UK Government

Smart Secure Electricity Systems (SSES) Programme

Government response to the 2025 consultation on SSES Enduring Governance

Department for Energy Security and Net Zero (2025)

Contents

Ministerial Foreword

Clean, homegrown power is the way to deliver our country's energy security and to bring down bills for households and businesses. Clean flexibility will be critical in supporting this as set out in our Clean Power 2030 Action Plan[1].

The Clean Flexibility Roadmap[2] published alongside NESO and Ofgem, set out our vision for a clean, flexible, consumer-focused electricity system. This Roadmap reinforced how the country needs an electricity system that is more flexible as we meet the needs of homes and businesses whilst harnessing the intermittent nature of renewable energy. The Roadmap is instrumental in providing a plan for our commitment to meeting our clean power ambitions, as we aim to scale consumer-led flexibility from 2.5GW in 2023 to 10GW to 12GW by 2030.

We know consumer participation is key to unlocking greater flexibility across Britain, leading to benefits to households, businesses and the environment. Increasing consumer-led flexibility will allow consumers to reap the benefits of lower energy bills whilst also ensuring enhanced control over their bills. Consumer-led-flexibility is therefore key to fulfilling our commitment to reduce energy bills.

The Smart Secure Electricity Systems (SSES) Programme is crucial for establishing robust technical and security frameworks for Energy Smart Appliances and load controllers to support this drive towards flexibility. The Enduring Governance arrangements set out in the August 2025 consultation and this Government response will be instrumental in ensuring these frameworks keep pace with evolving technology and the sector as it grows.

This Government response confirms our position to modify the Balancing and Settlement Code enabling Elexon to deliver Technical and Security Governance Groups as part of SSES Enduring Governance. This is key to ensuring industry has a role in maintaining and evolving technical and security frameworks over time. Elexon is already a key player in the energy governance sector, delivering other aligning work such in its role as the Market Facilitator for Flexibility. I expect Elexon to ensure cost effective delivery and strong engagement across the sector including with consumer groups so that governance of SSES technical and security frameworks continues to consider a wide range of stakeholder views.

I would like to thank those who responded to this consultation for their time in engaging with our proposals on Enduring Governance. The publication of this Government response is a key step towards a flourishing consumer-led flexibility sector, minimising bills for consumers, maintaining security of supply and meeting our Clean Energy Superpower Mission.

Michael Shanks MP, Minister for Energy

[1] Clean Power 2030 Action Plan - GOV.UK
[2] Clean flexibility roadmap - GOV.UK

Executive Summary

The Smart Secure Electricity Systems (SSES) Programme is putting in place technical and regulatory requirements for Energy Smart Appliances (ESAs) to ensure interoperability, maintain cyber security and protect grid stability. To ensure that the technical and security requirements for ESAs and load control licensees continue to align with the evolving needs of industry and Government policy objectives, we will establish industry-led governance arrangements. These arrangements will oversee the relevant frameworks and provide recommendations for changes to Government and regulators.

These Enduring Governance arrangements will include the set up and delivery of Technical and Security Governance Groups delivered by Elexon, details of which are set out in this Government response.

We are also working with the Retail Energy Code Company (RECCo) to implement Time-of-use Tariff Data Interoperability which will require energy suppliers to comply with a tariff data specification set out in the Retail Energy Code. This will be part of ongoing governance arrangements for the SSES Programme but is outside of the scope of this consultation and Government response.

Following the consultation[3] on SSES Enduring Governance earlier this year, this document summarises the Government's decisions on each of the questions posed in the consultation and sets out the next steps for putting in place Enduring Governance arrangements for SSES technical and security frameworks.

Strategic Context

As set out in the Clean Power 2030 Action Plan, a significant increase in clean flexibility is critical to reaching Clean Power in 2030. The Clean Flexibility Roadmap published earlier this year is an important milestone in the Government's Clean Energy Superpower Mission. A key element of the Roadmap is setting the pathway for increasing consumer-led flexibility (CLF) which involves the voluntary shifting of electricity use to times when supply is more abundant, cheaper, and cleaner, and away from peak periods.

Transitioning to a clean, flexible electricity system will bring numerous benefits. The energy system will become more cost-effective by utilising low-cost renewable energy. By using flexibility to reduce peak demand and distributing sources of generation, we will require less grid infrastructure, which will help to minimise consumer bills.

To support the development of nascent flexibility markets within the energy sector effectively, SSES Enduring Governance will play a pivotal role in connecting Government, industry and regulators in the maintenance of technical and security frameworks. This will ensure close

[3] Smart Secure Electricity Systems Programme (SSES): enduring governance - GOV.UK

alignment with other CLF components such as Market-wide Half-Hourly Settlement, the Market Facilitator role, and initiatives aimed at boosting consumer confidence.

Given the emerging nature of these markets, it is essential that governance structures are industry-led. This approach enables the agility and responsiveness needed to adapt to market signals and evolving consumer needs. By fostering a dynamic governance environment, we can better unlock consumer benefits, drive cost savings in regard to energy infrastructure development, and deliver in line with Government policy.

Key Policy Decisions and Outcomes

We welcome the 31 responses to this consultation and following the general support for our proposals have decided to:

- modify the Balancing and Settlement Code (BSC) to enable Elexon to deliver the Technical and Security Governance Groups. This modification will be made alongside publication of this Government response and enable Elexon to prepare sufficiently for the Technical and Security Governance Groups becoming operational from mid-2026;
- set up the Technical and Security Governance Groups as Balancing and Settlement Code Panel Subcommittees; and
- implement cost recovery for the transition phase through BSC costs. However, we will keep this under review and reassess the cost recovery mechanism when load controllers become licensed.

We recognise that the implementation of code reform[4] has implications for how the SSES Technical and Security Governance Groups are delivered and for our cost recovery proposals. Ofgem intend to consult on what roles will be part of the code manager business, and this may include the SSES Enduring Governance role. We will continue to work with Ofgem to ensure alignment on delivery going forwards.

Next Steps

Section 245 of the Energy Act 2023 gives the Secretary of State powers to make modifications to industry codes. Alongside the publication of this Government response, a Decision Notice has been issued to Elexon requiring it to implement the BSC code modification as set out in an Annex to this Government response.

The Modification will take effect from 5th December 2025.

Building on the RASCI (Responsible, Accountable, Supportive, Consulted, Informed) Matrix published as part of this Government response, we will continue to work with Ofgem, OPSS, Elexon and other industry stakeholders to ensure a detailed target operating model for SSES Enduring Governance is in place prior to full industry-led arrangements being established. We will work with Elexon to develop the required documents which will sit under the BSC setting

[4] Second consultation on the implementation of the energy code reform

out voting and membership arrangements, responsibilities and functions and change processes for documents in the SSES Governance Framework. These will be based on decisions set out in this Government response.

Once the necessary documents sitting under the BSC are in place, Elexon will then be responsible for managing the nomination and voting process for initial group membership to ensure the Technical and Security Governance Groups can be operational from mid-2026. Anyone will be able to nominate members as long as the person being nominated meets the required criteria and then there will be a subsequent closed vote for those nominated. Voting will be undertaken within each category e.g. load controllers vote for load controller representatives.

Once the Technical and Security Governance Groups are operational, Government will be transitioning functions currently undertaken through the Government-led Technical and Security Working Groups to the industry-led Governance Groups. We recognise that not all members of the existing Technical and Security Working Groups will be members of the industry-led Technical and Security Governance Groups; however, we expect the Technical and Security Governance Groups to set up subgroups to gather input from wider stakeholders as needed. We will keep the Technical and Security Working Groups informed of detailed timelines of when these Government-led groups will be closing.

The timeline below sets out the expected dates for SSES Enduring Governance milestones. It also includes wider activities which may impact the work of the Technical and Security Governance Groups. We will work closely with Ofgem to ensure that we are aligned as much as possible with Code Reform programme timings.

Activity	**Date**
Government response to the 2025 SSES Enduring Governance consultation published.	November 2025
Implement code changes to the BSC using Energy Act Section 245 Powers. This will establish the Technical and Security Governance Groups as BSC Panel subcommittees and give Elexon the responsibility for administering SSES Enduring Governance (this marks the beginning of the transition phase of SSES Enduring Governance).	5th December 2025
Development of documents under the BSC setting out voting, nomination and Technical and Security Governance Groups arrangements. This will include responsibilities of load controllers under the BSC.	Early 2026
Nomination and voting for membership of the Technical and Security Governance Groups.	Spring/Summer 2026

Technical and Security Governance Groups operational.	From mid-2026
Code Manager Licence granted to BSC Code Manager.	2026 (subject to wider Code Reform)
Load Control Licence applications open.	Expected by the end of 2026
Government-led Technical and Security Working Groups close.	Late 2026
Load Control Licence in force requiring licensees to be party to the BSC.	Expected by the end of 2027
First phase ESA regulations in force.	By the end of 2027 at the latest
Second phase ESA regulations in force mandating the companion specification (a document which sets out the specification for ESAs including which open standards and protocols must or must not be implemented). This marks the beginning of the delivery phase of SSES Enduring Governance.	From mid-2029

The above plan is indicative, and subject to Parliamentary approval of legislation, but provides a timeline setting out the key milestones for delivery of Enduring Governance alongside relevant wider milestones.

The Government positions set out in the following chapters provide detail on the key policies describing how Enduring Governance will be delivered through the Technical and Security Governance Groups, administered by Elexon. We remain committed to working with the grain of industry and we will continue to engage stakeholders via a range of working and advisory groups.

Enduring Governance

Section 1 - Governance Body

Overview:

As the SSES Programme enters the transition phase we require an Enduring Governance body to be in place to support the development and ensure the maintenance of technical and security frameworks for ESAs and load controllers. The consultation proposed that Elexon deliver the Technical and Security Governance Groups as part of Enduring Governance arrangements through modifications to the Balancing and Settlement Code (BSC). This proposal followed a structured assessment of potential governance bodies, including NESO, RECCo, and the Smart Energy Code Company (SECCo), with Elexon identified as the most suitable due to its existing roles, stakeholder relationships, and alignment with its other flexibility market responsibilities.

1. Do you agree that the Balancing and Settlement Code administered by Elexon is the most suitable code to house SSES Enduring Governance functions?

Summary of responses

A strong majority of respondents agreed that the BSC administered by Elexon is the most suitable code to house SSES Enduring Governance functions. Of the 29 respondents to this question, 24 agreed, 2 disagreed and 3 were not sure.

Of those who agreed, 7 cited that this was due to the overlap with Elexon's existing roles and SSES Enduring Governance, including the role of the Market Facilitator and Flexibility Market Asset Register.

Although there was overall agreement, several respondents (6) expressed concern at Elexon's capacity to stand up the Technical and Security Governance Groups alongside their other existing delivery responsibilities, including Market-wide Half-Hourly Settlement. Respondents recommended reviewing Elexon's delivery timescales to identify potential overlaps with other deliverables, and to require Elexon to develop contingency plans that mitigate risks to key delivery milestones.

Of those who responded, 7 highlighted the overlap between the SSES Enduring Governance arrangements and other energy governance codes such as the Retail Energy Code (REC) and Smart Energy Code (SEC). Respondents suggested ensuring join up between the SSES Enduring Governance arrangements and the REC and SEC.

Some (3) respondents expressed their agreement with the Technical and Security Governance Groups being able to stand up subgroups citing that this would enable a wider level of expertise to support decision-making.

Government response

Following support for our minded-to position for Elexon to deliver SSES Enduring Governance through modifications to the BSC we have decided to progress with implementing the BSC modification to establish the Technical and Security Governance Groups as BSC Panel subcommittees and give Elexon the responsibility for administering the groups. Elexon's responsibilities will include:

1. **providing secretariat responsibilities** – ensuring Technical and Security Governance Groups are scheduled with an agenda that reflects the functions of each of the groups. This would include administrative responsibilities such as taking notes and actions in the meetings and distributing them to group members or wider stakeholders where appropriate such as to any subgroups;
2. **facilitating stakeholder engagement sessions** – providing a format for industry engagement for all relevant stakeholder groups. This could include: participation by industry representatives in the governance itself; stakeholder engagement exercises such as convening subgroups with wider stakeholder membership; and through the production of guidance documents and other supporting materials for the technical framework;
3. **procurement of services** – there may be instances where the Technical and Security Governance Groups are required to procure services, for example if testing of devices is required. Elexon would be responsible for procurement on behalf of the groups. This includes management of any procured services;
4. **considering implications on the wider flexibility market** – Elexon's other roles will enable them to have an understanding of the implications of decisions of the Technical and Security Governance Groups on the wider flexibility market and vice versa, and to provide this insight to the groups where required through technical and security specialists' engagement with the Technical and Security Governance Groups chairs;
5. **supporting membership arrangements** – facilitating the nomination and voting process for both the chair and the wider Technical and Security Governance Group membership, and ensuring any non-BSC Parties such as manufacturers can take part in this process; and
6. **cost recovery arrangements** – providing a funding mechanism to support the activities of the Technical and Security Governance Groups.

We noted that several responses to the consultation set out concerns around Elexon's ability to deliver SSES Enduring Governance alongside their other responsibilities. As part of the process to develop proposals for this consultation and Government response we have been engaging with Elexon to ensure they are aware of the resources required to deliver the Technical and Security Governance Groups. These costs will be accounted for in Elexon's upcoming budget for financial year 2026/27 enabling any necessary recruitment to be undertaken to fill required roles. In order to ensure timely delivery for 2026 we have also been working with Elexon to plan for the set-up of the Technical and Security Governance Groups. DESNZ will continue to work with Elexon to ensure timely progress against the relevant milestones set out in the timeline included in this Government response.

We recognise that the functions to be delivered by the Technical and Security Governance Groups bear some relation to the activities undertaken under the SEC and REC. We agree with respondents that coordination between Elexon, the relevant SEC subcommittees and RECCo will help build on existing best practice and facilitate the sharing of lessons learnt. This will be particularly important as RECCo progresses work on Time-of-Use Tariff Data Interoperability.

To support join-up between relevant codes we will ensure:

- Elexon engage with SECCo in the set-up phase of SSES Enduring Governance so experience in delivering Technical and Security Groups can be shared;
- Chairs of the Technical and Security Governance Groups have regular meetings and engagement with the chairs of the SEC Governance Groups to enable sharing of expertise and join-up in delivering technical and security governance;
- Chairs of the Technical and Security Governance Groups will be able to invite wider industry specialists to meetings as and when required, which could include participation by individuals from other code bodies;
- Usual cross-code engagement between SECCo, RECCo and Elexon to ensure clarity for effected stakeholders.

In addition, we recognise the rich seam of information and data held by these organisations on market developments. This presents a valuable opportunity for enhanced collaboration with Government and regulators, supporting more informed decision-making and enabling a more agile and responsive governance framework.

Section 2 - Governance Functions

Nomination process for Technical and Security Governance Groups

This section of the consultation set out further detail on the governance model for delivering the Technical and Security Governance Group functions. This followed on from confirmation in our April 2025 SSES Government Response that SSES Enduring Governance would be delivered through two new groups: the Technical Governance Group and the Security Governance Group.

The Technical and Security Governance Groups will include voting members (those who can cast a vote as part of decision making within the groups) from industry and non-voting members (those who will be able to engage in discussion but not cast votes on decisions) from DESNZ, Ofgem, and OPSS[5]. We proposed that there would be a two-year term limit for all members, though members can be voted in for subsequent terms.

[5] This follows precedent for arrangements within other energy governance groups such as the Smart Energy Code.

2. Do you agree with the suggested term limit of two years for the SSES Technical and Security Governance Group members?

Summary of responses

Of those who responded, a majority supported our suggested term limit of two years for membership of the Technical and Security Governance Groups. Of the 29 respondents, 18 agreed, 5 disagreed and 6 were not sure.

Of those who agreed, 4 set out that this approach aligned with governance arrangements in the sector and for future Stakeholder Advisory Forums which will be implemented by Ofgem as part of wider Code Reform.

Many respondents (8) supported the proposal that members could be voted in for consecutive terms, highlighting that this would ensure continuity of expertise. This would enable there to be a mechanism for continuity and knowledge retention in specialist technical and security matters.

Several respondents (5) recommended staggered membership terms to maintain some degree of continuity on the groups. It was suggested that the Enduring Governance arrangements could begin with staggered initial term limits, with some members serving a three-year term and others a two-year term, followed by standard two-year terms thereafter.

Several respondents (5) set out that a three-year term limit for group members would be preferable. Reasons included ensuring that any longer-term activities being undertaken by the groups are not disrupted by membership changes and that the initial transition phase for SSES Enduring Governance is three years.

Government response

Following general support for the proposed two-year term limit for Technical and Security Group members, we can confirm term limits for these groups will be two years.

We noted that some respondents expressed concern around disruption caused by term limits for members all ending in the same year. We will therefore ensure that members' terms end on a staggered basis to retain expertise in the group and prevent all group members being changed in one year. This would mean an initial three-year term for half of the first set of members of the group and a two-year term limit for remaining members. This is in line with Elexon's membership arrangements for the Data Integration Platform Change and Advisory Board and upcoming Stakeholder Advisory Board for the Market Facilitator Role. As set out in the consultation we will ensure that members can be reappointed to the Technical and Security Governance Groups so that those with significant expertise and sector support can maintain membership in the groups.

We plan to set out in a document under the BSC that nomination and voting arrangements of the Technical and Security Governance Groups will be conducted by Elexon. Organisations will not need to accede to the BSC to take part in nomination and voting arrangements. We expect the arrangements to be as follows:

- Open nominations - anyone can nominate an individual to be a member on the Technical or Security Governance Group. There will be clear criteria on eligibility for being nominated. For manufacturer and load controller nominees it will need to be clear to which manufacturer type or load controller type they belong;

- Once Elexon have collated the nominations for group members there will need to be a vote to determine which nominees become members of the Technical or Security Governance Group;

- Closed voting - Elexon will hold an approved-list of who can vote for some categories e.g. manufacturers, load controllers and consumer representatives;

- Groups of eligible affiliated companies under the same parent organisation will be restricted to having one vote;

- Voting will be undertaken within each category e.g. load controllers vote for load controller group members.

Members of the Technical and Security Governance Groups would be required to act independently of their organisation or employer when participating in group discussions and activities. They will be required to provide a letter from their employer stating that they are content for the individual to dedicate the time required to the Technical or Security Governance Group and that they recognise they will be undertaking this role in an independent capacity. This is to ensure individuals are bringing their sector specific knowledge to group discussions whilst not acting for the commercial interest of their employer. These particular considerations and arrangements won't apply to DESNZ, Ofgem, OPSS and NESO members who will represent government and/or their organisations.

SSES Technical Governance Group: overview

This section specifically sought views regarding the documents in the technical framework that the Technical Governance Group should manage. These included:

- A regulated document: The Interoperable GB Consumer-led Flexibility Companion Specification - setting out which requirements from open standards and protocols must be implemented and which requirements from open standards and protocols must not be implemented. It will also provide information to ensure consistent implementation of requirements. Additional requirements that are not part of existing open standards and protocols as well as testing requirements key to interoperability may also be set out as part of the companion specification. Compliance with the companion specification will be mandated by ESA Phase 2 regulations;

- Unregulated design documents. This could be a suite of guidance documents such as:
    - Business architecture design document – setting out how different business models are facilitated (made interoperable) by the companion specification;

- Technical architecture design document – setting out how different standards / protocols are used between ESAs and flexibility service entities;

- Plain language schema – document setting out the commands and data items used to select and maintain open standards / protocols in the companion specification.

3. Do you agree that the business architecture design, technical architecture design, plain language schema and the GB Interoperable CLF Companion Specification should be managed by the SSES Technical Governance Group? If you disagree, please provide information on how these documents should continue to be managed.

Summary of responses

A strong majority of respondents supported our proposal that the business architecture design, technical architecture design, plain language schema and the companion specification should be managed by the Technical Governance Group. Of the 26 respondents, 23 agreed, 1 disagreed and 2 were not sure.

Some (4) respondents noted the overlap with the management of documents in the Smart Energy Code's Technical and Business Architecture Sub-committee (SEC TABASC) and how this governance framework already works well in practice. There were recommendations that the Technical Governance Group should engage with the SEC TABASC to ensure expertise is shared where appropriate.

Several (6) respondents set out that the Technical Governance Group needed to have the appropriate expertise within the membership to provide the required oversight of the business architecture design, technical architecture design, plain language schema and the companion specification. Views included that the Technical Governance Group would need to consist of the appropriate industry experts and be sufficiently resourced.

Some respondents (3) also highlighted the requirement for the documents to align with international standards. Responses set out that it was important for members of the Technical Governance Group to understand international product standards or for there to be involvement of representatives operating across international markets.

Of those who agreed, 3 respondents set out that there should be a clear and transparent change mechanism for these documents with 2 respondents highlighting the requirement for an open consultation on any changes.

Government response

Following support for this proposal, we will progress plans to give responsibility to the Technical Governance Group to manage the business architecture design, technical architecture design, plain language schema and the companion specification.

We agree with respondents that activities of the Technical Governance Group have similarities with those of the SEC TABASC. We will ensure lessons learned are shared between SECCo

and Elexon and will be recommending that the chair of the SEC TABASC meets with the chair of the Technical Governance Group to share expertise and ensure alignment as required.

We also agree with respondents that it is important for members of the Technical Governance Group to have sufficient expertise to engage with highly technical documents. In the nomination and voting process we expect those nominated for group membership to provide relevant information about their suitability for membership so those voting can take this into account.

We recognise the importance of aligning with international standards and protocols for products where possible. The Terms of Reference for the Technical Governance Group will include an obligation to monitor changes in international standards and protocols and consider their impacts on the companion specification.

We also recognise the importance of having a clear and transparent mechanism for managing changes to documents. Documents managed by the Technical Governance Group will be hosted on Elexon's website where they will be publicly accessible. The site will provide information on how to request changes, along with a record of previous queries and amendments. For certain documents, like the companion specification, any substantive changes to the document will require public consultation and approval from Government and/or regulators before they are adopted.

4. **Do you agree that Government and/or regulators should make the final decision on changes to the companion specification? Please explain your answer.**

Summary of responses

A majority of respondents agreed that Government and/or regulators should make the final decision on changes to the companion specification. Of the 29 respondents, 22 agreed, 4 disagreed and 3 were not sure.

Of those who agreed, 6 set out that Government and/or regulators would need to ensure wider industry engagement on the proposals prior to final decisions being taken. Suggestions included a public consultation being held on the proposed changes to the companion specification to ensure wider technical expertise is considered. Some respondents (3) noted that Government and/or regulator oversight over changes to the companion specification would further enhance consumer protection.

Some (3) respondents recommended that to streamline the process, Government and/or regulators should only make final decisions on substantive or major changes to the companion specification. It was noted that this would follow the usual change process for the BSC whereby only substantive modifications are required to be approved by Ofgem.

Several (6) respondents raised concerns that including additional Government and/or regulator oversight in the change process for the companion specification would introduce delays. Respondents therefore requested that any additional Government and/or regulator oversight be streamlined or that a 'fast track' process for emergency changes be introduced.

Of those respondents who disagreed, 3 set out that Government and regulators may not have the necessary expertise to make a final decision on changes to the companion specification. It was recognised that the companion specification will be a technical document and therefore recommended that the Technical Governance Group, with its suitable technical expertise, should be the decision-making body.

Government response

We note the support for Government and/or regulators (Ofgem and OPSS) having the final decision on changes to the companion specification and will ensure the change process includes this level of oversight. This continued Government and/or regulator oversight will ensure that the companion specification continues to be managed in line with Government policy requirements and ensures enhanced consumer protection.[6]

The companion specification will set out what ESA manufacturers need to do to demonstrate compliance with interoperability requirements that will be set out in Phase 2 ESA device regulations. The companion specification will also inform load controllers how to build their systems to ensure they are interoperable with ESAs. Therefore, it is appropriate for Government and/or regulators to have the final decision on substantive updates. Government and regulators, as non-voting members of the Technical Governance Group, will usefully have sight of all change proposals at the earliest stages.

We expect there will be a change process for the companion specification that will accommodate two types of change:

1. A change to the companion specification to introduce new functionality; and

2. A change to the companion specification arising from the Issue Management Process e.g. to fix an ambiguity in the companion specification.

The process below outlines how these changes will be managed. Government will work with Elexon to agree the detail of these processes for the transition and delivery phases.

- **Issue Raised**: Any person will be able to raise a technical issue regarding the companion specification with the group. The Technical Governance Group could also raise an issue themselves if needed, for example in response to business process changes as the sector evolves, or in response to updates to international standards.
- **Issue Assessment**: The Technical Governance Group (with support from delegated subgroups) will assess the reported technical issue to determine the appropriate course of action. There will be a published log of all previous queries and changes to the companion specification to ensure the same technical issues and changes are not raised repeatedly. The assessment process could conclude that:

[6] This will mean that the companion specification becomes a ‘bespoke’ document under the BSC rather than a Code Subsidiary Document (as defined in Section H1.2.4 of the BSC) which would follow an existing BSC Change Proposal process. A bespoke document under the BSC carries the same legal weight as content in a Code Subsidiary Document, but for which a separate change process can be created.

    - **No change is needed:** The companion specification is not at fault. The issue lies elsewhere (e.g. a device's specific implementation or with a particular system's operation), or that it stems from a misinterpretation of the existing companion specification text rather than a defect in the specification itself. Resolutions to this type of issue could include an official explanation clarifying the correct interpretation, or potentially an update to industry guidance notes or communications. The outcome will be documented and published to ensure a transparent record of the decision;
    - **Change is required:** The Technical Governance Group after assessment determines that the reported technical issue requires a change to the companion specification. They will work with support from subgroups to develop a proposed solution to the technical issue, which can then be scrutinised as part of the formal change process.
- **Technical Governance Group Review**: The proposed solution is scrutinised by the Technical Governance Group to decide whether the modification is suitable for progression or to recommend any changes before it progresses to the next stage. Further subgroups may be set up during this stage to support development of the change, and the Security Governance Group will be engaged on any potential changes. We also expect that the Technical Governance Group would engage with consumer representatives at this stage to ensure consumer views are taken into account.
- **Government and/or Regulator Initial Review**: Government and/or regulators will have an opportunity to review the proposed modification to provide an initial view prior to Elexon holding a public consultation on the proposed changes. This provides the opportunity for Government and/or regulators to give a view on whether a modification is likely to be approved: including, for example, whether it would be helpful to seek additional information through the consultation.
- **Stakeholder Engagement**: Public consultation delivered by Elexon, on behalf of the Technical Governance Group, setting out the proposed modification, the rationale for implementation, an impact assessment and timelines for implementation.
- **Government/regulator decision**: Utilising the information from the consultation, the Technical Governance Group will put a recommendation to Government and/or regulators on the proposed change. Government and/or regulators will review the Technical Governance Group recommendation prior to approving or rejecting the final proposals.

We believe this process strikes the correct balance between ensuring technical expertise is utilised in developing proposals for changes, gathering wider stakeholder views via public consultation and oversight to ensure changes align with Government policy and support consumer interests. Although the additional step of Government and/or regulator approval may increase the time for a change to be implemented, we take the view that this oversight is required to ensure that the companion specification continues to evolve in line with Government objectives and in a way that supports consumer uptake of CLF.

We agree that minor changes to the companion specification should not need Government and/or regulator approval. Minor changes could include providing clarity, but not constituting any material change to the companion specification. Government is content for these types of

minor changes to be approved without Government and/or regulator oversight. This is in line with other change processes in the code landscape.

We expect that the final approver of changes to the companion specification will be either Government or a regulator rather than it being a joint responsibility. We will continue to work with Ofgem and OPSS, and will provide further information on how such final approvals to the companion specification are to be given in a consultation on the companion specification in 2026.

Technical Governance Functions

This section specifically sought views regarding the functions of the Technical Governance Group which included:

1. reviewing the technical framework – ensuring the technical framework remains aligned with the Policy Principles set by Government, suggesting modifications where this may no longer be the case, and reviewing the outcomes of revision processes to ensure that the development of the framework continues to meet Government objectives;

2. considering the addition of new documents to the technical framework – this could be through a gap analysis within the technical framework as the sector evolves, or through the assessment of newly developed documents (such as new technical standards). This could also be conducted if new requirements or policy proposals arise. Once Government and/or regulators decide that a document should be included within the technical framework, the governance system will need to work with Government and regulators to make the case for the document to be added to it;

3. maintaining any assurance regimes – an appropriate and proportionate approach to assurance will be necessary to ensure consumers, industry and Government can be confident that interoperability requirements are being met. There could be a role for the Technical Governance Group in developing, operating and/or maintaining the assurance regime - for example, the design and potential operation of dispute resolution for any alleged non-compliance.

5. Do you agree that the SSES Technical Governance Group should have a longer-term role in assurance and testing?

Summary of responses

A strong majority of respondents agreed that the Technical Governance Group should have a longer-term role in assurance and testing. Of the 29 respondents, 24 agreed, 1 disagreed and 4 were not sure.

Some respondents (4) noted that the Technical Governance Group and/or Elexon should be responsible for procurement of independent testing providers. These established testing providers would be able to develop suitable test frameworks and test plans for ESAs.

Of those who responded, 3 set out that further clarity on costs would be useful and that the testing and assurance regime should remain proportionate.

Government response

We acknowledge respondents' support for the Technical Governance Group to have a longer-term role in assurance and testing.

We are currently developing the companion specification with support from our existing government-led Technical Working Group and Companion Specification subgroup: the companion specification will set out testing and assurance approaches for ESA interoperability. We expect that Government will lead on the initial testing as part of the development of the companion specification. As the industry-led Technical Governance Group becomes operational, we may transfer some of the testing responsibility, such as procurement and hosting of these test events.

We will work with relevant enforcement bodies as required on dispute resolution.

Membership of the SSES Technical Governance Group

This section sought views on the membership arrangements of the Technical Governance Group. We consulted on the Technical Governance Group being comprised of nine voting members along with an independent chair.

- An independent chair (Government assigned during the transition phase)
- Three ESA manufacturers: these could be organisations and/or trade bodies
- Three load controllers: these could be organisations and/or trade bodies
- One distribution network party representative e.g. DNO or a DSO
- One representative from NESO
- One consumer interest group representative
- One representative from a relevant standard body (Non-voting)
- One Government representative (Non-voting)
- One OPSS representative (Non-voting)
- One Ofgem representative (Non-voting)

6. Do you agree with the categories for seat allocation and the suggested split of seats for the SSES Technical Governance Group?

Summary of responses

A small majority of respondents agreed with the categories for seat allocation and the suggested split of seats for the Technical Governance Group. Of the 30 respondents, 16 agreed, 5 were not sure and 9 disagreed.

Several respondents (9) were concerned there was not sufficient representation from manufacturers on the Technical Governance Group firstly in terms of overall seats, but also due to the number of device types in scope of SSES and concerns not each type of manufacturer type would be guaranteed a seat. There were suggestions to design the

nomination and voting process to ensure that manufacturers of each type (smart heat, Electric Vehicle Smart Charge Point (EVSCP) and smart domestic-scale battery energy storage systems) were represented on the Technical Governance Group to ensure expertise on each product type.

Alongside concerns about manufacturer representation, 7 respondents noted that a split between types of load controllers would also strengthen cross-sector representation. Responses called for representation from suppliers who are load controllers, solely load control organisations, and Flexibility Service Providers (FSPs) to ensure representation across all such organisations involved in load control activity. Rationale for this split included ensuring that organisations who engage with consumers can provide views on this to the group.

Some respondents (4) set out that there should be a mechanism in place to review the composition of the Technical Governance Group to ensure it remains suitable as the sector evolves. Suggestions included a periodic review or maintaining flexibility within the governance arrangements for membership changes.

Government response

We have carefully considered seat allocation following a range of views provided in response to this question. We will be progressing with membership arrangements as consulted on (and as supported by a majority of respondents) but will take views on representation within the manufacturer and load controller categories into account when finalising nomination and voting arrangements to be included in documents under the BSC. We will also ensure membership arrangements and the Terms of Reference of the group are regularly reviewed to make sure they continue to support wider programme objectives. We will review membership arrangements prior to the delivery phase.

Also, in the consultation we set out that ‘one distribution network party’ could include representation from either a DNO or DSO. We recognise that the Energy Networks Association (ENA) may be a useful representative on the Technical Governance Group so will include the ENA in scope of organisations that could provide network representation as part of this category.

Other Reflections on the Technical Governance Group

We recognised the range of information covered in the Technical Governance Group section of the consultation and therefore sought views on wider elements of the Technical Governance structure not covered in previous questions.

7. Do you have any other reflections on the proposed governance structure for the SSES Technical Governance Group?

Summary of responses

We received 26 responses to this question, and of these, 6 respondents highlighted the overlap between the Technical Governance Group and other governance groups, such as

those run by the SECCo. There were calls for the sharing of lessons learnt between SECCo and Elexon to ensure a smooth set-up and operation of the Technical Governance Group.

Alongside this, some respondents (4) highlighted SSES Enduring Governance arrangements could have implications across the energy code landscape, particularly for the REC and SEC. Suggestions to ensure alignment included increasing the membership of the Technical Governance Group to contain SEC and REC members and ensuring RECCo and SECCo are consulted as part of the developed change process.

Some respondents (4) called for more clarity on the nomination and voting process to ensure there is time for industry to prepare. A further 2 respondents highlighted a need for greater consumer representation on the Technical Governance Group, with reference to the SSES Programme supporting Consumer-Led Flexibility.

Of those who responded, 3 expressed their agreement with the proposal in the consultation that the Technical Governance Group should be able to stand up subgroups containing technical experts to provide further input into the work of the Technical Governance Group.

Government response

We thank respondents for the additional views on the Technical Governance Group shared in response to this question.

We recognise the support for engagement and alignment between the Technical Governance Group and other energy governance groups and will be moving forward with these proposals:

- Join-up between Elexon and the SEC TABASC. The Technical Governance Group and SEC TABASC are carrying out similar functions so it would be beneficial to ensure lessons learned are carried over when establishing the Technical Governance Group;
- Usual cross-code engagement between SECCo, RECCo and Elexon to ensure clarity for affected stakeholders. Elexon to facilitate further join-up as required, including through chairs of relevant groups meeting as appropriate;
- Subgroups to be established to bring further expertise to the group as needed;
- The Technical Governance Group Chair to be able to invite wider technical experts to attend meetings as appropriate.

We are committed to ensuring any changes to interoperability requirements involve consideration of the effect on consumers. We have considered the suggestion to add more consumer representatives to the Technical Governance Group and have decided to keep one consumer representative. To strengthen the consumer voice, we will require a formal assessment of how any proposed change may impact consumers. This assessment will be shared during the public consultation which is part of the process for the Technical Governance Group getting approval to make any changes. Government and/or regulators will make the final decision, considering the Technical Governance Group's recommendations, public feedback, and the consumer impact assessment. As part of the change process the

Technical Governance Group may also set up a subgroup with consumer representatives. This approach balances consumer interests with industry input on technical matters.

We also note respondents' requests for further information on the nomination and voting process in response to this question. We have provided our minded-to position for the nomination and voting process in response to Question 4.

We agree that membership arrangements and seat allocation should be kept under review. This will be reviewed at the end of the transition phase to ensure the balance of group members remains suitable as the group enters the delivery phase.

Currently, technical input to the SSES Programme is delivered through our Government-led Technical Working Group. Once the Technical Governance Group is operational, we will transition functions of the Technical Working Group to the Technical Governance Group. The Technical Working Group will close once the Technical Governance Group is fully established and operational. We are committed to ensuring a wide range of stakeholders can contribute to technical governance arrangements and therefore will ensure the Technical Governance Group engages wider industry stakeholders, for example through subgroups. Elexon also has significant experience in stakeholder engagement and we expect them to utilise these skills to ensure a broad and inclusive range of stakeholders are kept engaged and informed of activities of the Technical Governance Group.

Security Governance Group: overview

This section sought views on the membership arrangements of the Security Governance Group. We consulted on the Security Governance Group being comprised of twelve voting members (those who can cast a vote on decisions taken within the groups) along with an independent chair as set out below:

- An independent chair (Government assigned during the transition phase)
- Three ESA manufacturers (these could be organisations and/or trade bodies)
- Six load controllers, representing both Operators of Essential Services[7] (OES's) and non-OES load controllers, who control load of consumer-owned ESAs (these could be organisations and/or trade bodies)
- Two network parties i.e. DNOs and/or DSO's
- One NESO attendee, to provide a view on grid stability considerations
- One Government representative (Non-voting)
- One OPSS representative (Non-voting)
- One Ofgem representative (Non-voting)

[7] We expect that under the Network and Information Systems Regulations (2018) there will be powers to designate load controllers as an OES'. It is likely that DESNZ will designate load control organisations as an OES if they are managing over 300MW of aggregate load. However, we expect DESNZ will also have the ability to designate organisations below this threshold if deemed appropriate. Organisations must determine whether they exceed the 300MW threshold. This threshold is calculated based on the combined maximum electrical capacity of all in-scope ESAs within the organisation. In-scope ESAs include electric vehicles, electric vehicle charge points, electrical heating appliances, battery energy storage systems, and virtual power plants. The maximum rated electrical capacity of each relevant ESA, as stated by the manufacturer, should be used for this calculation, not average capacity or operational output.

8. Do you agree with the proposed membership composition of the SSES Security Governance Group, including the number of members in each category?

Summary of responses

A small majority of respondents agreed with the proposed membership composition of the Security Governance Group. Of the 29 responses to this question, 16 agreed, 7 disagreed and 6 were not sure.

Of those that provided further comment, 8 stated they were content with the split and proposed no amendments. Several respondents (6) emphasised the need to have balanced representation in each seat category amongst the different types of ESA technology types (smart heat, EVSCPs and smart domestic-scale battery energy storage systems) and different types of load control organisations (i.e. suppliers who are load controllers, solely load control organisations and FSPs).

Some (4) respondents were concerned there was not sufficient representation from manufacturers on the Security Governance Group in terms of overall seats and as such, that their perspectives would be under-represented in group voting. Another 4 respondents proposed reviewing the membership arrangements after a certain period to ensure the membership split would enable the group to meet its objectives adequately.

Respondents (4) also mentioned that the success of the Security Governance Group would depend on the required technical expertise and resources being available. Views included that the groups arrangements should be reviewed during the transition phase to assess if any changes were needed, given the evolving nature of the sector and as the skills required become more apparent.

Some (3) respondents suggested that maintaining close links with the SEC Security Sub-Committee (SSC) would be important to ensure expertise is shared between the groups.

Government response

We have carefully considered seat allocation following a range of views provided in response to this question. We will be progressing with membership arrangements as consulted on but will take views on representation within the manufacturer and load controller categories into account when finalising nomination and voting arrangements to be included in documents under the BSC. We will also ensure membership and Terms of Reference of the group are regularly reviewed to make sure they continue to meet programme objectives.

We agree that membership arrangements and seat allocation should be kept under review. This will be reviewed at the end of the transition phase to ensure the balance of group members remains suitable as the group enters the delivery phase.

We would also like to emphasise that in addition to the voting and non-voting standing members of the group, subject matter experts and representatives such as those from the National Cyber Security Centre (NCSC) and the SEC SSC will be invited to attend meetings to contribute as appropriate. Recognising respondents' suggestions around alignment with the

SEC SSC, we will also be recommending a regular meeting between the SEC SSC and the Security Governance Group chairs alongside usual cross-code engagement.

In the consultation we set out that 'one distribution network party' could include the representation from a DNO or DSO. We recognise that the ENA may be a useful representative on the Security Governance Group so will include the ENA in scope of organisations that could be represented as part of this category.

We noted respondents' requests for further information on the nomination and voting process in response to this question. We have provided our minded to position for the nomination and voting process in response to Question 2.

Security Governance Functions

This section specifically sought views regarding the functions of the Security Governance Group, these are summarised below:

1. monitor existing, and propose new, cyber security, Internet of Things (IoT) and grid stability standards and requirements: Monitor the development of new and existing cyber security, IoT and grid stability standards across devices, organisations, and systems both domestically and internationally and ensure these are considered, where appropriate;

2. maintaining threat and risk assessments: Develop and maintain Threat and Risk Assessments, as well as continued monitoring of any Risk Treatment Plans, to ensure these are updated at least annually, and when material changes have occurred to the threat and risk landscape;

3. maintaining other key security documentation: Develop and maintain the following additional security documentation to ensure it is updated periodically and mitigates identified security risks: Trust Modelling, CLF Security Architecture, propose amendments to Security Requirements, Accompanying Guidance alongside organisational and device requirements;

4. supporting OPSS with a security assurance regime for ESAs: OPSS may choose to use the Security Governance Group for support with compliance and assurance activities, such as procuring test labs to assess self-assessment submissions, where appropriate and where OPSS sees fit. This may also include, but not be limited to, developing and maintaining relevant documentation to ensure the assurance process remains fit for purpose. OPSS remains responsible for the enforcement for ESA devices;

5. supporting Ofgem with the audit and assurance regime for organisations in scope of the load control licence: Annual Cyber Assessment Framework (CAF) returns and/or audits against the appropriate CAF profiles should be submitted to the Security Governance Group. Where organisations fail to meet assurance requirements, an independent auditor will identify remediation needs. The licensee will be responsible for developing a remedial action plan to address these findings. The Security

Governance Group will oversee and monitor the remediation process, ensuring that appropriate actions are implemented and tracked;

6. maintain key grid stability guidance and other required documentation: Ensure that the approach to devices, and load controllers' responsibilities with regards to grid stability remains fit for purpose;

7. providing ad hoc cyber security advice and support: Providing relevant regulators, Government and industry with advice and support on cyber security matters related to CLF.

9. Are the scope of the roles and responsibilities of the SSES Security Governance Group manageable and proportionate?

Summary of responses

A strong majority of respondents agreed that the roles and responsibilities of the Security Governance Group are manageable and proportionate. We received 28 responses to this question, and of these, 21 agreed, 1 disagreed and 6 were not sure.

Of those that provided further comment, some (3) highlighted potential for duplication of effort with existing frameworks, particularly for organisations which are active in multiple roles in the electricity sector. Views included that the Security Governance Group needs to ensure it doesn't replicate work already carried out by the SEC SSC.

Some (4) respondents noted the potential for capacity constraints within the Security Governance Group and highlighted the importance of effective planning and management to ensure adequate expertise and resources are available when needed. A further 2 respondents mentioned the need to review the arrangements once operational to ensure the activities continue to be appropriate and manageable.

A couple (2) of respondents highlighted the potential risk that confidentiality around security concerns could be perceived as the group having a lack of transparency, and consequently the need for a suitable information classification policy to allow for transparency where appropriate. A further 2 respondents highlighted the need to consider how commercial interests of members would be managed, especially in relation to members having access to competitors' CAF returns and remediation plans.

10. Should any responsibilities of the SSES Security Governance Group be added or removed?

Summary of responses

We received 20 responses to this question. Some respondents (4) suggested the Security Governance Group should have an explicit requirement to engage with smaller market participants and consumers to ensure diversity of input in decision-making. A further 2 respondents suggested including a mechanism for small companies and consumers to appeal against decisions. Some (4) also proposed that the Security Governance Group should have

responsibilities in horizon-scanning, co-ordinating responses to and post-incident analysis of major cyber incidents affecting ESAs or load control systems.

A couple (2) of respondents suggested that the Security Governance Group should also have responsibility for parties' compliance and as such need sufficient powers to deal with parties that do not comply. Another respondent proposed interaction and alignment with NCSC as an additional responsibility.

Some respondents (3) mentioned the need for alignment with existing arrangements in other codes, and with NCSC, to ensure consistency and avoid duplication.

Government response for Questions 9 and 10

Following broad industry consensus, we are confident the proposed roles and responsibilities for the Security Governance Group are both appropriate and achievable.

We acknowledge respondents' concerns regarding the Security Governance Group's resourcing and capacity to fulfil its objectives effectively. It's worth noting that we expect the group to procure technical support as needed to support the delivery of its functions. The Security Governance Group's performance will be reviewed during the transition phase to ensure objectives are being met appropriately, with adjustments implemented (as informed by lessons learned) in the delivery phase. Ongoing performance review mechanisms will be established to support the long-term effectiveness of the group.

We agree with respondents that the Security Governance Group should seek to build on existing frameworks and recognise the value of both close alignment with, and learning lessons from, the SEC SSC. As such, we intend to include provisions in the Terms of Reference to allow the Security Governance Group Chair to invite the SEC SSC Chair or nominated expert to attend Security Governance Group meetings where necessary. As mentioned in response to Question 8, we also expect the SEC SSC and Security Governance Group chairs to meet as required. This will ensure that frameworks across both arrangements remain consistent and proportionate, and that industry benefits from having streamlined governance arrangements across these frameworks.

We note respondents' concerns around transparency of the group's proceedings. We are committed to ensuring the arrangements preserve necessary confidentiality required for sensitive matters, as well as the need for stakeholders and interested parties to be able to track discussions, decisions, and progress on security-related issues. To support this, our intention is for meeting documentation, such as agendas, minutes and decisions, to be publicly available once suitably redacted. We are minded to follow the successful SEC SSC precedent of classifying security documentation using the Traffic Light Protocol. We will ensure Elexon have the technical controls in place to store data securely and that information is only available to individuals as required by their role.

We appreciate respondents' concerns around how commercial interests of group members will be managed. We are confident that governance consisting of industry experts will deliver the best outcomes. Security Governance Group members will have a duty to act independently

and in accordance with the Terms of Reference, which will set out a process for manging conflicts of interest.

Currently security input to the SSES Programme is delivered through our Government-led Security Working Group. Once the Security Governance Group is operational we will transition functions of the Security Working Group to the Security Governance Group. The Security Working Group will therefore close once the Security Governance Group is established and operational. We are committed to ensuring a wide range of stakeholders contribute to security governance arrangements and therefore will ensure the Security Governance Group engages wider industry stakeholders, for example through subgroups. Elexon also has significant experience in stakeholder engagement and we expect them to utilise these skills to ensure a broad and inclusive range of stakeholders are kept engaged and informed of activities of the Security Governance Group.

We acknowledge respondents' suggestions that the Security Governance Group should also be responsible for ensuring parties' compliance with cyber conditions in the load control licence, and that it should have the necessary powers to do so; however, enforcement will remain the responsibility of Ofgem. We expect non-OES load controllers will have a licence condition requiring compliance with the BSC; however, Ofgem will decide on enforcement action in cases of non-compliance. We would expect the Security Governance Group to escalate any instances of non-compliance to Ofgem as they are identified.

In addition to the roles set out in the consultation, we also expect the Security Governance Group to create a sub-sector State of the Sector report to feed into Ofgem's own analysis of the state of the sector. Together these will give Ofgem an indication of the overall health of the domestic and small non-domestic CLF sector, the year-on progress made, and examples of best practice demonstrated throughout the year. This Security Governance Group report would only be shared with DESNZ and NCSC due to its sensitivity.

We have been working with key stakeholders to identify the grid stability measures within existing grid codes to mitigate the grid stability risks which may be posed by load control activity. We are considering the implications that following existing code measures would have on the Security Governance Group's function to maintain key grid stability guidance with a view to preventing any unhelpful overlap of responsibilities between codes. More information will be provided within the upcoming load control licence consultation.

Section 3 – Interactions with the Load Control Licence

Overview:

Although a specific question on enduring governance interactions with the load control licence wasn't included as part of the consultation, having progressed our policy development in this area we are able to share further details on how licensees will interact with enduring governance arrangements in practice.

Security Governance Group's role in the load control licence application process

The load control licence will be open for applications by the end of 2026. It is expected that for the first 12 months from the application window opening, Ofgem will manage the full process of reviewing licence applications.

After this initial tranche of applications (up to roughly the end of 2027), it is expected that Ofgem will use the Security Governance Group to support the application process through its reviewing and assessing the cyber security evidence submitted by licence applicants. This means that, on an enduring basis, prospective applicants would be expected to submit their applications to Ofgem, who would then pass on any cyber security evidence provided to the Security Governance Group. The Security Governance Group would then assess this evidence, with a recommendation made to Ofgem on whether the cyber security evidence is satisfactory, to then inform Ofgem's decision on whether to approve or reject the application.

Further details on this process will be set out in the upcoming Ofgem consultation on implementing the load control licensing regime.

Load Control Licensee Obligations Under the BSC

We expect the load control licence will include a condition for load controllers not designated as an OES to become party to, and comply with, the BSC for the purposes of SSES Enduring Governance.

This will be critical in enabling the Security Governance Group to support Ofgem effectively in auditing and assuring load controllers' compliance with cyber requirements. The detailed obligations on licensees will be set out in documents under the BSC. These obligations could include the detailed processes for:

- Submitting annual returns against the CAF Profile to the Security Governance Group;
- Undergoing targeted third-party audit through the NCSC's Cyber Resilience Audit (CRA) scheme and submitting the outputs of this to the Security Governance Group;
- Reporting any significant or potentially significant cyber security incident to the Security Governance Group;
- Where non-compliance is identified, implementing remedial action plans and submitting evidence of the steps being taken to achieve compliance.

Acceding to the BSC

We are proposing that only organisations acting as load controllers that are subject to the cyber licence requirements will be required to become party to, and comply with, the BSC via licence conditions. In practice, this will mean that only licensed load controllers that are not designated as OES's under NIS will be required to become party to, and comply with, the BSC. The purpose of this requirement would be to place obligations on load controllers to ensure they comply with providing their remediation plans to the Security Governance Group as described above.

Licence conditions relating to cyber security would not apply to FSPs who are not also load controllers and as such, we are expecting that FSPs will not need to accede to the BSC. This demonstrates our commitment to ensure that any regulatory requirements for FSPs and load controllers are proportionate, justified and avoid unnecessary burdens on an emerging market. Further details on the proposals for certain load controllers to be subject to cyber security licence requirements and to become party to, and comply with, the BSC via licence conditions, as well as the threshold for designating load controllers as OES under NIS will be set out in our upcoming load control licence consultation.

The process for load controllers acceding to the BSC is yet to be confirmed; however, we expect this may include the following steps:

1. Signing a BSC Accession Agreement (which is available to view as the annex to BSC Section A);
2. Registering participation capacity, which for load controllers will be a newly created role. The BSC may require load controllers to complete a form for this purpose (with the current version of the form being BSCP65/01);
3. Under the current BSC processes, load controllers may need to opt out of Central Volume Allocation Qualification by completing form BSCP70/02;
4. Load controllers may also need to appoint an authorised signatory under BSCP38.

Load controllers will only need to comply with SSES Governance Frameworks and SSES Arrangements under the BSC alongside other standard BSC requirements for code parties. These include provisions regarding liability and confidentiality as well as rights to raise and participate in BSC Modifications.

The upcoming Ofgem consultation on implementing the load control licensing regime will set out further details on monitoring, compliance and enforcement activities with regard to the load control licence.

Section 4 – Implementation

Overview:

This section of the consultation sought views regarding implementation. It set out how SSES Enduring Governance will be delivered in phases. The transition phase begins with the Government-led modification to the BSC and a second phase of implementation is expected from mid-2029, following the introduction of the load control licence and second phase ESA regulations. We also proposed that the Technical and Security Governance Groups will be subcommittees under the BSC Panel.

Transition Phase BSC Modification

This section specifically sought views regarding the proposed modification to the BSC for the BSC Panel to establish the Technical and Security Governance Groups as subcommittees and for these to be administered by Elexon. This was set out in an Annex A to the main consultation document.

11. Do you agree with the proposed content of the BSC code modification set out in Annex A? If you disagree, please set out your reasonings and any suggested changes.

Summary of responses

A strong majority agreed with the proposed content of the BSC Modification set out in Annex A to the consultation document. We received 23 responses to this question. Of these, 19 agreed, 1 disagreed and 3 were not sure.

Many respondents (10) agreed that the draft legal text achieved the intended purpose as currently drafted. Some respondents (2) highlighted the need for the modification to enable non-BSC parties, such as ESA manufacturers, to engage with and participate in the governance arrangements.

Government response

Following the support for the proposed legal text, we can now confirm our intention to proceed with modifying the BSC as per the revised implementation stage legal text in Annex A to this Government response. This will be implemented by the Secretary of State using modification powers under Section 245 of the Energy Act 2023 in early 2026.

The implementation stage legal text has the following changes to the consultation stage modification:

- Clarification on the roles and responsibilities of the BSC Panel and Elexon (BSC Company) regarding SSES Enduring Governance;
- Clarification on technical and security regulatory frameworks being referenced;
- Clarification of the role of the Panel in the governance arrangements, and the scope of its powers;
- Inclusion of indemnity arrangements for Technical and Security Governance Group members;
- Clarification on how the Secretary of State will consent to documents being introduced to the framework prior to them taking effect;
- Clarification on how subsidiary documents and bespoke documents will be managed;

- Clarification that the Secretary of State will be able to approve changes to documents set out in the Governance Framework and SSES Arrangements, until such time that the Secretary of State makes a notice to transfer this responsibility to the Authority.

We can now also confirm our intention to establish subsidiary documents under the BSC that define the detailed functions, membership, and change processes for the Technical and Security Governance Groups and any documents they manage. The subsidiary documents will also set out the requirements on load controllers as part of the SSES Governance Arrangements as set out in Section 3. Subsidiary documents are typically used to provide the practical details necessary to implement the overarching rules and obligations defined in the main code. We plan for these subsidiary documents to be implemented into the BSC in early 2026.

As set out in the updated implementation stage BSC modification and explanatory notes in Annex A, we intend the details of the SSES Governance Framework and SSES Arrangements to be set out either in Code Subsidiary Documents (CSDs) as defined in Section H1.2.4 of the BSC, or ‘bespoke’ documents otherwise given legal effect under the BSC. For example, such documents will set out the roles and responsibilities for load controllers as per their obligations in relation to SSES Governance Arrangements. These documents will only take effect once consented to by the Secretary of State.

Government, in collaboration with Elexon, OPSS and Ofgem, will develop these documents over the coming months based on the positions in this Government response and wider SSES policy consultations. Stakeholder engagement will play a key role in ensuring that these documents support the needs of industry whilst also enabling robust governance arrangements.

We note respondents' concerns around non-BSC parties and their ability to participate in the SSES governance arrangements. However, we are confident that clause 18.6(c)(i) of the BSC modification is sufficient to ensure that the SSES Governance Framework can provide for ESA manufacturers, FSPs (who are not also load controllers) and other relevant stakeholders who are not BSC Parties to enter into a bi-lateral agreement with Elexon to access documents within the SSES Governance Framework and take the benefit and burden of any rights and obligations set out in these documents. This will include participation in the nomination and voting processes for group members, access to relevant subgroups and consultations.

12. Do you agree the SSES Technical and Security Governance Groups should report into the BSC Panel (recognising the proposals in this consultation are subject to change following the outcomes of code reform consultations)?

Summary of responses

A strong majority of respondents agreed that the Technical and Security Governance Groups should report into the BSC Panel. We received 29 responses to this question. Of these, 20 agreed, 3 disagreed and 6 were not sure.

Several (6) respondents agreed that having the Technical and Security Governance Groups report into the BSC Panel would be practical whilst waiting for code reform to be implemented by Ofgem, and considering how the groups will function within the new framework.

Respondents (6) highlighted some concerns that the current BSC Panel membership may not contain the specific expertise required, and that going forward, the BSC Panel elect at least one member with significant expertise in CLF. Another 6 respondents raised concerns around the ability of non-BSC Parties (such as ESA manufacturers) being able to engage with arrangements under the BSC. They highlighted the need for clear participation channels (e.g. subgroups) to ensure all relevant stakeholders are considered in decision-making.

Some respondents (2) noted that reporting obligations should avoid creating unnecessary bureaucracy or slow down decision-making on urgent matters, and that consideration should be given to protecting the integrity of the expert-led decisions and recommendations of the groups.

Government response

In light of the support for our proposals, we intend to proceed with having the Technical and Security Governance Groups report into the BSC Panel as BSC Panel subcommittees. This will include regular reporting of activities to the BSC Panel.

As part of code reform, the functions of the BSC Panel will transition to a licensed Code Manager and a Stakeholder Advisory Forum (SAF),[8] and this is expected to take place in 2026.

We recognise concerns put forward regarding the lack of specific expertise on CLF within the Panel; however, as the Panel has strong representation from across the energy sector, including consumer representatives, we have taken the view that this is a proportionate and practical interim arrangement ahead of code reform being implemented.

Ofgem intend to consult on what roles will be part of the code manager business, and this may include SSES Enduring Governance. We will continue to work closely with Ofgem to consider how the Technical and Security Governance Groups will interact with the SAF and licenced Code Manager under the new framework.

Section 5 - Cost Recovery

Overview:

This section of the consultation sought views regarding cost recovery for SSES Enduring Governance. The consultation proposed that Elexon recover costs through existing BSC mechanisms during the transition phase. The consultation proposed these costs would be treated as BSC Costs, paid by code parties based on their market role.

[8] Energy code reform: second implementation consultation | Ofgem

We also proposed Government would review cost recovery arrangements once the load control licence and Phase 2 ESA regulations come into force. This may include expanding the funding base to include licenced load controllers, reflecting their role and benefits from the governance functions.

13. Do you agree that the set-up costs during the Transition Phase for SSES Enduring Governance should be treated as BSC Costs, subject to review prior to the delivery phase?

Summary of responses

A strong majority of respondents were supportive of the proposed approach to cost recovery during the transition phase. We received 28 responses to this question. Of these, 21 agreed, 4 disagreed and 3 were not sure.

Many respondents (9) recognised the proposal as proportionate for the transition phase but emphasised the need for the arrangements to be reviewed ahead of the delivery phase to ensure that costs are allocated more fairly amongst beneficiaries.

Several respondents (8) highlighted that other organisations who stand to benefit, such as manufacturers and load controllers who are not BSC Parties, should be brought into scope of contributing to SSES Enduring Governance costs.

Government response

In light of the strong support from respondents, we can confirm our intention to proceed with our proposed approach of treating transition phase costs for SSES Enduring Governance as BSC Costs. Following the development of a more detailed view of the groups' activities, we have refined our assessment of the technical and security expertise and resources required including potential procurement activity. As such, we have revised the cost estimate to £2.3 million per annum (previously £1.7 million per annum). These cost estimates have increased to reflect the additional expertise required on an enduring basis to support the Technical and Security Governance Groups and that Elexon may support ongoing testing of ESAs against the companion specification. We recognise the importance of costs representing strong value for money going forwards, and these costs will be consulted on as part of Elexon's wider budget.

We note respondents' feedback that as things stand, load controllers and ESA manufacturers will not contribute directly to the set-up costs. Our intention is that once load controllers become licensed, those who become party to the BSC would be responsible for contributing to costs.

We also noted in response to Question 2 that we may transfer responsibilities related to testing of the companion specification to the Technical Governance Group during the transition phase. We expect that ESA manufacturers, load controllers and FSPs who wish to participate in testing events will fund their own participation. This will ensure that the costs associated with provision of this service are recovered from those who benefit.

We also re-affirm our commitment to review the approach to costs prior to the delivery phase to ensure that costs are recovered from a broader range of parties benefiting from these arrangements.

Section 6 – Accountability

Overview:

This section of the consultation sought views on our proposed approach to ensuring accountability for the Technical and Security Governance Groups. To ensure the Technical and Security Governance Groups operate in line with Government expectations, the consultation proposed that Government will retain the right to change the independent chairs of the Technical and Security Governance Groups if necessary, particularly if the groups are not delivering intended outcomes or if impartiality is compromised.

14. Do you agree that Government reserving the right to change the chair is a sufficient method to hold the SSES Technical and Security Governance Groups to account for their activities?

Summary of responses

Respondents were broadly supportive of our proposal of Government reserving the right to change the chair as a method to hold the groups to account. We received 28 responses to this question, and of these, 17 agreed, 5 disagreed and 6 were not sure.

Of those that agreed, 5 expressed that this alone would not be enough to ensure accountability. Some (5) respondents also underscored the need for transparency on any Government decision to remove the chair.

Several (6) respondents proposed adopting defined reporting requirements, and 4 respondents suggested that independent reviews could also be useful tools to ensure accountability.

Some (3) respondents suggested having a structured escalation mechanism for groups to raise concerns with Government about certain decisions, group progress or a chair's perceived impartiality.

Government response

We thank respondents for their considered feedback to this question. We can confirm our intention for Government to retain the right to change the chairs of the Technical and Security Groups if required, as one mechanism to ensure accountability. We recognise respondents' views that additional measures to ensure accountability will be needed.

We also intend to ensure further oversight in the transition phase through attendance by Elexon and the Technical and Security Governance Group chairs at the DESNZ-led SSES Programme Board. This internal government meeting will be used to review the performance of

the groups, obtain updates on the latest progress of initiatives, and review any cross-cutting issues which may require policy and/or regulatory oversight.

We also intend to put in place a mechanism for Technical and Security Governance Group members and wider stakeholders where relevant to escalate concerns and appeals to the BSC Panel/Code Manager, Government or regulators. We will consider setting out these arrangements in documents under the BSC in 2026.

Ofgem intend to consult on what roles will be part of the code manager business, and this may include the SSES role. If Elexon is appointed as the licenced Code Manager for the BSC, they would be accountable to Ofgem for the delivery of this role.

Section 7- Next Steps

Overview:

This section of the consultation set out our proposed next steps for implementation of SSES Enduring Governance following the publication of the consultation and this Government response. This included the timelines for implementing the BSC modification and delivering the Technical and Security Governance Groups.

15. Are there any key elements we are not including in the timeline which will need to be factored into our roll-out of SSES Enduring Governance?

Summary of responses

We received 20 responses to this question. Some (5) respondents highlighted the importance of including key milestones of related programmes which included Market-wide Half Hourly Settlement, Data Sharing Infrastructure, Consumer Consent Solution and the NESO Digitalisation Plan.

A couple (2) of respondents specifically mentioned the need to consider how the implementation of code reform could impact the milestones set out in the timeline.

Some respondents (3) expressed concerns about Elexon's capacity given their wider programme of work, including the work to establish the Market Facilitator role, and that consideration should be given to ensure they are adequately resourced to deliver SSES Enduring Governance.

Respondents (3) also suggested that the timeline include details on how the proposed groups will interface with existing governance arrangements such as those under the SEC, as well as with Ofgem and OPSS, to avoid duplication of effort. Some (2) respondents requested more clarity on the timelines for the nomination and voting process for the groups.

Government response

We thank respondents for their considered feedback on our timeline. We noted respondents' concerns about Elexon's capacity and ability to deliver the arrangements given their wider commitments. We plan to work closely with Elexon to develop a detailed delivery plan and target operating model which will account for key dependencies, resources and potential capacity constraints to minimise risks to delivery. Regarding wider dependencies with other programmes of work, we are confident that the SSES Enduring Governance timeline is sufficiently independent to ensure confidence of delivery. We have included an updated timeline in the Key Policy Decisions and Outcomes section earlier in this Government response.

RASCI Matrix

In the consultation we committed to work with Elexon, Ofgem and OPSS to ensure roles and responsibilities between industry, Government and regulators are clearly defined. Below we set out the remit of each of the organisations and groups involved in SSES Enduring Governance.

DESNZ:

DESNZ is the lead Government department responsible for policy development, strategic oversight, and regulatory design for the SSES Programme. DESNZ ensures that governance arrangements, technical standards, and security frameworks align with government ambitions for energy, including decarbonisation, consumer protection, and system resilience.

Ofgem:

Ofgem is the independent energy regulator for Great Britain. Within the SSES Programme, Ofgem will be responsible for assessing licence applications and granting licenses (with support from the Security Governance Group), monitoring licensees' compliance with regulations (with support from the Security Governance Group), and enforcing compliance where necessary for organisations involved in load control activities. It will ensure that licenced entities meet cyber security, consumer protection, and grid stability standards, supporting a secure and flexible electricity system.

Elexon:

Elexon administers the BSC which governs the electricity balancing and settlement arrangements in Great Britain. This Government response confirms our position that the Technical and Security Governance Groups will become subcommittees of the BSC Panel and that Elexon will administer these Technical and Security Governance Groups. Elexon's role will be formalised through modification to the BSC enabling them to deliver the required governance functions.

Security Governance Group:

The Security Governance Group will be responsible for maintaining and evolving the security framework that underpins the safe operation of ESAs and load control activities. As part of the SSES Enduring Governance Framework, the Security Governance Group will ensure that cyber security requirements remain proportionate, risk-based, and aligned with Government policy and regulatory frameworks. The Group will also be responsible for supporting Ofgem through its reviewing and assessing the cyber security evidence submitted by load control licence applicants.

The Security Governance Group will include representatives from manufacturers, load controllers (including those designated as an OES and non-OES load controllers), and network operators, with NESO as a permanent member. DESNZ, Ofgem, and OPSS will participate as non-voting members. The group will be chaired independently, with the chair appointed by Government during the transition phase and selected by industry thereafter.

Technical Governance Group:

The Technical Governance Group will be responsible for maintaining and evolving the technical framework that underpins interoperability for ESAs. As part of the SSES Enduring Governance Framework, the Technical Governance Group will ensure that technical standards remain aligned with Government policy objectives and responsive to innovation and market developments.

The Technical Governance Group will include representatives from manufacturers, load controllers, network operators, NESO, and consumer interest groups, with DESNZ, Ofgem, and OPSS participating as non-voting members. The group will be chaired independently, with the chair appointed by Government during the transition phase and selected by industry thereafter.

Office for Product Safety and Standards (OPSS):

OPSS is the UK Government regulator for product safety. Within the SSES Programme, OPSS is responsible for enforcing compliance with ESA regulations and ensuring that devices placed on the market meet the required standards to protect consumers and the electricity system.

Industry Stakeholders:

Stakeholders who will be directly impacted by and participate in SSES Enduring Governance arrangements include FSPs, Load Control Licensees and ESA Manufacturers.

RASCI Table

The table below details which organisation and/or group is responsible, accountable, supportive, consulted and informed for each activity.

- Responsible (R) – the organisation(s) who do the work to deliver the activity.
- Accountable (A) – the organisation ultimately answerable for the correct and thorough completion of the activity.
- Supportive (S) – the organisations who help the Responsible organisation deliver the activity. They provide resources or play a supporting role.
- Consulted (C) – the organisations who provide input based on their expertise and are consulted before a decision or action is taken.
- Informed (I) – the organisations who need to be kept up to date on progress or decisions but are not directly involved in the work.

Role	Elexon	Ofgem	DESNZ	OPSS	SGG	TGG	Industry
Policy Design							
Designing the SSES Enduring Governance framework	C	S	R, A	S			C, I
Initial Approval of Governance Framework Documents		S	R, A	S			
Chairing arrangements – development of independent chair arrangements and appointing chair in transition phase.	S	C	R, A	C			I
Design change process for governance documents	C	S	R, A	S			I
Administration/Operational Delivery							
Administrative co-ordination & Delivery of SSES Enduring Governance Arrangements	R, A	C	S	C			C, I
Nomination and voting process for governance group membership	R, A	S	C	S			I
Security Governance							

Role	Elexon	Ofgem	DESNZ	OPSS	SGG	TGG	Industry
Assurance for non-OES load controllers: processing annual CAF returns	S	A	I		R		I
Assurance for non-OES load controllers: Remediation	S	A	I		R		I
Assurance for non-OES load controllers: Non-compliance	S	A	I		R	C	I
Organisation Assurance: Enforcement Action	S (where appropriate)	R, A	I		S	S	I (where appropriate)
Device compliance, assurance & enforcement	S	C	A	R	S	S	I
Updates to DESNZ owned CAF profile and associated documents	I	S	R, A		C		I, C
Updates to Ofgem owned assurance documents	I	R, A	S		C		I, C
Cyber checks on load control license applicants (Expected by the end of 2027)	S	A			R		I
State of sub-sector report	S	A	I	I	R		
Technical Governance							
Development of Companion Specification	S	C	R, A	C		S	I

Role	Elexon	Ofgem	DESNZ	OPSS	SGG	TGG	Industry
Ongoing maintenance of Companion Specification	S	Accountable party to be confirmed		C	I	R	I
Enforcement action: Devices	S	C	A	R	S	S	

Glossary

Term	Definition
Balancing and Settlement Code (BSC)	Defines the rules and governance for the balancing mechanism and imbalance settlement processes of electricity in Great Britain. It is administered by Elexon.
Consumer-Led Flexibility (CLF) (formerly Demand Side Response)	Changing electricity demand to help meet the needs of the energy system, typically to benefit the transmission network, distribution network, or another third party.
GB Interoperable Consumer-led Flexibility Companion Specification	A Companion Specification is an implementation guide as to how to build a device against a given existing standard to help deliver interoperability usually for some sort of “constrained” implementation e.g. such as within a given geography. A Companion Specification will have its own Governance, separate from that of any underlying standards. This helps where an Authority is required to ensure the Companion Specification is delivering against specific objectives/ policy intents without being directly bound by existing standards governance which may be subject to conflicting interests. A Companion Specification is generally developed and followed by device manufacturers through commercial incentives or regulatory requirements. Example of Companion Specifications for smart metering include: GBCS, IDIS, G3.
Cyber Assessment Framework (CAF)	The framework of that name established by NCSC to assist in carrying out cyber resilience assessments.
Flexibility Service Provider (FSP) – formally Demand Side Response Service Provider (DSRSP)	An organisation entering into a legally enforceable arrangement with a consumer to provide load control at that consumer’s premises to that consumer.
Distribution Network Operator (DNO)	Owns the local networks and feeds low voltage electricity through to homes or business property.

Term	Definition
Distribution System Operator (DSO)	Has a role to monitor, control and actively manage the power flows on the distribution system to maintain a safe, secure, and reliable electricity supply.
Energy Smart Appliance (ESA)	A device which is communications-enabled and capable of responding automatically to price and/or other signals by shifting or modulating its electricity consumption and/or production.
Electric Vehicle Smart Charge Point (EVSCP)	A smart charge point means a chargepoint must have the ability to— (a) send and receive information; and (b) respond to external signals by modulating the rate of electricity flowing through the charge point. This term can be used interchangeably with Electric Vehicle Supply Equipment EVSE, Electric Vehicle Charge point and Charge point.
First Phase ESA Regulations	This legislation will: • establish a smart mandate for electric heating products in scope, requiring that they are placed on the market with smart functionality (consumers will always retain the option to use their devices in non-smart mode); • incorporate, with some planned amendments, existing requirements regarding EVSCPs into a single set of regulations; • contain a set of minimum requirements in relation to smart functionality, cybersecurity, and grid stability for the smart electric heating appliances, EVSCPs and smart domestic-scale battery energy storage systems (BESS). The regulations will require compliance with provisions of the ETSI EN 303 645 standard for IoT cybersecurity and require devices to be configured to deliver in aggregate a randomised delay up to 10 minutes where there is a risk of herding.
Interoperability	The ability of a product or system to operate in conjunction with other products and systems. For the SSES programme, interoperability in reference to ESAs, specifically refers to the ability of the ESA to change its FSP without the need for a visit to the premises and whilst maintaining the ability to provide consumer-led flexibility.
Load Control Signal	A digital communication sent via a relevant electronic communications network to an energy smart appliance for the purpose of causing or

Term	Definition
	otherwise facilitating an adjustment in the immediate or future flow of electricity into or out of the energy smart appliance.
Load Controller	An organisation that: 1. creates a load control signal; 2. changes a load control signal; 3. controls the timing of the sending of a load control signal for the purpose of adjusting the immediate or future flow of electricity into or out of an energy smart appliance or another appliance in response to the load control signal.
National Cyber Security Centre (NCSC)	The organisation of that name established by the UK Government to, amongst other things, provide advice in relation to cyber security.
National Energy System Operator (NESO)	An operationally independent and impartial body which is the licensed electricity system operator for the GB electricity transmission system. NESO has a range of other responsibilities across both the electricity and gas systems, as well as general duties, in carrying out its functions to drive progress towards net zero while maintaining energy security and minimising costs for consumers.
Network and Information Systems (NIS) Regulations	The Network and Information Systems Regulations 2018, that require organisations to meet specified cyber security requirements.
Public Key Infrastructure	A system for managing cryptographic material that is used to secure and encrypt communications.
Retail Energy Code (REC)	A central industry document that sets out how centralised information is managed including, for example, which energy supplier supplies which consumer.
Second Phase ESA Regulations	We will take forward a second phase of ESA legislation later in this Parliament. This second phase will further protect consumers who choose to participate in CLF by giving them the confidence that the ESAs they purchase can be used with different FSPs, should they decide to switch. The framework will require (as a minimum) ESAs to comply with an interoperability standard and FSPs to integrate with this standard, thus ensuring a base level of interoperability.

Term	Definition
Smart Energy Code (SEC)	A central industry document that sets out how energy suppliers and other parties communicate with Smart Meters.
Smart	Means, in relation to a device, the ability of the device to respond in real time to remote communication signals, using digital technologies, to deliver a service.
Smart Secure Electricity Systems Programme (SSES)	A DESNZ programme with the primary objective of unlocking the benefits of a smart and flexible electricity system for domestic and small non-domestic consumers, whilst protecting consumers and the grid.
Tariff	The charges applied to a consumer for their energy supply (and the associated contract terms).
Tariff Data Interoperability	In relation to an ESA, the ability of an ESA to be used with a tariff from any energy supplier, easily and without a service provider visit to the ESA.
Time-Of-Use Tariff (TOUT)	An electricity Tariff under which the unit price for electricity varies throughout the day.

This publication is available from: www.gov.uk/desnz

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.