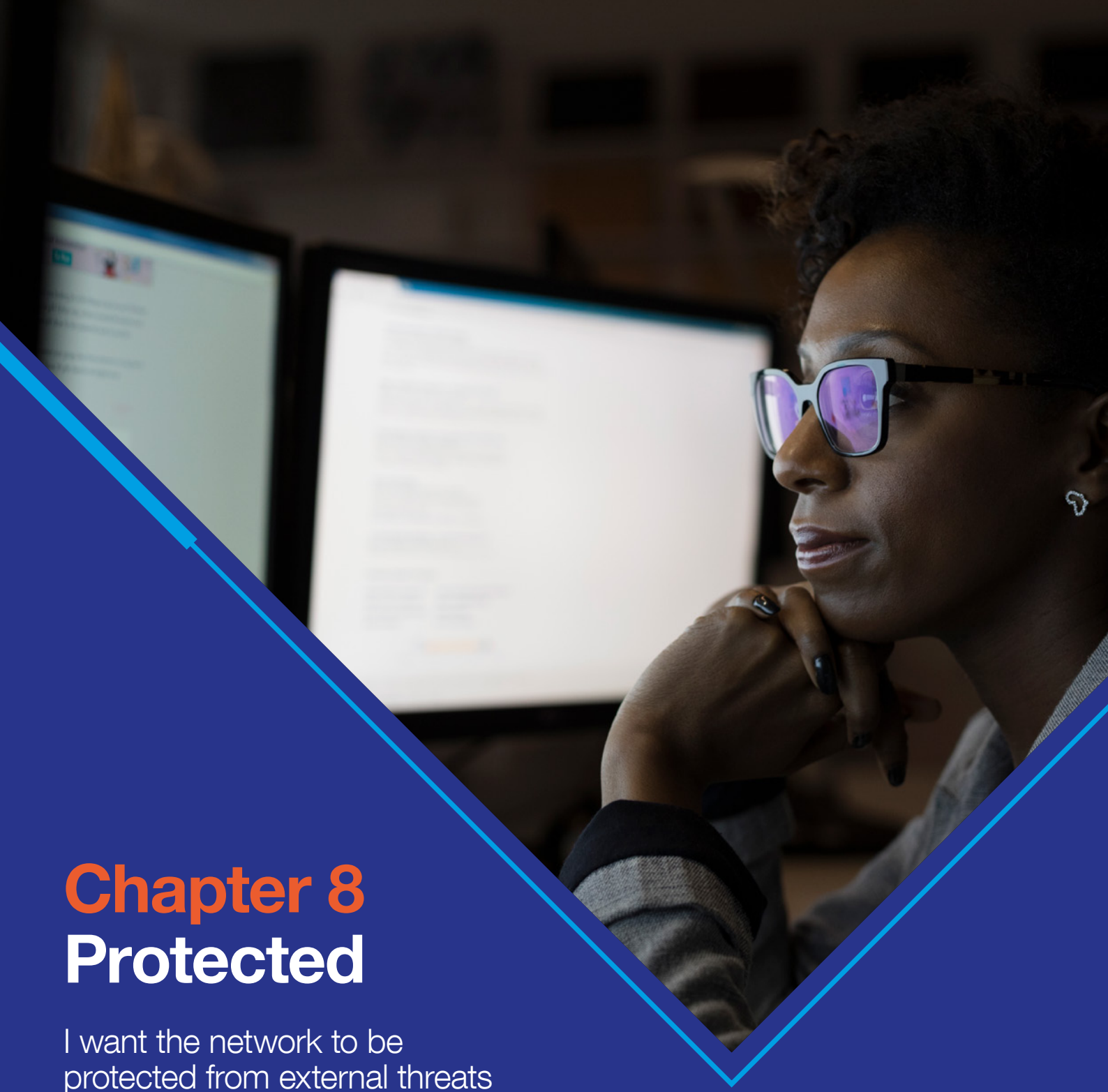

Chapter 8
Protected

I want the network to be protected from external threats

Electricity Transmission

nationalgrid

8. I want the network to be protected from external threats

What this stakeholder priority is about

Our customers and consumers depend on our network to provide a continuous supply of electricity. We have a responsibility to protect the network – and its systems – from a range of threats and to respond to any incidents quickly and effectively.

We want to manage external threats in a way that is supported by the Government, relevant agencies and our stakeholders. We'll continue to invest in protecting our network from cyber-attacks, physical attacks and extreme weather – and to recover from shutdowns.

Summary of what our stakeholders have told us so far

You have told us you want us to protect the electricity transmission network from threats. Incidents that put the performance of our assets and systems in jeopardy, and can have a direct impact on our stakeholders and consumers, include:

- Cyber-attacks.
- Physical attacks.
- Extreme weather.

We also need to recover from incidents if they happen. Therefore, we'll be enhancing our capabilities to recover from a full or partial shutdown of the network, known as a Black Start.

The Government and relevant agencies play an important role in setting minimum requirements for how we manage external threats. There is potential for us to do more, but only if stakeholders want us to. This could become more important as society grows increasingly dependent on electricity in the future.

Our current performance on protecting the network from external threats

At the start of the T1 period, it was unclear how much we would need to invest in protecting the network from external threats. As threats have changed and new ones emerged, we have adapted our plans and invested in effectively protecting our network.

Cyber-threats have changed significantly within the T1 period. The Government has recognised this by introducing new regulations in this area. We forecast we will have invested over £30m in detecting, protecting, responding to and recovering from cyber-attacks during T1. We were not explicitly funded for this in the T1 period. However, we considered it was the right thing to do to protect consumers.

In terms of protecting our network from physical attack, we're on track to deliver our RIIO-T1 Physical Security Upgrade Programme (PSUP). We have invested around £200m in improving the physical security of our sites to levels agreed with the Department for Business, Energy and Industrial Strategy (BEIS) and the Centre for the Protection of National Infrastructure (CPNI).

We are expecting to invest around £100m in installing flood defences at 50 sites in the T1 period. This is part of a co-ordinated approach by the energy sector based on thorough flood risk assessments and prioritisation of flood defence investment.

We continue to maintain the capability to respond to a full or partial shutdown of the network, known as a Black Start event. We've carried out extensive tests and exercises involving our control room and field staff. This ensured we have the skills and plans in place for an effective recovery.

We have been closely monitoring how the threats we face have changed during the T1 period. We have been engaging with key stakeholders, such as BEIS, CPNI and the National Cyber Security Centre (NCSC), as well as using the latest threat intelligence from other external organisations. It's important we continue to be flexible in this area. We need to constantly assess whether our plans are appropriate, so we can protect our stakeholders and consumers from emerging and changing threats.

Our direction of travel following stakeholder feedback so far

We are in the process of building our business plan with our stakeholders. In this section, we'll playback the feedback we have heard from you – and ask for your views on what we suggest could happen next.

The benefits to consumers

Our plans for making the network more resilient will benefit consumers by:

- Building trust that we are a responsible business.
- Ensuring electricity is there when needed.

Based on what our stakeholders have told us, this section looks at different aspects of resilience in the T2 period. We worked with BEIS, the Environment Agency, the Welsh Government, the National Infrastructure Committee, other energy companies, universities and research councils on the Energy Research Partnership's recent report on the Future Resilience of the UK Electricity System. The report found that society and businesses are becoming increasingly dependent on electricity, and networks are increasingly at risk of cyber, physical and climate-change threats.

Enhancing our cyber resilience

You have told us that you want us to protect our network from cyber-attacks. In recent years, there have been several notable cyber-attacks, which have demonstrated the tenacity of would-be attackers and the potential impact a successful attack could have on critical networks. The 2015 attack on the Ukraine energy network was one example.

In response to this growing threat, the UK Government has published its first two National Cyber Security Strategy documents and adopted new regulations around security, called Network and Information Systems (NIS) regulations.

The NIS regulations came into effect in May 2018. They aim to minimise the risk of cyber-attacks and the resulting impact on the UK's Critical National Infrastructure (CNI) and economy. As an Operator of an Essential Service (OES), we have obligations under the NIS regulations. These include ensuring we have appropriate security measures in place to protect our networks and information systems from cyber-security incidents. We are in the process of agreeing the appropriate level of security for our electricity transmission systems with the Government.

With all of that in mind, our intention for the T2 period is to make sure we have appropriate levels of cyber resilience, agreed with the Government. We'll continue to work with the Government, CPNI and Ofgem to establish levels of security that align with the NIS regulations. We'll then develop a process for responding to these changes in requirements during the T2 period. Our stakeholders have told us they are satisfied with the approach we are taking.

We plan to continually assess both the threat and levels of security on our network and systems. This includes monitoring live threats and attacks against our network. We will continue to improve our cyber security capabilities, where necessary, to meet agreed levels of resilience with the Government.

The landscape for cyber threats is changing rapidly. So we must be ready to consider further investment as and when new risks arise. We will work with the Government to agree an approach to effectively respond to any changes in our threat and resilience requirements.

To meet the cost of our cyber-resilience plans, we intend to request a baseline allowance from Ofgem for the work we know is required. We will also work with Ofgem to find the best way to adjust our allowance during the T2 period, should there be any changes in our resilience requirements. Due to the sensitive nature of our plans for cyber resilience, we won't be able to share these with stakeholders. However, we will provide transparency about our costs where we can.

Enhancing our physical security

Physical attacks are another key threat we need to protect our assets against. The PSUP is a Government-supported programme to protect the UK's critical infrastructure. The CPNI has worked with BEIS to identify and prioritise spending on PSUP assets.

Our intention for the T2 period is to continue working with the Government to agree the appropriate levels of physical resilience for our sites and equipment. The majority of PSUP upgrades are due to be completed within the T1 period. Only a small amount of additional investment will be required in T2 to complete this.

With the introduction of new NIS regulations, we will also work with Ofgem and BEIS to ensure our investment in physical resilience meets the Government's requirements for cyber security.

The threat of a physical attack, as well as the Government's requirements for physical security, can change quickly. So we must be ready to consider further investment should it be needed. Our plans for the T2 period are based on the threats we currently face. We plan to request a baseline allowance from Ofgem for the work we know is required. We will engage with Ofgem to find the best way to adjust our allowance during the T2 period to effectively respond to any changes in our requirements.

Protection from extreme weather

We are also aiming to increase our resilience to natural hazards. One example is our project to introduce and enhance flood defences. Our current plans for the T2 period include investing around £60m to protect our assets from surface water flooding. We will also develop a strategy to understand what long-term measures we need to put in place to address wider natural hazards.

Recovery from a shutdown event – Black Start

You have told us that a resilient network is important to you. An important part of that is making sure energy supplies can be restored following any loss of electricity. A Black Start is the recovery from a full or partial shutdown of the network. It could be either national or regional. While such events are rare, the South Australian blackout of September 2016, which was caused by storm damage, left almost the entire state without its electricity supply.

A cross-industry working group is developing a GB Black Start Restoration Standard. This will define a time limit for restoring electricity demand following a network shut down. BEIS will oversee the standard, ensuring it continues to meet resilience requirements. We are currently working with key stakeholders such as BEIS to understand both the desired, and realistic, timescales in which demand can be fully restored. Any proposals made through this workgroup will be subject to consultation. Following this, it's likely that we will be required to meet its target timescale for a Black Start recovery.

Based on BEIS's direction, we envisage increasing some of our asset performance targets, and reviewing the availability of our workforce. This will be built into our plans for T2.

We will adjust our plans to reflect the GB Black Start Restoration Standard when it is issued following a consultation later this year. The best place for stakeholders to share their views is through the cross-industry group's consultation on the standard.

What it could cost

Low £0.10bn | **T2 annual spend range** | **Higher if required**

T1 annual expenditure (forecast) £0.05bn

We estimate that our minimum expenditure on resilience for T2 will be £0.10bn a year. Much of this will be spent on cyber security. This reflects both the increasing threat of cyber-attacks and the fact we have already invested significant amounts in improving our resilience to physical attacks and extreme weather during the T1 period.

We are also interested in stakeholders' views on whether we should invest beyond the Government's current requirements for resilience. You might see benefit in this, particularly as society is expected to become more dependent on electricity in the future.

If stakeholders do see benefit in this, then our costs will be above the minimum annual expenditure.

There is uncertainty over our upper spend on resilience, because it depends what threats emerge over the period. We will continue to work with the Government and relevant agencies on any new requirements. We will also work with Ofgem and our stakeholders on appropriate mechanisms for adjusting our baseline funding. This could be required if we need to spend more on resilience in the T2 period than expected at the start.

How we will continue to engage with our stakeholders

We welcome feedback on this chapter of the consultation, including whether we have identified all the main threats to our network.

We are also interested in stakeholders' views on whether we should be investing beyond the Government's current requirements for resilience. One possible case for this would be society's anticipated growth in electricity dependency in the future.

We welcome your views:

Question:
What are your views on our direction of travel and investment drivers in relation to resilience in the T2 period?

Submit your feedback online here:

How to use this document
We want your feedback

Who is this consultation aimed at?

We are interested in the views of all stakeholders who are impacted by what we do or interested in shaping the future of electricity transmission. This includes the views of all users of our network, government, regulatory bodies and energy industry professionals.

Tell us what you think

This consultation is open until 31 March 2019. You may give us feedback in the ways outlined below. We particularly seek your views in response to the specific questions we have posed. These are summarised on page 9. You may respond to all questions or just those relevant to your specific views.

Ways to feedback:

Make notes

Throughout the document, we have provided space for you to read and make notes at the start of each chapter (opposite). Use the section numbering as a way to reference accurately. You can then type up your notes and send them in an email or submit them online.

Interactive pdf notes

Alternatively, we will be sending out editable pdf versions of this document with note fields for you to type directly into.

Email

We have a dedicated email address specifically for your feedback to this document. We welcome your thoughts at: **gary.stokes@nationalgrid.com**

Alternatively, you can put your thoughts in writing and send to: **Gary Stokes, National Grid House, Warwick Technology Park, Gallows Hill, Warwick CV34 6DA.**

Online

You can go directly to the website and submit your comments here.

You can learn more about how we are working with stakeholders by visiting our website. This site makes it easy to follow our progress and shows you how to get involved.

Please share your thoughts:

Type here>