UK Government

DESNZ Scoping Guidance for the Load Control sub-sector

March 2026
Version: Draft for Consultation

Table of Contents

DRAFT

1 Introduction

1.1 Purpose and Approach

This guidance is for organisations operating in the load control sub-sector of Great Britain (GB). These organisations are designated based on their aggregated load capacity as follows:

- **Large Load Controllers (Tier 1):** Organisations controlling an aggregated load of 300MW or more. These are designated as Operators of Essential Services (OES) under the NIS Regulations 2018. As such, they have a legal obligation under Regulation 10(1) to take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their essential service relies. Furthermore, under Regulation 10(2), they must take appropriate and proportionate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of an essential service, with a view to ensuring the continuity of those services.
- **Load Controllers (Tier 2):** Organisations controlling an aggregated load of less than 300MW. These organisations are subject to the requirements set out in the standard conditions of the Load Control Licence, in particular Condition 9, which requires licensees to implement appropriate and proportionate technical and organisational measures to manage cyber security risks and their load control systems. The Tier 2 CAF supports this by providing a structured framework for assessing the maturity and effectiveness of those measures.

Load Controllers managing an aggregate load of 300 MW or more are expected to be designated as Operators of Essential Services (OES) under the NIS Regulations 2018, subject to the parliamentary passage of the Cyber Security and Resilience Bill (CSRB).

The primary objective of this document is to assist Load Controllers in accurately defining the functional boundary of their service. This guidance is applicable to both Tier 1 and Tier 2 Load Controllers and should be applied proportionately, reflecting the scale of load under control, system complexity, and potential impact on the electricity system. Defining the correct scope is a technical prerequisite for effective security operations. Without a clearly delineated scope, it is not possible to maintain an accurate asset inventory or conduct meaningful risk and threat assessments.

By establishing a clear and proportionate scope from the outset, Load Controllers, regardless of whether they are designated based on the 300 MW threshold or operating below it, can ensure their security assessments are robust and that any subsequent evidence provided, as required by the relevant regulator, , accurately reflects their security posture. This approach enables organisations to focus resources on the systems and third-party dependencies that support the load control function, avoiding unnecessary regulatory burden on the wider organisation while ensuring that all critical assets, including those with safety or operational technology implications, are appropriately captured within the cyber security management system.

1.2 Target Audience

This guidance applies to all organisations that provide load control services. This includes providers of Domestic and Small Non-Domestic Consumer-Led Flexibility (CLF) focusing on domestic Energy Smart Appliances (ESAs), EV chargepoints heating systems, and domestic battery storage, as well as large load controllers managing industrial and commercial assets such as Battery Energy Storage Systems (BESS) and Virtual Power Plants (VPPs).

The primary audience for this document consists of the practitioners responsible for the design, implementation, and maintenance of the security management system. However, it also serves as a point of reference for those with oversight responsibilities:

- **Technical and Operational Teams:** Personnel in Cyber Security, IT, and Operational Technology (OT) roles. This includes those responsible for Industrial Control Systems (ICS), safety-critical infrastructure, and cloud-based application programme interface (API) platforms who must identify the assets, networks, and data flows comprising the load control service. These teams will use this guidance to build and maintain the asset inventory required to support risk management, security operations, and CAF-based assurance activities, ensuring that the intersection of cyber security and operational safety is fully addressed across both domestic aggregator and grid scale environments.

DRAFT

- **Policy and Compliance Teams:** Individuals responsible for mapping the technical scope to regulatory requirements, ensuring that all components of the essential service are captured within the organisation's compliance and audit frameworks, whether managing distributed consumer devices or centralised energy storage.
- **Product and Service Development Teams:** Teams involved in the creation of CLF technologies, ESA integrations, and grid scale control platforms, ensuring that security boundaries are considered during the design and integration of new systems.
- **Third-Party Suppliers and Partners:** External entities involved in the supply chain or the provision of outsourced services, such as cloud service providers or managed service providers, where their systems form part of the functional boundary of the load controller's service.
- **Senior Management and Board Members:** While not the primary users of the technical methodology, this group should use the guidance to understand the importance of accurate scoping in fulfilling their statutory duties and ensuring that the organisation is appropriately managing its cyber risk profile, including risks to safety and service continuity.

1.3 Supporting Documents

This scoping guidance is part of a broader, integrated collection of regulatory and technical documents designed to facilitate the implementation of the Load Control Licence. These documents are intended to be read as a bundle to provide a comprehensive view of the legal duties, technical expectations, and procedural requirements for the sector.

- **DESNZ Policy Guidance: Cyber Security Requirements for Load Controllers [*to be published following consultation]*:** This is the primary policy document for the load control sub-sector. It establishes the overarching regulatory framework for the implementation of the licensing regime, including the methodology for the 300 MW designation threshold and the defined methodology for the calculation of aggregated load. It provides the definitive policy link between the Standard Conditions of the Load Control Licence and the statutory requirements of the NIS Regulations, ensuring a consistent approach to grid stability across both regulatory tiers.
- **DESNZ Scoping Guidance for the Load Control Subsector (This document):** This document provides the technical methodology for defining the functional boundary of a load control system. It offers specific guidance for both established Downstream Gas and Electricity (DGE) organisations already designated as an OES and newer CLF providers. For the latter, it provides the framework for identifying and isolating the components of the essential service from wider enterprise services, as well as assisting in the identification of relevant ESAs and assets that fall within the technical scope of the load control function.
- **Load Control Licence Standard Conditions:** These are the legally enforceable conditions issued under the Electricity Act 1989. They establish the mandatory baseline for all participants, with Condition 9 and Condition 10 defining the statutory requirements for cyber security and operational load control checks[1]
- **Large Load Control Tier 1 & Load Control Tier 2 CAF Profiles:** These profiles provide a tailored set of indicators used to assess the extent to which a load control organisation has implemented security measures that are appropriate and proportionate to the risks posed to their operations and the wider grid. By mapping expectations against the NCSC Cyber Assessment Framework (CAF) Contributing Outcomes (COs), the profiles establish the technical benchmark used by the regulator to verify compliance within each regulatory tier.
- **CAF Overlay for the Load Control sub-sector:** This document provides a technical interpretation of the NCSC CAF Contributing Outcomes (COs) and Indicators of Good Practice (IGP) specifically for the load control environment. It offers practical examples of the evidence required across the people, process, and technology dimensions, assisting organisations in understanding the technical benchmarks used by the regulator to verify compliance.
- **The NCSC Cyber Assessment Framework Collection[2]:** This collection is provided by the NCSC, the UK's national technical authority for cyber security. It represents the primary technical standard upon which the load control profiles are built, providing the foundational objectives and principles for managing cyber security risks to essential functions, ensuring a structured and outcome-based approach to resilience.

[1] https://assets.publishing.service.gov.uk/media/6937f1fb5cc812f50aa41e19/standard-conditions-load-control-licence.pdf (As of Feb '26 currently subject to consultation)
[2] https://www.ncsc.gov.uk/collection/cyber-assessment-framework

DRAFT

- **NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain v3.0**[3]**:** This document is a procedural guide provided by Ofgem to assist organisations designated as an OES. It provides the formal framework for performing statutory duties under the NIS Regulations, including incident reporting and the setting of security objectives.
- **DESNZ Policy Guidance for the Implementation of the Network and Information Systems Regulations**[4]**:** This is a policy-level document provided by the DESNZ which provides a comprehensive summary of the legal landscape for an OES. It defines the specific roles and responsibilities of the Competent Authorities, being Ofgem and DESNZ, and outlines how regulatory oversight and enforcement will be conducted. Crucially, the document establishes the mandatory thresholds for incident reporting, provides the necessary templates for notification, and contains the relevant contact information required for an OES to fulfil its statutory duties.
- **NIS Security Assurance Guidance (Concept) for Downstream Gas & Electricity**[5]**:** This document supports the wider programme of regulatory assurance activity conducted under Regulation 16 of the NIS Regulations. It is intended for an OES and approved cyber security consultancies to manage a structured cycle of verification activities. The guidance details the expected outcomes for three core assurance pillars, being independent CAF based audits, operational exercising to test incident response capabilities, and technical testing, which includes vulnerability assessments and penetration testing of essential systems.

2 Load Measurement

2.1 Overview of Load Measurement

The measurement of aggregated load within the defined functional scope determines whether a load control organisation is deemed to be designated as an OES and therefore subject to the statutory duties laid out in the NIS Regulations 2018[6]. Load controllers with an aggregated load under the threshold amount will be subjected to Condition 9 of the licence conditions.

2.2 Aggregated Load Calculation Methodology

The proposed threshold for determining whether an organisation falls within scope of the load control essential service will be calculated based on its potential electrical control, which is combined maximum electricity capacity of all relevant ESAs managed by the controller. Schedule 2, paragraph 5B of the revised NIS Regulations sets out how the potential electrical control is measured. The intent is to ensure that the measure reflects the potential impact of the electricity system, rather than average usage or operational output.

Load Controllers should use the following criteria to determine their total managed capacity for the purposes of threshold monitoring:

- **Inclusion of all Managed Assets:** Aggregated load is the sum of the maximum potential load, or nameplate capacity, of all ESAs managed by the load controller.
- **Peak Potential Load**: The calculation should be based on the maximum load that the load controller has the technical capability to control at any given time, regardless of whether that control is exercised for commercial, technical, emergency or any other purposes. The maximum flow of electricity into and out of a relevant ESA is to be determined by reference to the electricity capacity of that ESA as stated by the manufacturer.
- **Geographic Scope:** Only those assets and appliances located within the GB electricity system are to be included in the calculation. This reflects the territorial scope of the GB electricity system and the regulatory remit of DESNZ and Ofgem, noting the NIS Regulations apply across the United Kingdom[7].

[3] www.ofgem.gov.uk/sites/default/files/2026-01/NIS_Guidance_for_Downstream_Gas_and_Electricity_Operators_of_Essential_Services_in_GB_v3.0.pdf
[4] https://assets.publishing.service.gov.uk/media/6530f145927459000df959e3/implementation-of-the-network-and-information-systems-regulations-guidance.pdf
[5] https://www.ofgem.gov.uk/sites/default/files/2025-07/Ofgem-NIS-Security-Assurance-Guidance-Concept-for-DGE-Sector.pdf
[6] Load controllers below this threshold can also be specifically designated as an OES by the competent authorities under Regulation 8(3).
[7] The Department of Finance is the Competent Authority for the NIS Regulations in Northern Ireland.

DRAFT

- **Continuous Monitoring:** Load controllers should monitor their aggregated load. If an organisation's portfolio reaches the 300 MW threshold, they are obliged under NIS to notify the competent authority (in writing) within three months of the thresholds being met or exceeded.

2.3 Relevant Energy Smart Appliances

The requirement to hold a Load Control Licence is a baseline for market participation for those performing a licensable load control activity. The Energy Act 2023 (s.238) provides the foundational statutory definitions for ESAs and load control signals that underpin this regime. Under the terms of the licence, in-scope organisations are obliged to meet specific cyber security requirements as set out in Condition 9 or their statutory duties under the NIS Regulations.

The following ESA device types are in scope for a DESNZ licence:

- Domestic EV Charge Points
- Domestic Battery Energy Storage Systems (BESS)
- Smart Heat Devices, such as heat pumps.

For Load Controllers that meet the 300 MW threshold (see Section 1), and subject to the passage of the CSRB, a wider range of ESAs may be considered in scope due to their potential system impact. These requirements are more comprehensive to reflect the complexities of large scale load control platforms, OT, grid scale assets, and the broader systemic risk inherent in larger scale load control operations. The following categories of appliance are in scope for load control under NIS:

- Electric vehicles (EVs)
- EV charge points, both public and private
- Electrical heating appliances
- Grid Scale Battery Energy Storage Systems, both domestic and grid scale
- Virtual power plants used to aggregate load.

The proposed measures will capture load control of above 300MW in aggregate of relevant ESAs in any setting, whether domestic, commercial, or industrial. Organisations in scope may have a variety of relevant ESAs in their portfolio, or may manage only one type of ESA.

3 Capturing Load Control Scope

Accurately defining the network and information systems scope to which the Load Control CAF Profile applies is the foundational step for any load control organisation. The scope dictates the boundaries of the assessment and ensures security measures are proportionate to risk.

It is the responsibility of the Load Controller to ensure that this scope is complete, accurate, and maintained over time. The scope must capture all systems, services, and components used to facilitate load control, including (but not limited to) relevant hardware, software, infrastructure, platforms, and sites/locations supporting the service, as well as any dependencies that support the delivery, operation, or security of the service. This includes internal systems, external integrations, and third-party services where they form part of the control chain or are relied upon for the provision of the load control function.

Where functions are delegated to third parties, including Software as a Service platforms or Managed Service Providers, the Load Controller remains responsible for ensuring that those services are appropriately secured and managed. This may include services that may fall within the scope of forthcoming regulatory frameworks, such as Managed Service Providers under the Cyber Security and Resilience Bill, where they support or influence the delivery of the load control service.

3.1 Load Control Blueprints

3.1.1 Objective of the Blueprints

The objective of defining Load Control Blueprints is to provide a representative framework for the sub-sector. It is recognised that while regulatory requirements remain consistent, the technical implementation and business models vary. These blueprints are intended to be illustrative archetypes that cover representative architectures seen within the load control sub-sector, rather than exhaustive technical specifications.

DRAFT

When identifying the functional boundary, organisations should refer to the relevant ESAs as defined in Section 2.3 and covered in extended detail in the supporting documents listed in Chapter 1.3. These archetypes help ensure that security measures are focused on ESAs specified in associated regulations.

Broadly, the sub-sector is characterised by a clear delineation between three primary blueprints:

- Consumer-Led Flexibility: Focused on the aggregation and management of domestic and small non-domestic ESAs such as EV chargers, smart heating technologies such as heat pimps, and domestic BESS.
- Industrial & Commercial (I&C) BESS and VPP: Focused on the control of grid-scale assets, specifically Grid-BESS and the orchestration of VPPs.
- I&C: Public EV Charging: Focused on high-capacity charging hubs and rapid-charging networks managed through multi-party commercial ecosystems.

Organisations may find that their operations align strictly with one blueprint, or in more complex cases, operate a hybrid model that spans both domestic and industrial environments.

It is important to note that the roles described within these blueprints are logical functions rather than fixed corporate definitions. In practice, a single organisation may be responsible for one, several, or all of these functions. For example, vertically integrated entities often consolidate these logical roles, acting as the infrastructure provider, the load controller, and the flexibility aggregator simultaneously across their chosen portfolio. Conversely, an organisation may only perform a single function within the overall ecosystem.

It should also be recognised that the separation of these logical functions does not necessarily imply physical separation of systems or networks. In practice, these functions may be implemented across physically distinct environments, logically segregated within shared infrastructure, or delivered through a combination of both approaches. Where functions coexist within the same environment, appropriate logical controls, such as network segmentation, access control, and security zoning, should be applied to maintain separation. Where required by operational or safety considerations, physical separation may also be necessary. Organisations should consider both logical and physical segregation when defining scope, ensuring that boundaries between functions are clearly understood and appropriately secured.

The following sections expand on these concepts by providing representative architectural views of the load control environment. These illustrate how logical functions, control layers, and dependencies are typically arranged in practice, supporting organisations in identifying the systems and interfaces that fall within scope.

3.1.2 Load Control Ecosystem View

The designation of load control as an essential sub-sector reflects its role in maintaining the security of the GB energy system. As outlined in the Cyber Security and Resilience Bill, [8]the proliferation of high-wattage ESAs and EV charging infrastructure has introduced new risks to national grid stability. Load control provides the technical mechanism to deliver Flexibility and Demand Side Response (DSR), which are essential for balancing a grid increasingly reliant on intermittent renewable generation.

By orchestrating the adjustment of demand through digital signals, load control ensures that the energy system can maintain frequency and manage constraints in real time. Because these control systems now aggregate enough capacity to influence the wider network, they are considered critical components of the energy landscape. The regulation of this sub-sector ensures that the technical platforms and their dependencies, facilitating these services are resilient against cyber threats that could otherwise lead to significant disruptive effects on the grid.

The following table illustrates where load control sits in relation to established energy sub-sectors:

Energy Sub-Sector	Role in Ecosystem	Interaction with Load Control
Generation	Bulk production of electricity.	Load control provides balancing services to mitigate generation volatility and intermittency.

[8] https://www.gov.uk/government/collections/cyber-security-and-resilience-bill

Transmission	High-voltage transport of power across GB.	Load control supports frequency response services to ensure national grid stability.
Distribution	Low-voltage delivery to homes and businesses.	Load control is used for active network management to relieve local constraints and manage peak demand.
Supply	Commercial sale of energy to end consumers.	Some suppliers act as load controllers to deliver smart tariffs and reward consumer-led flexibility.
Load Control	Technical orchestration of Flexibility and DSR.	Aggregates distributed capacity to provide stability and balancing services to the whole system.

Table 3-1 OES Sub-Sectors

3.1.3 Consumer-Led Flexibility Blueprint

The Consumer-Led Flexibility blueprint represents the most common model for managing distributed energy resources at the domestic and small non-domestic level. This archetype is characterised by the orchestration of high volumes of diverse ESAs across multiple manufacturer ecosystems.

The core of this blueprint is the digital communication chain that links grid signals or market prices to the physical load at the consumer premise.

In this model, the service is delivered through a series of logical entities and interfaces:

- **Flexibility Service Provider (FSP):** The commercial entity that enters into arrangements with the consumer. The FSP receives flexibility instructions from System Operators (NESO/DSO) or wholesale market signals and translates these into demand response strategies.
- **Load Controller:** The technical entity responsible for the secure construction and dispatch of load control signals. This platform orchestrates the necessary adjustments required across the portfolio to meet the FSP's objectives.
- **Energy Smart Appliance Manager (ESAM):** A logical function (often a cloud-to-cloud API integration but can also exist on the ESA itself) that provides the interface between the load controller and the individual ESAs. The ESAM manages device-specific communication and reports on ESA status and availability.
- **Energy Smart Appliance (ESA):** The physical asset at the consumer premises, such as an EV charger or heat pump. While the physical device and its internal firmware are typically outside the direct technical assessment scope of the Load Control CAF Profile, the integrity of the signal reaching the device is a primary security concern.

DRAFT

3.1.4 Industrial & Commercial Blueprint

This blueprint provides a representative architectural view of load control systems operating within the Industrial and Commercial environment. It is important to recognise that this blueprint is illustrative in nature and does not represent a definitive or exhaustive model of all implementations within the sub-sector.

The load control sub-sector includes a range of technical architectures, deployment models, and organisational arrangements. This blueprint is therefore intended to provide a structured reference point to support consistent scoping, rather than to prescribe how systems must be designed or implemented.

Specifically, this blueprint focuses on the sub-set as outlined in the CSRB and updated to OES in NIS:

- **Grid-scale Battery Energy Storage Systems (BESS)**. These are large-scale electrochemical energy storage systems connected to the transmission or high-voltage distribution network, capable of storing and discharging electricity to support grid stability, frequency response, and energy balancing services.
- **Virtual Power Plants (VPPs)**. These are aggregated networks of distributed energy resources, including storage, generation, and controllable load, which are coordinated through a central platform to operate as a single flexible asset for grid support and market participation.

Grid-scale BESS may be deployed for a range of purposes, including frequency response, market participation, co-location with generation assets, or resilience and backup functions. Where such systems are capable of being controlled, aggregated, or influenced as part of a load control service, they should be considered within scope.

The purpose of this blueprint is to support organisations in defining the functional boundary of load control services that directly influence grid stability and energy balancing at scale.

This blueprint reflects environments where assets are high-capacity and grid-connected, control actions have immediate system-level impact, and OT and ICS are central to service delivery. These systems should be understood as cyber-physical control architectures where digital instructions directly affect physical electrical behaviour.

Architectural Context

I&C BESS and VPP environments align with recognised operational technology architectural principles, including those described in:

- NIST SP 800-82[9].
- ISA/IEC 62443[10].
- IEC 62264[11].
- Industrial Internet Consortium reference architecture[12].

These environments are composed of multiple logical layers that together form a control chain from signal origin to physical execution. Separation between these layers may be logical or physical depending on design, safety, and operational requirements.

Logical Layers (for Scoping)

Layer	Description	Typical Components
Physical asset layer	Equipment that alters or measures electrical behaviour.	BESS arrays, inverters, EV charging infrastructure, sensors.
Local control layer	Real-time control and safety enforcement at site level.	PLCs, protection systems, local EMS, site gateways.
Supervisory control layer	Central monitoring and command execution.	SCADA or equivalent control environments.

[9] https://csrc.nist.gov/pubs/sp/800/82/r3/final
[10] https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
[11] https://www.isa.org/certification/certificate-programs/isa-95-iec-62264-enterprise-control-system-integra
[12] https://www.iiconsortium.org/iira/

DRAFT

Control and orchestration layer	Aggregation and coordinated dispatch of assets.	Load control platforms, VPP orchestration systems.
Integration and communications layer	Transport of control signals and telemetry.	APIs, message brokers, telecommunications networks.
Enterprise and market interface layer	Generation and influence of control instructions.	Market systems, optimisation platforms, trading systems.

Reference to Architectural Models and Layered Considerations

Recognised architectural models such as the Purdue Enterprise Reference Architecture[13], ISA/IEC 62443, IEC 62264, and Industrial Internet Consortium reference models provide a conceptual basis for understanding layered OT environments.

These models support:

- Layered system understanding.
- Identification of control domains.
- Definition of communication paths.
- Recognition of trust boundaries.

They should be treated as reference approaches rather than prescriptive designs.

When defining scope, organisations should consider the full architectural stack across all layers, including:

- Physical processes and field devices.
- Local and site-level control systems.
- Supervisory and control environments.
- Integration and communications layers.
- Enterprise and external systems.

Separation between layers may be logical or physical, depending on operational, safety, and security requirements.

OT System Representations and Examples

To support a broader understanding of how operational technology environments are structured, organisations To support understanding of how operational technology environments may be structured, organisations may refer to external guidance such as NIST SP 800-82 (Guide to Operational Technology Security), which provides illustrative system representations and examples of common OT architectures. Organisations may also use equivalent recognised industry guidance where appropriate. These materials are intended to aid understanding of system composition, dependencies, and control relationships, and should not be interpreted as prescriptive or exhaustive. Organisations should apply approaches appropriate to their own technical environment and risk profile.

These diagrams illustrate typical OT system layouts and control relationships across a range of implementations, including:

- SCADA systems.
- Distributed Control Systems (DCS).
- Programmable Logic Controller (PLC) based systems.
- Building Automation Systems (BAS).
- Physical Access Control Systems (PACS).

These examples demonstrate how control systems are composed of interacting components, communication paths, and control layers that extend from enterprise systems through to physical processes.

[13] https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf

DRAFT

It is important to recognise that these diagrams are logical representations intended to aid understanding. They are not exhaustive and should not be interpreted as prescriptive designs. Real-world implementations will vary based on organisational structure, technology choices, and operational requirements.

Organisations should use these examples to:

- Understand typical OT system compositions.
- Identify where their own systems align with established patterns.
- Recognise dependencies across control, communication, and physical layers.

Control Chain and Dependencies

A defining characteristic of I&C BESS and VPP environments is the control chain linking external signals to physical system response.

Stage	Description	Example Systems
Signal generation	Creation of control intent.	Market platforms, grid operator signals, optimisation engines.
Dispatch and orchestration	Conversion into coordinated actions.	VPP platforms, dispatch engines.
Signal transmission	Delivery of instructions.	APIs, telecoms networks, secure channels.
Local execution	Translation into equipment commands.	Site controllers, gateways, PLCs.
Physical response	Change in electrical behaviour.	Batteries, chargers, load assets.

Each stage represents a dependency and must be considered in scope where it contributes to service delivery, integrity, or resilience.

Implications for Scoping

A common scoping error is focusing only on central control platforms. This is insufficient for grid-scale load control systems.

Organisations must include all systems that contribute to the control chain and its secure operation.

In-Scope Considerations

Category	Examples
Control systems	SCADA environments, load control platforms, VPP orchestration systems.
Site systems	Local controllers, gateways, protection systems.
Communications	Network infrastructure, telecommunications, APIs.
Cloud and integration	Cloud platforms, external interfaces, data exchange services.
Market and enterprise	Market systems, optimisation engines, trading platforms.
Security and support	Identity services, monitoring, logging, security tooling.
Third-party dependencies	External providers forming part of the control chain.

Supporting ancillary systems should also be considered where they contribute to the delivery, operation or security of the load control service.

Failure to include these elements may result in incomplete scope definition and unmanaged risk.

Summary

The I&C BESS and VPP blueprint ensures that load control systems are assessed as complete cyber-physical control architectures rather than isolated platforms.

By considering all layers of the system, including both logical and physical separation, and the full control chain, organisations can define a scope that is complete, defensible, and aligned with recognised operational technology principles.

3.1.5 Public EV charging Blueprint

The Public EV Charging blueprint describes the orchestration of high-capacity charging hubs and rapid-charging networks. In this context, the aggregated load of multiple high-powered chargers is managed to provide system flexibility while ensuring the infrastructure remains available for the end-user. This blueprint reflects a complex ecosystem of commercial and technical players who collaborate to provide a seamless charging experience and grid-balancing services.

As with CLF the system can be represented as a hierarchical control structure. This illustrates how control actions propagate through the system and how different entities interact based on data inputs, such as device or system telemetry.

This view highlights the flow of information and control between components, from external signals and orchestration platforms through to the end devices. It also shows how telemetry and feedback loops inform control decisions, enabling dynamic adjustment of load in response to system conditions

Logical View of the Public EV Charging Blueprint

This blueprint defines the interaction between commercial management platforms and site-level energy control systems:

- **e-Mobility Service Provider (eMSP) Platform**: Provides the customer interface, managing subscriptions, payments, and session authorisations. It communicates EVSE availability and session requests between the consumer and the central management system.
- **Charge Point Management System (CPMS):** A cloud-based software platform designed to monitor, manage, and optimise electric vehicle charging station networks remotely. It provides essential tools for operators to handle billing, user access, energy consumption, and real-time troubleshooting to ensure high uptime and efficient infrastructure. It receives session requests from eMSPs and banking systems, calculates current limits based on planned consumption, and dispatches control actions to the physical chargers.
- **Local Energy Management System (Local EMS**): Acts as the site-level controller, monitoring constraints from the local Feeder Pillar or Substation. It establishes local power limits and communicates these to the CPMS to ensure flexibility events do not compromise local distribution integrity.
- **Electric Vehicle Supply Equipment (EVSE):** The physical charger that executes control actions (e.g., setting current limits) received from the CPMS. It provides real-time telemetry, including power consumption and vehicle identification, back to the control chain.
- **Flexibility Service Provider (FSP):** This role involves the technical and commercial participation in flexibility markets. It is often consolidated by the CPO or a third-party aggregator to translate grid signals into orchestrated charging schedules across the broader charging network.

3.2 Importance of Accurate Scoping

Defining a precise scope ensures that cyber security, operational resilience, and broader system resilience efforts are focused on the systems most critical to the provision of load control services. This applies across both Tier 1 and Tier 2 organisations and should be implemented proportionately based on aggregated load, system criticality, and potential impact on the electricity system. This is fundamental to meeting obligations under the NIS Regulations and the requirements set out in Condition 9 of the Load Control Licence, which establishes the expectation for appropriate cyber assurance arrangements.

An accurately defined scope ensures:

DRAFT

- **Risk Relevance**: Risk and resilience assessments are comprehensive, relevant to the functions being performed, and effective against identified threats to the load control service.
- **Proportionality:** Security and resilience measures are appropriate and proportionate to the organisation's scale, aggregated load, and potential impact on the electricity system.
- **Assurance Clarity:** There is clear, defensible evidence of what is in scope to support CAF based assurance activities, including self-assessment and independent assurance, as well as inspection and verification by the relevant regulator.

Failure to accurately capture the scope can lead to critical systems being overlooked, resulting in unmanaged risk to the essential service, or effort being misdirected towards systems not essential to service provision, resulting in unnecessary cost. An organisation's defined scope may be subject to challenge during assurance or regulatory inspection activities, requiring reassessment and remediation.

Load Controllers are expected to continually monitor and maintain their scope to ensure it remains accurate and reflective of the systems, services, and dependencies supporting the load control function. This includes:

- Ongoing identification of changes to systems, architectures, dependencies, and aggregated load.
- Regular validation that the defined scope continues to meet regulatory and licence expectations.

Where material changes occur that affect the scope, the organisation must inform the relevant regulator. Where a system or service is proposed to be removed from scope, the organisation must engage with the relevant regulator to confirm that the removal is appropriate and does not compromise the integrity of the load control service.

3.3 Defining the Functional Boundary of Load Control

The functional boundary refers to the perimeter that encompasses all components necessary for the essential service of load control to operate securely and reliably.

For organisations already designated as an OES within the Downstream Gas and Electricity sector, the load control function may represent an extension of existing essential services. In such cases, Load Controllers must ensure that the interdependencies between load control systems and other essential energy functions are clearly mapped and secured.

For newer CLF providers and market entrants, the challenge often involves defining an essential service for the first time. In these environments, the functional boundary must be drawn to include the core control platforms, the communication infrastructure used to signal appliances, and the specific data sets used to trigger load control events.

3.4 Scope Considerations

This section of the guidance focuses specifically on the technical application for the network and information systems essential for the delivery of CLF based load control. This environment is typically characterised by cloud native architectures, consumer facing interfaces, and extensive third party API integrations used to manage flexible load at the domestic and small non domestic level. Where organisations control or are approaching aggregated load at or above 300 MW, these considerations should also be applied in the context of wider resilience obligations.

Accurately defining this scope is fundamental, ensuring cyber security and resilience efforts are focused solely on systems essential to the service provision. This includes not only protection against cyber threats, but also the ability to maintain safe, reliable, and continuous operation of the load control service under a range of conditions, including system failure, loss of connectivity, degraded performance, or external disruption. The functional boundary for organisations utilising CLF technology typically encompasses the core platforms and digital interfaces used to manage and operate the flexible load. These examples are not exhaustive and are intended to provide a representative view of common implementations.

To identify these systems, organisations should apply the identification principles below, in addition to any systems, services, or dependencies that the organisation determines to be critical to the delivery, operation, or security of the load control service.

DRAFT

3.5 General Principles for Identifying In-Scope Systems

To ensure a consistent and auditable boundary, organisations utilising blueprints may apply a set of identification principles. These principles serve as the filter to determine if a system, service, software, facility, infrastructure, technology, organisational system, shared platform, or data set resides within the functional boundary of the load control service.

- **Directly Used for Service Provision:** This includes the core technical platforms and software logic without which the load control service cannot be delivered. Examples include, but are not limited to, the primary load control platform, dispatch systems, customer applications and interfaces, organisational endpoints such as laptops and servers used for system management, and any supporting facilities or infrastructure required to operate these components.
- **Relied Upon for Service Security or Resilience:** These are systems that provide the foundational security, protection, or management layer for the core platform. This includes, but is not limited to, identity and access management platforms, network security services, privileged access solutions, monitoring and logging capabilities, and any physical security controls or supporting systems required to protect critical assets and ensure their continued operation.
- **Supply Chain Managed Systems:** Given the reliance on external partners, any third party service essential for the operation, protection, or security of the in scope systems must be included. This includes, but is not limited to, cloud infrastructure providers, managed service providers, managed security providers, third party API gateways, and any externally hosted platforms or technologies that form part of the control chain or support the essential function.

The systems, services, and facilities used to configure, update, monitor, maintain, or physically protect any of the above components, including security tools, administrative endpoints, and supporting infrastructure, are also considered firmly in scope for the assessment.

3.5.1 Technical Assessment Scope

This refers to the systems, networks, and data flows where the load controller has direct administrative control:

- Load Control Platform: This includes the core orchestration logic, server environments, and database systems. The organisation has full responsibility for patching, identity management, logging, and overall security and resilience within this boundary.
- Communication Channel (APIs): The security of the egress point and the protocols used to transmit load control signals are firmly in scope. This requires robust encryption, authentication, integrity protection, and measures to prevent signal spoofing or manipulation.

3.5.2 Functional Pillars

Once identified, in scope systems should be categorised into three functional pillars. This ensures that the security and resilience assessment covers the entire lifecycle of a load control event.

Pillar 1: Direct Load Management and Orchestration
This pillar captures the core of the load control service. It includes the server environments and control logic responsible for managing device state, processing flexibility signals, and orchestrating events. For organisations using load control technology, this usually resides within a virtual private cloud or a containerised environment. This pillar may also include site level control components and any supporting infrastructure required to directly execute control actions.

Pillar 2: Service Interfacing and Data Flows
This pillar encompasses the entire communication chain required to reach the end asset. It includes:

- Consumer Applications: Mobile applications and web portals used by consumers to set preferences or initiate manual overrides. These are significant entry points for control instructions.
- Technical Interconnects: Third party APIs and cloud to cloud links used to reach appliances across different manufacturer ecosystems.
- External Data Sources: Triggers such as price signals or weather data that drive automated events. Manipulating these flows can lead to unintended grid impacts.

DRAFT

This pillar should also include dependencies on external services and third party providers that facilitate communication, data exchange, or control execution.

Pillar 3: Supporting and Common Services
This pillar identifies the shared infrastructure upon which the operational pillars rely. Many systems traditionally viewed as general enterprise functions fall into this category, such as corporate collaboration tools or identity platforms.
This includes, but is not limited to, supporting services and dependencies such as identity and access management, monitoring and logging platforms, security tooling, managed service providers, cloud hosting environments, and other third party services.
Physical security controls and supporting facilities that protect critical systems and infrastructure should also be considered within this pillar where they are necessary to ensure the secure and reliable operation of the load control service.

3.5.3 Security Governance Responsibility and Dependency Management

This refers to components that are not subject to direct technical assessment within the load controller's administrative control boundary, but which remain integral to the delivery, security, and resilience of the load control service. These components should not be considered out of scope. Instead, they form part of the broader system dependencies that should be actively managed.

The load controller retains overall responsibility for the end to end operation, security, and resilience of the load control service, including where elements of the control chain are delivered by third parties or external platforms.

This includes, but is not limited to:

- **Third Party ESA Cloud Platforms**: While the internal infrastructure of a manufacturer's cloud platform is not directly assessed by the load controller, the integration and reliance on that platform introduces a dependency that must be managed. This should be supported through vendor due diligence, assurance activities, contractual controls, and an understanding of how the platform contributes to the control chain.
- **Energy Smart Appliances (ESAs):** These devices are not subject to direct technical assessment within this scope. However, they represent the end point of the control signal and therefore form part of the overall service dependency chain. Load Controllers should consider the role of connected devices when managing risks to the security and resilience of the load control service, including taking appropriate steps to mitigate risks arising from device behaviour, interoperability, and integration. This may include having regard to applicable UK security requirements (such as ETSI EN 303 645) and relevant interoperability specifications. Consideration should also be given to the security posture of device manufacturers and any associated platforms that support device operation

Because the load control service relies on an end to end chain of systems, platforms, and devices, all dependencies that contribute to the delivery of the control signal and its execution must be identified, understood, and managed as part of the organisation's cyber security and resilience framework.

3.6 Additional OES NIS Scope Considerations

The NIS reporting requirements require Operators of Essential Services to provide clear and comprehensive details of the essential services, functions, systems, and sites that fall within scope of the NIS Regulations. The NIS Scope must set out full details of the network and information systems on which the essential service relies, or which are used for its provision. The NIS Regulations define the meaning of both 'network and information systems' and 'essential service', and these definitions must be applied when establishing scope.

Within the NIS Regulations (Regulation 2(1)), 'network and information systems' includes:

- Electronic communications networks as defined in the Communications Act 2003.
- Devices or groups of interconnected devices that perform automated processing of digital data.
- Digital data stored, processed, retrieved, or transmitted by such systems for their operation, use, protection, and maintenance.

An ‘essential service’ is defined as a service which is essential for the maintenance of critical societal or economic activities. Within the Downstream Gas and Electricity sector, these services are further defined in Schedule 2 of the NIS Regulations. Operators should consider Regulation 8(1), including threshold requirements, when determining whether their services meet the criteria for designation. This includes not only capacity considerations, but also the potential impact on consumers and the wider energy system.

Operators of Essential Services are expected to adopt a consistent and well evidenced approach to defining and maintaining their NIS Scope. This includes ensuring that all relevant systems, dependencies, and supporting services are identified, and that scoping decisions are documented with clear rationale and supporting assumptions.

While this section is framed in the context of NIS and Tier 1 organisations, the underlying principles of structured scoping, dependency identification, and evidence based decision making apply equally to Tier 2 Load Controllers. Tier 2 organisations are expected to apply a comparable methodology, proportionate to their scale and impact, when defining the functional boundary of their load control service.

Tier 2 organisations operating below the 300 MW threshold should recognise that they may, over time, meet the criteria for designation as Operators of Essential Services. It is therefore prudent to adopt a level of rigour in scoping and documentation that aligns with NIS expectations, such that, if designated, the organisation can demonstrate compliance without significant rework. This includes maintaining sufficient evidence and governance to support the implementation of appropriate and proportionate measures, and to prevent and minimise the impact of incidents affecting the load control service.

Organisations may align to recognised and generally accepted good practice when developing their scope, such as the concept of a ‘system under consideration’ described in ISA 62443-3-2. However, it should be recognised that the NIS Scope may extend beyond traditional industrial control system boundaries to include wider network and information systems, supporting platforms, and external dependencies that contribute to the delivery of the essential service.

Regardless of designation, all load controllers should ensure that their approach to scoping is systematic, repeatable, and capable of supporting assurance, audit, and regulatory engagement.

3.6.1 OES NIS Principles

The following principles are expected to be followed by OES when identifying their NIS Scope:

- Any network and information system must be included in the NIS Scope if the system, sites and network and information systems on which the essential service relies, or which are used for the provision of an essential service.
- Any network or information system must be included in the NIS Scope if the system could suffer an incident that would result in a significant impact on the continuity of the essential service which the OES provides.
- Network and information systems that are not owned or operated by an OES may nevertheless pose risks to the essential service that the OES provides. Third party dependencies on which the essential service relies, or which are used for the provision of an essential service must be identified within the NIS Scope.
- Network and information systems which only temporarily connect to an OES’s networks must still be in the NIS Scope if they enable the provision of the essential service that the OES provides or if they could suffer an incident that results in a significant impact on the continuity of the essential service which the OES provides.
- Network and information systems related to maintenance, integration, security, or similar activity, that might not necessarily be required during immediate essential service operations but are required for the long-term provision of the essential service, should be included within the NIS Scope.
- For those OES that are designated as a result of exceeding a cumulative or total capacity threshold requirement under Schedule 2 of the NIS Regulations, all sites and systems relevant to meeting said threshold requirement should be detailed within the NIS Scope.
- OES must not use the incident reporting thresholds, that they are to have regard to when notifying incidents under Regulation 11, when defining the functions, sites or network and information systems within their NIS Scope.

DRAFT

3.6.2 OES NIS Scope Examples

The examples below illustrate the types of network and information systems that are likely to support the provision of an essential service. These examples are not exhaustive and are intended to provide a representative view of the types of systems that may be considered within scope.

Core Operational Systems

Category	Examples
Operations Management	Operations management systems
Control Systems	SCADA, DCS, local controllers (PLC, electronic controllers)
Safety and Protection	Safety instrumented systems (SIS), protection systems
Field Devices	Intelligent electronic devices, remote terminal units (RTUs), sensing equipment
Control Platforms	Demand management systems, balancing systems, real time operation systems
Infrastructure	Data centre systems, cloud platforms (including cloud based SCADA)
Communications	Critical communications networks, including wireless
Business Critical IT	IT systems deemed critical for delivery of the essential service

Supporting and Ancillary Systems

Category	Examples
Utilities and Facilities	HVAC, power supply, chilled water, instrumentation air
Control Continuity	Backup control centres, backup systems
Access and Connectivity	Remote access solutions
OT Management	OT configuration management, change management systems, OT asset management
Monitoring and Management	Cloud or on premise monitoring and management platforms
Facilities Management	Building management systems
Security	Physical security systems, cyber security systems
Commercial Interfaces	Trading systems and interfaces

Functional Areas to Consider in Scope

When determining the scope, load controllers should consider all functions, sites, and network and information systems on which the essential service relies, or which are used in its provision. This may include:

Functional Area	Description
Physical Process	Physical process controls and execution
Operations	Operational control and monitoring
Planning	Operational preparation, planning, and management
Support Functions	Business planning, maintenance, and logistics
Assurance	Operational confidence and assurance, including safety and security
Environmental	Environmental protection systems and controls
Governance	Business policy and regulatory compliance

This structured view is intended to support a consistent and comprehensive approach to identifying in scope systems across both Tier 1 and Tier 2 organisations.

DRAFT

3.7 Scope viewpoints

To ensure a comprehensive and auditable understanding of the assessed boundaries, Licensed Load Control providers should document the scope of their network and information systems using interconnected viewpoints. These viewpoints, adapted from established energy sector practice, link the organisational context, essential functions, supporting technology, and external dependencies. Viewpoints should be approved by an individual able to make executive decisions on behalf of the organisation.

3.7.1 The Scope Register View

Section	Content
Description	This view is used to establish clear boundaries for the CAF assessment. It can take the form of a formal document or asset register detailing all identified In-Scope and Out-of-Scope systems.
Purpose	To document the definitive boundary of the assessment, providing a defensible rationale for exclusion for both the provider and the assurance auditor.
Representation Options	Formal document, asset or risk register entry, or structured spreadsheet.
Requirements	Should include a clear rationale for the exclusion of any system, ensuring the boundaries are auditable.

3.7.2 The Essential Service View

Section	Content
Description	This viewpoint describes the essential service the OES provides at a high-level. It should identify the relevant subsector, and service-type provided (e.g. generation, transmission, system operation, load control etc.). This view should also consider the OES's operational role within the respective subsector and identify, where possible, the regions and customers served. In addition, any wider aspects that make the OES's essential service important to consumers (e.g. electricity restoration capability) should be detailed. It formally documents the definition of the licensed service, describing what the service achieves, who it serves, and its role in the energy flexibility market.
Purpose	To provide an overview of the essential service and context for subsequent scoping views. To indicate the inherent criticality of the service.
Representation Options	Descriptive text, overview diagram, or organisational chart illustrating service flow.
Requirements	• Subsector • Service-type and description • Considerations with regard to Regulation 8(1). Nature of essential service under Schedule 2 and (if relevant) details of which threshold requirements apply. • Geography • Number of customers served

3.7.3 The Functional View

Section	Content
Description	This view provides a breakdown of the load control service into the various logical functions that enable its secure delivery (e.g., consumer authentication, flexibility signal dispatch, operational monitoring). It should identify the high-level functions,

DRAFT

	and the relationships between those functions, to provide an overview of the approach an OES takes to delivering their essential service.
Purpose	To provide an overview of the essential service from a functional perspective. To support the identification of in-scope network and information systems and their associated security requirements. To provide context to criticality and impact assessments.
Representation Options	Capability taxonomy/mapping diagram, functional breakdown diagrams, or process flow diagrams.
Requirements	Breakdown of high-level functions enabling the essential service; description of the relationships and dependencies between these functions.

3.7.4 The Systems View

Section	Content
Description	This view identifies the relevant network and information systems required to deliver the OES's functions and essential service. This view should provide a formal description of the system architecture that is employed by the load controller to deliver the essential service and should be aligned to a reference architecture model such as the Purdue Enterprise Reference Architecture[14] for OT / ICS, in addition security zones and conduits may also be presented. This viewpoint should clearly identify the groups of network and information systems on which the essential service relies, or which are used for the provision of an essential service and those that are not, including connectivity across those boundaries. In addition, internal and external access points into the OES's network and information systems should be captured. This is the technical core of the scope documentation. It details the specific applications, APIs, databases, cloud services, and network infrastructure that deliver the functions identified in the Functional View. This view should clearly identify the groups of network and information systems that are in scope and those that are not.
Purpose	• To provide details of the OES's system architecture. • To identify those network and information systems on which the essential service relies, or which are used for the provision of the essential service or that could directly impact it if an incident occurred. • To identify the boundary between network and information systems used for the provision of essential services and those that are not.
Representation Options	System architecture diagrams, network diagrams, data flow diagrams, or asset inventories. Zone and conduit diagrams
Requirements	Should clearly illustrate networks, information systems, and data flow. Should identify connectivity across NIS scope boundaries and link components back to the Functional View.

3.7.5 The Dependencies View

Section	Content
Description	Considering the Licensed Load Control organisation as an open system, this view presents the various external dependencies required to enable the delivery of the essential service and functions.
Purpose	To document the organisation's dependence on external products and services, providing necessary context for assessing Supply Chain Assurance (CAF Objective A4) maturity.

[14] https://www.sciencedirect.com/science/article/pii/S1474667017485326

DRAFT

Representation Options	Context diagram, dependency mapping diagram.
Requirements	Documentation of all dependencies required, including product/service suppliers, integration/maintenance providers, and interdependence on other sector participants.

3.7.6 The Site View

Section	Content
Description	This view identifies the physical and logical locations relevant to the licensed service. This typically includes corporate offices, data centres (or cloud provider regions) or any other site necessary for the provision of your service.
Purpose	To provide an overview of the physical estate related to the essential service. To document the class of remote premise for assessing aggregate risk exposure.
Representation Options	Site inventories/lists, geographic network diagram.
Requirements	Definition and description of site types/classes; Description of inter-site relationships; Documenting the class of remote premise and logical groupings where large numbers of sites are present.

3.8 Descope Reporting and Governance

Organisations must treat the removal of any system, asset, technology, or dependency from scope as a controlled governance activity. Descoping decisions must be evidenced, risk assessed, and subject to appropriate oversight to ensure the integrity of the load control service is not compromised.

Where a system is proposed to be removed from scope, the organisation should document, as a minimum:

- System Identification: Name and description of the system, asset, or technology.
- Rationale for Removal: Clear justification explaining why the component is no longer considered in scope.
- Dependency Assessment: Confirmation of whether the system supports, interfaces with, or underpins any other in scope systems, assets, or technologies.
- Impact Assessment: Evaluation of the potential impact if the system were compromised, including impacts to life, the economy, and the electricity system.
- Risk Assessment: A documented risk assessment demonstrating why the system can be safely removed from scope without introducing unmanaged risk to the load control service.

Governance and Approval

Descoping should be governed through formal change management and assurance processes. Organisations should ensure that:

- All descoping decisions are reviewed as part of scope governance activities.
- Material changes to scope are communicated to the Competent Authority where required.
- The organisation maintains an auditable record of scope changes over time.

Formal executive accountability should be demonstrated through periodic governance processes. This may include:

- A summary of scope changes, including systems removed from scope, captured within an annual return or equivalent assurance submission.

DRAFT

- Executive or board level sign off confirming that the organisation considers the revised scope to be accurate and that risks associated with descoped components have been appropriately assessed and accepted.

Descoping should not be treated as a one-time activity. Organisations must ensure that any removal from scope is continuously validated as part of ongoing monitoring, risk management, and assurance processes.

4 Glossary of Terms

Term / Acronym	Definition/ Meaning
Application Programming Interface (API)	Application Programming Interface: A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.
Artificial intelligence (AI)	Artificial intelligence (AI) describes computer systems which can perform tasks usually requiring human intelligence.
Cyber Assessment Framework (CAF)	The CAF is a collection of cyber security guidance for organisations that play a vital role in the day-to-day life of the UK, with a focus on essential functions. It is aimed at helping an organisation achieve and demonstrate an appropriate level of cyber resilience in relation to certain specified vitally important functions performed by that organisation, functions that are at risk of disruption as a result of a serious cyber incident.
CAF Assessment (CAF)	A Cyber Assessment Framework (CAF) Assessment is either a self-assessment, or a third-party audited assessment as directed by the Authority, of the licensee's security posture against a relevant CAF Profile.
CAF Contributing Outcome (CO)	A Contributing Outcome is a specific requirement in CAF that supports the achievement of a broader security outcome.
CAF Indicators of Good Practice (IGPs)	CAF Indicators of Good Practice are associated with each CAF Contributing Outcome. They provide examples of effective security measures but are not an exhaustive, prescriptive checklist.
Consumer Led Flexibility (CLF)	Consumer Led Flexibility means an arrangement between a Flexibility Service Provider and a Customer in relation to activities undertaken as defined by 4(3)(3J)(b) of the Electricity Act 1989).
Charge Point Operator (CPO)	A Charge Point Operator (CPO) is the entity responsible for the installation, management, maintenance, and operation of electric vehicle (EV) charging infrastructure.
Cyber Security and Resilience Bill (CSRB)	The Cyber Security and Resilience Bill will reform and add to the existing Network and Information Systems (NIS) Regulations 2018, to increase UK defences against cyber-attacks.
Demand Side Response (DSR)	Demand Side Response (DSR), also known as demand response or demand-side flexibility, refers to mechanisms that allow energy consumers to actively change their electricity consumption, such as reducing, shifting, or increasing demand, in response to signals from the grid.
Department for Energy Security and Net Zero. (DESNZ)	Department for Energy Security and Net Zero (DESNZ) leads on the government's mission to make the UK a clean energy superpower.
Domestic Consumer / Customer	Domestic Consumer / Customer is a consumer provided with or seeking to be provided with a Consumer-Led Flexibility service located at a Domestic Premises but excludes such Customer insofar as they are provided with or seeking to be provided with a Consumer-Led Flexibility service at a premises other than Domestic Premises.
Domestic Premises	Domestic Premises means premises at which a supply of electricity is taken wholly or mainly for domestic purposes.

DRAFT

eMSP	An e-Mobility Service Provider (eMSP or EMSP) is a company that acts as an intermediary in the electric vehicle charging ecosystem, providing drivers with access to a network of charging points through digital platforms, such as mobile apps or RFID cards.
Energy Smart Appliance (ESA)	ESA has the meaning given to this term in section 238 of the Energy Act 2023, where it relates to an electric vehicle, electric vehicle charge point, hydronic heat pump, storage heater, heat battery, hot water heat pumps, standalone direct electrical hot water cylinders, hybrid heat pump, or battery energy storage system.
ESA Manager (ESAM)	An ESA Manager (ESAM) is a logical entity that provides an interface to Load Controllers and that represents one or more ESAs.
Essential services	Under the Network and Information Systems (NIS) regulations, an essential service is one that is critical for maintaining societal or economic activities.
Flexibility	flexibility is the ability of an energy system to adjust electricity generation or consumption (demand) in real time, or shift it to different times, in response to grid signals, market prices, or renewable energy fluctuations.
Flexibility Service Provider (FSP)	Flexibility Service Provider: organisations entering into flex arrangements directly with a consumer. Any person undertaking activity as defined by 6BAA(1)(b) of the Electricity Act 1989.
HVAC	Heating, Ventilation, and Air Conditioning
ICS	Industrial Control Systems (ICS) are specialised, integrated hardware and software configurations used to monitor, control, and automate industrial processes.
Internet of Things (IoT)	Internet of Things (IoT) is the technology describing everyday objects (rather than computers and smartphones) that can connect to the internet. Examples include speakers, televisions, security cameras and consumer ESAs.
Joint Competent Authority	The Department for Energy Security and Net Zero and Ofgem are the designated Joint Competent Authority under the Network and Information Systems Regulations 2018.
Load Control System (or Load Control Platform)	Load Control System (or Load Control Platform) means any systems which are operated by or on behalf of a Load Controller and used in whole or in part for: (a) constructing load control communications to Energy Smart Appliances; (b) sending load control communications to Energy Smart Appliances; (c) receiving, sending, storing, using or otherwise carrying out any processing in respect of load control communications with Energy Smart Appliances; (d) receiving responses or alerts from Energy Smart Appliances, intended for the Load Controller.
Load Controller	A Load Controller means any persons undertaking activity under 6BAA(1)(a) of the Electricity Act 1989.
National Cyber Security Centre (NCSC)	The NCSC is a part of GCHQ that helps businesses, the public sector and individuals protect the online services and devices that the UK depend on, and act as the National Technical Authority for cyber security.
National Energy System Operator (NESO)	The National Energy System Operator (NESO) was created as a result of the UK's 2023 Energy Act. NESO is at the centre of the UK's energy system and act as a neutral voice and look at the whole picture to suggest fair solutions for energy that work for everyone across the country.
network and Information system (lower case)	"network and information system" means: (a) an electronic communications network; (b) any device or group of interconnected or related devices which performs automatic processing of digital data; and (c) digital data stored, processed, retrieved or transmitted by elements covered under (a) or (b) for the purposes of their operation, use, protection and maintenance. See 2.2.4
Network & Information Systems (NIS) (upper case)	Network & Information Systems Regulations (NIS Regulations) 2018.

DRAFT

Operational Technology (OT)	OT is defined as technology that interfaces with the physical world and includes Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events.
Operator of Essential Services (OES)	“Operator of Essential Services” means an entity designated or deemed to be designated such as under Regulation 8 of the Network and Information Systems Regulations 2018.
RTU	A Remote Terminal Unit (RTU) is a microprocessor-controlled device that interfaces physical field sensors and actuators to a SCADA system, enabling remote monitoring and control.
SCADA	Supervisory Control and Data Acquisition (SCADA) is an industrial control system (ICS) architecture comprising software and hardware, used to monitor, gather, and process real-time data from equipment, machines, and processes across remote locations.
Smart Secure Electricity Systems (SSES)	The DESNZ Smart Secure Electricity Systems (SSES) Programme is designed to create the technical and regulatory frameworks to enable the untapped flexibility from small scale devices, such as domestic electric vehicle charge points and heat pumps.
TTPs	TTP stands for Tactics, Techniques, and Procedures, which are the methods and behaviours used by threat actors to carry out cyberattacks. Analysing TTPs helps security teams understand how adversaries operate, allowing them to detect, mitigate, and predict attacks more effectively.

DRAFT