UK Government

Large Load Controllers: Tier 1 Cyber Assessment Framework and Associated Guidance

Consultation

Closing date: 1 September 2026

Department for Energy Security and Net Zero (2026)

Contents

Summary of proposals

The 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. Government has published a number of consultations in this area[1], which established the policy intent to bring organisations remotely controlling large amounts of electrical load in scope of the Network and Information Systems (NIS) Regulations 2018.

The Cyber Security and Resilience (Network and Information Systems) Bill will update the existing NIS Regulations 2018 to tackle the evolving cyber threats faced by the UK. It will protect more essential and digital services from cyber attacks, enable cyber regulators to be more effective, and provide the Government with the flexibility to respond to new threats in the cyber landscape. The Bill intends to bring a new essential service of load control into scope of the NIS Regulations, which covers organisations remotely controlling electrical load of 300MW or more in aggregate, where it relates to relevant energy smart appliances.

The NIS Regulations do not prescribe the specific security measures that Operators of Essential Services (OES) should have in place, instead requiring OES to implement appropriate and proportionate risk management measures. In order to provide further detail on specifics, the National Cyber Security Centre (NCSC) developed the Cyber Assessment Framework (CAF). The CAF provides a systematic method for assessing the extent to which OES are meeting their security duties under the NIS Regulations.

Load controllers provide flexibility services to the grid and consumers, supporting the efficient and resilient management of the electricity system. Government is aware of the fact that the load control sector has not previously been regulated for cyber security and resilience, and many load controllers have a different composition from traditional energy companies, with a generally higher prevalence of IT systems and high levels of interconnectivity. Therefore, in collaboration with key partners including Ofgem and the NCSC, DESNZ has developed **a new CAF profile** (the Tier 1 CAF profile for Large Load Controllers, or Tier 1 CAF profile). This has been designed with the load control market in mind, using the CAF profile that applies to the rest of the electricity sector as a foundation, to set Government's view of appropriate risk management in order to meet the changing nature of the threat.

The purpose of this consultation is to seek views on the proposals for the attainment levels and implementation of the Tier 1 CAF Profile for the anticipated load control subsector under the NIS Regulations, subject to parliamentary scrutiny, as well as accompanying guidance. This is to gather feedback from industry on **cost, feasibility, proportionality, and clarity**. We will use the feedback to consider if changes should be made to the proposals for implementing the profile prior to its envisaged publication in Autumn 2026.

[1] See section 5.2 of this consultation for detail on previous consultations.

As above, we are seeking views on the initial target attainment levels in the CAF profile and associated guidance products. This includes:

- **Annex A: Large Load Control Tier 1 CAF Profile**[2]: This profile provides a tailored set of outcomes and 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.
- **Annex B: 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). It offers practical examples of the evidence required across the people, process, and technology dimensions, assisting load control organisations in understanding the technical benchmarks used by the regulator to verify compliance.
- **Annex C: DESNZ Scoping Guidance for the Load Control Subsector**: This document provides the technical methodology for defining the functional boundary of a Load Control System. It offers guidance for both established Downstream Gas and Electricity (DGE) organisations already designated as an OES and load controllers who are new to cyber regulation. 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.

[2] Due to the sensitive nature of this document, please email cyber.policy@energysecurity.gov.uk to receive a copy.

General information

Why we are consulting

The purpose of this consultation is to seek views on the proposals for the attainment levels and implementation of the Tier 1 CAF Profile for the anticipated load control subsector under the NIS Regulations, subject to parliamentary scrutiny, as well as accompanying guidance.

Consultation details

Issued: 23 June 2026

Respond by: 1 September 2026

Enquiries to:

Cyber Policy Team
Department for Energy Security and Net Zero
EOC Annex
Old Admiralty Building
London
SW1A 2EG

Email: cyber.policy@energysecurity.gov.uk

Consultation reference: Large Load Controllers: Tier 1 Cyber Assessment Framework and Associated Guidance

Audiences:

We are seeking views from organisations involved in the load control and flexibility service ecosystem, including those that may be designated as Operators of Essential Services (OES) in future, as well as wider stakeholders such as electricity sector participants, technology providers and cybersecurity experts.

Territorial extent:

Great Britain

How to respond

Respond online at: https://energygovuk.citizenspace.com/energy-security/large-load-controllers-framework-and-guidance

When responding, please state whether you are responding as an individual or representing the views of an organisation.

Your response will be most useful if it is framed in direct response to the questions posed, though further comments and evidence are also welcome.

Confidentiality and data protection

Information you provide in response to this consultation, including personal information, will be available to both DESNZ and Ofgem and may be disclosed in accordance with UK legislation (the Freedom of Information Act 2000, the Data Protection Act 2018 and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential please tell us, but be aware that we cannot guarantee confidentiality in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not be regarded by us as a confidentiality request.

We will process your personal data in accordance with all applicable data protection laws. See our privacy policy.

We will process your personal data in accordance with all applicable data protection laws. See our privacy policies: DESNZ privacy policy, Ofgem privacy policy. Unless otherwise stated against specific questions, we will summarise all responses and publish this summary on GOV.UK. The summary will include a list of names or organisations that responded, but not people's personal names, addresses or other contact details.

Quality assurance

This consultation has been carried out in accordance with the government's consultation principles.

If you have any complaints about the way this consultation has been conducted, please email: bru@energysecurity.gov.uk.

Introduction

As the Prime Minister has made clear, Clean Power is one of the five key missions in the Government's Plan for Change and delivering it is an urgent national priority.[3] Achieving flexibility and decarbonisation is creating a more complex, more interdependent energy system. In meeting this challenge there is huge potential benefit for the grid, for GB's energy independence, and for consumers.

Consumer-led flexibility (CLF) gives households and businesses the choice to shift electricity use to off-peak times when power is cheaper and more abundant. The government aims to achieve 10-12 GW of CLF by 2030, a significant increase from 2.5 GW in 2023. A key enabler of this ambitious goal is the control of electricity to Energy Smart Appliances (ESAs), known as load control.

Load control enables electricity usage on ESAs to be automatically adjusted in response to system or price signals while also allowing consumers or customers to set preferences or override controls to suit their needs. At the domestic level, ESAs, such as Electric Vehicles (EVs), Electric Vehicle Smart Charge Points (EVSCPs), smart heat pumps, and batteries can be programmed to be charged or operated during off-peak hours when the cost of electricity is cheaper, helping consumers reduce their bills, and can also respond to system signals to help manage grid demand and support overall energy system stability. By enabling flexible consumption patterns, load control supports the balancing of supply and demand, reduces peak loads, and flattens the overall demand curve, ultimately underpinning a more efficient and resilient electricity system.

At an industrial and commercial scale, Battery Energy Storage Systems (BESS) provide vital support in managing fluctuating renewable energy sources and helping to maintain grid stability. Optimising energy usage across the GB energy system supports reduced costs for consumers through reducing the need for new infrastructure and reducing peak demand charges. Increasingly, organisations can opt to contract out the management of BESS alongside other ESAs to electricity aggregators. An aggregator is a service provider that bundles together a portfolio of ESAs, managing load through a central remote platform, often known as a virtual power plant[4], for the purpose of offering services that support grid balancing and generate revenue.

In tandem, the government is driving forward the expansion of public charging infrastructure so that everyone, no matter where they live or work, can confidently make the switch to an electric vehicle (EV). As of February 2026, there were over 88,500 publicly available charging devices in the UK, representing an increase of almost 20% year on year. Our Local EV Infrastructure Fund will deliver another 100,000 in England by 2030. We estimate that there will be demand for between 250,000 and 550,000 public chargepoints in 2030. As the network grows,

[3] Clean Power 2030 Action Plan - GOV.UK
[4] A draft definition of a virtual power plant is at section 1.2.

chargepoint operators will control increasingly large amounts of load in aggregate, posing a potential grid risk if they are vulnerable to cyber threats.

As both the electricity network and consumers demand greater flexibility, the volume of electrical load managed by organisations delivering load control services is expected to rise significantly. Load control will not only remain central to CLF and grid management but will increasingly underpin other digital business models, such as EV charging networks, in order to adapt to new usage patterns. A major compromise of a load controller could therefore have cascading effects across the electricity network, impacting reliability and consumer confidence.

Digitalisation and increase in the remote management of energy presents new challenges, but it is also an excellent opportunity to build trust and resilience into the system from the outset. By ensuring strong security standards, we can protect critical operations while giving businesses and consumers confidence to adopt innovative services and enabling the unlocking of the full benefits of flexibility and digitalisation across the energy sector.

The load control market is extremely diverse, with a variety of organisations and business models. Managing the different sources of risk is a key challenge. However, we must balance the need to mitigate risk alongside a pragmatic and proportionate approach to regulation and standards, that targets the greatest sources of risk and reduces the overall surface area for attack without being overburdensome. Establishing clear, enforceable requirements will help safeguard critical infrastructure, maintain system stability, and ensure the benefits of digitalisation can be realised securely.

Currently, there are no legislative cyber security requirements for load controllers, and the sector largely relies on self-regulation through measures such as industry-led codes of practice. However, both DESNZ and the NCSC have assessed that voluntary, industry-led approaches are unlikely to deliver the consistent and robust level of cyber resilience needed to manage the growing risk of cyber-attacks over the long term.

Government has already consulted on its intention to require all organisations controlling large electrical loads (300MW and above in aggregate) via relevant ESAs in any setting to comply with the provisions of the NIS Regulations, and to be assured by the CAF. Under the Cyber Security and Resilience Bill, it is intended that load control will be introduced as a new essential service under Schedule 2 of the NIS Regulations[5]. This will mean that any organisation managing relevant ESAs, i.e. controlling the flow of electricity into and out of the relevant ESA by way of load control signals, will be captured by the regulation provided they control 300MW or more in aggregate.

This is an important measure to improve security of the energy system as a whole and to mitigate the risks of potentially highly disruptive cyber-attacks. More information on the NIS Regulations and why this legislative approach was taken can be found at section 2.

[5] Clause 6 of the Cyber Security and Resilience Bill, Cyber Security and Resilience (Network and Information Systems) Bill

Next Steps

Following the closure of this consultation, consideration of feedback, and the publication of government's response to this consultation, we are aiming to publish a finalised version of the Tier 1 CAF Profile and relevant guidance in late 2026 to align with the opening window for the SSES Programme's Load Control Licence applications[6]. This will enable organisations already above the 300MW threshold to begin scaling up their cyber maturity ahead of being designated under the NIS Regulations. We will also share the profile with organisations meeting the 300MW threshold (or on a journey to meet it) who do not need a load control licence, such as organisations managing load in a purely industrial or commercial setting, so they too can build maturity ahead of the changes to the NIS Regulations coming into force[7].

We expect the Cyber Security and Resilience Bill to receive Royal Assent in Spring 2027, subject to the parliamentary process, meaning the legislation will be in force around Autumn 2027.

Finally, we recognise organisations will need time to familiarise themselves with new requirements and build capability. We therefore propose a grace period prior to formal assurance of the new regime. We propose year end 2029 as an appropriate timeframe for large load controllers to be fully meeting the profile[8]

[6] The application window for licence applications to Ofgem will be open for 12 months, following which a licence for load control in the domestic and small scale industrial settings will be mandatory for operation.
[7] See Smart Secure Electricity Systems (SSES) Programme: draft load control licence regulations and conditions - GOV.UK
[8] Load controllers that are designated after 2027 should seek to meet the profile as soon as feasibly possible, but Ofgem and DESNZ can agree to extend the 2029 deadline on a case by case basis or in exceptional circumstances

1. Legislative Approach

1.1 NIS Regulations

Government previously consulted on the intention to introduce a new essential service of load control into the NIS Regulations (see section 5 for more detail on previous consultations). The below section gives an overview of the regulations and key changes.

What are the Network and Information Systems (NIS) Regulations?

The NIS Regulations came into force on 10 May 2018 and are aimed at improving the protection of the network and information systems that are critical for the delivery of the UK's essential services including transport, energy, water, health, and digital infrastructure services as well as to online marketplaces, online search engines, and cloud computing services (as digital service providers).

Operators of Essential Services (OES) are required to demonstrate active cyber security risk management, report incidents that disrupt the continuity of the service and take action to rectify those incidents. The NIS Regulations identify a role for one or more regulatory bodies ('Competent Authorities') to ensure compliance. This regulatory activity is further supported by the UK's technical authority, the NCSC.

Further information on how the NIS Regulations apply in the energy sector, and how organisations can be designated can be found in the DESNZ Policy Guidance for the Implementation of the Network and Information Systems Regulations, and in **section 4.5 in Annex B.**

Roles and Responsibilities

DESNZ is specified in Schedule 1 of the NIS Regulations as the joint Competent Authority with Ofgem for the electricity and downstream gas subsectors, which will also apply to the load control subsector. DESNZ is responsible for the overall energy policy framework relating to the NIS Regulations, as well as associated international liaison matters, while the day-to-day compliance and enforcement activities of the Competent Authority are carried out by Ofgem for the electricity and downstream gas sectors.

OES are required under the NIS Regulations[9] to take appropriate and proportionate measures to protect their systems, including but not limited to the following duties:

- manage risks posed to the security of the network and information systems on which their essential service relies;

[9] Regulation 10 of the NIS Regulations - The Network and Information Systems Regulations 2018

- 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.
- These measures must, having regard to the state of the art, ensure a level of security of network and information systems appropriate to the risk posed.
- Notify the competent authority in writing about any incident which has a significant impact on the continuity of the essential service they provide.

DESNZ and Ofgem work jointly as Competent Authorities for the NIS Regulations in the energy sector, with distinct but complementary roles. DESNZ has led the development of the policy framework for bringing load control into scope, including the design of the Tier 1 Cyber Assessment Framework (CAF) profile. It has also produced initial drafts of supporting guidance in close collaboration with Ofgem and the National Cyber Security Centre (NCSC).

As the regulator responsible for day-to-day oversight and enforcement, Ofgem will ultimately own and maintain the sector-specific guidance and assurance materials, including the CAF overlay and scoping guidance, ensuring they remain up to date as the load control market evolves.

Table 2: Overview of the key responsibilities of DESNZ and Ofgem for the purposes of the NIS Regulations in the load control subsector in Great Britain:

Function	Overall Responsibility
Joint Competent Authority for the NIS Regulations	DESNZ and Ofgem
Responsibility for cyber policy direction, setting government risk appetite for the energy sector	DESNZ
Designation and revocation of OES	DESNZ
Assessing compliance of OES against the requirements of the NIS Regulations, including but not limited to inspections and third-party assessments	Ofgem
Receipt of incident notification, and incident investigations.	DESNZ and Ofgem
Compliance and Enforcement	Ofgem
Issuing penalties under the NIS Regulations	Ofgem

What is changing?

The Cyber Security and Resilience Bill, introduced into Parliament in November 2025, includes a measure establishing load control as a new essential service under the NIS Regulations[10]. Subject to the Bill's Royal Assent, and further details to be set out in secondary legislation, organisations controlling 300MW and above of electrical load via relevant ESAs (see section 3.2) will be designated as OES and be required to comply with the provisions of the Regulations.

Load control is defined as the ability to control the flow of electricity into and out of relevant ESAs by way of load control signals[11]. Load control can be carried either directly by a load controller or via intermediaries. Our intent is to capture both direct load controllers and intermediaries who play an **active role** in load control. An active intermediary is one that is capable of adjusting or processing load control signals to a relevant ESA, and is **authorised** to do so by a load controller. In this scenario both the ultimate load controller and the intermediary will be captured by the regulations **provided they individually meet the 300MW threshold.**

Adjusting or processing could encompass a range of activities:

- Creating a load control signal
- Changing a load control signal
- Controlling the timing of sending the load control signal for the purpose of effecting load control.

The definition of load control in the CSRB, alongside the categories of ESAs in scope (see section 3.2 below), means that:

Load controllers who manage load control on relevant ESAs are in scope irrespective of the system or software they employ to effect the load control adjustment. For example, if load is controlled on an ESA via a home energy management system (HEMS), we intend for this to fall within scope of the legislative definitions in the same way as if load is controlled directly on an ESA.

Regarding the SSES Load Control Licence to be administered by Ofgem (see section 5 for further information), Government's proposed position is that only load control activity supporting grid operation and balancing (as opposed to device optimisation at the local device level by ESA manufacturers) will be licensable.

Similarly, under the NIS Regulations it is our intention that **ESA manufacturers will only be in scope where they are actively engaging in load control for the purpose of grid operation and balancing**. ESA manufacturers that embed load control functionality into an ESA purely for local device optimisation using another piece of hardware physically attached to the ESA, and/or software remotely connected across the internet such as a cloud platform will not be in

[10] Clause 6 of the Cyber Security and Resilience Bill
[11] See section 238 of the Energy Act 2023 for full definitions.

scope. Nevertheless, load control platforms that are provided by the manufacturer may be a critical part of the essential service for the ultimate load controller, and load controllers will be expected to manage their supply chains in accordance with CAF outcomes.

Neither the SSES Load Control Licence, nor the NIS regulatory regime will capture ESA manufacturers who are not explicitly authorised or have an active role in managing load. Organisations managing or sending signals other than load control signals to ESAs, such as manufacturers sending firmware updates to ESAs, signals to protect the device from safety malfunctions, or data platforms sending time-of-use-tariff, weather or carbon intensity data, without also configuring the load control response of the ESA in relation to that data, will be out of scope of SSES licence and NIS requirements.

Neither the SSES licence nor the NIS Regulations are intended to capture passive intermediaries. Passive intermediaries might have networks and systems that load control signals pass through (for example telecoms networks), but they are either unable to adjust or process or change the load control signals, or they are not authorised to do so (in other words they are not responsible for managing load on behalf of the load controller).

The Cyber Security Resilience Bill includes provisions to bring relevant managed service providers into scope of the NIS Regulations where certain criteria are met[12]. We recognise that load controllers may use third-party providers for their load control platforms, some of which may meet the criteria in the Bill for relevant managed service providers. In some cases, these providers may support the operation of load control systems, including creation, modification or transmission of load control signals.

We are therefore seeking further evidence to understand how these roles interact in practice from any organisations who think they fall within both the load control and managed service provider definitions for the same service. We welcome views from organisations that consider this may apply to them (see section 1.2, question 7)

It is important to note that the CSRB will bring in other changes, including changes to incident reporting requirements and enabling regulators to designate critical suppliers to organisations regulated under NIS. The competent authority will update guidance for all operators to ensure clarity on any changes.

For more information on the potential changes to the NIS Regulations click here.

1.2 Threshold and Relevant ESAs

The 300MW threshold, developed in consultation with the National Energy System Operator (NESO), defines the point at which DESNZ considers a load controller to be providing an essential service. This is due to the potential for grid impacts should a load controller of this

[12] See Clause 9, Cyber Security and Resilience (Network and Information Systems) Bill for full definition.

size be compromised or manipulated when the grid is already in a vulnerable state. To summarise:

- Any load controller managing an aggregated potential load of 300 MW or more, in relation to the relevant ESAs, and in any setting, will be designated as an OES under the NIS Regulations[13]. Any load controller managing an aggregated potential load of less than 300 MW in domestic and small-scale commercial settings, in relation to the relevant ESAs, will be licensed by Ofgem under the SSES Load Control Licence, and subject to the obligations as outlined in Condition 9 of the Standard Conditions of the Load Control Licence.

As outlined in clause 6 of the Cyber Security and Resilience Bill, the threshold for determining whether an organisation falls within scope of the load control essential service will be calculated based on the **combined maximum electrical capacity**[14] all relevant ESAs are capable of achieving under its control. This ensures that the measure reflects the potential impact on the electricity system rather than average usage or operational output. We recognise that for some organisations, the maximum electrical capacity of devices in their portfolio will be higher than the amount of load that is technically controlled in practice. However, we propose that using combined maximum electrical capacity provides a uniform way to calculate aggregated load across every organisation in scope. See Annex C section 2 for further details.

Load controllers must therefore use the following criteria to determine their total managed electrical control for the purposes of threshold monitoring:

- **Inclusion of all controllable ESAs**: Aggregated load is defined as the sum of the maximum potential load, or nameplate capacity, of all relevant ESAs currently registered to or managed by the load controller.
- **Peak potential load**: The calculation must be based on the peak load that the load controller has the technical capability to influence or control at any given time, regardless of whether that control is exercised routinely for commercial, technical, or emergency purposes.
- **Geographic Scope:** Only those assets and appliances located within the Great Britain (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 that the NIS Regulations apply across the United Kingdom[15].
- **Continuous Monitoring**: Load controllers have an ongoing duty to monitor their aggregated load and are responsible for notifying the Competent Authority if they meet the 300MW threshold.

For the purpose of load control under the NIS Regulations, we propose to build on definitions of ESAs contained within the Energy Act 2023[16] (below). These were recently consulted on as

[13] Those managing over 300MW of load to domestic and small scale non-domestic ESAs will also be required to obtain a SSES Load Control Licence from Ofgem, but cyber requirements will stem from the NIS Regulations.
[14] The calculation should use the maximum rated electrical capacity of each ESA as stated by the manufacturer.
[15] The Department of Finance is the Competent Authority for the NIS Regulations in Northern Ireland.
[16] Section 238 of the Energy Act 2023

part of the Smart Secure Electricity Systems ESA Phase 1 Regulations consultation. However, we will make some additions to the list of relevant ESAs to reflect the broader application of NIS to load control in industrial and commercial settings. The legal definitions of the additional relevant ESAs for load controllers under NIS will be updated in due course.

Section 238 Energy Act 2023:

(2)"Energy smart appliance" means an appliance which is capable of adjusting the immediate or future flow of electricity into or out of itself or another appliance in response to a load control signal; and includes any software or other systems which enable or facilitate the adjustment to be made in response to the signal.

(4)"Load control signal" means a digital communication sent via a relevant electronic communications network to an energy smart appliance for the purpose of causing or otherwise facilitating such an adjustment.

Our intention is to include the following categories of appliance in scope for load control under NIS[17]:

- Electric Vehicles (EVs)
- EV charge points, both public and private
- Electrical heating appliances
- Battery energy storage systems, both domestic and grid scale
- Virtual power plants used to aggregate load.

Where there are existing legal definitions for energy smart appliances (such as the proposed Energy Smart Appliance Regulations) we will seek to align. This applies to EVs, domestic and public EV chargepoints, and electrical heating appliances. We will develop new definitions to cover virtual power plants and a definition for BESS that encompasses grid scale battery storage. Proposals for these definitions are below:

A smart BESS is a device that:

- Has a battery pack – this refers to a set of rechargeable battery cells that are encapsulated within an outer casing to form a complete unit

A virtual power plant is:

- A software-based network that aggregates decentralised energy resources (DER) to operate as a single, coordinated power plant or load, aggregating the management of assets that are individually too small for utility scale use.

[17] See Smart Secure Electricity Systems Programme: Energy Smart Appliances.

The proposed measures will capture load control of the above 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. For example, a charge point operator controlling more than 6,000 public charge points rated at 50 kW each would exceed the threshold and fall within scope of NIS. We also recognise some organisations will be managing load to the relevant ESAs at under 300MW in aggregate in domestic and small-scale commercial settings, and will be in scope of Ofgem licensing. Further work being led by the Office for Zero Emission Vehicles will scope the need for regulating public chargepoint operators managing under 300MW.

Consultation Questions

1. **What are your views on the intended list of relevant energy smart appliances for large load controllers under the NIS Regulations? Please provide any suggested changes, and why.**
2. **Are the accompanying draft definitions for virtual power plants and BESS clear and applicable? If not, please provide a rationale and suggested amendments if possible.**
3. **If you are a load controller, do you envisage any challenges with identifying relevant energy smart appliances in your portfolio?**
4. **If you are a load controller, do you envisage any challenges in calculating the maximum nameplate capacity of the energy smart appliances in your portfolio?**
5. **Are there any technical limitations that would prevent you from controlling the maximum nameplate capacity of all the relevant energy smart appliances in your portfolio (in other words, your total aggregate capacity)? If so, please provide details.**
6. **Do you envisage any challenges in applying the active and passive intermediary criteria referenced above?**
7. **Do you consider your organisation to fall within both the definition of a Managed Service Provider (MSP) and a Large Load Controller (LLC)? If so, please provide details on how your organisation meets both definitions, and any challenges or areas of uncertainty this creates in understanding your regulatory obligations.**

1.3 Assurance and Compliance

Assurance Approach under NIS

The NIS Regulations aim to improve the security and resilience of essential services against cyber threats. However, they do not prescribe specific technical measures for OES. This flexibility is intentional, allowing organisations to adopt security practices that are proportionate to their size, complexity, and risk exposure.

To support this approach, the NCSC developed the CAF. The CAF provides a structured method for assessing how well OES meet their security duties under the NIS Regulations. Focusing on outcomes rather than prescriptive controls has the following advantages:

- Flexibility for innovation: The energy market is evolving rapidly, with new technologies and business models emerging. Prescriptive rules could stifle innovation and create unnecessary burdens.
- Proportionate regulation: Organisations can tailor their security measures to their operational context and risk profile, rather than adopting a one-size-fits-all solution.
- Future-proofing: Cyber threats evolve quickly. An outcome-based framework allows adaptation without constant regulatory overhaul.

Government is of the view that this is the most appropriate method for regulating a nascent and dynamic sector while maintaining resilience and security.

What is the Cyber Assessment Framework (CAF)?

The CAF provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible. It is built around 14 principles, grouped into five overarching objectives:

- Objective A: Managing Security Risk: Governance, risk management, and supply chain security.
- Objective B: Protecting Against Cyber Attack: Protective technology, identity and access control, and data security.
- Objective C: Detecting Cyber Security Events: Monitoring and detection capabilities.
- Objective D: Minimising Impact of Incidents: Response and recovery planning.
- Objective E: Protecting against non-cyber risks: Physical security and resilience.

Each principle describes an outcome that OES should achieve, rather than prescribing how to achieve it. Each principle is accompanied by a set of Indicators of Good Practice (IGPs), which provide further examples of steps industry can take to demonstrate compliance with the principle. To measure progress, the CAF uses attainment levels that indicate the maturity of an organisation's security posture based on a RAG rating from not achieved, partially achieved to achieved.

Government recognises the challenges in achieving every element of the profile. In order to take a proportionate approach, the Competent Authority sets a CAF profile with attainment levels for each outcome that reflects security expectations for the specific sector. This can take into account a variety of factors, such as risk, proportionality, feasibility and cost. OES remain responsible for assessing the risk to their essential service and implementing mitigations that are appropriate and proportionate to those risks The CAF profiles set by the Competent Authority are used to assess security and resilience, but do not constitute a compliance standard. The Competent Authority may take enforcement action where measures

implemented are not deemed to be appropriate and proportionate, including where these fall beyond the scope of the CAF profile.

You can find further general information about the Cyber Assessment Framework here: Cyber Assessment Framework - NCSC.GOV.UK

See Section 4 for more information on the Tier 1 Load Control CAF Profile.

Compliance and Monitoring

Compliance and monitoring will be conducted by Ofgem in its role as joint competent authority. OES will be expected to submit annual assessments to Ofgem, including but not limited to risk assessments, self-assessments of their organisational security against the Tier 1 CAF Profile and remediation plans to demonstrate how they intend to demonstrate compliance with any outstanding CAF requirements. Ofgem will also be responsible for taking compliance and enforcement action in line with Ofgem's usual approach as set out in NIS Guidance.

Enforcement Timeline

OES will be expected to comply with the NIS Regulations from the date of designation. However, we propose to introduce an appropriate grace period, with Ofgem requiring operators to begin progressing towards the Tier 1 CAF Profile from designation and to achieve full alignment with the profile by the end of 2029.

This phased approach is intended to provide OES with sufficient time to adapt their systems, processes, and organisational practices, while still ensuring timely progress toward the regulatory objectives. It reflects our commitment to balancing resilience with proportionality and recognises the complexity of implementing higher attainment levels for large load control operations.

The Competent Authorities will retain discretion to review and, if necessary, amend this deadline in response to sector-specific challenges or emerging risks.

OES have a legal duty under the NIS Regulations to take appropriate and proportionate measures to mitigate risks to the delivery of the essential service. The Competent Authorities may therefore still choose to take enforcement action where they deem OES are not meeting the core legal requirements of the NIS Regulations. This right applies regardless of the Tier 1 CAF profile compliance deadline of 2029. You can find more information on NIS Enforcement Guidelines, and Penalty Policy, at this reference[18].

Consultation Questions

8. **Operators who are designated under the NIS Regulations for multiple essential services will have to submit separate annual returns to Ofgem for each essential service, including load control.**

[18] NIS Enforcement Guidelines and Penalty Policy 20221669742648165.pdf

a. **How will this reporting requirement impact your organisation?**

b. **Will organisations who expect to be designated under multiple essential services centralise NIS Regulations compliance via a single function?**

1.4 Support to OES

To support organisations that may fall within scope of the new requirements (subject to Royal Assent of the Cyber Security and Resilience Bill), government has developed a suite of draft guidance documents. These resources are designed to clarify expectations from the Competent Authority and assist organisations in preparing for compliance. They represent an initial proposal and are subject to change based on stakeholder feedback and further policy development.

These documents include:

- Annex A: The Tier 1 CAF Profile Document
- Annex B: Load Control CAF Overlay
- Annex C: Scoping Guidance for the Load Control subsector

The following sections of this consultation will set out further detail on these documents and questions designed to gather feedback. Whilst DESNZ are leading on the consultation of these documents, Annex B and C will be iterated and ultimately owned by Ofgem in future.

1.5 Impacts to Business

Introduction

To support consistent and proportionate implementation, a tailored Cyber Assessment Framework (CAF) profile has been developed for large load controllers, accompanied by supporting guidance. Organisations in scope must have regard to this guidance under NIS Regulation 10(4). Though use of the CAF is not mandatory, it is strongly encouraged to ensure alignment with the Competent Authorities' security expectations for OES under the NIS Regulations.

This section assesses the potential impacts on businesses of engaging with the proposed CAF profile and supporting guidance. It focuses on one-off familiarisation costs and sets out how ongoing reporting and compliance costs already captured in DSIT's published impact assessment apply to activities related to the CAF profile.

Impacts on Businesses

The regulatory impacts relevant to large load controllers arise from the decision, implemented through the Cyber Security and Resilience Bill, to bring this subsector into scope of the Network and Information Systems (NIS) Regulations. All enforceable obligations originate from the NIS Regulations.

The CAF profile and guidance serve distinct purposes. The CAF profile provides a structured framework for assessing cyber security arrangements against the outcomes set out under the NIS Regulations. The accompanying guidance supports organisations by clarifying how these existing obligations may be interpreted and applied in practice.

The costs associated with bringing large load controllers into scope of the NIS Regulations have been assessed by DSIT in their published Cyber Security and Resilience (Network and Information Systems) Bill: impact assessment19. Over a 10-year period (in 2025 prices), DSIT estimates the total monetised cost to businesses:

Scenario	Present Value of Total Business Costs over 10 Years in 2025 Prices
Low	£27m
Central	£40m
High	£64m

Table 1 – derived from Table 9.1 (page 96) in IA – total monetised cost – combines one off costs and annual costs over 10-year appraisal period in the form of total present value of the cost in 2025 prices

The figures in table 1 capture both one-off costs – such as familiarisation with the NIS Regulations, physical security upgrades and contract changes – and ongoing costs related to incident reporting, cybersecurity enhancements and annual compliance activities. These are driven by the regulatory requirements rather than the CAF guidance.

The DSIT Impact Assessment estimates that 8 organisations will be in scope in the first year under the low scenario, 11 under the central scenario, and 22 under the high scenario. These estimates are based on internal market analysis undertaken in 2023. Over the appraisal period, the number of large load controllers is expected to increase as the market develops.

This consultation summarises key findings from the DSIT IA and welcomes feedback on how the CAF profile may work in practise and whether it is clear and practical to apply.

[19]https://assets.publishing.service.gov.uk/media/69317f29375aee4a15ee8be9/Cyber_Security_and_Resilience_Bill_-_Impact_Assessment_updated.pdf

Cost Categories Considered in the DSIT IA for Bringing Load Control into Scope of the NIS Regulations (Central Scenarios):

	Central Scenario Cost Figures, 2025 Prices
One-off costs	
Familiarisation costs	£0.012m
Physical security improvements	£1.26m
Contract changes	£0.018m
Ongoing annual costs	
Incident reporting for existing regulated firms	£0.43m
Incident reporting for newly regulated firms	£0.50m
Additional cyber security spending by large load controllers*	£2.00m - £2.32m
Compliance costs reporting requirements* (Annual CAF completion or updating effort falls within the broader "compliance costs" category)	£0.006m

Table 2 – Central scenario figures in 2025 prices (22% overheads applied, except physical security improvements). *For the final two rows, the DSIT IA reports annual costs on a per-organisation basis rather than as aggregate annual totals. The figures shown here are DESNZ-derived central scenario annual estimates, calculated by multiplying the DSIT annual per-organisation cost assumptions by 11 large load controllers, the central first-year estimate. The compliance cost category refers to the broader DSIT compliance/reporting cost category, within which CAF completion or updating may fall. Note – these figures are not expressed in present value terms and are therefore not directly comparable with the PV estimates shown in other tables.

The cost estimates in table 2 are derived from statutory obligations under the NIS Regulations. Only the compliance cost category includes CAF-related activity; all other cost categories relate solely to wider NIS requirements. While the DSIT IA confirms that the broader compliance cost category includes completing the CAF profile, the estimates are not CAF-

specific. As they were produced using a top-down approach, the compliance cost figure also captures a range of wider NIS-related activities. CAF-related activity therefore represents only a subset of the compliance costs estimated in the DSIT Impact Assessment, meaning the estimates overstate impacts attributable solely to the CAF profile and do not include any one-off costs associated with the accompanying guidance.

This assessment therefore attempts to firstly identify any additional one-off costs and secondly specify CAF-related costs within the wider compliance cost category covered by the DSIT Impact Assessment.

CAF-Related Business Impacts

The CAF profile and guidance are expected to result in an ongoing, voluntary administrative effort for businesses: reading the CAF profile and guidance, familiarisation and understanding its structure, and completing the CAF annually as part of internal assurance processes.

We assume that familiarisation costs in the IA cover reading the NIS Regulations, but do not include reviewing the CAF profile or its supporting guidance. Reviewing CAF materials would therefore be an additional familiarisation cost for businesses. DSIT's breakdown indicates that firms typically allocate a small number of professional hours from legal, IT, and technical teams when reviewing guidance documents (e.g. IT/telecommunication input taking around half the time required for legal input). Therefore, DESNZ has produced indicative estimates of the expected voluntary familiarisation and compliance costs associated with the CAF profile and guidance.

One-off familiarisation costs

These estimates reflect the time required for organisations to review and understand the CAF profile and accompanying guidance. Estimates assume input from one legal professional and one IT/telecommunications director, with the IT role spending half the time of the legal role. Costs include a 22% overhead and vary according to assumed reading speed to capture uncertainty around document length, internal review processes, and levels of prior familiarity.

Scenario	Indicative Cost Per Large Load Controller	Assumptions
Low	£1,295	1 legal professional and 1 IT/telecommunications director (50% time), +22% overhead, 100 words per minute reading speed, average number of words per page = 500, 207 pages of CAF profile and guidance.

Central	£1,727	1 legal professional and 1 IT/telecommunications director (50% time), +22% overhead, 75 words per minute reading speed, average number of words per page = 500, 207 pages of CAF profile and guidance.
High	£2,591	1 legal professional and 1 IT/telecommunications director (50% time), +22% overhead, 50 words per minute reading speed, average number of words per page = 500, 207 pages of CAF profile and guidance.

Table 3 – One-off familiarisation costs (per organisation, assumptions-based) using 2025 wages from ONS[20]

Annual voluntary CAF self-assessment costs

Organisations may also choose to undertake an annual CAF self-assessment as part of their internal assurance and governance arrangements. While such activity falls within the broader "compliance costs" category in the DSIT Impact Assessment, the estimates below provide an indicative breakdown of the CAF-specific element but should not be interpreted as introducing new or incremental costs beyond those assessed in the DSIT IA and have only been derived for completeness and transparency.

Scenario	Indicative Cost Per Large Load Controller	Assumptions
Low	£130	Assumed to represent one-quarter of the high-scenario effort
Central	£260	Assumed to represent half of the high-scenario effort
High	£519	DSIT IA compliance cost (cited in table 2 above) used as an anchor; assumed to reflect CAF completion or updating

Table 4 – Annual voluntary CAF self-assessment costs (per organisation)

To provide transparency on the indicative scale of CAF-related activity, DESNZ has estimated the total present value of CAF-related costs over a 10-year appraisal period (Table 5). These

[20] https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/datasets/occupation4digitsoc2010ashetable14

estimates combine one-off familiarisation costs (Table 3) and ongoing voluntary annual CAF self-assessment costs (Table 4), expressed in 2025 prices. Present values are calculated using the HM Treasury Green Book discount rate of 3.5%, with 2025/26 as the base year and 2026/27 treated as year 1 of the appraisal period. The calculations also apply DSIT's assumptions on the expected growth in the number of large load controllers over the appraisal period, so that annual costs reflect the estimated number of organisations in scope in each year.

The present value estimate comprises a one-off familiarisation component incurred in 2026/27, alongside an ongoing self-assessment component assumed to commence in 2027/28 and continue annually over the remainder of the 10-year appraisal period, reflecting the expected implementation timeline of the legislative regime. As outlined above, the annual CAF self-assessment cost is already covered under the DSIT Impact Assessment and is not an additional cost.

Scenario	One-Off Familiarisation Component	Annual voluntary CAF Self-Assessment Component	Total Present Value Of CAF-Related Business Costs Over 10 years In 2025 prices
Low	£0.01m	£0.02m	£0.03m
Central	£0.02m	£0.04m	£0.06m
High	£0.06m	£0.14m	£0.18m

Table 5 – CAF-related total monetised cost: estimated total present value of CAF-related costs over a 10-year appraisal period, combining one-off familiarisation costs and ongoing annual CAF self-assessment costs. Costs are expressed in 2025 prices and discounted at 3.5%, in line with HM Treasury Green Book guidance. Assumed growth for large load controllers. Note – figures may not sum to totals due to rounding.

In addition to the above, organisations may also require resource to build internal capability to meet cyber security outcomes. This is likely to extend beyond CAF familiarisation and returns, reflecting the need to develop or enhance capability to deliver against the required outcomes. However, the scale of this will vary significantly depending on organisational size and existing cyber maturity, and is therefore not quantified at this stage.

Overall Impact Conclusion

Although adherence to the CAF profile is not a legally binding obligation, it is reasonable to expect that large load controllers will adopt it as part of their compliance processes under the NIS Regulations. Their use will therefore involve some additional time and resource costs for businesses.

In line with better regulation guidance, DESNZ has produced indicative estimates of the time and resource use associated with (a) one-off familiarisation with the CAF profile and supporting guidance and (b) annual completion of a CAF self-assessment as part of internal assurance.

Consultation questions

This consultation seeks views on the proposed Tier 1 CAF profile and supporting guidance. Stakeholders are invited to comment on their clarity, proportionality, and practicality for compliance and are invited to respond to the following questions:

9. **Are the costs estimates presented in the consultation accurate based on your organisation's experience?**

10. **If not, where are they different? Where possible, please set out any differences by the following categories:**

    a. **Familiarisation with the CAF profile**

    b. **Familiarisation with the sector-specific guidance**

    c. **Initial assessment**

    d. **Subsequent assessments (if applicable)**

11. **Any other relevant costs (please specify). In particular, have we missed any costs in the areas below, or elsewhere? This may include, but is not limited to:**

    a. **Assurance activities (e.g. independent audit or verification)**

    b. **Scoping activities to identify systems within scope and maintain asset inventories**

    c. **Development and tracking of remediation plans following CAF assessments**

    d. **Additional staffing or specialist resource**

    e. **Training or third-party support required to meet expected outcomes**

2. Tier 1 CAF Profile: Indicative Target Attainment Levels

This section should be read in conjunction with Annex A: Tier 1 Cyber Assessment Framework Profile for Large Load Controllers. Due to its sensitive nature, the Tier 1 CAF profile is not included as an Annex to this document, but will be shared via email. Please contact cyber.policy@energysecurity.gov.uk to receive a copy.

The Tier 1 CAF Profile reflects DESNZ's view of appropriate and proportionate measures to manage risks and minimise the impact of incidents affecting the security of networks and information systems essential to service provision. With a flexible, stepped methodology, DESNZ aims to deliver robust cyber resilience for the load control subsector without constraining innovation or market development.

Your input will help us determine whether these levels are realistic, proportionate, and achievable, and whether they strike the right balance between ensuring robust cyber resilience and enabling practical, cost-effective implementation.

The Tier 1 CAF Profile document sets out the following:

- Development methodology
- Regulatory Interaction and Dual Applicability
- Understanding the profile
- Outcome levels

It is essential that these requirements support secure innovation and market development, and help load controllers scale up in a resilient way, rather than create unnecessary barriers. Setting the right profile and attainment levels supports the following aims:

- Enabling proportionate improvements to the resilience of essential services, ensuring security measures are practical and risk-based.
- Reducing regulatory uncertainty, giving organisations clarity on expectations and enabling effective reporting against progress.
- Assisting organisations in implementing security measures that meet the high-level principles (IGPs) and associated outcomes referenced in the CAF profiles.
- Ensuring achievability and feasibility, ensuring evidential requirements are clear, proportionate, and do not impose unnecessary burdens on emerging business models.

2.1 Development of the Tier 1 CAF Profile

The load control subsector is an emerging market with limited historical case studies of cyber-attacks to inform tailored CAF profiles. It is also an extremely diverse sector, with a large variety of business models and technologies participating in load control activities, and some unique challenges that differ from traditional energy infrastructure. This includes:

- An expanded attack surface: the necessity of integrating a large number of consumer-owned ESAs via the load control platform's Application Programming Interface (APIs) and manufacturer cloud services significantly broadens the attack surface, creating multiple entry points across a complex environment of interdependent systems.

- Vulnerabilities in domestic ESA environments: Inherent vulnerabilities in consumer ESAs, load control platforms, or third-party software components can be exploited to manipulate significant blocks of flexible load.
- Manipulation of [load] control signals: The interception and alteration of [load] control signals to ESAs could lead to incorrect operational responses that could impact grid balance.
- Denial of service (DoS/DDoS) attacks: Attacks targeting Load Control Platforms or communication networks could prevent flexible resources from responding to grid balancing signals, reducing available flexibility during critical periods.
- Exploitation of interdependencies: load control systems depend on various communication networks and IT infrastructure. Vulnerabilities in these underlying systems can be leveraged to disrupt load control operations and, consequently, grid stability.
- Supply chain complexity: The diversity of ESA manufacturers and the use of global supply chains for firmware development introduce the risk of backdoor vulnerabilities or tampered updates being pushed to devices at scale. Widespread use of common platforms amongst large load controllers amplifies this risk.

In recognition of this variety, the risks outlined, and in the absence of real-world examples of cyber attacks on load controllers domestically and internationally, DESNZ has adopted a hybrid approach to developing the proposed Tier 1 CAF profile, as set out below.

Our Methodology

To ensure proportionate mitigation of these risks, DESNZ undertook the following steps:

1. **System Theoretic Process Analysis (STPA):** We began by identifying potential loss scenarios[21] across the subsector, focusing on domestic and small non-domestic consumer led flexibility. These scenarios were assessed at three points in time (2023, 2025 and saturation, i.e. when load control markets reached similar levels to small power stations), and considered attacks ranging from system operators down to individual devices. It is important to note that the STPA primarily focused on domestic-scale ESAs.
2. **Risk and Threat Assessment:** Each scenario was scored for impact and threat and combined to determine overall inherent risk. Based on this analysis, we identified mitigation measures to address the majority of the risks. This ensured prioritisation aligned with sector realities.
3. **Mapping to CAF Principles**: The identified mitigation controls were mapped to NCSC's CAF high-level principles (IGPs). This mapping determined the most appropriate maturity levels for each principle. In some areas, attainment levels were adjusted to ensure expectations were realistic and proportionate for different organisational contexts.

[21] Situations that could lead to an unacceptable loss.

After developing the initial Tier 1 CAF profile, we tested it with industry stakeholders via a survey and engagement sessions, enabling us to gather feedback on the impact of each contributing outcome (CO) across factors such as time, process, cost, resources, and tools.

We recognise that organisations engaging in load control operate under a wide range of business models, spanning both industrial and commercial contexts. This diversity introduces specific cybersecurity challenges, particularly around securing operational technology[22] environments, which differ significantly from traditional IT systems. These challenges include legacy systems, limited patching options, and the need to maintain operational continuity while implementing security measures.

In light of this, we believe a more balanced and pragmatic approach to CAF attainment is needed for the load control sector, to account for varying business models and technologies. **We have therefore proposed reduced attainment levels in the original Tier 1 profile in some areas**, to align some COs with the CAF Enhanced Profile that exists for the rest of the electricity and downstream gas subsectors. We believe the iterated profile reflects sector-specific complexities and ensures expectations are achievable without compromising operational resilience. We welcome views on how best to achieve this balance and invite stakeholders to share their perspectives on practical solutions.

We recognise that organisations engaging in load control are at varying stages of their cyber maturity journey. Importantly, the Tier 1 CAF Profile is intentionally set at a higher level of attainment than the Tier 2 CAF Profile for organisations managing less than 300MW of load in domestic and small-scale commercial settings. This reflects DESNZ's view that large load controllers have a higher risk profile, due to their potential to impact the grid if compromised. Setting Tier 1 at a higher level provides a clear benchmark for organisations to work towards as part of their cyber maturity journey.

Timeframe for the Tier 1 Profile and Assurance

Following the closure of this consultation, consideration of feedback, and the publication of government's response to this consultation, we are aiming to share a finalised version of the Tier 1 Profile in Autumn 2026. The aim is to align this with the opening window for Ofgem's load control licence applications[23]. This will enable organisations already above the 300MW threshold to begin scaling up their cyber maturity if needed, ahead of NIS coming into force. We will also share the profile with organisations meeting the 300MW threshold (or on a journey to meet it) who do not need a load control licence.

Royal Assent is subject to Parliamentary passage and timetabling. We expect this to happen in early 2027. Once the Bill becomes an Act, secondary legislation, guidance, and other products will be required to operationalise and implement the new stronger framework. We expect the regime to be fully in force, with the additional products, in 2028 at the earliest.

[22] Hardware and software that interacts with the physical world to monitor and control industrial operations, processes and equipment, such as Industrial Control Systems.
[23] The application window will be open for 12 months, following which a licence for load control in the domestic and small scale industrial settings will be mandatory for operation.

We recognise organisations will need time to familiarise themselves with new requirements and build capability. We therefore propose a grace period prior to formal assurance of the new regime. We propose the end of 2029 as an appropriate timeframe for large load controllers to meet the profile outcomes, with formal assurance beginning from 2030.

Consultation Questions

12. **Does the tailored Tier 1 CAF Profile reflect an appropriate and proportionate response to the cyber risks posed by large load controllers? Please explain your response.**

13. **Are there any challenges you foresee in implementing the Tier 1 CAF Profile within your organisation, taking the guidance drafts into account? Please outline any challenges in relation to:**

    a. **Technology and operational delivery**

    b. **Integration with existing processes, or organisational structures**

    c. **Any other practical or implementation challenges**

14. **What are your views on the proposed date of end of 2029 for designated load controllers to meet Tier 1 CAF Profile requirements? If applicable, please provide details of any expected challenges for your organisation in meeting this deadline.**

3. Load Control CAF Overlay

This section should be read in conjunction with the Annex B: Load Control CAF Overlay

Ofgem developed the NIS Supplementary Guidance and CAF Overlay for the Downstream Gas and Electricity (DGE) Sector in 2023[24]. The document provides DGE sector-specific guidance to OES which will assist them to achieve and demonstrate the security outcomes in the NCSC's CAF. Effective use of the CAF, and the DGE supplementary guidance, aims to assist OES in meeting their security duties as set out at Regulation 10 of the NIS Regulations.

The CAF Overlay is used to provide sector-specific interpretations of the CAF contributing outcomes and IGPs. The aim is to better clarify their intended application within the DGE sector and help OES to better understand how they might demonstrate their attainment. The information provided in Ofgem's interpretations detail indicative actions and behaviours that illustrate or exemplify achievement of a contributing outcome. The interpretations are provided on a non-binding basis with the intention of guiding OES toward achieving and demonstrating attainment of the security outcomes.

[24] NIS Supplementary Guidance and CAF Overlay for DGE Sector

As part of this consultation we are sharing a Load Control specific CAF Overlay. This is very similar to the existing CAF Overlay for DGE, with some distinctions where needed to ensure it is applicable to the load control ecosystem. It also introduces a number of new IGPs where relevant to support new COs or attainment levels in line with CAF 4.0[25].

Consultation Questions

15. **What are your views on the usability of the CAF Overlay document for understanding the load control CAF profiles?**

16. **If your organisation has been designated under NIS Regulations for Downstream Gas and Electricity, and may also be designated as an OES for the purposes of load control, what are you views on the following approaches to CAF overlay guidance? Which option would you prefer, and why?**

    a. **Separate CAF overlay documents specific to the current Downstream Gas and Electricity sector and the new load control sub sector.**

    b. **A singular, sector-agnostic CAF overlay calling out specific areas of guidance pertinent to the relevant subsector?**

    c. **Other, please provide details of any potential alternatives.**

17. **Are there any interpretations provided in the overlay which require additional information or which you disagree with?**

18. **Is there anything that could be added as part of this overlay which would be helpful in better understanding the load control CAF profiles?**

4. DESNZ Scoping Guidance for the Load Control subsector

This section should be read in conjunction with the Annex B: Draft DESNZ Scoping Guidance for the Load Control Subsector.

4.1 Scope

Scoping is the process of identifying the specific network and information systems, data, software, hardware, infrastructure, technologies, facilities/locations/sites, organisational systems and shared/common platforms that are required for the delivery of load control related services.

[25] CAF 4.0 was developed by the National Cyber Security Centre in 2025. It contains new sections on building a deeper understanding of attacker methods and motivations to inform better cyber risk decisions, ensuring software used in essential services is developed and maintained securely, updates to the section on security monitoring and threat hunting to improve the detection of cyber threats, and finally, there is improved coverage of AI-related cyber risks throughout the CAF.

A clear scope is necessary for two primary reasons. Firstly, it ensures that the "appropriate and proportionate" security measures required by the Load Control Licence and the NIS Regulations are applied to the correct technical estate. Secondly, the measurement of aggregated load within that scope determines whether a Load Control Organisation is subject to the baseline requirements of Tier 2 or the enhanced statutory duties of Tier 1.

This proposed guidance aims to provide clarity on how organisations should determine which systems could fall within scope and are therefore subject to regulatory requirements under the NIS Regulations. It sets out information covering the following topics:

- Load measurement
- Capturing load control scope, including blueprints of different load control settings
- Scope considerations for load control licensees/load controllers in scope of the NIS Regulations
- Scope viewpoints

Ultimately, it is the responsibility of each OES to identify the network and information systems used for the provision of their essential service. For organisations already designated as an OES within the Downstream Gas and Electricity sector, the load control service may share common services already utilised as part of existing essential services. In such cases, load controllers must ensure that the interdependencies between load control systems and other essential energy functions, also subject to OES and NIS are clearly mapped and secured.

For load controllers that have not previously been regulated for cyber security, the challenge often involves defining for the first time the network and information systems, data, software, hardware, infrastructure, technologies, facilities/locations/sites, organisational systems and shared/common platforms that comprise the essential service. In these environments, the functional boundary must be drawn to include the core control platforms, the communication infrastructure used to signal appliances, the specific data sets used to trigger load control events, anything used to facilitate the essential service.

The Competent Authority will not prescribe which systems are in scope. However, it may request an OES to share:

- The list of systems it considers in scope.
- The process followed to identify these systems.

The Competent Authority may raise questions if it believes critical systems have been omitted or if areas appear incomplete. This ensures that all systems essential to service provision are appropriately considered.

Consultation Questions

19. What are your views on the proposed Scoping Guidance? Does it provide sufficient information to determine which network and information systems should be considered within scope of the CAF profile?

20. **What are your views on how the load control ecosystem is represented in the proposed Scoping Guidance? Please provide any comments on the accuracy of definitions or descriptions, and any suggestions for improvement based on your experience.**

21. **If your organisation may transition from the load control licensing regime to the NIS regime (from Tier 2 to Tier 1 of the Cyber Assessment Framework) does the proposed Scoping Guidance provide adequate support for this transition? If not, please explain why and highlight any areas where further guidance or clarification would be helpful.**

22. **What specific technologies or protocols would you expect to be present in network architecture for load control through the following Energy Smart Appliances:**

    a. **Industrial Battery Energy Storage Systems**

    b. **Domestic Battery Energy Storage Systems**

    c. **Virtual Power Plants**

    d. **Heating appliances?**

    e. **Electric Vehicles**

    f. **Electric Vehicles Charges**

5. DESNZ Load Control Policy: Licence vs NIS

5.1 The Smart Secure Electricity Systems Programme

Ensuring the cyber resilience of load controllers forms part of a wider programme called Smart Secure Electricity Systems, designed to create the technical and regulatory frameworks to enable the untapped flexibility from domestic-scale ESAs such as domestic electric vehicle chargepoints. A number of consultations have been published providing additional details on different elements of this programme. These can be summarised as follows:

Consultation	Summary	Large Load Controller references

Delivering a smart and secure electricity system: the interoperability and cyber security of energy smart appliances and remote load control (2022)	Proposals for minimum standards for ESAs and remote load control to ensure interoperability, cybersecurity, and consumer protection. It proposed a licensing regime for organisations that control electrical load remotely, with stricter requirements for large load controllers.	Sets out the policy intention that organisations remotely controlling more than 300 MW aggregate load must comply with Network and Information Systems (NIS) Regulations and the National Cyber Security Centre (NCSC) Cyber Assessment Framework, recognising their critical system impact.
Delivering a smart and secure electricity system: implementation (2024)	The consultation sought feedback on proposed regulations for ESAs, a licensing regime for organisations controlling electrical load, consumer protections, and time-of-use tariff data interoperability.	Builds on 2022 proposals. Confirms licensing for load controllers including those above 300MW. Proposal stands that large load controllers remain subject to NIS/CAF while licensing regime develops.
Smart Secure Electricity Systems Programme (SSES): enduring governance (2025)	Proposal for a long-term governance framework to oversee technical and cybersecurity standards for smart energy technologies like EV chargers and heat pumps. Proposed nominating Elexon as responsible for governance through changes to the Balancing and Settlement Code, establishing two new subcommittees (Technical and Security Governance Groups), and setting cost-recovery arrangements.	Not specific to LLCs. Focuses on governance structure for standards and security oversight for organisations managing below 300MW.

Smart Secure Electricity Systems (SSES) Programme: draft load control licence regulations and conditions (2025-26)	Proposals for new licensing framework under the Electricity Act 1989 to regulate domestic-scale ESAs. It outlined licensable activities and defined offences for unlicensed load control, introduced a 12-month transition period before licence obligations take effect, and set out standard licence conditions, including cybersecurity measures, and consumer protection for flexibility service providers.	Reference to obligations relevant for LLCs in scope of licensing regime, related to consumer protection, cybersecurity, operational/financial resilience, and code compliance.

5.2 Distinctions between NIS and Licensing

We recognise that stakeholders will need clarity on how the proposed SSES Programme Load Control Licence, to be administrated by Ofgem differs from the intended provisions for load control under the NIS Regulations. This section sets out the key distinctions in scope, compliance obligations, and enforcement mechanisms to help stakeholders understand the implications of each approach.

As set out within the Smart Secure Electricity Systems (SSES) Programme: draft load control licence regulations and conditions consultation, the SSES Load Control Licence introduces a formal, proactive regulatory framework for organisations controlling load on relevant ESAs. It applies to two categories of activity:

- Load controllers controlling load on relevant ESAs
- Consumer-facing FSPs contracting with consumers to provide load control[26].

The scope of the SSES Load Control Licence is focussed on organisations interacting with domestic and small non-domestic consumers and relevant domestic-scale ESAs[27]. All organisations performing licensable activities within scope must apply for a load control license[28].

Licence conditions include cyber security requirements based on a tailored CAF profile known as Tier 2 Consumer-Led Flexibility CAF profile for organisations managing less than 300MW. This profile contains the same outcomes as the Tier 1 CAF profile, but attainment levels are

[26] Exact definitions for these activities are subject to DESNZ' consultation response, which will be published later in 2026.
[27] The licence framework includes certain exclusions and scope limitations, as set out in the draft load control licence regulations and associated consultation documents.
[28] https://www.ofgem.gov.uk/consultation/smart-secure-electricity-systems-implementing-load-control-licensing-regime

broadly lower to ensure the profile is feasible and proportionate to organisations managing less load. Consumer protection requirements for FSPs include fair treatment, clear contract terms, and access to complaints and alternative dispute resolution. Technical obligations for load controllers include compliance with industry codes and measures to maintain grid stability.

Under the SSES Load Control Licence, Elexon will play a key role in supporting cyber assurance and technical governance. Load controllers requiring a licence who are not designated as OES under NIS will need to accede to the Balancing and Settlement Code (BSC), enabling Elexon's Security Governance Group to review compliance evidence and provide recommendations to Ofgem. This industry-led governance model ensures that cyber security standards remain robust and adaptable as the market evolves.

Enforcement will be administered by Ofgem, which will have powers to issue enforcement orders, financial penalties, and revoke licences where necessary. The objective of this approach is to provide predictable, proportionate regulation that builds consumer trust, supports innovation, and mitigates systemic risks.

Table 3

The below table sets out a high level view of differences between the SSES Load Control Licence and the NIS Regulations.

Feature	SSES Load Control Licence Licensing Approach	Load Control under NIS Regulations
Regulatory Basis	Licence under Electricity Act 1989	Statutory designation under NIS Regulations
Scope	Load control of domestic-scale and small non domestic ESAs and consumer-facing services	Capacity-based (≥300 MW) from relevant ESAs in any setting, including industrial and commercial
Assurance	Tier 2 CLF CAF Profile and third party audits	Tier 1 CLF CAF Profile and third party audits.
Enforcement	Ofgem licence enforcement (penalties, revocation)	Competent Authority enforcement under NIS (including penalties)[29]

[29] Operators designated as OES for load control that also hold a load control licence may be subject to licence revocation where they fail to comply with a NIS Enforcement Notice or Penalty.

5.3 Navigating NIS and Licensing

Subject to the Cyber Security and Resilience Bill receiving Royal Assent and implemented via the necessary secondary legislation, the NIS Regulations will be updated to introduce Load Control as a new essential service, introducing obligations on operators.

Load controllers with an aggregate load of 300MW or above from specified relevant ESAs will have three months to notify DESNZ that they meet the threshold to be deemed designated. In addition, load controllers operating ESAs within the domestic and small non-domestic market must apply for a Load Control licence from Ofgem, regardless of whether they meet the 300 MW threshold (See the SSES License consultation and Ofgem consultation for more information).

Once an organisation is designated as an OES for the essential service of load control, it will report to DESNZ for onboarding under the NIS regulatory regime, as set out in section 8(2) of the Regulations. At this point, the entity will no longer be required to comply with the cybersecurity requirements set out under the Load Control licence. Instead, it must adhere to the cybersecurity obligations defined in the NIS Regulations. For example, reporting requirements will transition to DESNZ and Ofgem rather than the Security Governance Group.

However, all other licence requirements, such as management and financial controls, will continue to apply, regardless of whether the load controller is designated as an OES.

If the situation occurs at any point, where an OES applies to have their designation revoked under NIS, for example if an operator downsizes its assets and can provide proof that the 300MW threshold is no longer met, it will revert to complying with the cybersecurity requirements under the load control license, if in scope, for example managing domestic ESAs.

Tiered Regulatory Obligations

Licensees managing an aggregated load of less than 300MW in domestic and small scale non-domestic settings will follow the Tier 2 regulatory path. This recognises that while these organisations do not yet pose an immediate systemic risk to the national grid, they remain integral to the security of the wider energy ecosystem. For these organisations, Licence Condition 9 provides the formal basis for the application of the Load Control Tier 2 Profile (Under 300 MW) CAF profile, which is designed to establish a consistent and robust security baseline across the sector.

The primary focus for Tier 2 is on ensuring that licensees implement appropriate and proportionate measures to protect their systems from exploitation. Furthermore, the Tier 2 profile serves as an essential foundation for a licensee's security maturity journey. These baseline requirements are designed to align with the structural expectations of Tier 1, ensuring that as an organisation's portfolio grows, its security framework remains scalable and robust. This approach ensures that, should a licensee reach the 300 MW threshold, the transition to Tier 1 status is an evolution of an existing, mature security framework rather than an isolated compliance event.

Load controllers managing an aggregated load of 300 MW or more will be designated as OES and will be subject to the Tier 1 CAF Profile. Instead of meeting cyber requirements in the licence, organisations must fulfil the statutory duties set out in NIS Regulations 10(1) and 10(2) (as well as other requirements and obligations contained within the NIS Regulations). Crucially, NIS Regulations 10(1) and 10(2) establish the fundamental requirements for the security of network and information systems. Regulation 10(1) mandates that an OES must take appropriate and proportionate technical and organisational measures to manage risks, while Regulation 10(2) requires measures to prevent and minimise the impact of incidents.

Regulation 10(3) further requires OES to have regard to guidance issued by the Competent Authority when fulfilling these duties. This includes the Cyber Assessment Framework and associated sector-specific guidance, which provide a structured means for organisations to interpret and demonstrate how they are meeting their obligations under the NIS Regulations.

While the CAF profile provides a structured baseline for demonstrating compliance, the statutory duty under NIS 10(1) and 10(2) requires OES to assess the specific threats and risks inherent to their unique operating environment. Consequently, an organisation must implement measures that are appropriate for the specific threats they face, which may require going above and beyond the baseline settings of the CAF profile.

Transition between tiers

We recognise for some organisations there may be challenges around navigating the two regimes. We also recognise that some organisations may periodically move above or below defined criteria due to operational changes, market conditions, or service demand.

DESNZ will develop a policy guidance document with an overview of DESNZ load control related policy. This will seek to cover load controllers in scope of Ofgem's load control licence (domestic and small scale non domestic settings, below 300MW) and those in scope of the NIS Regulations (above 300MW in any setting), as well as any challenges related to transitioning between tiers.

Consultation Questions

23. **Do you understand the distinctions between NIS Regulations and the licensing regime? If not, please specify which aspects are unclear.**

24. **Are there any particular areas we should cover in policy guidance to support organisations in navigating the two regimes?**

Consultation questions

1.2 Thresholds and Relevant ESAs

1. What are your views on the intended list of relevant energy smart appliances for large load controllers under the NIS Regulations? Please provide any suggested changes, and why.

2. Are the accompanying draft definitions for virtual power plants and BESS clear and applicable? If not, please provide a rationale and suggested amendments if possible.

3. If you are a load controller, do you envisage any challenges with identifying relevant energy smart appliances in your portfolio?

4. If you are a load controller, do you envisage any challenges in calculating the maximum nameplate capacity of the energy smart appliances in your portfolio?

5. Are there any technical limitations that would prevent you from controlling the maximum nameplate capacity of all the relevant energy smart appliances in your portfolio (in other words, your total aggregate capacity)? If so, please provide details.

6. Do you envisage any challenges in applying the active and passive intermediary criteria referenced above?

7. Do you consider your organisation to fall within both the definition of a Managed Service Provider (MSP) and a Large Load Controller (LLC)? If so, please provide details on how your organisation meets both definitions, and any challenges or areas of uncertainty this creates in understanding your regulatory obligations.

1.3 Assurance and Compliance

8. Operators who are designated under the NIS Regulations for multiple essential services will have to submit separate annual returns to Ofgem for each essential service, including load control.

a. How will this reporting requirement impact your organisation?

b. Will organisations who expect to be designated under multiple essential services centralise NIS Regulations compliance via a single function?

1.5 Business Impacts

9. Are the costs estimates presented in the consultation accurate based on your organisation’s experience?

10. If not, where are they different? Where possible, please set out any differences by the following categories:

a. Familiarisation with the CAF profile

b. Familiarisation with the sector-specific guidance

c. Initial assessment

d. Subsequent assessments (if applicable)

11. Any other relevant costs (please specify). In particular, have we missed any costs in the areas below, or elsewhere? This may include, but is not limited to:

a. Assurance activities (e.g. independent audit or verification)

b. Scoping activities to identify systems within scope and maintain asset inventories

c. Development and tracking of remediation plans following CAF assessments

d. Additional staffing or specialist resource

e. Training or third-party support required to meet expected outcomes

2.1 Development of the Tier 1 CAF Profile

12. Does the tailored Tier 1 CAF Profile reflect an appropriate and proportionate response to the cyber risks posed by large load controllers? Please explain your response.

13. Are there any challenges you foresee in implementing the Tier 1 CAF Profile within your organisation, taking the guidance drafts into account? Please outline any challenges in relation to:

a. Technology and operational delivery

b. Integration with existing processes, or organisational structures

c. Any other practical or implementation challenges

14. What are your views on the proposed date of end of 2029 for designated load controllers to meet Tier 1 CAF Profile requirements? If applicable, please provide details of any expected challenges for your organisation in meeting this deadline.

3. Load Control CAF Overlay

15. What are your views on the usability of the CAF Overlay document for understanding the load control CAF profiles?

16. If your organisation has been designated under NIS Regulations for Downstream Gas and Electricity, and may also be designated as an OES for the purposes of load control, what are you views on the following approaches to CAF overlay guidance? Which option would you prefer, and why?

a. Separate CAF overlay documents specific to the current Downstream Gas and Electricity sector and the new load control sub sector.

b. A singular, sector-agnostic CAF overlay calling out specific areas of guidance pertinent to the relevant subsector?

c. Other, please provide details of any potential alternatives.

17. Are there any interpretations provided in the overlay which require additional information or which you disagree with?

18. Is there anything that could be added as part of this overlay which would be helpful in better understanding the load control CAF profiles?

4.1 Scope

19. What are your views on the proposed Scoping Guidance? Does it provide sufficient information to determine which network and information systems should be considered within scope of the CAF profile?

20. What are your views on how the load control ecosystem is represented in the proposed Scoping Guidance? Please provide any comments on the accuracy of definitions or descriptions, and any suggestions for improvement based on your experience.

21. If your organisation may transition from the load control licensing regime to the NIS regime (from Tier 2 to Tier 1 of the Cyber Assessment Framework) does the proposed Scoping Guidance provide adequate support for this transition? If not, please explain why and highlight any areas where further guidance or clarification would be helpful.

22. What specific technologies or protocols would you expect to be present in network architecture for load control through the following Energy Smart Appliances :

a. Industrial Battery Energy Storage Systems

b. Domestic Battery Energy Storage Systems

c. Virtual Power Plants

d. Heating appliances?

e. Electric Vehicles

f. Electric Vehicles Charges

5.3 Navigating NIS and Licensing

23. Do you understand the distinctions between NIS Regulations and the licensing regime? If not, please specify which aspects are unclear.

24. Are there any particular areas we should cover in policy guidance to support organisations in navigating the two regimes?

Section 4: Demographic Questions

25. Are you responding as an individual or on behalf of an organisation?

- **a. Individual**
- **b. Organisation**

26. If an individual, what is your interest in this space?

- **a. [include text box here]**

27. If an individual, which of the following statements best describes your role?

- **a. Cyber Security Professional**
- **b. Operations / Engineering**
- **c. Policy / Regulation**
- **d. Legal / Compliance**
- **e. Executive / Senior Leadership**
- **f. Other [include text box]**

28. If an organisation, what is your organisation's name?

- **a. [include text box]**

29. If an organisation, what type of organisation do you represent?

- **a. Load Controller**
- **b. Ofgem Licensee**
- **c. Government**
- **d. Academia**
- **e. Trade Body**
- **f. Developer**

g. **Original Equipment Manufacturers (OEMs) or Distributors**

h. **Other [include open textbox]**

30. **If an organisation, how many people work for your organisation? If unsure, please provide your best estimate.**

a. **Under 10**

b. **10-49**

c. **50-249**

d. **250-499**

e. **Not sure**

31. **If you are a load controller or OEM, please use the following definitions to determine which role(s) apply to your organisation (You can select more than one option)**

a. **Energy Supplier – Flexibility Service Provider: ES – FSPs are either owned by energy suppliers or are energy suppliers that provide both Implicit (consumer-driven, responding to price changes) and Explicit DSR (direct control or request from grid operators or aggregators to manage energy demand).**

b. **Pure Play – Flexibility Service Provider: PP-FSPs are organisations that provide flexibility services which include both Explicit and Implicit flexibility services but are not an energy supplier. They provide flexibility services where the connection to the device is agnostic to the Device Manufacturer. They either connect to assets via an API to the backend of the Device Manufacturer's cloud environment or develop an integrated control unit that connects to devices.**

c. **Technology Platform Providers: TPPs operate consumer devices on behalf of Energy Suppliers. They connect to assets via the backend of the device manufacturer's cloud environments.**

d. **Device Manufacturers FSPs: DM-FSPs are organisations that provide flexibility services which include both Explicit and Implicit DSR but are not an energy supplier. They provide Domestic-scale DSR services for devices that they manufacture and directly operate.**

e. **Device Manufacturers: DMs are organisations that do not provide flexibility services directly but instead manufacture Energy Smart Appliances that support DSR type services to the energy industry and consumers.**

f. **Load Control Aggregators: LCAs are organisations that specialise in managing and controlling energy loads across multiple devices and systems. They provide Explicit DSR services by directly controlling or requesting adjustments to energy consumption from connected devices to balance grid demand. LCAs can work independently or in collaboration with energy suppliers, technology platform providers,**

and device manufacturers to optimise energy usage and enhance grid stability.

g. None of the above apply – Free text box: How would you describe the role of your organisation if the above does not apply.

32. If you are a load controller, which best describes the total aggregate load (combined maximum potential capacity in MW) of all relevant energy smart appliances in your portfolio?

a. Less than 300MW

b. 300MW or more

c. Currently less than 300MW but projected to exceed 300MW by 2030

33. If you are licensed by Ofgem, is your organisation an Operator of Essential Services under the NIS Regulations?

a. Yes

b. No

34. If you hold an electricity generation licence, what types of assets does your organisation manage? [allow ability to select multiple responses]

a. Offshore Wind Generation

b. Onshore Wind Generation

c. Solar Generation

d. Battery Energy Storage Systems (BESS)

e. Long Duration Energy Storage (excluding BESS)

f. Non-renewable Generation

g. Other – please specify [Text box here]

This publication is available from: www.gov.uk/government/consultations/large-load-controllers-tier-1-cyber-assessment-framework-and-associated-guidance

Any enquiries regarding this publication should be sent to us at: cyber.policy@energysecurity.gov.uk

If you need a version of this document in a more accessible format, please email alt.formats@energysecurity.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.