ISA GLOBAL CYBERSECURITY ALLIANCE



ISAGCA Whitepaper

Japan's Economic Security Promotion Act: Essential Infrastructure Regime and ISA/IEC 62443

www.isagca.org

Document Notice

This paper explains the policy structure of Japan's Economic Security Promotion Act (ESPA) and examines how the ISA/IEC 62443 series of standards can support the implementation of cybersecurity-related risk management measures under the essential infrastructure regime. It is intended for professionals working in legal, regulatory, procurement, engineering, operations, product security and industrial cybersecurity functions.

This paper is provided for technical and informational purposes and does not constitute legal advice.

The Japanese-language Act, Cabinet Orders, Ministerial Orders and official notices are controlling. English translations and English-language Cabinet Office materials are provided for reference and accessibility. Applicability should be assessed against the current sector-specific Ministerial Orders, forms and filing instructions and, where necessary, confirmed through consultation with the competent ministry. [1–9]

ISA/IEC 62443 publications are copyrighted standards. This paper summarizes their scope and uses them as a basis for analysis but does not reproduce their normative text. Conformity with an ISA/IEC 62443 standard, certification against an ISA/IEC 62443 standard, or an assessment result does not, by itself, demonstrate compliance with ESPA.

Prepared for ISA Global Cybersecurity Alliance by:

ShangJyh "SZ" Lin (林上智)

Chief Cybersecurity Advisor, Sun Square Co., Ltd.
sunsquare.tech



Copyright © 2026 International Society of Automation. All rights reserved.

Table of Contents

Executive Summary 3

Purpose, Scope and Method 4

1. ESPA Policy and Regulatory Framework 5
    1.1 Policy Architecture 5
    1.2 Chapter III Regulatory Perimeter 5
    1.3 Facility Introduction and Critical Maintenance 6
    1.4 Notification, Screening and Change 8
    1.5 Risk Management Measures and Evidence 9

2. ISA/IEC 62443 Overview 11
    2.1 Applicability Boundary 11
    2.2 Relevant Publications 12
    2.3 Stakeholder Roles 13
    2.4 Security Levels and Evidence Boundaries 13

3. Mapping ESPA to ISA/IEC 62443 14
    3.1 Mapping Method 14
    3.2 Overall Alignment Across the Cybersecurity Lifecycle 14
    3.3 Detailed Mapping of Cabinet Office Risk-Management Measures 15
    3.3.1 Introduction of Specified Critical Facilities 16
    3.3.2 Entrustment of Critical Maintenance and Management 24
    3.4 Role and Evidence Chain 30

4. Gaps and Implementation Risks 31
    4.1 Requirements Outside the Scope of ISA/IEC 62443 31
    4.2 Areas of Partial Alignment 31
    4.3 Common Implementation Failure Modes 32
    4.4 Practical Implementation Challenges 33
    4.5 Evidence Sufficiency 33

5. Industry Guidance 35
    5.1 Asset Owners 35
    5.2 System Integrator 35
    5.3 Maintenance Service Provider 35
    5.4 Product Supplier 36
    5.5 Cross-Stakeholder Coordination 36

6. Conclusion 38

Glossary 39

References 41

Executive Summary

Japan's Economic Security Promotion Act establishes legal measures to strengthen economic security, including measures to protect the stable provision of specified essential infrastructure services. Under Chapter III of the Act, operators designated as Specified Essential Infrastructure Service Providers are generally required to submit an introduction or entrustment plan to the competent minister for prior screening before introducing a specified critical facility or entrusting its critical maintenance and management to another party. [1,3–8]

The screening examines whether the specified critical facility is highly likely to be used, in connection with the proposed introduction or entrustment arrangement, as a means for a specified disruptive action taken from outside Japan to interfere with the stable provision of specified essential infrastructure services. [1,3–8] The ISA/IEC 62443 series of standards provides requirements and processes for managing industrial automation and control systems (IACS) cybersecurity. It can support IACS risk assessment, system security requirements, secure integration and maintenance, secure product development, vulnerability management and evidence of implementation. Its relevance is strongest where a regulated facility or maintenance arrangement involves an IACS or an automation solution. Its application is less direct where the arrangement concerns only enterprise IT, cloud or information-processing services outside the IACS environment. [10–21]

ESPA establishes legally binding obligations concerning regulated activities, disclosures, government screening and enforcement. ISA/IEC 62443 is an international cybersecurity standards series that provides technical and organizational requirements for managing IACS security. It can support the cybersecurity aspects of an ESPA submission, but it does not determine whether ESPA applies or replace statutory filings, corporate and jurisdictional disclosures, or the competent minister's assessment.

For IACS-related cases, practical implementation requires coordination across the relevant functional roles, including asset owners, system integrators, maintenance service providers, and product suppliers. The Specified Essential Infrastructure Service Provider remains the statutory filer, while relevant evidence may be distributed across system architecture, product development records, component security capabilities, remote access controls, maintenance records and confidential corporate disclosures. The evidence should therefore be distinguished as regulatory, product, system and operational evidence, with clear responsibility for producing, submitting and maintaining each evidence set.

Purpose, Scope and Method

This paper has three purposes. First, it explains the policy and regulatory structure of ESPA, with particular emphasis on the Chapter III essential infrastructure regime. Second, it summarizes the parts of ISA/IEC 62443 most relevant to the introduction of specified critical facilities and the entrustment of critical maintenance and management. Third, it maps the relevant ISA/IEC 62443 publications to cybersecurity-related ESPA expectations by stakeholder role, while identifying legal, corporate, supply-chain, jurisdictional and continuity matters that remain outside the standards.

The principal audience comprises Specified Essential Infrastructure Service Providers and organizations that supply relevant products, integrate systems, perform critical maintenance and management, or develop and maintain IACS products. The analysis uses four functional roles: asset owner, system integrator, maintenance service provider, and product supplier. These roles are used for analytical purposes and do not replace the legal categories established by ESPA. System integrator and maintenance service provider represent distinct activities within the broader service-provider context of ISA/IEC 62443, and one organization may perform more than one role. Product supplier refers to an organization that develops or maintains the relevant IACS product.

The legal analysis is based on the Act, including the amendments enacted by Act No. 38 of 2026 and their applicable commencement status as of the source cut-off date. It also considers the Order for Enforcement, the Basic Guidelines, applicable sector-specific Ministerial Orders, current Cabinet Office implementation materials and the current list of designated providers.[1–8] The standards analysis uses official International Electrotechnical Commision (IEC) publication scopes and publication status, together with International Society of Automation (ISA) descriptions of stakeholder roles and shared responsibility.[10–21]

The mapping classifications used in this paper are analytical tools rather than classifications issued by the Government of Japan, ISA or IEC. Their definitions and application are set out in Section 3.1.

1. ESPA Policy and Regulatory Framework

1.1 Policy Architecture

The Diet enacted ESPA in 2022 to promote economic measures that contribute to national security in a comprehensive and coordinated manner. The Act established systems addressing the stable supply of specified critical products, the stable provision of specified essential infrastructure services, the development of specified critical technologies and the non-disclosure of selected patent applications. [1,2,7]

This paper focuses on the essential infrastructure regime because it establishes prior notification and government screening for the introduction of specified critical facilities and the entrustment of critical maintenance and management. The policy concern extends beyond technical cybersecurity risks such as malicious code or exploitable vulnerabilities. The screening considers whether a specified critical facility is highly likely to be used, in connection with its introduction or entrustment arrangement, as a means of specified disruptive action affecting the stable provision of specified essential infrastructure services. Cybersecurity therefore forms part of a broader economic security assessment rather than the sole subject of review. [3–5]

The 2026 amendments are addressed in this paper only where they affect the scope, commencement or operation of the Chapter III regime.

1.2 Chapter III Regulatory Perimeter

The scope and operation of Chapter III are defined through a layered set of legal and administrative instruments. The Act establishes the broad sector categories, principal notification obligations and government powers. Cabinet Orders specify the businesses covered within those sector categories. Sector-specific Ministerial Orders establish designation criteria, identify specified critical facilities and critical maintenance and management activities, define the required notification information and prescribe applicable risk management measures. The competent minister then designates individual operators as Specified Essential Infrastructure Service Providers by public notice. The Basic Guidelines and official implementation materials explain the policy objectives, review approach and filing procedures, but they do not amend or replace the requirements established by the Act, Cabinet Orders or Ministerial Orders. [1,3–5,8]

Table 1. Legal and Administrative Instruments Relevant to Chapter III

Instrument	Primary function	Implementation consequence
Act	Defines the broad sector categories, principal notification obligations, screening powers, recommendations, orders and continuing oversight.	Establishes the statutory basis, legal obligations and government authority.
Cabinet Orders	Specify the businesses covered within the statutory sector categories.	Inclusion in a broad sector category does not by itself establish applicability.
Ministerial Orders	Establish designation criteria, identify specified critical facilities and critical maintenance and management activities, define notification information and prescribe sector-specific risk management measures.	Applicability and filing requirements must be assessed under the rules for the relevant sector.
Designation Notices	Identify individual operators designated as Specified Essential Infrastructure Service Providers.	Notification obligations apply to formally designated providers, subject to the applicable commencement and transitional provisions.

Basic Guidelines	Explain the policy objectives, regulatory principles and government review approach.	Guide interpretation and implementation but do not amend the requirements established by the Act, Cabinet Orders or Ministerial Orders.
Official implementation materials	Provide procedural explanations, examples of supporting evidence, filing instructions and consultation information.	Support filing preparation and implementation but do not replace the applicable legislation or sector-specific requirements.

Cabinet Office materials for the 2026 framework identify sixteen covered business sectors: Electricity, Gas, Petroleum, Water, Railway, Truck Transport, International Maritime Cargo, Port and Harbor Transportation, Air Transport, Airports, Telecommunications, Broadcasting, Postal Service, Medical Care, Financial Services and Credit Cards. Medical Care was added by the 2026 amendment but will enter into force on a date specified by Cabinet Order within eighteen months of promulgation. It was therefore not yet part of the operational Chapter III notification regime as of the source cut-off date. The operational regime covered fifteen sectors, and 258 operators had been designated as Specified Essential Infrastructure Service Providers as of 1 July 2026. [4–7]

Table 2. Commencement Status of Selected 2026 Chapter III Amendments

Amendment	Commencement rule	Status as of 14 August 2026
Filing by newly designated providers during the transitional period	One month after promulgation	In force from 17 July 2026. A newly designated provider may submit an introduction or entrustment plan during the six-month transitional period following designation.
Self-supplied specified critical facilities containing prescribed components supplied by another enterprise	On a date specified by Cabinet Order within six months after promulgation	Not yet in force; scheduled to enter into force on 16 December 2026. Implementing Ministerial Order amendments have been promulgated.
Addition of the Medical Care sector	On a date specified by Cabinet Order within eighteen months after promulgation	Added to the Act but not yet in force under Chapter III as of the source cut-off date.

1.3 Facility Introduction and Critical Maintenance

Applicability depends on a cumulative set of conditions. The relevant business must fall within the scope defined by Cabinet Order, the operator must be formally designated as a Specified Essential Infrastructure Service Provider, and the planned activity must involve either the introduction of a specified critical facility or the entrustment of an activity prescribed as critical maintenance and management under the applicable Ministerial Order.

For equipment introduction, the regulated object is the specified critical facility. The applicable Ministerial Order identifies the prescribed component facilities. Information concerning those facilities and their suppliers must be provided under the applicable filing requirements. Other components used within the system do not automatically fall within the statutory notification scope. The treatment of a facility

supplied by the designated provider itself but containing prescribed components supplied by another enterprise must be assessed according to the commencement status of the relevant 2026 amendment.

The introduction route generally applies when a designated provider plans to introduce a specified critical facility supplied by another enterprise, subject to the statutory exclusions, transitional provisions and urgent procedures. The designated provider is the statutory filer, but relevant information may be held by the facility supplier, suppliers of prescribed component facilities, the System Integrator, where relevant, or other parties involved in the introduction. Required information may include corporate details, direct voting-right holders, relevant officers, manufacturing locations, specified transactions with foreign governments or related public bodies, and evidence of applicable risk management measures. [1,3–5,8,23(a)] The maintenance route applies when a designated provider entrusts another enterprise with work that the applicable sector-specific Ministerial Order prescribes as critical maintenance and management.

Commercial titles do not determine applicability. A vendor, managed service provider, engineering contractor or System Integrator may fall within the regulated maintenance chain where the work it actually performs falls within the prescribed activity. Conversely, an organization does not enter the Chapter III disclosure chain merely because it appears elsewhere in a broader commercial or subcontracting arrangement. [1,3–5,8,23(b)]

For critical maintenance and management, required disclosure generally follows the contracting chain to the organizations that actually perform the regulated activity. Information concerning certain deeper-tier subcontractors may be omitted only where the conditions prescribed by the applicable Ministerial Order are satisfied.

Remote or overseas performance does not, by itself, remove a maintenance arrangement from the scope of Chapter III. Applicability depends on whether the work performed falls within the prescribed definition of critical maintenance and management. The place from which the work is performed and the subcontracting arrangements remain relevant to the filing. The systems accessed and privileges granted may also be relevant when determining the nature of the activity and its cybersecurity risk. [1,3–5,8,23(b)]

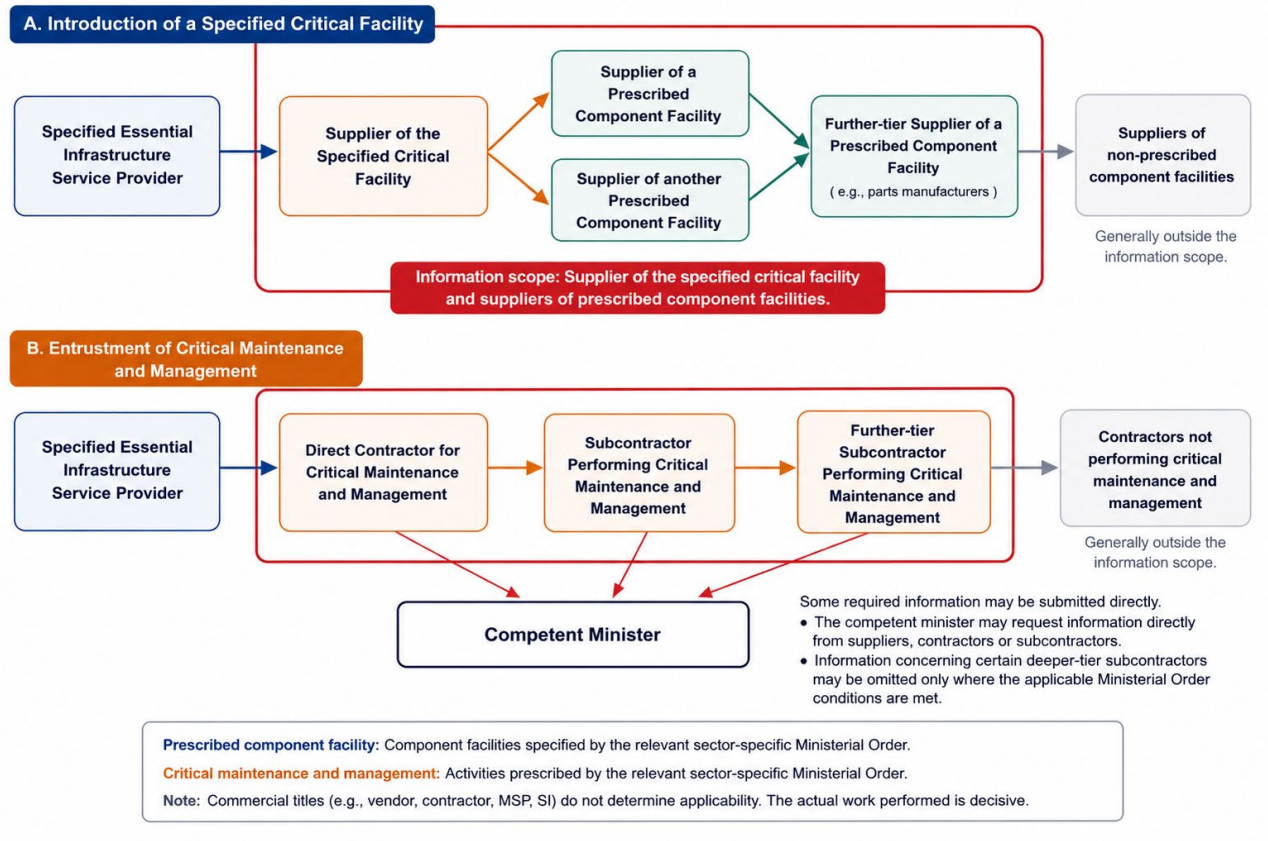

Figure 1. Scope of supply-chain information under ESPA

Source: Cabinet Office implementation material, simplified by the author. Equipment introduction and critical maintenance use different disclosure logic.

1.4 Notification, Screening and Change

The designated provider generally submits an introduction or entrustment plan before the regulated activity begins. Once the competent minister receives the plan, the provider is normally prohibited from proceeding for 30 days. The period may be shortened where further screening is unnecessary or extended to a maximum of four months from receipt where additional examination is required. The expiry or shortening of the period does not constitute certification or a general approval of the facility or arrangement. It means that the statutory prohibition period has ended, subject to any recommendation, order or other applicable requirement. [1,3–5]

Where the competent minister considers that the specified critical facility is highly likely to be used, in connection with its introduction or the entrustment of its critical maintenance and management, as a means of specified disruptive action, the minister may recommend that the provider amend the plan, take necessary measures to prevent the specified disruptive action, or suspend the proposed introduction or entrustment. The provider must notify the minister within ten days whether it accepts the recommendation and must provide reasons if it does not. A legally binding order may follow where the statutory conditions are met. [1,3–5]

Urgent procedures permit the introduction or entrustment to proceed without prior submission of the plan only where the prescribed conditions are satisfied. These conditions address urgency, the absence of intentional evasion of the prior-notification requirement, the necessity of the introduction or entrustment to remove or prevent difficulty in providing the specified essential infrastructure service, and the absence of appropriate alternatives. The provider must submit the required notification without delay after proceeding. [1,4,5]

After a plan has been filed, a material change generally requires prior notification and a further prohibition period. Other prescribed changes must be reported without delay, while minor changes defined by Ministerial Order require neither prior notification nor subsequent reporting. A change that constitutes the introduction of a new specified critical facility requires a new plan rather than an amendment to the existing plan. [1,4,5]

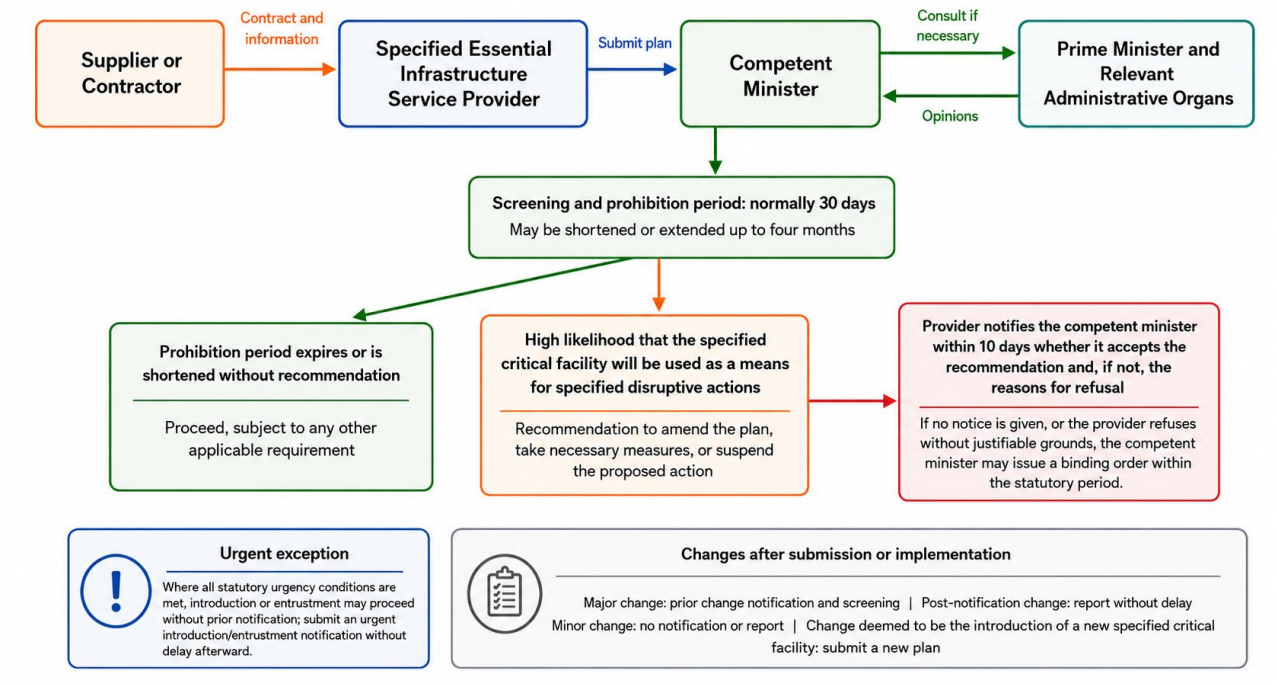

Figure 2. ESPA notification and government screening process

Source: Cabinet Office implementation material and the statutory process summarized for this paper.

1.5 Risk Management Measures and Evidence

The risk management measures listed in the applicable Ministerial Order forms are not required in every case. The designated provider is expected to assess the relevant risk and take measures proportionate to the extent and level of that risk. The introduction or entrustment plan identifies the measures that have been taken and must be accompanied by documentation supporting their implementation. Where a listed measure has not been taken, equivalent risk-management efforts may be described in the Notes section and considered as part of the screening. The competent minister assesses the implementation status of the measures and the provider's risk-management efforts in light of the circumstances of the relevant service or business. [3–5,8]

The Cabinet Office implementation materials group the risk-management measures according to the parties whose cooperation is expected or that are mainly expected to take the measures. Section 3.3 provides a detailed cross-reference between these measures and the relevant ISA/IEC 62443 publications. Supporting documentation is not limited to contracts or manuals and may take other forms where it demonstrates implementation of the relevant risk-management measure. The sufficiency of the evidence remains subject to the applicable filing and screening process.

Corporate ownership, direct voting-right holders, officer information and specified transactions with foreign governments or related public bodies are separate filing and screening inputs. These items are not cybersecurity controls and should not be treated as evidence that risk management measures have been implemented. [5,8,23(a),23(b)]

Certain prescribed supplier, contractor or subcontractor information and some documents supporting risk management measures may be submitted directly to the competent minister without passing through the designated provider. Eligibility for direct submission is item-specific and is determined by the applicable Ministerial Order and form instructions. Direct submission does not change the designated provider's role as the statutory filer. Cabinet Office guidance recommends confirming that all required directly submitted materials have reached the competent ministry before the main plan is submitted, because the notification cannot be accepted and screening cannot begin until the necessary materials have been received.

2. ISA/IEC 62443 Overview

The ISA/IEC 62443 series of standards addresses cybersecurity for industrial automation and control systems across asset-owner, service-provider, system, product-development and component levels. It is relevant to this ESPA analysis because it provides common concepts, role-specific responsibilities and lifecycle requirements for assessing and managing IACS cybersecurity. The series does not define Japanese regulated sectors, determine ESPA applicability, establish filing obligations, prescribe corporate disclosures or replace government screening.

2.1 Applicability Boundary

The mapping in this paper applies where the relevant specified critical facility or prescribed component facility forms part of or materially affects an IACS or automation solution, or where the maintenance arrangement concerns such an IACS or automation solution. The presence of digital technology, network connectivity or remote access does not, by itself, establish that ISA/IEC 62443 is the appropriate technical basis. Its relevance should be assessed from the function, architecture, interfaces and operational dependencies of the regulated facility or maintenance arrangement.

Across the sectors covered by ESPA, some regulated facilities may include IACS or automation solutions, while others may consist primarily of enterprise IT, cloud, communications or sector-specific information-processing systems. Where the relevant scope does not form part of or materially affect an IACS, other cybersecurity standards may provide a more appropriate technical basis. This does not alter the applicability of ESPA or any associated statutory obligation. The boundary used here is an analytical limitation of this paper, not a classification issued by the Government of Japan, ISA or IEC.

Table 3. ISA/IEC 62443 Relevance by Technical Context

Technical context	ISA/IEC 62443 relevance	Key boundary
System or subsystem within an IACS or Automation Solution	Provides a principal standards basis for IACS cybersecurity risk assessment, security requirements, integration, operation and maintenance.	Separate ESPA analysis remains necessary for legal applicability, filing, corporate and jurisdictional information, and government screening.
IT, communications or remote-service component included in the system under consideration (SUC), or interfacing with or materially affecting the IACS	Where included in the defined IACS scope, the relevant ISA/IEC 62443 requirements apply to that scope. Where external to the SUC, ISA/IEC 62443 remains relevant to the IACS-side interfaces, conduits and dependencies.	Define the SUC, zones, conduits, external interfaces and role responsibilities explicitly. Other cybersecurity standards may also be needed for the external system or service.
Enterprise IT, cloud or information-processing system adjacent to, but outside, the SUC	ISA/IEC 62443 may address the IACS-side boundary, access paths and dependencies, but it is not the primary control framework for the external system.	Another appropriate cybersecurity standard or framework may be needed for the external system. Selective use should not be presented as conformity with an ISA/IEC 62443 standard unless its defined scope and applicable requirements are satisfied.
Entity or service with no IACS-related technical function	Outside the scope of this paper's ISA/IEC 62443 mapping.	Do not assign an ISA/IEC 62443 stakeholder role solely because the entity appears in an ESPA supply or contracting chain. ESPA disclosure or due-diligence

	requirements may still apply.

The table reflects the scope distinction between an IACS or automation solution and adjacent systems or services. An organization should not be assigned an ISA/IEC 62443 stakeholder role solely because it appears in an ESPA supply or contracting chain; the applicable role depends on the function actually performed.

2.2 Relevant Publications

The mapping is based primarily on the ISA/IEC 62443 publications that address asset owner security programs, patch management, integration and maintenance services, system risk assessment and security requirements, secure product development, and component security capabilities. Supplementary publications are referenced only where they provide additional implementation or evaluation guidance.

Table 4. Primary ISA/IEC 62443 Publications Used in This Paper

Publication	Primary scope	Use in this paper
IEC 62443-2-1:2024	Asset owner security program policy and procedure requirements for an IACS in operation.	Asset owner governance, operational security processes, incident response, continuity and compensating measures for legacy IACS.
IEC 62443-2-4:2023	Security-related process requirements for IACS service providers during integration and maintenance of an automation solution.	System integration, maintenance delivery, personnel competence, controlled service activities and evidence of service-provider security processes.
IEC 62443-3-2:2020	Security risk assessment for system design, including definition of the SUC, zones and conduits, risk assessment, SL-T and documented security requirements.	System risk analysis, security architecture inputs and documented system security requirements.
IEC 62443-3-3:2013	System security requirements and security levels for industrial automation and control systems.	Technical system security requirements and control-system capability levels used in system design and assessment.
IEC 62443-4-1:2018	Secure product development lifecycle requirements for developers and maintainers of IACS products.	Product security requirements, design, implementation, verification, validation, defect management, patch management and product end of life.
IEC 62443-4-2:2019	Technical security requirements for IACS components.	Component security requirements and SL-C (component) evidence. It does not establish the SL-T or SL-A of the complete system.

IEC PAS 62443-2-2:2025, IEC TS 62443-6-1:2024 and IEC TS 62443-6-2:2025 may provide supplementary implementation or evaluation guidance where relevant, but they are not primary sources for the ESPA mapping.

IEC 62443-4-1 applies to the developer and maintainer of the product. Accordingly, for the purposes of this paper, the product supplier role is assigned in relation to IEC 62443-4-1 where the organization develops or maintains the relevant product. Selling, distributing, assembling or configuring equipment alone is not sufficient. IEC TR 62443-2-3 is directed primarily to asset owners and IACS product suppliers.

A maintenance service provider may apply relevant parts of the technical report where patch assessment, deployment or installation activities have been contractually delegated by the asset owner. [14,18]

2.3 Stakeholder Roles

The ISA/IEC 62443 series uses a shared-responsibility model involving the organizations that operate, integrate, maintain and supply an IACS. The asset owner operates the IACS and is accountable for system-level cybersecurity risk decisions and security requirements. The system integrator translates those requirements into the design, configuration, integration and verification of an automation solution. The maintenance service provider performs maintenance through defined security processes, including access control, change control, maintenance records and decommissioning activities. The product supplier develops or maintains the relevant product and provides its security capabilities, vulnerability-management and lifecycle support. A single organization may perform more than one role, but the associated responsibilities and evidence remain distinct.

For IACS-related cases, the asset owner is the closest functional correspondence to the Specified Essential Infrastructure Service Provider. This correspondence is functional rather than legal. ESPA does not use system integrator, maintenance service provider or product supplier as standalone statutory role labels. An organization's position under ESPA depends on the activity it performs, its position in the facility supply or maintenance chain and the applicable sector-specific Ministerial Order.

2.4 Security Levels and Evidence Boundaries

Security-level terminology requires careful use in procurement, assurance and regulatory submissions. ISA/IEC 62443-3-2 establishes target security levels, SL-T, for the relevant zones and conduits through the system risk-assessment process. ISA/IEC 62443-3-3 defines technical control-system requirements and associated capability security levels, SL-C(control system). ISA/IEC 62443-4-2 defines technical security requirements and capability security levels for IACS components, SL-C(component).

The achieved security level, SL-A, represents the actual level of security achieved within the assessed system scope. It is distinct from both the target security level and the capability security level. SL-A is outside the scope of ISA/IEC 62443-4-2, which addresses component capability rather than the security achieved by an implemented system.

A component certificate or capability claim therefore does not, by itself, demonstrate that the complete automation solution satisfies the asset owner's SL-T or has achieved a particular system-level SL-A. Product and component evidence must be considered together with system risk assessment, architecture, integration, configuration, verification and operational evidence.

For the purposes of this paper, product, system, operational and regulatory evidence are treated as separate evidence domains. Evidence from one domain may support another, but it does not, by itself, establish assurance beyond its defined scope. Product evidence does not establish the security of the complete automation solution; system design and integration evidence does not, by itself, demonstrate continuing operational effectiveness; and technical cybersecurity evidence does not replace the corporate, jurisdictional or regulatory information required under ESPA.

3. Mapping ESPA to ISA/IEC 62443

3.1 Mapping Method

The mapping examines the cybersecurity-related aspects of Chapter III expectations and the Cabinet Office risk-management measures. It does not assert legal equivalence between ESPA provisions and ISA/IEC 62443 requirements. Each topic is assessed according to whether the relevant ISA/IEC 62443 publication applies to the appropriate stakeholder role, addresses the relevant cybersecurity objective and can generate records or evidence relevant to implementation and assurance. The competent minister determines whether the measures and supporting documents are sufficient for the specific facility, maintenance arrangement and sector.

Table 5. Analytical Mapping Classifications

Classification	Meaning
Direct Support	ISA/IEC 62443 contains directly relevant organizational, lifecycle, service-provider or technical requirements that substantially address the cybersecurity-related aspect of the ESPA expectation or Cabinet Office risk-management measure. Implementation of those requirements may generate directly relevant supporting records and evidence.
Partial Support	ISA/IEC 62443 addresses a material part of the cybersecurity-related aspect of the ESPA expectation or Cabinet Office risk-management measure, while additional measures are needed to address aspects relating to legal, corporate, supply-chain, jurisdictional, continuity or other ESPA-specific considerations.
Indirect Support	ISA/IEC 62443 does not directly address the complete ESPA expectation or Cabinet Office risk-management measure, but its governance processes, implementation activities or resulting evidence can support assessment, implementation or assurance activities.
Outside Scope	The matter does not have a direct counterpart within the defined scope of ISA/IEC 62443. It therefore needs to be addressed through the applicable ESPA legal, corporate, contractual, jurisdictional or governmental processes, or through other relevant mechanisms where appropriate.

The classifications are analytical and apply only to the contribution that ISA/IEC 62443 can make to the cybersecurity-related aspect of the relevant ESPA expectation. A Direct Support rating does not imply legal equivalence, automatic acceptance of evidence or compliance with ESPA as a whole.

3.2 Overall Alignment Across the Cybersecurity Lifecycle

Alignment is strongest where ESPA risk-management measures concern cybersecurity governance, system risk assessment, security requirements, controlled integration and maintenance, secure product development, vulnerability management, incident response and recovery. Across these areas, the relevant ISA/IEC 62443 publications can provide structured requirements, processes and supporting evidence.

Alignment becomes partial or falls outside the scope of ISA/IEC 62443 where ESPA addresses corporate ownership and control, jurisdictional exposure, foreign-government relationships, manufacturing or service locations, business stability, prescribed supplier or contractor disclosures, statutory notification and government screening. ISA/IEC 62443 evidence may support the cybersecurity portion of the ESPA process, but these matters require separate treatment under the applicable legal and regulatory framework.

ESPA Area	Direct Support	Partial Support	Indirect Support	Outside Scope
Cybersecurity governance	●			
IACS cybersecurity risk assessment	●			
System security requirements	●			
Secure product development	●			
Component security capability (component level)	●			
System integration and security verification	●			
Maintenance and remote access controls	●			
Vulnerability and patch management	●			
Incident response, backup and recovery	●			
Supplier and subcontractor assurance		●		
Development and manufacturing integrity		●		
Product support continuity and alternative arrangements		●		
Evidence of implementation			●	
Statutory notification and screening				●
Corporate ownership and control				●
Foreign-government relationships and jurisdictional exposure				●
Government recommendations, orders and inspections				●
National and economic security assessment				●

Figure 3. ESPA–ISA/IEC 62443 Alignment and Gap Matrix

Source: Analytical mapping in this paper.

The following section examines the Cabinet Office risk-management measures individually to show where ISA/IEC 62443 provides direct, partial or indirect support and where ESPA-specific measures remain necessary.

3.3 Detailed Mapping of Cabinet Office Risk-Management Measures

This section maps the Cabinet Office risk-management measures for the introduction of specified critical facilities and the entrustment of critical maintenance and management to relevant ISA/IEC 62443 requirements and processes. Each listed measure is retained separately to preserve one-to-one traceability to the Cabinet Office materials, including measures that appear under more than one implementation or cooperation grouping. The measure wording follows the Cabinet Office overview materials, while the detailed briefing materials are used to clarify scope and implementation context.

The mapping addresses only the cybersecurity-related contribution of ISA/IEC 62443 and does not establish legal equivalence with an ESPA requirement. The analytical classifications defined in Table 5 are applied consistently throughout the detailed mapping. The measures applicable to an actual filing remain subject to the relevant sector-specific Ministerial Order and notification form, and their implementation remains risk-based.

The parties identified in the headings of Tables 6-11 are ESPA implementation or cooperation groupings, not ISA/IEC 62443 stakeholder-role assignments. Throughout these tables, the Specified Essential Infrastructure Service Provider remains responsible under ESPA for submitting the applicable introduction or entrustment plan and for making the confirmations attributed to it. Suppliers, contractors and subcontractors may implement measures or provide supporting evidence, including by submitting certain supporting documents directly to the competent minister where permitted. In IACS-related cases, the Specified Essential Infrastructure Service Provider corresponds most closely, in functional terms, to the ISA/IEC 62443 asset owner. This correspondence does not imply legal or normative equivalence. ISA/IEC 62443-2-4 uses the term IACS Service Provider differently: it refers to an organization that offers security-related processes to the asset owner during integration or maintenance activities. [5,12,15]

Tables 8 and 11 principally address asset owner responsibilities. In Table 6, integration, installation, configuration and verification activities generally correspond to the system integrator acting as an IACS service provider. If the Supplier of a Specified Critical Facility develops or maintains a relevant IACS product, product supplier requirements may also apply to that scope. Table 7 addresses product supplier activities only if the Supplier of a Component Facility develops or maintains the relevant IACS product. Tables 9 and 10 address maintenance service provider activities only if the contractor or subcontractor actually performs the relevant maintenance function. Position in the contracting chain alone does not establish an ISA/IEC 62443 role. A single organization may perform more than one role, but the responsibilities and supporting evidence associated with each role remain distinct. [5,12,15,18]

In Tables 6, 7, 9 and 10, citations to ISA/IEC 62443-2-1 support asset owner governance or oversight. They do not assign the asset owner role to the supplier, contractor or subcontractor identified in the table heading. References to ISA/IEC 62443-3-3 and ISA/IEC 62443-4-2 identify system-level and component-level technical requirements, respectively, rather than organizational roles. [12,17,19]

3.3.1 Introduction of Specified Critical Facilities

For the introduction of specified critical facilities, the Cabinet Office materials group measures under cooperation of Suppliers of Specified Critical Facilities, cooperation of Suppliers of Component Facilities, and measures mainly taken by the Specified Essential Infrastructure Service Provider. A Supplier of a Specified Critical Facility is the supplier of the facility that is the subject of the proposed introduction, and is an entity that manufactures or supplies the facility in a state in which its functions as a specified critical facility are fulfilled. An entity that merely sells the facility to the Specified Essential Infrastructure Service Provider is not included, and the supplier is not necessarily the provider's direct contractual counterparty.

A Supplier of a Component Facility is similarly an entity that manufactures or supplies a component facility prescribed by the applicable Ministerial Order in a state in which its functions as a component facility are fulfilled. An entity that merely sells the component facility to the Supplier of the Specified Critical Facility is not included, and the term does not extend automatically to every upstream component supplier.

Where a measure number uses the suffix "-1" or "-2," the suffix identifies the supplier position to which that occurrence applies: "-1" for the supplier of the specified critical facility and "-2" for the supplier of a component facility. Measures identified as mainly taken by the designated provider indicate its principal implementation position but do not exclude cooperation from other relevant parties. These ESPA groupings do not, by themselves, determine an ISA/IEC 62443 stakeholder role. BR means base requirement and RE means requirement enhancement. SAR, EDR, HDR and NDR denote software-application, embedded-device, host-device and network-device requirements, respectively. Other prefixes retain the element identifiers used in the cited edition. Where the supplier of the specified critical facility also develops or maintains the relevant IACS product, the applicable ISA/IEC 62443-4-1 requirements identified for the corresponding component-supplier measures in Table 7 also apply.

Table 6. Detailed Mapping for the Introduction of Specified Critical Facilities - Under cooperation of Suppliers of Specified Critical Facilities

Notification Form Measure No.	Cabinet Office risk-management measure	Relevant ISA/IEC 62443 support	Assessment	Remaining ESPA-specific consideration
①-1	Develop a verification procedure such as acceptance inspections (by a third party) and conduct vulnerability tests	**IEC 62443-2-4:2023:** SP.02.01 BR; SP.02.02 BR and RE(2). **IEC 62443-3-3:2013:** SR 3.3 and applicable REs.	Direct Support	The ESPA measure additionally requires the designated provider to confirm an appropriate pre-introduction inspection and vulnerability-testing arrangement. Inspections and vulnerability tests performed by the facility supplier or component suppliers are excluded from this measure.
②-1	Implement information security requirements (such as latest security patches and anti-malware software, etc.)	**IEC 62443-2-4:2023:** SP.10.02 BR; SP.11.01 BR, SP.11.02 BR, SP.11.06 BR. **IEC 62443-3-3:2013:** SR 3.2.	Partial Support	ISA/IEC 62443 supports patch management, malicious-code protection and controlled service processes. ESPA additionally requires facility-specific confirmation, before introduction, that the supplier has fulfilled the information-security requirements specified in the contract, including the current status of applicable security patches and anti-malware measures.
③-1	Establish a quality assurance structure	**IEC 62443-2-4:2023:** SP.02.01 BR.	Partial Support	IEC 62443-2-4 SP.02.01 provides an assurance process for verifying that automation solution components have security commensurate with their risk. ESPA additionally requires confirmation that the supplier has a reliable quality-assurance system covering the manufacturing process, including the development process.
④-1	Regularly or properly check unauthorized modifications, etc. in the development and manufacturing processes	**IEC 62443-2-1:2024:** ORG 1.6, ORG 2.3. **IEC 62443-2-4:2023:** SP.06.03 BR.	Partial Support	ESPA additionally requires the designated provider to confirm that the supplier periodically or as necessary checks for unauthorized changes to the manufacturing process, including the development process. ISA/IEC 62443 supports related supplier requirements and, where applicable, configuration-

				integrity verification, but does not directly address this broader manufacturing-process checking.
⑤-1	Conduct physical (ex. entering and leaving the room) and logical (control the access to system) access control in the development and manufacturing environment	**IEC 62443-2-1:2024:** ORG 3.1, USER 1.4, USER 2.1.	Partial Support	IEC 62443-2-1 addresses physical access control, access-right assignment and authorization within the asset owner's IACS security program. ESPA additionally requires the designated provider to confirm that appropriate physical and logical access controls are applied in the supplier's development and manufacturing environment.
⑦	Develop a structure to prevent unauthorized modifications, etc. upon installation by suppliers and persons involved in the introduction	**IEC 62443-2-1:2024:** ORG 1.6, CM 1.4. **IEC 62443-2-4:2023:** SP.01.02 RE(1), SP.03.09 BR	Direct Support	ESPA additionally requires the designated provider to confirm that the supplier of the specified critical facility and other parties involved in the introduction have the required arrangements in place to prevent unauthorized changes during installation.
⑧-1	Ensure cooperation among suppliers to investigate matters which may become the causes of unauthorized modifications	**IEC 62443-2-1:2024:** ORG 1.6, EVENT 1.7, EVENT 1.8. **IEC 62443-2-4:2023:** SP.08.01 BR.	Partial Support	ISA/IEC 62443 supports supplier cybersecurity requirements, event analysis, incident investigation and response. ESPA additionally requires the designated provider to confirm that the supplier will cooperate in detailed investigations and on-site inspections when unauthorized changes are found or suspected after introduction.
⑨-1	Ensure provision of service after introduction by suppliers (responses to failures and vulnerability, etc.)	**IEC 62443-2-1:2024:** ORG 1.6, ORG 2.3. **IEC 62443-2-4:2023:** SP.03.03 BR; SP.11.01–SP.11.06 BR.	Partial Support	ISA/IEC 62443 supports supplier lifecycle-support requirements, vulnerability management and security-patch support. ESPA additionally requires the designated provider to confirm that the supplier guarantees sufficient after-sales service, including responses to failures and vulnerabilities. Broader after-sales service and non-cybersecurity failure support remain outside the defined scope of ISA/IEC 62443.

⑩-1	Consider alternate means in the case that service provided by suppliers become unavailable	**IEC 62443-2-1:2024:** ORG 1.6, COMP 3.5, AVAIL 1.1, AVAIL 1.2. **IEC 62443-2-4:2023:** SP.11.02 RE(2).	Partial Support	ISA/IEC 62443 supports continuity planning and, where applicable, mitigation measures when normal vulnerability remediation cannot be applied. ESPA additionally requires the designated provider to consider alternatives or other necessary actions for the possible unavailability of the supplier's after-sales service itself.
⑬	Implement a mechanism for controlling and supervising unauthorized access to the facilities	**IEC 62443-2-1:2024:** ORG 1.6. **IEC 62443-2-4:2023:** SP.03.07 BR, SP.08.02 BR. **IEC 62443-3-3:2013:** SR 1.1, SR 1.2, SR 2.1, SR 2.8, SR 6.2.	Direct Support	ESPA additionally requires the designated provider to confirm, before introduction, that either the designated provider itself or the supplier of the specified critical facility will implement the required access-control system and unauthorized-access monitoring functions.
⑭-1	Check any violations to domestic laws and regulations and international standards in the last three years	No direct ISA/IEC 62443 counterpart.	Outside Scope	ESPA requires the designated provider to confirm the supplier's compliance with applicable domestic laws and international standards, including its compliance history for the three years preceding the notification. This legal and regulatory compliance-history review is outside the scope of ISA/IEC 62443.
⑮-1	Ensure to receive reports on a possible breach of contract due to legal environment, etc. in a foreign country	No direct ISA/IEC 62443 counterpart.	Outside Scope	ESPA requires the designated provider to establish a contractual reporting obligation for possible breaches of contract resulting from foreign legislation or instructions from an external entity, including explicit or tacit instructions. This legal and foreign-influence reporting requirement is outside the scope of ISA/IEC 62443.
⑰	Ensure the provision of detailed information on suppliers	**IEC 62443-2-1:2024:** ORG 1.5, ORG 1.6.	Indirect Support	ISA/IEC 62443 supports supplier cybersecurity requirements and cybersecurity competence and training requirements for personnel interacting with the IACS.

				ESPA additionally requires broader supplier information, including corporate identity, location, officers, capital ties, business information, manufacturing location, relevant personnel information, and timely notification of changes to such information.

Table 7. Detailed Mapping for the Introduction of Specified Critical Facilities - Under cooperation of Suppliers of Component Facilities

Notification Form Measure No.	Cabinet Office risk-management measure	Relevant ISA/IEC 62443 support	Assessment	Remaining ESPA-specific consideration
①-2	Develop a verification procedure such as acceptance inspections (by a third party) and conduct vulnerability tests	**IEC 62443-2-4:2023:** SP.02.01 BR; SP.02.02 BR and RE(2).	Direct Support	ISA/IEC 62443-2-4 directly supports the service-provider inspection and vulnerability-testing arrangement for component facilities before introduction. The designated provider must confirm that the arrangement covers the relevant component facilities; this confirmation may be made through the supplier of the specified critical facility. Testing performed by the supplier of each component facility is excluded from this ESPA measure. Supplier-performed IEC 62443-4-1 SVV-3 testing may support product assurance but does not, by itself, satisfy this measure.
②-2	Implement information security requirements (such as latest security patches and anti-malware software, etc.)	**IEC 62443-4-1:2018:** SUM-1, SUM-4, SUM-5. **IEC 62443-4-2:2019:** applicable SAR/EDR/HDR/NDR 3.2; applicable EDR/HDR/NDR 3.10 and RE(1).	Partial Support	ISA/IEC 62443-4-1 and ISA/IEC 62443-4-2 support security-update processes, update capability and protection from malicious code, but they do not establish that the latest applicable security patches and anti-malware updates have been applied to the component facility before introduction. ESPA additionally requires the designated provider to confirm fulfillment of the information-security requirements specified at the time of contracting; this confirmation may be made through the supplier of the specified critical facility.
③-2	Establish a quality assurance structure	**IEC 62443-4-1:2018:** SM-1, SM-12, SM-13.	Partial Support	ISA/IEC 62443-4-1 provides secure-development process governance, process verification and continuous improvement. ESPA additionally addresses the broader quality-assurance system for the manufacturing process,

				including the development process.
④-2	Regularly or properly check unauthorized modifications, etc. in the development and manufacturing processes	**IEC 62443-2-1:2024:** ORG 1.6, ORG 2.3. **IEC 62443-4-1:2018:** SM-1, SM-7.	Partial Support	ESPA requires confirmation that each relevant component supplier periodically or as necessary checks for unauthorized changes to the manufacturing process, including the development process. ISA/IEC 62443 provides relevant supply-chain and secure-development integrity controls, while the broader manufacturing-process checking remains specific to the ESPA measure.
⑤-2	Conduct physical (ex. entering and leaving the room) and logical (control the access to system) access control in the development and manufacturing environment	**IEC 62443-2-1:2024:** ORG 1.6. **IEC 62443-4-1:2018:** SM-7.	Partial Support	ISA/IEC 62443 supports supply-chain security requirements and, where applicable, protection of the product development environment. ESPA additionally requires confirmation of appropriate physical and logical access controls across the relevant manufacturing environment, including the development environment.
⑧-2	Ensure cooperation among suppliers to investigate matters which may become the causes of unauthorized modifications	**IEC 62443-2-1:2024:** ORG 1.6, EVENT 1.7, EVENT 1.8. **IEC 62443-4-1:2018:** DM-1, DM-2, DM-3.	Partial Support	ISA/IEC 62443 supports supplier cybersecurity requirements and, where applicable, product-security issue investigation and root-cause analysis. ESPA additionally requires confirmation that the component supplier will cooperate in detailed investigations and on-site inspections when unauthorized changes are found or suspected after introduction.
⑨-2	Ensure provision of service after introduction by suppliers (responses to failures and vulnerability, etc.)	**IEC 62443-2-1:2024:** ORG 1.6, ORG 2.3. **IEC 62443-4-1:2018:** DM-1–DM-5; SUM-1–SUM-5.	Partial Support	ISA/IEC 62443 supports supplier lifecycle-support requirements and, where applicable, product vulnerability handling, remediation, disclosure and security-update delivery. ESPA additionally requires confirmation that the component supplier guarantees sufficient after-sales service, including responses to failures and vulnerabilities. Broader after-sales service and non-cybersecurity failure support remain outside the defined scope of ISA/IEC 62443.
⑩-2	Consider alternate means in the case that service provided by	**IEC 62443-2-1:2024:** ORG 1.6, COMP 3.5, AVAIL 1.1, AVAIL 1.2. **IEC 62443-4-1:2018:** DM-4, SUM-2, SUM-5	Partial Support	ISA/IEC 62443 supports continuity planning and, where applicable, alternative vulnerability-treatment measures when a security patch cannot be deployed, including compensating mitigations. ESPA additionally requires

	suppliers become unavailable			the designated provider to consider alternatives or other necessary actions for the possible unavailability of the supplier's after-sales service itself.
⑭-2	Check any violations to domestic laws and regulations and international standards in the last three years	No direct ISA/IEC 62443 counterpart.	Outside Scope	ESPA requires confirmation of each relevant component supplier's compliance with applicable domestic laws and international standards, including its compliance history for the three years preceding the notification. This legal and regulatory compliance-history review is outside the scope of ISA/IEC 62443.
⑮-2	Ensure to receive reports on a possible breach of contract due to legal environment, etc. in a foreign country	No direct ISA/IEC 62443 counterpart.	Outside Scope	ESPA requires a contractual reporting obligation for possible breaches of contract by relevant component suppliers resulting from foreign legislation or instructions from an external entity, including explicit or tacit instructions. This legal and foreign-influence reporting requirement is outside the scope of ISA/IEC 62443.
⑰	Ensure the provision of detailed information on suppliers	**IEC 62443-2-1:2024:** ORG 1.5, ORG 1.6. **IEC 62443-4-1:2018:** SM-2, SM-4.	Indirect Support	ISA/IEC 62443 supports supplier cybersecurity requirements and, where applicable, defined security responsibilities, personnel competence and security training. ESPA additionally requires broader corporate, ownership, business, manufacturing-location and personnel information, together with timely notification of changes after contracting.

Table 8. Detailed Mapping for the Introduction of Specified Critical Facilities - Mainly Taken by Specified Essential Infrastructure Service Providers

Notification Form Measure No.	Cabinet Office risk-management measure	Relevant ISA/IEC 62443 support	Assessment	Remaining ESPA-specific consideration
①	Develop a verification procedure such as acceptance inspections (by a third party) and conduct vulnerability tests	**IEC 62443-2-1:2024:** ORG 2.2. **IEC 62443-2-4:2023:** SP.02.01 BR; SP.02.02 BR and RE(2). **IEC 62443-3-3:2013:** SR 3.3 and applicable REs.	Partial Support	ISA/IEC 62443 supports the discovery of vulnerabilities and other security anomalies, security testing of the automation solution, and evidence that components provide security commensurate with their risk. ESPA additionally requires the designated provider to confirm, before introduction, that an acceptance-inspection or other

				verification arrangement has been established and that vulnerability testing will be completed. Testing performed by the supplier of the specified critical facility or by a supplier of its component facilities is excluded from this measure.
⑥	Implement functions to prevent unauthorized access when connecting to the internet and prepare manuals	**IEC 62443-2-1:2024:** NET 1.1, NET 1.7. **IEC 62443-3-3:2013:** SR 1.13, SR 5.2.	Direct Support	ESPA requires the designated provider to apply these controls specifically when the specified critical facility is connected to the Internet and to establish and follow the related manuals and guidance.
⑩	Consider alternate means in the case that service provided by suppliers become unavailable	**IEC 62443-2-1:2024:** ORG 1.6, AVAIL 1.1, AVAIL 1.2.	Partial Support	ISA/IEC 62443 supports asset owner supply-chain and operational-continuity planning. ESPA specifically requires contingency planning for the possible unavailability of supplier-provided service, including consideration of alternative means or other necessary actions.
⑪	Develop a structure to enable continued provision of services even in the situation with interference	**IEC 62443-2-1:2024:** AVAIL 1.1, AVAIL 1.2, AVAIL 2.1, AVAIL 2.3, AVAIL 2.4, AVAIL 2.5. **IEC 62443-3-3:2013:** SR 7.3, SR 7.4.	Direct Support	ESPA applies these continuity and recovery arrangements to the continued provision of essential infrastructure services during disruptions and expressly includes replacement of the specified critical facility with a substitute facility as a possible measure.
⑫	Develop a policy and procedure to make responses upon an incident	**IEC 62443-2-1:2024:** EVENT 1.7, EVENT 1.8.	Direct Support	ESPA requires the designated provider to maintain the incident-response policy and arrangements and identifies documented manuals and periodic incident drills as examples of implementation.
⑬	Implement a mechanism for controlling and supervising unauthorized access to the facilities	**IEC 62443-2-1:2024:** USER 2.1, EVENT 1.1, EVENT 1.4. **IEC 62443-3-3:2013:** SR 1.1, SR 1.2, SR 2.1, SR 2.8, SR 6.2.	Direct Support	ESPA additionally requires the designated provider to ensure that the required access-control and unauthorized-access monitoring functions are in place before introduction.
⑯	Check the appropriateness of the handling of information of video equipment (places to install specified critical facilities)	No direct ISA/IEC 62443 counterpart.	Outside Scope	Where video-acquisition equipment, such as a surveillance camera or drone, is installed or used at a place where the specified critical facility is installed or used, ESPA requires the designated provider to confirm that the appropriateness of

				handling the video information is not affected by the legal environment of the location of the equipment supplier's head office, including that of any person that directly or indirectly holds a majority of the supplier's voting rights. This jurisdictional and legal-environment assessment is outside the scope of ISA/IEC 62443.

3.3.2 Entrustment of Critical Maintenance and Management

For the entrustment of critical maintenance and management, the Cabinet Office materials group measures under Contractor's Cooperation, under Subcontractor's Cooperation, and measures mainly taken by the Specified Essential Infrastructure Service Provider. Some measures appear in more than one grouping because implementation, confirmation or supporting evidence may involve different parties in the contracting chain.

For certain measures, the contractor may confirm the implementation status of a subcontractor. This does not make the contractor and subcontractor the same role. Contractor and subcontractor are ESPA contracting-chain positions and should be mapped to the ISA/IEC 62443 maintenance service provider role only where the organization actually performs the corresponding maintenance-service function.

Table 9. Detailed Mapping for the Entrustment of Critical Maintenance and Management - Under Contractor's Cooperation

Notification Form Measure No.	Cabinet Office risk-management measure	Relevant ISA/IEC 62443 support	Assessment	Remaining ESPA-specific consideration
①	Keep operational logs and task histories, etc. and check unauthorized modifications regularly or as needed	**IEC 62443-2-4:2023:** SP.01.02 RE(1), SP.03.10 RE(2), SP.06.01 RE(1), SP.06.03 BR, SP.08.02 BR and RE(2), SP.08.03 BR.	Direct Support	Cabinet Office guidance further specifies that the contractor's procedures should record the person or device performing the activity and the accurate date and time, define the operational logs and work histories to be collected and a retention period of at least one year, protect the collected records against unauthorized deletion, alteration and access, and use the records to check periodically or as necessary for unauthorized operations or changes. Facility-specific retained records are therefore still required; a service-provider procedure or certificate alone does not demonstrate performance for the relevant maintenance activities.
③	Conduct physical (ex. entering and leaving the room) and logical	**IEC 62443-2-4:2023:**	Partial Support	ISA/IEC 62443 supports protection of asset owner confidential information and logical access control for sensitive

	(control the access to system) access control regarding information on design documents, equipment, etc. they hold	SP.01.03 BR, SP.03.10 BR, SP.03.10 RE(1).		data. ESPA additionally requires the contractor to apply appropriate physical as well as logical access controls to the relevant design specifications and facility information in its possession.
④	Conduct physical (ex. entering and leaving the room) and logical (control the access to system) access control in the environment where the entrusted duties are performed	**IEC 62443-2-4:2023:** SP.01.02 BR, SP.01.02 RE(1), SP.01.07 BR, SP.03.07 BR, SP.09.01 BR, SP.09.02 BR, SP.09.04 BR.	Partial Support	ISA/IEC 62443 supports personnel security requirements and logical access control for maintenance and engineering activities. ESPA additionally requires appropriate physical and logical access controls across the environment in which the entrusted duties are performed.
⑤	Provide cybersecurity education	**IEC 62443-2-4:2023:** SP.01.01 BR, SP.01.02 BR.	Partial Support	ISA/IEC 62443 requires relevant service-provider personnel to be informed of and comply with applicable cybersecurity requirements, responsibilities, policies and procedures. Cabinet Office guidance further specifies periodic cybersecurity training, at least once in each fiscal year, for all personnel who perform or support critical maintenance and management activities, as well as their responsible managers.
⑥	Confirm specified essential infrastructure service provider's approval is condition for each subcontract	**IEC 62443-2-1:2024:** ORG 1.6. **IEC 62443-2-4:2023:** SP.01.01 RE(1).	Indirect Support	ISA/IEC 62443 supports supply-chain security requirements and security requirements for subcontractor personnel, but does not require the contractor to obtain the designated provider's prior approval before each subcontract.
⑦	Secure subcontractors' cybersecurity measures at the same level as those of contractors	**IEC 62443-2-1:2024:** ORG 1.6. **IEC 62443-2-4:2023:** SP.01.01 RE(1), SP.01.02 BR, SP.02.03 RE(1).	Partial Support	ISA/IEC 62443 supports recursive supply-chain cybersecurity requirements and the application of relevant requirements and procedures to subcontractor personnel. ESPA additionally requires the contractor to secure, throughout all subcontracting tiers, cybersecurity measures equivalent to those of the contractor.
⑧	Check the stability of business based on business plans, etc.	**No direct ISA/IEC 62443 counterpart.**	Outside Scope	ESPA requires confirmation of the business stability of the contractor and each relevant subcontractor based on factors such as business plans, financial health and service records. This business and financial due-diligence assessment is outside the scope of ISA/IEC 62443.
⑨-1	Check any violations to domestic laws and regulations and	**No direct ISA/IEC 62443 counterpart.**	Outside Scope	ESPA requires confirmation of the contractor's compliance with applicable domestic laws and

	international standards in the last three years			international standards, including its compliance history for the three years preceding the notification. This legal and regulatory compliance-history review is outside the scope of ISA/IEC 62443.
⑩-1	Ensure to receive reports on a possible breach of contract due to legal environment, etc. in a foreign country	**No direct ISA/IEC 62443 counterpart.**	Outside Scope	ESPA requires the contractor's agreement to require immediate reporting to the designated provider when a foreign legal environment or instructions from an external actor, whether explicit or tacit, may have caused conduct that breaches the contractor's agreement with the designated provider. This legal and foreign-influence reporting condition is outside the scope of ISA/IEC 62443.
⑫	Ensure the provision of detailed information on suppliers	**IEC 62443-2-1:2024:** ORG 1.3, ORG 1.6. **IEC 62443-2-4:2023:** SP.01.05 BR, SP.01.06 BR, SP.01.07 BR.	Indirect Support	ISA/IEC 62443 can provide security-related information concerning roles, security contacts, personnel qualifications and changes in assigned personnel. ESPA additionally requires contractually secured provision of the contractor's and relevant subcontractors' names and locations, officers and ownership relationships, business plans and track records, places where critical maintenance and management is performed, and the affiliations and expertise of the personnel involved, together with timely notification of changes after contracting.

Table 10. Detailed Mapping for the Entrustment of Critical Maintenance and Management - Under Subcontractor's Cooperation

Notification Form Measure No.	Cabinet Office risk-management measure	Relevant ISA/IEC 62443 support	Assessment	Remaining ESPA-specific consideration
①	Keep operational logs and task histories, etc. and check the existence of any unauthorized modifications regularly or as needed	**IEC 62443-2-4:2023:** SP.01.02 RE(1), SP.03.10 RE(2), SP.06.01 RE(1), SP.06.03 BR, SP.08.02 BR and RE(2), SP.08.03 BR.	Direct Support	Cabinet Office guidance further specifies that each relevant subcontractor's procedures should record the person or device performing the activity and the accurate date and time, define the operational logs and work histories to be collected and a retention period of at least one year, protect the collected records against unauthorized deletion, alteration and access, and use the records to check periodically or as necessary for unauthorized operations or changes.

				The designated provider may confirm implementation through the contractor, but facility-specific retained records are still required; a service-provider procedure or certificate alone does not demonstrate performance for the relevant maintenance activities.
③	Conduct physical (ex. entering and leaving the room) and logical (control the access to system) access control regarding information on design documents, equipment, etc. they hold	**IEC 62443-2-4:2023:** SP.01.03 RE(1), SP.03.10 BR, SP.03.10 RE(1).	Partial Support	ISA/IEC 62443 supports confidentiality obligations for subcontractor personnel and logical protection of sensitive data. ESPA additionally requires each relevant subcontractor to apply appropriate physical as well as logical access controls to the relevant design specifications and facility information in its possession.
④	Conduct physical (ex. entering and leaving the room) and logical (control the access to system) access control in the environment where the entrusted duties are performed	**IEC 62443-2-4:2023:** SP.01.01 RE(1); SP.01.02 BR and RE(1); SP.01.07 BR; SP.03.07 BR; SP.09.01 BR; SP.09.02 BR; SP.09.04 BR.	Partial Support	ISA/IEC 62443 supports security requirements and access-related controls for subcontractor personnel. ESPA additionally requires each relevant subcontractor to apply appropriate physical and logical access controls across the environment in which the entrusted duties are performed.
⑤	Provide cybersecurity education	**IEC 62443-2-4:2023:** SP.01.01 RE(1), SP.01.02 BR.	Partial Support	ISA/IEC 62443 requires relevant subcontractor personnel to be informed of and comply with applicable cybersecurity requirements, responsibilities, policies and procedures. Cabinet Office guidance further specifies training for all personnel who perform or support critical maintenance and management and for responsible managers at least once in each fiscal year. Newly assigned personnel should complete the training within three months of assignment unless there is a reasonable justification for a later date; participation and understanding should be tracked and the content kept current.
⑥	Confirm specified essential infrastructure service provider's approval is condition for each subcontract	**IEC 62443-2-1:2024:** ORG 1.6. **IEC 62443-2-4:2023:** SP.01.01 RE(1).	Indirect Support	ISA/IEC 62443 supports recursive supply-chain security requirements and security requirements for subcontractor personnel, but does not require a subcontractor to obtain the designated provider's prior approval before further subcontracting.
⑦	Secure subcontractors' cybersecurity measures	**IEC 62443-2-4:2023:**	Partial Support	ISA/IEC 62443 supports the application of relevant cybersecurity requirements and procedures to subcontractor

	at the same level as those of contractors	SP.01.01 RE(1), SP.01.02 BR, SP.02.03 RE(1).		personnel and activities. ESPA additionally requires cybersecurity measures equivalent to those of the contractor to be secured throughout all further subcontracting tiers.
⑨-2	Check any violations to domestic laws and regulations and international standards in the last three years	No direct ISA/IEC 62443 counterpart.	Outside Scope	ESPA requires confirmation of each relevant subcontractor's compliance with applicable domestic laws and international standards, including its compliance history for the three years preceding the notification. This legal and regulatory compliance-history review is outside the scope of ISA/IEC 62443.
⑩-2	Ensure to receive reports on a possible breach of contract due to legal environment, etc. in a foreign country	No direct ISA/IEC 62443 counterpart.	Outside Scope	ESPA requires the applicable subcontracting arrangement to require immediate reporting to the designated provider or the party that made the subcontract when a foreign legal environment or instructions from an external actor, whether explicit or tacit, may have caused conduct that breaches the applicable agreement. This legal and foreign-influence reporting condition is outside the scope of ISA/IEC 62443.
⑫	Ensure the provision of detailed information on suppliers	**IEC 62443-2-1:2024:** ORG 1.3, ORG 1.6. **IEC 62443-2-4:2023:** SP.01.01 RE(1), SP.01.07 BR.	Indirect Support	ISA/IEC 62443 provides limited security-related information concerning subcontractor personnel and changes in personnel assignments. ESPA additionally requires contractually secured provision of each relevant subcontractor's name and location, officers and ownership relationships, business plans and track record, place of performance, and the affiliations and expertise of the personnel involved, together with timely notification of changes after contracting.

Table 11. Detailed Mapping for the Entrustment of Critical Maintenance and Management - Mainly Taken by Specified Essential Infrastructure Service Providers

Notification Form Measure No.	Cabinet Office risk-management measure	Relevant ISA/IEC 62443 support	Assessment	Remaining ESPA-specific consideration
②	Regularly manage assets through means such as the application of the latest security patch	**IEC 62443-2-1:2024:** CM 1.1, COMP 3.2, COMP 3.3, COMP 3.5.	Direct Support	Cabinet Office guidance expects the designated provider to manage periodically the status of the specified critical facility and its component facilities, including checking whether the latest applicable security patches have been applied, and to apply equivalent periodic asset management to equipment planned as replacements. The designated provider therefore needs current, facility-specific inventory and patch-status evidence. Product-supplier patch information alone does not establish the deployed status, and any applicable patch that is not installed requires documented facility-specific risk treatment.
⑥	Confirm specified essential infrastructure service provider's approval is condition for each subcontract	**IEC 62443-2-1:2024:** ORG 1.6.	Indirect Support	Cabinet Office guidance expects the designated provider to ensure through contract or equivalent arrangements that its prior approval is a condition for the contractor's subcontracting and for any further subcontracting. ISA/IEC 62443 supports asset owner supply-chain governance but does not establish this ESPA-specific prior-approval condition.
⑧	Check the stability of business based on business plans, etc.	No direct ISA/IEC 62443 counterpart.	Outside Scope	ESPA requires the designated provider to assess and confirm the business stability of the contractor and relevant subcontractors. ISA/IEC 62443 does not establish requirements for evaluating business plans, financial health or overall business viability.
⑪	Check the appropriateness of the handling of information on video equipment (places for critical maintenance and management, etc.)	No direct ISA/IEC 62443 counterpart.	Outside Scope	Where video-acquisition equipment, such as a surveillance camera or drone, is installed or used at a place where critical maintenance and management is performed, ESPA requires the designated provider to confirm that the appropriateness of handling the video information is not affected by the legal environment of the location of the equipment supplier's head office, including that of any person that directly or indirectly holds a majority of the supplier's voting rights. This jurisdictional and legal-environment assessment is outside the scope of ISA/IEC 62443.

3.4 Role and Evidence Chain

The designated provider is the statutory filer and, in practice, coordinates information and evidence held by multiple organizations. Within the functional model used in this paper, the asset owner provides governance, cybersecurity risk decisions and operational evidence; the system integrator provides architecture, configuration, installation, verification and acceptance evidence; the maintenance service provider provides personnel, access, work and change records; and the product supplier provides secure-development, component-capability, vulnerability-management and lifecycle evidence. Corporate and jurisdictional information may be held by these organizations or by other parties in the regulated supply or maintenance chain.

Each material claim in the filing should therefore have an identified evidence owner, defined scope, current version or status where applicable, and an update trigger. Contracts should establish the information and evidence that relevant parties must provide, arrangements for direct submission where applicable, confidentiality requirements and notification of changes that may affect previously filed information. Cabinet Office guidance recommends confirming that required directly submitted documents have been provided before the introduction or entrustment plan is submitted. [5]

Conformity assessment or certification results can support assurance only within the scope actually assessed. Product, component or service-provider evidence does not, by itself, replace system risk assessment, secure integration, operational evidence or the legal, corporate and jurisdictional information required under ESPA.

4. Gaps and Implementation Risks

The remaining gaps reflect the different purposes and scopes of ESPA and ISA/IEC 62443 rather than deficiencies in either. The Chapter III essential infrastructure regime under ESPA is a legally binding economic security screening regime. ISA/IEC 62443 is an international standards series for industrial automation and control systems cybersecurity.

Implementation risk arises when evidence developed for a defined ISA/IEC 62443 scope is treated as sufficient for an ESPA requirement that extends beyond that scope. Product, system, service-provider or operational evidence may support an ESPA filing, but it does not, by itself, determine legal applicability, satisfy required corporate or jurisdictional disclosures, or replace government screening and decision-making.

4.1 Requirements Outside the Scope of ISA/IEC 62443

A number of core ESPA requirements have no direct counterpart in ISA/IEC 62443. The standards do not determine whether a business or operator falls within the Chapter III regulatory perimeter, whether a facility is a specified critical facility, whether an activity constitutes critical maintenance and management, or whether a statutory notification is required. They also do not establish the prior-notification process, prohibition period, government screening procedure, recommendations, orders, information requests or inspections administered by the competent minister. [1,3–5,8]

ISA/IEC 62443 also does not establish the corporate and economic-security disclosures used in ESPA screening, including prescribed ownership and officer information, direct voting-right holders, relevant foreign-government relationships, jurisdictional exposure, manufacturing or service locations, and applicable business-stability or historical compliance information. Cybersecurity supplier governance may assist in managing related operational risks, but it does not replace these legal and due-diligence requirements.

Technical and organizational change-management processes under ISA/IEC 62443 can support assessment of the cybersecurity impact of a change. They do not determine whether the change requires prior notification, subsequent reporting, no filing, or submission of a new plan under ESPA. Those determinations remain subject to the Act, applicable Ministerial Orders, filing instructions and competent-ministry assessment.

4.2 Areas of Partial Alignment

Partial alignment occurs where an ESPA measure combines cybersecurity assurance with broader supply-chain or economic-security considerations. ISA/IEC 62443 can support supplier and service-provider security requirements, personnel competence, secure service delivery, development-process assurance and technical evidence. ESPA may additionally require information concerning ownership, officers, voting-right holders, manufacturing or service locations, foreign-government relationships, subcontracting arrangements and subsequent changes. Development and manufacturing assurance presents a similar boundary: ISA/IEC 62443-4-1 supports secure product development, but it is not a comprehensive manufacturing quality, site-security or economic-security framework.

Product-support continuity also extends beyond product vulnerability and patch management. ISA/IEC 62443 can support vulnerability handling, security updates, mitigation and lifecycle planning, while ESPA may require the designated provider to consider the consequences of supplier-service unavailability and alternative arrangements needed to preserve the stable provision of the essential infrastructure service.

These broader dependency and continuity considerations therefore require additional procurement, supply-chain and operational measures.

4.3 Common Implementation Failure Modes

Table 12. Common Implementation Failure Modes

Failure mode	Consequence	Corrective action
Starting with a generic ISA/IEC 62443 checklist before confirming ESPA scope	Resources may be directed toward controls or evidence that do not correspond to the statutory trigger, regulated facility or sector-specific filing requirements.	Establish an ESPA applicability and filing decision point before supplier selection, contracting and detailed technical design.
Assigning the Ppoduct supplier role solely because an entity sells or distributes the equipment	The actual product developer and maintainer may remain outside the security and evidence process.	Assign ISA/IEC 62443 roles according to actual development, maintenance, integration and service responsibilities.
Using component certification as sufficient evidence of system security	The evidence does not demonstrate system risk assessment, architecture, integration, configuration, acceptance or continuing operation of the complete automation solution.	Combine product and component evidence with ISA/IEC 62443-3-2 risk analysis, ISA/IEC 62443-3-3 system requirements, integration evidence and operational records.
Treating secure remote access as sufficient to address maintenance risk	Contractor identity, personnel, work location, subcontracting, ownership, jurisdiction and external influence may remain unaddressed.	Assess technical access controls together with the corporate, contractual, jurisdictional and supply-chain information required under ESPA.
Collecting information and evidence immediately before filing	Missing direct submissions, incomplete supplier information or outdated corporate records may delay acceptance of the filing and commencement of screening.	Define disclosure duties, evidence responsibilities, submission deadlines and update triggers in procurement and service contracts.
Treating documented controls as proof of effective implementation	Policies or procedures may exist without records showing deployment, operation, testing or corrective action.	Evaluate whether each measure is documented, implemented, verified and maintained, and retain evidence for each status.
Failing to monitor changes after filing	Changes to facilities, components, suppliers, ownership, access arrangements or contractors may create an unrecognized notification or reporting obligation.	Operate a continuing process for receiving changes, assessing technical and regulatory impact, updating evidence and completing any required ESPA filing.
Treating automatic renewal of a critical maintenance contract as having no ESPA consequence.	A required entrustment filing may be missed even where the service scope remains unchanged.	Treat each renewal of a regulated critical maintenance and management arrangement as a regulatory checkpoint and confirm the applicable filing requirement before renewal becomes effective.

4.4 Practical Implementation Challenges

Brownfield and legacy systems

Long-lived infrastructure may include hardware or software that is no longer supported or lacks technical capabilities needed to meet current security requirements. ISA/IEC 62443-2-1 recognizes this condition and permits compensating security measures to be incorporated into the asset owner's security program where native capabilities are unavailable.

A legacy limitation should not, by itself, justify taking no further action. The asset owner should document the limitation, assess the associated cybersecurity risk, identify appropriate compensating measures and maintain evidence of their implementation and effectiveness where applicable. Where such a measure is used to support an ESPA risk-management measure, it should be distinguished from the separate ESPA concept of equivalent risk-management efforts described in Cabinet Office guidance.

Remote, Overseas and Multi-Tier Arrangements

Remote or overseas performance does not, by itself, remove a maintenance arrangement from the Chapter III regime. Applicability depends on whether the work performed constitutes prescribed critical maintenance and management. Technical controls for identification and authentication, authorization, restricted data flow, system integrity and event recording can address the IACS cybersecurity aspects of remote access, while ESPA may separately require information concerning contractors, subcontractors, work locations, corporate relationships and jurisdictional exposure.

Facility introduction and critical maintenance and management also follow different disclosure logic. For facility introduction, the information scope extends to suppliers of component facilities prescribed by the applicable Ministerial Order rather than automatically to every upstream supplier. For critical maintenance and management, the information scope generally follows the contracting chain to organizations that actually perform the regulated activity, subject to the applicable rules for deeper-tier subcontractors. Organizations should therefore distinguish the regulatory disclosure chain from the technical dependency chain used for cybersecurity and continuity analysis.

Direct Submission and Project Timing

Certain prescribed information and supporting documents may be submitted directly to the competent minister by the relevant information holder. This can reduce unnecessary disclosure of sensitive information through the commercial chain, but the designated provider remains responsible for coordinating the filing. A submission index can be used to track the information owner, submission status, scope and change status without reproducing protected content.

ESPA applicability, evidence ownership and direct-submission arrangements should be addressed during procurement and project planning rather than at final commissioning. The statutory prohibition period normally begins only after the required notification can be accepted, and Cabinet Office guidance indicates that screening cannot begin until required filing materials, including applicable direct submissions, have been received. Early consultation with the competent ministry is appropriate where the regulated scope, maintenance chain or required supporting evidence is uncertain. [4,5]

4.5 Evidence Sufficiency

For the purposes of this paper, evidence is considered at three analytical levels: documented, implemented and effective. These are not official classifications under ESPA or ISA/IEC 62443. Documented evidence shows that an approved policy, procedure, architecture, specification or other control description exists.

Implemented evidence shows that the measure has actually been deployed or performed and is supported by current records. Effective evidence shows, through appropriate verification, monitoring, testing, exercises or review, that the measure operates as intended for the relevant facility or maintenance arrangement.

Documentation alone may not be sufficient for an ESPA filing. Cabinet Office materials require supporting documents that demonstrate the implementation status of the selected risk-management measures. The form of those documents is not fixed, but they should show that the relevant measures are actually in place.

Evidence must also remain current. Changes to facilities, products, suppliers, officers, manufacturing or service locations, remote-access arrangements, subcontractors or risk-management measures may affect previously submitted information and may trigger prior notification, subsequent reporting or, in some cases, a new plan. The designated provider should therefore maintain traceable and current evidence rather than treating the filing as a one-time documentation exercise.

5. Industry Guidance

The preceding mapping and gap analysis have practical implications for organizations involved in an IACS-related ESPA filing. The designated Specified Essential Infrastructure Service Provider remains the statutory filer, while the technical activities, corporate information and supporting evidence may be distributed across the organizations that operate, integrate, maintain and supply the relevant system. The following guidance focuses on how those functional roles can support the cybersecurity and evidence process without replacing the applicable ESPA requirements.

5.1 Asset Owners

The asset owner should establish the cybersecurity scope and requirements for the regulated facility in coordination with the ESPA applicability assessment. ISA/IEC 62443-3-2 provides the basis for defining the SUC, establishing zones and conduits, assessing cybersecurity risk, determining SL-T and documenting system security requirements. ISA/IEC 62443-3-3 provides the related technical system requirements. These activities support the cybersecurity aspects of the filing but do not determine ESPA applicability or satisfy separate corporate and jurisdictional requirements.

Procurement and service arrangements should allocate responsibility for cybersecurity requirements, supporting evidence, vulnerability and lifecycle support, subcontractor controls, direct submissions and notification of relevant changes. The designated provider should be able to determine who holds each required item of information and whether it has been provided through the appropriate filing channel. After implementation, the asset owner should maintain a continuing process for assessing changes to facilities, components, suppliers, access arrangements, contractors, subcontractors and relevant corporate or operational information. Technical change approval should remain distinct from the ESPA determination of whether a change requires prior notification, subsequent reporting or a new plan.

5.2 System Integrator

The system integrator should translate the asset owner's cybersecurity risk decisions and system security requirements into the architecture, configuration and integration of the automation solution. Relevant activities include defining zones, conduits, interfaces and access paths, implementing security functions and approved compensating measures, and maintaining traceability between requirements and the products, versions, firmware, software and configurations used in the system.

Integration evidence should include, as applicable, the as-built architecture, configuration baseline, installation controls, security-verification results, identified deviations, unresolved issues and formal handover information. Product substitutions, architecture changes and new access paths should be communicated before implementation where they may affect the system risk assessment, acceptance basis or information previously filed under ESPA.

5.3 Maintenance Service Provider

The maintenance service provider should define the actual service boundary, including the facilities accessed, functions performed, personnel involved, work locations, remote-access methods and subcontractors. A commercial label such as vendor, managed service provider or engineering contractor does not determine whether an activity constitutes critical maintenance and management.

ISA/IEC 62443-2-4 provides the principal requirements for controlled integration and maintenance service processes. The maintenance service provider should maintain defined responsibilities, personnel competence, approved procedures, access authorization, change control, work records and incident

escalation. Remote maintenance should be treated as controlled privileged access, with appropriate authorization and monitoring. Records should identify the relevant requester or approver, target system, purpose, access period, personnel and work performed. Where required by the applicable ESPA filing instructions, the actual remote work location and relevant subcontracting arrangements should also be identified.

Where patch-related activities have been delegated by the asset owner, the maintenance service provider should coordinate applicable supplier information, impact assessment, approval, deployment and rollback records. Subcontracting should be controlled according to the regulated activity, including designated-provider approval and equivalent subcontractor cybersecurity measures where required by the applicable ESPA risk-management measure. Changes to relevant personnel, access arrangements, work locations or subcontractors should be communicated where they may affect the filing or cybersecurity basis.

5.4 Product Supplier

For the purposes of this paper, the product supplier should maintain a secure product-development lifecycle covering security requirements, secure design and implementation, verification and validation, defect management, patch management and product end of life. It should provide the security capabilities, configuration guidance, environmental assumptions, known limitations and vulnerability-support information required by the asset owner and system integrator for system risk assessment and integration.

Product security evidence should be accompanied by lifecycle information concerning the support period, vulnerability-reporting process, security-update arrangements, end-of-support conditions and available migration or replacement options. These records support cybersecurity and continuity analysis but do not replace system-level integration or operational evidence.

Where the product supplier falls within the relevant ESPA information scope, it may separately need to provide prescribed corporate, manufacturing-location, component-supplier or jurisdictional information. Contracts should establish notification of changes that may affect previously filed information or continuing product support. Where prescribed information or supporting documents are eligible for direct submission, the supplier should complete the submission according to the applicable filing process and provide the designated provider with appropriate confirmation of status.

5.5 Cross-Stakeholder Coordination

The four functional roles should be coordinated within a common lifecycle beginning with ESPA applicability and role assignment, followed by cybersecurity risk assessment and requirements, due diligence and contracting, filing and evidence readiness, notification and screening, implementation and acceptance, and continuing operation and change review. These activities may overlap, but the statutory filing should not be treated as an activity performed only at the end of commissioning.

Role	1. Applicability and Role Assignment	2. Risk and Security Requirements	3. Due Diligence and Contracting	4. Filing and Evidence Readiness	5. Notification and Screening	6. Implementation and Acceptance	7. Operation and Change Review
Designated Provider (Statutory Filer) Legal responsibility under ESPA	Confirm ESPA scope and filing obligation	Align with regulatory requirements and sector-specific criteria	Coordinate information and evidence delivery under contracts	Coordinate filing dossier and direct submissions	Submit the plan and prescribed information; communicate with the competent ministry	Confirm expiry or shortening of the prohibition period; address any recommendation or order before commencement	Monitor changes and fulfil reporting or new plan obligations
Asset Owner (Operator) Closest functional correspondence	Define operational scope and regulated facilities; assign functional roles	Conduct system risk assessment; define SL-T and system security requirements	Lead due diligence; set disclosure duties and evidence needs	Approve risk management measures; review evidence adequacy	Support screening as requested	Accept the system or service; approve operational readiness	Manage operations, changes and continuous risk review
System Integrator (IACS Service Provider) Designs and implements the solution	Understand scope and interfaces; confirm technical boundaries	Define architecture, zones and conduits; select and integrate capabilities to meet system security requirements and support SL-T	Provide technical information and evidence commitments	Prepare system evidence: architecture, configuration, integration and test results	Provide clarifications and evidence as requested	Support installation verification and acceptance testing	Support changes, updates and evidence maintenance
Maintenance Service Provider Provides maintenance and support	Define service boundary: facilities, functions, locations, personnel, subcontractors	Assess maintenance risks; define access and operational requirements	Provide contractor information; confirm maintenance and security arrangements	Prepare operational evidence: access control, maintenance processes, personnel competence	Coordinate responses to screening enquiries	Deliver maintenance services; maintain records and monitoring	Monitor changes, subcontractors and reporting triggers
Product Supplier (Developer/Maintainer) Develops or maintains the product	Confirm product role (Developer/Maintainer) and scope	Define product security requirements and lifecycle support	Provide product information, security capabilities and vulnerability support	Provide product evidence: secure-development lifecycle records, SL-C(component), known limitations and support information	Provide additional information if requested	Support vulnerability handling and updates	Notify changes affecting filed information or support availability

Ongoing coordination among roles

ESPA NOTIFICATION AND SCREENING GATE
(Notification accepted and screening can begin only when all required materials, including any required direct submissions, have been received.)

Continuous monitoring and change management

Figure 4. Role-Based ESPA Readiness and Assurance Lifecycle.

Product, system, operational and regulatory evidence should remain distinguishable by scope and ownership while being coordinated through the same assurance process. Each material filing item or supporting evidence set should have an identified owner, current status and update trigger where applicable. Contracts should define evidence and information delivery, direct-submission coordination, confidentiality arrangements and notification of relevant changes. ISA/IEC 62443 can strengthen the cybersecurity portion of this process, but it does not replace the applicable legal, corporate, jurisdictional or government-screening requirements.

6. Conclusion

ESPA and ISA/IEC 62443 address different but complementary responsibilities. Chapter III establishes the legal framework for prior notification and government screening of the introduction of specified critical facilities and the entrustment of their critical maintenance and management. ISA/IEC 62443 provides organizational, system, service-provider and product requirements and processes for managing IACS cybersecurity.

The strongest alignment lies in cybersecurity governance, system risk assessment, security requirements, controlled integration and maintenance, secure product development, vulnerability management, incident response and recovery. ESPA extends beyond these areas to corporate ownership and control, jurisdictional exposure, foreign-government relationships, manufacturing and service locations, supplier dependency, statutory disclosure and government screening. ISA/IEC 62443 evidence can therefore support the cybersecurity-related aspects of an ESPA filing without establishing compliance with ESPA as a whole.

In practice, the designated provider needs to define the regulated scope, allocate responsibilities according to the functions actually performed, obtain current supporting evidence and maintain a process for assessing relevant changes. Product, system, operational and regulatory evidence should remain traceable to their respective scopes and owners. Used in this manner, ISA/IEC 62443 provides a structured basis for cybersecurity assurance while the applicable ESPA legal, disclosure and screening requirements remain separately addressed.

Glossary

Term	Meaning in this Paper
Achieved security level, SL-A	The security level actually achieved for a relevant zone or conduit in an implemented automation solution. It is not established by an ISA/IEC 62443-4-2 component capability claim.
Asset owner	The organization that owns or operates the IACS and is accountable for its cybersecurity program, risk decisions and system security requirements. It is used as the closest functional correspondence to the designated provider, not as a legal synonym.
Automation solution	The technical solution that implements the control, safety and complementary functions necessary for the IACS. It comprises hardware and software components installed and configured to operate within the IACS.
Competent minister	The minister responsible for administering Chapter III for the relevant regulated sector, including designation, notification, screening and related regulatory action.
Component capability security level, SL-C (component)	The security capability level of an IACS component under ISA/IEC 62443-4-2. It does not establish the SL-T or SL-A of the complete automation solution.
Contractor	The person or organization directly entrusted by the Specified Essential Infrastructure Service Provider to perform critical maintenance and management within the applicable ESPA scope. The term describes an ESPA contracting-chain position and does not, by itself, establish an ISA/IEC 62443 maintenance service provider role.
Control-system capability security level, SL-C (control system)	The capability security level associated with the technical control-system requirements defined in ISA/IEC 62443-3-3. It is distinct from SL-T and SL-A.
Critical maintenance and management	The shortened expression used in this paper for activities prescribed as critical maintenance and management under the applicable sector-specific Ministerial Order.
Designated provider	The short form used in this paper for a Specified Essential Infrastructure Service Provider.
Direct submission	A working term for the permitted submission of specified information or supporting documents directly to the competent minister by the relevant supplier, contractor, subcontractor or other information holder, without routing the content through the designated provider.
ESPA	Japan's *Act on the Promotion of Ensuring National Security Through Integrated Implementation of Economic Measures*, Act No. 43 of 2022, as amended.
IACS	Industrial automation and control system. In the ISA/IEC 62443 model, the IACS comprises the automation solution together with the organizational measures necessary for its design, deployment, operation and maintenance.
Maintenance service provider	The functional role that performs maintenance or operational support for an Automation Solution. It corresponds to an ESPA contractor or subcontractor only where the work performed falls within the regulated critical maintenance and management scope.
Prescribed component facility	A working term used in this paper for a component facility that is prescribed by the applicable Ministerial Order and for which supplier or other information must be provided under the relevant filing requirements.

Product supplier	The organization responsible for developing or maintaining the relevant IACS product for the purposes of ISA/IEC 62443-4-1. Selling, distributing, assembling or configuring equipment does not, by itself, establish this role.
Specified critical facility	A facility, device, equipment item or program prescribed under the applicable sector-specific Ministerial Order for the purposes of Chapter III.
Specified disruptive action	The English term used in current Cabinet Office materials for 特定妨害行為. Some reference English translations use "specified interference action."
Specified Essential Infrastructure Service Provider	An operator formally designated by the competent minister under Chapter III. The designated provider is the statutory filer for the relevant introduction or entrustment plan.
Subcontractor	A person or organization engaged by the contractor or another subcontractor to perform relevant work within the critical maintenance and management chain. Its filing relevance depends on the applicable Ministerial Order and the activities actually performed. The term does not, by itself, establish an ISA/IEC 62443 stakeholder role.
Supplier of a Specified Critical Facility	An entity that manufactures or supplies the specified critical facility in a state in which its functions as a specified critical facility are fulfilled. An entity that merely sells the facility to the Specified Essential Infrastructure Service Provider is not included, and the supplier is not necessarily the provider's direct contractual counterparty. The term describes an ESPA supply-chain position and does not, by itself, establish an ISA/IEC 62443 stakeholder role.
Supplier of a Component Facility	An entity that manufactures or supplies a component facility prescribed by the applicable Ministerial Order in a state in which its functions as a component facility are fulfilled. An entity that merely sells the component facility to the Supplier of the Specified Critical Facility is not included. The term does not refer to every upstream component supplier and does not, by itself, establish an ISA/IEC 62443 product supplier role.
System integrator	The functional role that designs, configures, integrates, installs, tests or commissions the automation solution. ESPA does not use this as a standalone statutory role label.
System under consideration, SUC	The system boundary defined for the ISA/IEC 62443-3-2 cybersecurity risk assessment.
Target security level, SL-T	The target security level established for each relevant zone and conduit through the ISA/IEC 62443-3-2 risk-assessment process.

References

Japanese-language legislation, Cabinet Orders, Ministerial Orders and official notices are controlling. English translations and English-language Cabinet Office materials are provided for accessibility and should be checked against the current Japanese texts and applicable commencement provisions. Online sources were last checked on 14 August 2026.

[1] Government of Japan:

(a) Act on the Promotion of Ensuring National Security Through Integrated Implementation of Economic Measures, Act No. 43 of 2022, as amended, including amendments enacted by Act No. 38 of 2026, subject to applicable commencement provisions, e-Gov Law Search.

(b) Order for Enforcement of the Act on the Promotion of Ensuring National Security Through Integrated Implementation of Economic Measures, Cabinet Order No. 394 of 2022, as amended, e-Gov Law Search.

[2] Cabinet of Japan, Basic Policy on the Promotion of Ensuring National Security Through Integrated Implementation of Economic Measures, Cabinet Decision, Sept. 30, 2022.

[3] Cabinet of Japan, Basic Guidelines for Ensuring the Stable Provision of Specified Essential Infrastructure Services by Preventing Specified Disruptive Actions, Cabinet Decision, Apr. 28, 2023.

[4] Cabinet Office, Government of Japan, System for Ensuring Stable Provision of Specified Essential Infrastructure Services under the Economic Security Promotion Act, Detailed Overview, July 2026.

[5] Cabinet Office, Government of Japan, System for Ensuring Stable Provision of Specified Essential Infrastructure Services under the Economic Security Promotion Act: Briefing Material, July 2026.

[6] Cabinet Office, Government of Japan, Entities Designated as Specified Essential Infrastructure Service Providers, July 1, 2026.

[7] Government of Japan, Act Partially Amending the Act on the Promotion of Ensuring National Security Through Integrated Implementation of Economic Measures and the Japan Bank for International Cooperation Act, Act No. 38 of 2026, promulgated June 17, 2026. See also Cabinet Office, Government of Japan, Overview of the Bill Partially Amending the Economic Security Promotion Act and the Japan Bank for International Cooperation Act, 2026.

[8] Cabinet Office, Government of Japan, Technical Explanation of the System for Ensuring Stable Provision of Specified Essential Infrastructure Services under the Economic Security Promotion Act, version dated Mar. 31, 2026.

[9] Ministry of Justice, Government of Japan, Act on the Promotion of Ensuring National Security Through Integrated Implementation of Economic Measures, Reference English Translation, Japanese Law Translation Database. The translation is non-authoritative and should be checked against the current Japanese Act and the 2026 amendment.

[10] ISA, ISA/IEC 62443 Series of Standards, overview of the series, stakeholder roles and shared responsibility.

[11] IEC, Industrial communication networks: Network and system security, Part 1-1: Terminology, concepts and models, IEC TS 62443-1-1:2009, Geneva, Switzerland, 2009.

[12] IEC, Security for industrial automation and control systems, Part 2-1: Security program requirements for IACS asset owners, IEC 62443-2-1:2024, Geneva, Switzerland, 2024.

[13] IEC, Security for industrial automation and control systems, Part 2-2: IACS security protection scheme, IEC PAS 62443-2-2:2025, Geneva, Switzerland, 2025.

[14] IEC, Security for industrial automation and control systems, Part 2-3: Patch management in the IACS environment, IEC TR 62443-2-3:2015, Geneva, Switzerland, 2015.

[15] IEC, Security for industrial automation and control systems, Part 2-4: Security program requirements for IACS service providers, IEC 62443-2-4:2023, Geneva, Switzerland, 2023.

[16] IEC, Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design, IEC 62443-3-2:2020, Geneva, Switzerland, 2020.

[17] IEC, Industrial communication networks: Network and system security, Part 3-3: System security requirements and security levels, IEC 62443-3-3:2013, Geneva, Switzerland, 2013. The current IEC copy incorporates Corrigendum 1:2014.

[18] IEC, Security for industrial automation and control systems, Part 4-1: Secure product development lifecycle requirements, IEC 62443-4-1:2018, Geneva, Switzerland, 2018.

[19] IEC, Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components, IEC 62443-4-2:2019, Geneva, Switzerland, 2019. The current IEC copy incorporates Corrigendum 1:2022.

[20] IEC, Security for industrial automation and control systems, Part 6-1: Security evaluation methodology for IEC 62443-2-4, IEC TS 62443-6-1:2024, Geneva, Switzerland, 2024.

[21] IEC, Security for industrial automation and control systems, Part 6-2: Security evaluation methodology for IEC 62443-4-2, IEC TS 62443-6-2:2025, Geneva, Switzerland, 2025. The document does not define a complete certification scheme or certification program.

[22] IEC, Security for industrial automation and control systems, Part 1-6: Application of the 62443 series to the Industrial Internet of Things (IIoT), IEC PAS 62443-1-6:2025, Geneva, Switzerland, 2025.

[23] Cabinet Office, Government of Japan:

(a) Outline of the Essential Infrastructure System and Required Information: Introduction of Specified Critical Facilities, June 2026.

(b) Outline of the Essential Infrastructure System and Required Information: Entrustment of Critical Maintenance and Management, etc., June 2026.