



OT-ISAC

OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

OT-ISAC TLP:CLEAR – Recipients may share **TLP:CLEAR** information without restriction. **TLP:CLEAR** information may be distributed freely, subject only to copyright controls. It is suitable for public release, including to media, the wider community, and external stakeholders, because it poses no foreseeable risk of misuse in its current form.

In the spirit of community-driven effort, we'd like to encourage our Members and Partners to share information to enable our community better to defend itself and improve situational awareness. Most importantly - If your organization require direct assistance from OT-ISAC, feel free to submit to OT-ISAC Member's Portal- our team will work with you to ensure all necessary support is available through the member submission and RFI process.

Disclaimer: This information is provided as-is for informational purposes only and comes with no expressed or implied warranties. While efforts have been made to ensure the accuracy and reliability of the information, the evolving nature of cybersecurity threats means that vulnerabilities, impacts, and best practices may change over time. You (and any individual or entity you represent) bear full responsibility for all actions and omissions made based on this information. OT-ISAC disclaims any responsibility or liability for any such actions or omissions.

APAC OT/CI Cyber Policy Intelligence Report

Cybersecurity, critical-infrastructure and OT/ICS policy developments

Data current as of 20 October 2026

Asia-Pacific with global policy context

Classification	TLP:CLEAR
Produced by	OT-ISAC Threat Intelligence Team
Reporting cut-off	20 October 2026
Primary focus	Cybersecurity laws, CI/CII rules, OT/ICS standards and formal policy developments
Audience	APAC critical-infrastructure operators, security leaders and OT engineers

Executive Policy Position

Across APAC, policy requirements are diverging between binding CI/OT controls, supervisory inspection, and non-binding strategy. Japan, India and Singapore warrant direct regulatory applicability checks; proposed measures in Vietnam and Singapore require separate monitoring rather than premature compliance claims.

Contents

TLP:CLEAR Handling Notice

Source Coverage and Methodology Note

Executive Summary

1. Policy Decision Matrix
2. Substantive Rules, Codes and OT/ICS Requirements
3. Proposed and Emerging Policy Developments
4. Member Action Priorities
5. Coverage Decisions, Evidence Gaps and Outlook
6. References – Primary Sources First

Status convention: in force / approved for future commencement / draft or consultation / formal non-binding strategy.

Retrospective additions are dated and labelled rather than presented as current-week policy.

TLP:CLEAR Handling Notice

TLP:CLEAR – This report is based on publicly releasable information and may be shared without restrictions under FIRST TLP v2.0, subject to any applicable copyright or other source-use conditions.

Source Coverage and Methodology Note

Prepared from published legislation, government gazettes, regulator notices and public consultation portals available at the reporting cut-off. Legal status, publication dates and implementation dates are distinguished; OT/ICS applicability is assessed separately from operational criticality. Coverage is selective rather than exhaustive. Where primary legislation, implementing rules or official translations were unavailable, limitations are disclosed in the relevant section.

Executive Summary

This report covers substantive cybersecurity, critical-infrastructure and OT/ICS policy developments, excluding cyber incidents, threat activity, vulnerability announcements and generic defensive advisories. A 20 October editorial review has updated Singapore’s Digital Infrastructure Bill status and added three verified Vietnam policy instruments. Retrospective additions are dated explicitly; binding measures, formal non-binding policies and draft consultations are distinguished.

Key judgment. Japan’s unified critical-infrastructure standards (effective 1 October), India’s notified power-sector OT cybersecurity regulations (generally effective 1 April 2027), Singapore’s CII Code of Practice 2026 and Australia’s government legacy-technology direction reflect distinct regulatory approaches. Singapore’s Digital Infrastructure Bill passed Parliament on 7 October, although commencement of its proposed licensing obligations has not been verified. Vietnam has also formalised a national cybersecurity architecture and assurance index, while consulting on a national IoT device standard. ^{[1][4][6][8][14][15][16][18]}

Additional policy developments. Australia’s ASD Essentials for OT, published on 15 October 2026, introduces purpose-built government cybersecurity guidance for industrial environments. Taiwan’s control-system baseline, issued 16 September and effective 1 January 2027, establishes requirements for designated communications and broadcasting CI providers. Singapore’s Cybersecurity Strategy 2026 and October quantum-safe advisory and grant initiatives reinforce policy attention to critical infrastructure, technology dependencies and long-term cryptographic resilience. These developments are distinguished by legal status and scope. ^{[19]–[24]}

Freshness distinction. Singapore’s parliamentary passage (7 October), Vietnam’s Cybersecurity Assurance Index (12 October) and national IoT standard consultation (14–24 October) were not captured in the prior report. Vietnam’s National Cybersecurity Architecture Framework (30 September) is a retrospective addition. Other previously tracked instruments are retained because commencement, implementation and consultation milestones remain relevant. ^{[12][14]–[18]}

1. Policy Decision Matrix

Jurisdiction	Instrument / policy	Status / date	OT/CI relevance	Legal character
Japan	CI Unified Standards	In force, 1 Oct	Direct CI / OT implementation	Substantive standard ^[1]
India	CEA Power-Sector Cyber Regulations	Notified; 1 Apr 2027*	Direct OT (power)	Binding sector regulation ^{[6][7]}
Australia	PSPF Direction 002-2026	Issued, 29 Sep	Government / OT where scoped	Binding direction ^[4]
China	MPS Inspection Measures, Order 176	In force, 1 Oct	CII / OT-adjacent	Binding supervisory rule ^[5]
Singapore	CII Code of Practice 2026	Issued, 29 Jul	Direct CII / OT	Binding code ^{[8][9]}
Australia	ASD Essentials for OT	Issued, 15 Oct 2026	Direct OT/ICS	Official non-binding guidance ^{[19][20]}

Jurisdiction	Instrument / policy	Status / date	OT/CI relevance	Legal character
Taiwan	Control-System Security Baseline	Issued 16 Sep; effective 1 Jan 2027	Direct; designated communications/broadcasting CI	Regulatory requirements ^[21]
Japan	Special CI cyber event-reporting order	Consultation until 31 Oct	Direct CI	Proposed amendment ^[2]
Japan	Economic Security supplier/equipment rules	Consultation until 31 Oct	Transport/maritime/aviation	Proposed amendment ^[3]
South Korea	Major Infrastructure vulnerability criteria	Draft, 11 Sep	Direct CI; OT as applicable	Administrative consultation ^[11]
Sarawak, Malaysia	Cybersecurity Strategy 2030	Launched, 5 Oct	CI / OT-adjacent	Non-binding policy ^[12]
Singapore	Digital Infrastructure Bill	Passed Parliament, 7 Oct; commencement unverified	Cloud/data-centre OT dependencies	Passed Bill; not confirmed in force ^{[10][14]}
Singapore	Cybersecurity Strategy 2026	Launched, 13 Oct 2026	Direct CI strategic relevance	Non-binding national strategy ^[22]
Singapore	Quantum-Safe Migration Guidance	CII guidance Jun; additional advisory 14 Oct	Direct CII; OT-adjacent elsewhere	CII-specific guidance / wider advisory ^{[23][24]}
Vietnam	National Cybersecurity Architecture Framework v1.0	Decision 1875, 30 Sep (retrospective)	Public-sector / CI-adjacent	Issued PM decision; in effect ^[15]
Vietnam	Cybersecurity Assurance Index	Decision 1964, 12 Oct; pilot 2027–28	Government info systems; OT applicability unproven	Issued PM decision; phased assessment ^{[16][17]}
Vietnam	Draft National IoT Cybersecurity Standard	Consultation 14–24 Oct	IoT / potential industrial devices	Draft standard only ^[18]

* Six specified CEA provisions have separate commencement mechanisms. All dates are local to the relevant jurisdiction. The issue date is not always the legal commencement date.

2. Substantive Rules, Codes and OT/ICS Requirements

2.1. Japan – Unified Critical Infrastructure Cybersecurity Standards

Status: In force; government-led cross-sector baseline | **Date(s):** Adopted 31 Jul; effective 1 Oct 2026

Applicability: CI ministries and designated operators via sector implementation | **OT relevance:** Direct CI; sector-specific OT details pending | **Assessment confidence:** High

CONFIRMED POLICY DEVELOPMENT. Japan's NCO confirms that the Unified Standards for Cybersecurity Measures for Critical Infrastructure, adopted on 31 July, and accompanying sector-standard guidelines, issued on 11 September, entered into force on 1 October 2026. They establish a cross-sector baseline emphasising management-level engagement, organisation-wide risk management and supply-chain resilience. The complementary revised Critical Infrastructure Cybersecurity Action Plan promotes incident preparedness, continuous improvement and public–private, cross-sector information sharing. Sector-specific implementation remains relevant. ^[1]

OT-ISAC ASSESSMENT. The change reinforces that OT resilience depends on governance, supplier oversight, exercises and trusted information sharing—not technical controls alone. Shared signals and operational lessons can strengthen collective preparedness, but the policy does not establish uniform new PLC/SCADA controls. Individual operator obligations require sector-specific validation.

MEMBER ACTION. Japanese CI operators should map the unified baseline against existing sector and OT requirements; assess governance, supplier dependencies, response exercises and established information-sharing channels; and monitor ministry implementation guidance before changing technical controls.

2.2. India – CEA Cyber Security in Power Sector Regulations, 2026

Status: Notified regulation; future commencement | **Date(s):** Notified 31 Jul (CEA site 12 Aug); generally effective 1 Apr 2027

Applicability: Covered power entities, OT-connected IT, specified generation/storage thresholds | **OT relevance:** Direct OT/ICS |

Assessment confidence: High

CONFIRMED POLICY DEVELOPMENT. India's Central Electricity Authority notified the 2026 Cyber Security in Power Sector Regulations. The regulations expressly address entities managing OT associated with the interconnected power system and IT physically or logically connected to such OT, with prescribed scope exceptions and generating/storage capacity thresholds. General commencement is 1 April 2027; specified clauses are subject to later orders. ^[6] ^[7]

OT-ISAC ASSESSMENT. Unlike broad enterprise cyber policies, this is an explicit industrial-power regulatory requirement. It may materially affect segmentation, governance, audits, monitoring, incident handling, vendors and operational recovery. Applicability should be mapped from the final notification and asset role rather than assumed from industry sector alone.

MEMBER ACTION. Power-sector members should validate scope, prepare a clause-by-clause gap assessment and a vendor-aware implementation roadmap; account for patch testing, safety constraints and industrial maintenance windows.

2.3. Australia – PSPF Direction 002-2026 on Legacy Technology

Status: Mandatory for scoped Commonwealth entities | **Date(s):** Issued 29 Sep; milestones 31 Dec 2026 and 31 Mar 2027

Applicability: Non-corporate Commonwealth entities and declared SoGS | **OT relevance:** OT-adjacent / direct if systems fall in scope
| **Assessment confidence:** High

CONFIRMED POLICY DEVELOPMENT. Direction 002-2026 requires covered entities by 31 March 2027 to stocktake legacy technologies, prepare and maintain a legacy-technology risk-management plan, and report specified completion evidence. Entities operating Systems of Government Significance (SoGS) have additional measures and stocktake reporting by 31 December 2026. It defines technology scope using PSPF criteria. ^[4]

OT-ISAC ASSESSMENT. This is a binding direction on specified Australian Government entities, not a general SOCI or private-sector OT mandate. Where covered estates include industrial support systems, it may require structured compensating controls and documented lifecycle decisions; the direction itself does not prescribe unsafe immediate OT patching.

MEMBER ACTION. Covered entities should document the applicability decision; inventory legacy systems and supplier support arrangements; prioritise public-facing and significant systems; and map SoGS-specific deadlines to accountable owners.

2.4. China – Order 176, Cyberspace Security Supervision and Inspection Measures

Status: Binding departmental rule in force | **Date(s):** Issued 6 Aug; effective 1 Oct 2026

Applicability: Network operators, data processors and other regulated entities, including covered CII | **OT relevance:** CII / OT-adjacent
| **Assessment confidence:** High

CONFIRMED POLICY DEVELOPMENT. The Ministry of Public Security's revised Measures for Public Security Organs' Supervision and Inspection of Cyberspace Security replace the previous inspection framework. They provide for online and on-site supervision of compliance with existing cybersecurity, data and information-security obligations; the legal basis includes CII protection rules. ^[5]

OT-ISAC ASSESSMENT. This is an inspection/enforcement-process change, not a new PLC/SCADA technical standard. Impacts for industrial operators will depend on their legal classification, regulated systems and relevant underlying obligations.

MEMBER ACTION. Covered organisations should confirm inspection readiness, document applicable legal controls, reconcile cybersecurity/data-security evidence, and maintain remediation and supplier-accountability records.

2.5. Singapore – CII Cybersecurity Code of Practice 2026

Status: Issued Code under Cybersecurity Act | **Date(s):** Issued 29 Jul 2026

Applicability: Designated Singapore CII owners | **OT relevance:** Direct CII/OT | **Assessment confidence:** High

CONFIRMED POLICY DEVELOPMENT. CSA lists the CCoP 2026 as issued on 29 July. Its published policy description covers board oversight, cyber-resilience frameworks, oversight of interconnected systems, network visibility/detection, exercises and Cyber Trust Mark expectations. CSA separately signalled future cloud-hosted CII requirements; these are not yet assumed to be issued. ^{[8] [9]}

OT-ISAC ASSESSMENT. The explicit focus on interconnected systems makes this directly relevant to OT environments with enterprise identity, engineering support, remote maintenance and OT-DMZ dependencies. The exact applicable clause and implementation schedule must be validated from the CCoP text and CII designation.

MEMBER ACTION. Singapore CII owners should perform an evidenced CCoP delta review covering OT-connected networks and third parties, and track official cloud-specific CCoP publication separately.

2.6. Australia – ASD Essentials for Operational Technology

Status: Official non-binding cybersecurity guidance | **Date(s):** Published 15 Oct 2026

Applicability: Government, critical-infrastructure operators and organisations managing OT | **OT relevance:** Direct OT/ICS |
Assessment confidence: High

CONFIRMED POLICY DEVELOPMENT. The Australian Signals Directorate (ASD) introduced ASD Essentials on 15 October 2026, extending its Essential Eight guidance into dedicated chapters for enterprise IT, operational technology (OT) and cloud environments. Essentials for OT provides risk-informed guidance

across eight domains and priority phases, including critical processes, network boundaries, identity services, privileged environments, governance and response. The framework defines 'vital OT' as systems whose extended unavailability would be unacceptable for maintaining minimum safe service delivery. ^{[19][20]}

OT-ISAC ASSESSMENT. The guidance explicitly recognises safety, availability, legacy equipment and interconnected-system dependencies. It is an official cybersecurity framework, not a new statutory OT control baseline. ASD states that organisations should continue meeting existing regulatory obligations until regulators communicate changes.

MEMBER ACTION. Australian critical-infrastructure operators should compare Essentials for OT with existing security practices and applicable SOCI/CIRMP obligations, prioritising vital OT, IT/OT boundaries, remote access, supplier dependencies and operational recovery.

2.7. Taiwan – Cybersecurity Protection Baseline for Critical Infrastructure Control Systems

Status: Issued regulatory requirements; future commencement | **Date(s):** Issued 16 Sep; effective 1 Jan 2027

Applicability: Designated communications and broadcasting CI providers | **OT relevance:** Direct control-system security | **Assessment confidence:** High

CONFIRMED POLICY DEVELOPMENT. Taiwan's Ministry of Digital Affairs issued the Cybersecurity Protection Baseline for Control Systems of Critical Infrastructure Providers in the Communications and Broadcasting Sectors on 16 September 2026. Effective 1 January 2027, it requires designated providers to implement the published cybersecurity controls for internally developed or outsourced control systems. Operators facing demonstrable technical or architectural constraints may request ministry approval for evidence-supported alternative controls. ^[21]

OT-ISAC ASSESSMENT. This is a directly relevant control-system requirement that recognises implementation constraints in specialised or legacy environments. The alternative-control mechanism enables regulatory review of cases where prescribed measures are impractical. The baseline applies to specified communications and broadcasting CI providers; it is not a universal OT requirement across Taiwan.

MEMBER ACTION. Affected operators should review their control-system security posture against the baseline, document gaps and prepare evidence-supported alternative measures where needed before 1 January 2027.

3. Proposed Regulations and Formal Policy Developments

3.1. Japan – Draft amendment to CI cyber-event reporting order

Status: Public consultation; not in force | Date(s): 1–31 Oct 2026

Applicability: Special Social Infrastructure Operators and covered important systems | OT relevance: Direct CI / possible OT reporting scope | Assessment confidence: High

CONFIRMED POLICY DEVELOPMENT. Japan's e-Gov portal opened consultation Case 095260880 on amendments to the order governing reports of specified intrusion events by Special Social Infrastructure Operators under the Act on Prevention of Damage Caused by Unauthorized Acts Against Critical Computers. ^[2]

OT-ISAC ASSESSMENT. The consultation is a genuine regulatory-development signal, but final thresholds, content requirements and commencement are not established by the existence of the consultation itself. CI operators should avoid treating the draft as current reporting law.

MEMBER ACTION. Local legal/incident-response owners should assess the proposed order and potential reporting workflow changes before the 31 October deadline; watch for the adopted text.

3.2. Japan – Proposed economic-security rules for CI equipment and suppliers

Status: Public consultation; not in force | Date(s): 1–31 Oct 2026

Applicability: Designated social infrastructure; MLIT filing covers land transport, maritime and aviation / procurement | OT relevance: OT supply chain | Assessment confidence: High

CONFIRMED POLICY DEVELOPMENT. Japan's e-Gov portal lists proposed amendments to MLIT implementing rules for specified social infrastructure operators under the Economic Security Promotion Act (Case 155261105). The 1 October consultation covers land transport, maritime and aviation sectors. ^[3]

OT-ISAC ASSESSMENT. This is a policy change under consideration in supply-chain/equipment assurance, but the notice alone does not substantiate a particular new vendor prohibition, technical OT control or procurement threshold. It merits tracking because industrial equipment introduction and maintenance arrangements can be regulated under this regime.

MEMBER ACTION. Procurement, legal and OT engineering teams supporting Japanese regulated assets should review the actual draft and filing forms before responding or changing purchasing policy.

3.3. South Korea – Draft major information-infrastructure vulnerability criteria

Status: Administrative notice; not yet final | Date(s): Published 11 Sep 2026

Applicability: Operators of designated Major Information and Communications Infrastructure | OT relevance: Direct CI / OT applicability depends on designation | Assessment confidence: High

CONFIRMED POLICY DEVELOPMENT. South Korea's Ministry of Science and ICT issued Notice 2026-947 proposing a partial amendment to the Vulnerability Analysis and Evaluation Criteria for Major Information and Communications Infrastructure. Official attachments contain the proposed text. ^[11]

OT-ISAC ASSESSMENT. This could affect how operators assess, evidence and treat technology risk. Without a verified comparison of the Korean-language draft attachments, the report does not assert changed vulnerability schedules, scoring rules or mandatory OT testing procedures.

MEMBER ACTION. Covered operators should retrieve the Korean draft and compare it with current assessment criteria; preserve safety-based test rules and compensating-control processes for production OT.

3.4. Sarawak, Malaysia – Cybersecurity Strategy and Roadmap 2030

Status: Formal strategic policy; not a new regulation | **Date(s):** Launched 5 Oct 2026

Applicability: Sarawak government, state-linked enterprises and CI stakeholder ecosystem | **OT relevance:** OT-adjacent / state CI policy | **Assessment confidence:** Moderate

CONFIRMED POLICY DEVELOPMENT. Sarawak's official Public Communications Unit confirms the launch of SCSR 2030, developed by the Sarawak Multimedia Authority, with 18 strategic initiatives across five pillars and stated engagement with critical-infrastructure operators. ^[12]

OT-ISAC ASSESSMENT. Its direction may influence future state-level assurance programmes and stakeholder coordination. The published launch material does not establish mandatory NCII obligations, and the full roadmap text and detailed implementation instruments have not been verified in this review.

MEMBER ACTION. Members with Sarawak operations should monitor the official roadmap and implementing instruments; do not assign legal obligations based solely on the strategy launch.

3.5. Singapore – Digital Infrastructure Bill

Status: Bill passed Parliament; commencement not verified | **Date(s):** First Reading 8 Sep; passed 7 Oct 2026

Applicability: Qualifying major cloud services and data-centre operators; CI dependent customers indirectly | **OT relevance:** OT-adjacent through shared digital dependencies | **Assessment confidence:** High

CONFIRMED POLICY DEVELOPMENT. Singapore's Parliament lists the Digital Infrastructure Bill (Bill No. 20/2026) as passed on 7 October 2026, following Second Reading. MDDI outlined two proposed licensing regimes: security and resilience for major data centres/cloud providers and environmental sustainability for qualifying data centres. MDDI proposed security/resilience coverage for co-location/cloud data centres with at least 10 MW critical IT load and major cloud providers meeting the specified S\$100 million revenue test. Parliamentary passage is verified; assent, commencement and final implementing codes were not verified in this review. MDDI expects the approved legislation to commence in stages in 2027, once subsidiary regulations, Codes of Practice and licensing arrangements are finalised. Existing operators will have six months after commencement to apply for a licence. This is a projected timetable, not a verified commencement date. ^{[10][14][25]}

OT-ISAC ASSESSMENT. The regulated entities will primarily be qualifying providers, not automatically every CI customer. Potential OT relevance arises through critical dependencies on cloud services, data-centre power and cooling, identity, operational telemetry and hosted support systems. Until commencement and subordinate obligations are established, the Bill should not be described as an in-force licensing requirement.

MEMBER ACTION. Providers should monitor assent, commencement orders, IMDA licensing rules and Codes of Practice; CI operators should map cloud/data-centre service dependencies, contractual recovery expectations and business-continuity arrangements without claiming immediate DIB compliance obligations.

3.6. Vietnam – National Cybersecurity Architecture Framework (Version 1.0)

Status: Issued government architecture decision | **Date(s):** Decision 1875/QĐ-TTg, issued/effective 30 Sep 2026 (retrospective)

Applicability: National/government cybersecurity architecture and shared capabilities | **OT relevance:** OT-adjacent; direct ICS scope not established | **Assessment confidence:** High

CONFIRMED POLICY DEVELOPMENT. Vietnam's Prime Minister issued Decision 1875/QĐ-TTg on 30 September 2026, approving the National Cybersecurity Architecture Framework (Version 1.0), effective the same day. The official policy text establishes national architecture principles for cybersecurity technology, data, governance and shared capabilities. This decision was issued before the prior reporting cutoff and is identified here as a retrospective addition. ^[15]

OT-ISAC ASSESSMENT. The framework is relevant to government-managed digital infrastructure and its dependencies but is not, on the evidence reviewed, a newly mandated PLC/SCADA or private-sector OT cybersecurity baseline. The potential CI impact depends on sector/system classification and implementing directives.

MEMBER ACTION. Public-sector and relevant CI organisations operating in Vietnam should review whether architecture-related investment, interoperability, integration or shared-security arrangements fall within the framework; avoid assuming automatic applicability to operational control assets.

3.7. Vietnam – National Cybersecurity Assurance Index

Status: Issued government decision; assessment pilot planned | **Date(s):** Decision 1964/QD-TTg, 12 Oct 2026; pilot 2027–2028

Applicability: Ministries, agencies and local authorities for pilot evaluation | **OT relevance:** OT-adjacent unless covered system scope established | **Assessment confidence:** High

CONFIRMED POLICY DEVELOPMENT. Prime Ministerial Decision 1964/QD-TTg, issued and effective 12 October 2026, establishes a National Cybersecurity Assurance Index with 29 criteria in three groups. General assessment criteria cover information-system security-level documentation; Level 3-and-above systems receive additional risk, asset, access, supplier, monitoring, recovery and security-management criteria. Government ministries/agencies and local authorities will pilot the index in 2027–2028; adoption for 2029 onward is subject to subsequent decision. Other organisations may use it voluntarily for self-assessment. ^{[16][17]}

OT-ISAC ASSESSMENT. The index signals increasing emphasis on demonstrable cybersecurity assurance and evidence, but the pilot is not a new blanket audit or technical mandate for privately operated ICS. Whether a specific operational system is assessed depends on its inclusion within the government information-system scope and applicable classification.

MEMBER ACTION. Government-sector operators should map applicable information systems and evidence owners, especially for Level 3+ systems; industrial operators should monitor any later sector instructions before extending these criteria to production OT.

3.8. Vietnam – Draft National IoT Device Cybersecurity Standard

Status: Draft technical standard for public comment; not approved or mandatory | **Date(s):** Consultation 14–24 Oct 2026

Applicability: Scope of covered IoT devices requires draft-text and final-standard review | **OT relevance:** Potential industrial IoT / embedded-systems adjacency | **Assessment confidence:** High for consultation, moderate for OT scope

CONFIRMED POLICY DEVELOPMENT. Vietnam's Ministry of Public Security opened a consultation on the draft national standard "Cybersecurity – Internet of Things (IoT) Devices – Basic Requirements" on 14 October 2026, with submissions closing 24 October. The official consultation lists the draft TCVN document but does not itself establish a final standard, mandatory conformity assessment or defined industrial control-system coverage. ^[18]

OT-ISAC ASSESSMENT. Connected sensors, industrial gateways and embedded equipment could share relevant product-security considerations, but there is insufficient verified evidence to conclude that PLCs, RTUs or safety controllers are within scope. National technical standards are not necessarily compulsory absent a separate legal adoption or conformity mechanism.

MEMBER ACTION. Vietnam-facing OT equipment suppliers and operators should review the draft scope, identify any overlap with industrial IoT procurement/security assurance, and submit technically grounded feedback before 24 October where relevant. Do not treat the draft as an operative control requirement.

3.9. Singapore – Cybersecurity Strategy 2026

Status: Formal non-binding national strategy | **Date(s):** Launched 13 Oct 2026

Applicability: CII owners, government and wider cybersecurity ecosystem | **OT relevance:** Direct strategic relevance | **Assessment confidence:** High

CONFIRMED POLICY DEVELOPMENT. Singapore's Cyber Security Agency (CSA) launched the Cybersecurity Strategy 2026 on 13 October 2026. Its four pillars are defending critical infrastructure, securing wider cyberspace, strengthening AI and quantum capabilities, and enhancing resilience through global partnerships. Supporting priorities address ecosystem and workforce capabilities. The strategy places emphasis on national cyber-defence capabilities, interconnected infrastructure and critical-infrastructure resilience. ^[22]

OT-ISAC ASSESSMENT. The strategy signals further national attention to cyber resilience, technology suppliers and connected operational environments. It may influence later OT security initiatives and sector guidance, but does not itself establish new statutory technical controls or independently amend existing CII obligations.

MEMBER ACTION. Singapore CII owners should map relevant strategic priorities against current programmes and monitor CSA's subsequent implementation measures, especially those affecting OT connectivity, third-party dependencies and operational resilience.

3.10. Singapore – Quantum-Safe Migration Guidance and Implementation Support

Status: CII-specific migration guidance; broader non-binding advisory | **Date(s):** CII guidance Jun 2026; advisory/grant 14 Oct 2026

Applicability: Designated CII owners and other organisations exposed to quantum risks | **OT relevance:** Direct CII cryptographic dependencies / OT-adjacent elsewhere | **Assessment confidence:** High

CONFIRMED POLICY DEVELOPMENT. CSA announced a broader quantum-safe migration advisory and the Quantum-Safe Kickstarter Grant on 14 October 2026. Earlier guidance issued to CII owners in June 2026 established milestones, including submission of CII migration plans by 31 March 2027, factoring quantum-safe requirements into new CII procurement from 2028, and completion of CII migration by 31 December 2031. The new October advisory recommends that other organisations exposed to quantum risks prepare migration plans by end-2027 and aim to complete migration by 2035. The grant supports pilots including cryptographic discovery and migration of OT, embedded and legacy systems. ^{[23][24]}

OT-ISAC ASSESSMENT. Migration can be difficult in OT environments with long-lived devices, proprietary protocols, certificate dependencies and limited firmware upgrade support. June's CII milestones and October's broader advisory have different applicability; the October announcement does not create a universal OT cybersecurity mandate.

MEMBER ACTION. CII owners should inventory cryptographic dependencies, assess OEM support and integrate quantum-safe planning into industrial technology refresh and procurement. Other operators should assess whether quantum exposure warrants a risk-based migration plan.

4. Member Action Priorities

- Immediate: verify applicable in-force requirements against asset designation and jurisdiction (Japan CI standards, China inspection rules and Singapore CII CCoP).
- Before 31 October: assess Japan's open reporting and economic-security consultations where operations or suppliers fall within scope.
- By 31 December 2026 / 31 March 2027: covered Australian Commonwealth entities should manage SoGS and legacy-technology direction milestones.
- Before 1 April 2027: Indian power-sector entities should prepare evidence-led OT/connected-IT implementation roadmaps, while tracking separately commenced clauses.
- Continuous: differentiate operational criticality from regulatory accessibility; document safety, availability, validation, compensating controls and responsibilities rather than assuming uniform enterprise IT controls apply to OT.
- Singapore DIB: monitor legal commencement and IMDA subordinate rules; do not assume parliamentary passage immediately activates licence obligations.
- Vietnam: review decisions 1875 and 1964 according to government-system applicability; evaluate the IoT draft only as a proposal before its 24 October consultation deadline.

5. Coverage Decisions, Evidence Gaps and Outlook

Excluded after policy relevance screening. MAS issued AI Risk Management Guidelines on 7 October 2026, but they target financial institutions and have limited direct OT/CI applicability; they are not a principal report item. Australia's data-centre consultation closed on 9 October but did not itself enact a cyber obligation. Taiwan's updated maintenance-plan template was not verified as changing an underlying legal requirement. Cyber incidents, threat activity and general defensive advisories are excluded by design.^[13]

Evidence gaps. India's full CEA notification was cross-checked against the official register and a professional regulatory review because of intermittent access to the original file. Detailed obligations in Japan and South Korea's pending amendments require primary-language redline comparison. Sarawak's complete roadmap text remains unverified. Singapore's DIB assent/commencement and licensing codes are not established here. The Vietnam IoT draft's full technical scope and any future mandatory adoption mechanism require review before making OT-specific compliance claims.

Near-term triggers: Vietnam's IoT standard consultation (24 October); Japan's reporting and economic-security consultations (31 October); Singapore DIB assent, commencement and IMDA Codes of Practice; Singapore Cloud CCoP; Australia's PSPF implementation; India CEA commencement guidance; Vietnam's 2027–2028 cybersecurity index pilot; and South Korea's final major-infrastructure vulnerability criteria. No other material new OT/CI policy development has been verified for New Zealand, Taiwan, Indonesia, Philippines, Thailand, Hong Kong or ASEAN/APEC in this targeted revision; this is not an exhaustive negative finding.

Analytical confidence: High for the existence, publication dates and stated legal status of the Singapore and Vietnam instruments; moderate for future OT applicability, dependent on designation, interpretation and implementing rules. Prior issue correction: Singapore's Digital Infrastructure Bill is no longer merely at First Reading—it passed Parliament on 7 October 2026. This is intelligence analysis, not legal advice.

6. References – Primary Sources First

- [01] Japan, Critical Infrastructure Unified Cybersecurity Standards and Implementation Status | National Cybersecurity Office (NCO), effective 1 October 2026 | <https://www.cyber.go.jp/policy/group/infra/policy.html>
- [02] Japan, Proposed Amendments to Special Social Infrastructure Cyber Event Reporting Order (Case 095260880) | e-Gov Public Consultation, 1 October 2026 | <https://public-comment.e-gov.go.jp/pcm/detail?CLASSNAME=PCMMSTDETAIL&Mode=0&id=095260880>
- [03] Japan, Proposed MLIT Economic Security Promotion Act Implementing Amendments (Case 155261105) | e-Gov Public Consultation, 1 October 2026 | <https://public-comment.e-gov.go.jp/pcm/detail?CLASSNAME=PCMMSTDETAIL&Mode=0&id=155261105>
- [04] Australia, PSPF Direction 002-2026: Strengthening Commonwealth Cyber Posture Against AI-Enabled Risks | Department of Home Affairs, issued 29 September 2026 | https://www.protectivesecurity.gov.au/system/files/2026-09/pspf-direction-002-2026_0.pdf
- [05] China, Ministry of Public Security Order No. 176: Cyberspace Security Supervision and Inspection Measures | Ministry of Commerce Official Policy Register, effective 1 October 2026 | <https://policy.mofcom.gov.cn/claw/clawContent.shtml?id=106601>
- [06] India, Cyber Security in Power Sector Regulations, 2026 | Central Electricity Authority (CEA), notification dated 31 July 2026; website publication 12 August 2026 | <https://cea.nic.in/notification/cyber-security-regulations/?lang=en>
- [07] India, CEA Cyber Security in Power Sector Regulations, 2026: Regulatory Analysis | PwC India, 2026 | https://www.pwc.in/research-insights/news_alert/regulatory-insights/cea-notifies-indias-first-comprehensive-and-legally-binding-cyber-security-regulatory-framework-for-the-power-sector.html
- [08] Singapore, Cybersecurity Code of Practice for Critical Information Infrastructure (CCoP 2026) | Cyber Security Agency of Singapore (CSA), issued 29 July 2026 | <https://www.csa.gov.sg/legislation/codes-of-practice/>
- [09] Singapore, CCoP 2026: Key Changes and Proposed Cloud-Specific Code of Practice | Cyber Security Agency of Singapore (CSA), 22 July 2026 | <https://www.csa.gov.sg/news-events/press-releases/cybersecurity-code-of-practice-for-critical-information-infrastructure-to-be-updated-to-address-apt-and-ai-enabled-threats/>
- [10] Singapore, Digital Infrastructure Bill: Introduction and Public Consultation Outcome | Ministry of Digital Development and Information (MDDI), 8 September 2026 | <https://www.mddi.gov.sg/newsroom/public-consultation-on-the-digital-infrastructure-bill/>
- [11] South Korea, Proposed Revision to Vulnerability Analysis and Evaluation Criteria for Major Information and Communications Infrastructure | Ministry of Science and ICT (MSIT), administrative notice 11 September 2026 | <https://www.msit.go.kr/bbs/view.do?bbsSeqNo=84&mId=109&mPid=103&nttSeqNo=3186402&sCode=user>
- [12] Malaysia (Sarawak), Sarawak Cybersecurity Strategy and Roadmap 2030 (SCSR 2030) | Sarawak Public Communications Unit (UKAS), launched 5 October 2026 | https://ukas.sarawak.gov.my/web/subpage/news_view/50056
- [13] Singapore, Guidelines on Artificial Intelligence Risk Management for Financial Institutions | Monetary Authority of Singapore (MAS), issued 7 October 2026 | <https://www.mas.gov.sg/regulation/guidelines/guidelines-on-artificial-intelligence-risk-management-for-financial-institutions>
- [14] Singapore, Digital Infrastructure Bill: Second Reading Closing Speech and Implementation Timeline | Ministry of Digital Development and Information (MDDI), 7 October 2026 | <https://www.mddi.gov.sg/newsroom/closing-speech-by-sms-tan-kiat-how-for-the-second-reading-of-the-digital-infrastructure-bill/>
- [15] Vietnam, Decision 1875/QĐ-TTg: National Cybersecurity Architecture Framework (v1.0) | Office of Government / Gazette, issued 30 September 2026 | <https://vanban.chinhphu.vn/?docid=219687&pageid=27160>
- [16] Vietnam, Decision 1964/QĐ-TTg: National Cybersecurity Assurance Index | Prime Minister / Government Legal Portal, issued 12 October 2026 | <https://vanban.chinhphu.vn/?docid=219945&pageid=27160>
- [17] Vietnam, National Cybersecurity Assurance Index: 29 Criteria and 2027–2028 Pilot Implementation | Government News Portal, 12 October 2026 | <https://baocinhphu.vn/chi-so-bao-dam-an-ninh-mang-gom-03-nhom-tieu-chi-va-29-tieu-chi-thanh-phan-102261012172316951.htm>
- [18] Vietnam, Draft National Standard on Cybersecurity for Internet of Things (IoT) Devices: Basic Requirements | Ministry of Public Security (MPS), public consultation 14–24 October 2026 | <https://mps.gov.vn/chinh-sach-phap-luat/lay-y-kien-du-thao/ho-so-du-thao-tieu-chuan-quoc-gia-tcvn-an-ninh-mang-thiet-bi-internet-van-vat-iot-yeu-cau-co-ban-1791963103>
- [19] Australia, ASD Essentials: Evolving Our Approach to Cybersecurity Resilience | Australian Signals Directorate (ASD), published 15 October 2026 | <https://www.cyber.gov.au/news/asd-essentials-evolving-our-approach-to-cyber-security-resilience>
- [20] Australia, ASD Essentials for Operational Technology | Australian Signals Directorate (ASD), published October 2026 | <https://www.cyber.gov.au/publication/essentials-for-ot>
- [21] Taiwan, Cybersecurity Protection Baseline for Control Systems of Critical Infrastructure Providers in the Communications and Broadcasting Sectors | Ministry of Digital Affairs (MODA), issued 16 September 2026; effective 1 January 2027 | <https://law.moda.gov.tw/LawContent.aspx?id=GL000203>
- [22] Singapore, Singapore's Cybersecurity Strategy 2026 | Cyber Security Agency of Singapore (CSA), launched 13 October 2026 | <https://www.csa.gov.sg/news-events/press-releases/singapore-launches-cybersecurity-strategy-2026-to-strengthen-national-cyber-resilience/>
- [23] Singapore, Quantum-Safe Migration Timeline for Organisations and Quantum-Safe Kickstarter Grant | Cyber Security Agency of Singapore (CSA), announced 14 October 2026 | <https://www.csa.gov.sg/news-events/press-releases/csa-sets-out-quantum-safe-migration-timeline-for-organisations-and-launches-new-grant/>

[24] Singapore, Quantum-Safe Kickstarter Grant and CII Migration Milestones | Cyber Security Agency of Singapore (CSA), updated 14 October 2026 | <https://www.csa.gov.sg/our-programmes/support-for-enterprises/quantum-safe-kickstarter-grant/>

[25] Singapore, Digital Infrastructure Bill (Bill No. 20/2026) | Singapore Statutes Online / Attorney-General's Chambers, published 8 September 2026 | <https://sso.agc.gov.sg/Bills-Supp/20-2026/Published/20260908>