maintain triage documentation and show awareness of Chinese vulnerability disclosures.

Flow-Down to Suppliers

- Contractually require Tier-1/2 suppliers to deliver machine-readable SBOMs (SPDX/CycloneDX) for each release.
- Collect supplier attestations on build provenance, signing, and vulnerability remediation windows to demonstrate CSMS control. *(This aligns with Auto-ISAC SBOM guidance used by many Chinese labs and consultancies as "good practice".)*

SBOM Deltas for Updates

- Maintain a linked "delta SBOM" for every OTA/offline update package (*required under GB 44496).*
- Provide a pre/post-update vulnerability impact analysis — new, resolved, introduced. (*This directly supports GB 44496 test items for authenticity/integrity and operational safety of updates.)*

Localisation & Audit Prep

- Prepare an audit binder with: SBOM generation SOPs, tool qualification notes, sampling logs per vehicle type, vulnerability correlation reports (incl. CNNVD), update safety assessments, rollback plans, and incident playbooks.
- Provide Chinese-language summaries of key procedures and evidence lists to accelerate type testing. *(GB 44495/44496 documentation sections explicitly call out management system evidence and same-type documentation.)*

Testing Cadence that Matches GB "Lifecycle" Expectations

- Demonstrate continuous monitoring: Regenerate SBOMs for release candidates, hotfixes, and post-SOP maintenance.
- Re-scan against CNNVD/NVD on a defined cadence.
- Retain history to prove issue aging/closure SLAs under the CSMS. *(Industry guidance and Auto-ISAC reporting back this expectation even if the GB text doesn't dictate a specific interval.)*

Data Residency & Cross-Border Awareness

SBOMs are usually non-personal, but your CSMS/SUMS evidence can reference telemetry and development logs. Cross-border data governance is primarily regulated by the CAC, with MIIT issuing sector-specific automotive guidance. If any CSMS/SUMS evidence contains vehicle or user-derived data, plan for local storage in China or be prepared to run a CAC cross-border data transfer assessment before exporting.

Plan accordingly if your vuln-intel or update validation relies on cloud systems outside China.

Quick Start Checklist

- [x] Pick one canonical format (SPDX 2.3+ or CycloneDX 1.5+), and enforce it across all suppliers.
- [ ] Generate SBOMs per ECU image + a merged system SBOM per vehicle type; sign them.
- [ ] Map each SBOM to type-approval config IDs and maintain version lineage.
- [ ] Automate correlation to CNNVD/CNVD + NVD/EPSS; capture triage reasoning.
- [ ] For every OTA/offline update, produce a delta SBOM + safety & security impact memo (pre/post).
- [ ] Localise key SOP summaries/evidence lists; pre-assemble your GB 44495/44496 audit pack.

FINITE STATE

GB 44495 / 44496 SBOM Compliance Playbook

The GB standards do not explicitly require or reference SBOMs. However, SBOMs are the most practical, defensible mechanism for proving software inventory, update integrity, and vulnerability-monitoring processes required under CSMS (GB 44495) and SUMS (GB 44496).

Scope & Standards

- **GB 44495-2024** — Cybersecurity Management System *(CSMS)*
- **GB 44496-2024** — Software Update Management System *(SUMS)*
- Applies to all new type approvals from Jan 2026 & to existing type approvals by Jan 2028

Core SBOM Deliverables

- **Per-ECU SBOMs:** Firmware, middleware, bootloaders, apps.
- **System SBOMs:** Aggregated by "vehicle type" as defined in type approval.
- **Delta SBOMs:** For every OTA/offline update (pre/post comparison).
- **Audit Evidence:** SOPs for SBOM generation, tool qualification, vulnerability triage reports, linkage to CSMS & SUMS controls.

Workflow Integration

CSMS (GB 44495)

- Continuous vulnerability monitoring tied to SBOM
- Incident response playbooks referencing component/version lineage

SUMS (GB 44496)

- Update planning validated via SBOM deltas
- Rollback safety analysis linked to component dependency chains.
- Authenticity/integrity of update packages checked against signed SBOM metadata.

Vulnerability Intelligence Challenges

- **NVDB** (国家漏洞库) & **CNNVD** (中国国家信息安全漏洞库) are authoritative for GB audits.
  - They are often geo-restricted, slow to sync with NVD, & may list CVEs under different IDs.
  - Proof of monitoring requires local presence or proxy arrangements — you can't just show NVD/EPSS correlation.
- **Compliance Pitfall:** Auditors may ask for evidence that your monitoring pipeline queries CNNVD/NVDB inside China & that triage reports explicitly note both "found" & "not-found" results.

Supplier Management

- Flow down SBOM delivery requirements (SPDX 2.3 or CycloneDX 1.5+) to Tier-1/2s.
- Require signed attestations of build provenance, vuln scans (including CNNVD), & remediation SLA alignment.
- Integrate supplier SBOMs into system SBOMs before type approval submission.

Government Approval Nuances

- MIIT-recognised labs may require attestation that your SBOM vuln checks run against CNNVD/NVDB within China.
- In some cases, OEMs need to contract local partners (Chinese test labs, JV subsidiaries) to host vulnerability scanning infrastructure inside China.
- Exporting SBOMs or vuln logs for processing outside China can trigger cross-border data transfer assessments — particularly if logs contain operational or telemetry data.

Lifecycle Evidence Pack

- English + Chinese summary of SBOM policies & SOPs.
- SBOM generation logs, sampling reports tied to “same-type” ID.
- Vulnerability monitoring records: NVD + CNNVD/NVDB correlation, triage memos.
- Update integrity package: Delta SBOMs, rollback tests, authenticity proofs.
- Incident response drills showing SBOM use in vuln containment.

Common Gaps to Anticipate

- **Tool qualification:** Proving SBOM tools generate reproducible outputs auditors can trust.
- **CNNVD access:** OEMs often fail because their vuln intelligence is purely NVD-based.
- **Local scanning requirement:** Lack of infrastructure in China to run automated checks.
- **Supplier drag:** Tier-1s may resist sharing full SBOMs; regulators will not accept “black box” components without inventory.

Next Step Recommendations

- Stand up a China-based vuln monitoring node (either JV partner or lab-hosted) to query CNNVD/NVDB & log correlation results.
- Build an SBOM compliance binder (English/Chinese) with sample ECU SBOM, system SBOM, delta SBOM, CNNVD triage report, update safety analysis.
- Dry-run the binder with a local GB lab to catch interpretation issues before mandatory testing begins.