10. We will protect the network from external threats

What you can find in this chapter

What this stakeholder priority is about

This stakeholder priority is about how we protect our network from external threats such as cyber-attacks, physical attacks and extreme weather. It also ensures we can respond to and recover from incidents when they happen.

Due to the confidential and sensitive nature of our cyber security and physical security business plans, we are unable to fully share detailed information with stakeholders and have agreed to provide our plans directly to Ofgem for assessment. Included within our submission are the two cyber business plan documents requested by Ofgem, these are:

1. Business IT Security Plan
2. Cyber Resilience Plan

What you have told us so far

Your daily lives are becoming more dependent on an available supply of electricity. You want us to protect the electricity transmission network from threats that could impact your supply of electricity. You also want us to be able to quickly recover from incidents if they happen to minimise disruption. As well as responding to stakeholder views, many of the investments in this chapter meet new and expected regulations that have been introduced to minimise the threat against our network.

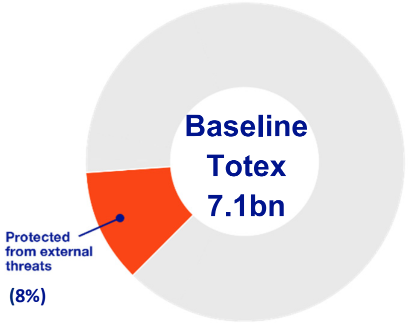
What we will deliver

We will invest over £550m to protect the network from threats such as cyber-attack, physical attack and extreme weather. As a result, we will be able to prevent, withstand, respond to and adapt to the impact and/or duration of such events.

Due to the frequent change in threats, we also propose ways in which future changes in requirements and business plans can be managed to protect consumers. The uncertainty mechanisms we propose in this chapter will help us to be agile so that we can respond to new intelligence or expected changes in the threats we face throughout the T2 period.

The total cost of delivering these baseline proposals is £555m. This represents 8% of the overall business plan as reflected in figure 10.1 below.

Figure 10.1 Proportion of expenditure



1. What this stakeholder priority is about

This stakeholder priority is about how we protect our network from external threats such as cyber-attack, physical attack and extreme weather. It also ensures that we can respond to and recover from incidents when they happen. By doing this, we will minimise the impact of any incidents on our customers and end consumers.

We will manage external threats in a way that is supported by the Government, relevant agencies and stakeholders to minimise the impact of any incident. We will invest to protect our network from a range of threats. We will also improve capabilities to respond to and recover from any incidents quickly and effectively, including incidents which cause a full or partial shutdown of the network.

Sectors that provide consumer services within the UK are more integrated than ever before. With Electricity Transmission enabling services such as transport, media and communications, it is essential that any loss of power event is kept at a minimum and that power supply is restored as quickly as possible. This has also been recognised by Government and many of the investments in this chapter are driven by increased regulation to protect the network from threats.

Some of the topics in this chapter are either of a confidential or sensitive nature which means that we have only shared a limited amount of information on our business plans with our stakeholders and the RIIO-2 Challenge Group. We have agreed that we will share the required information directly with Ofgem to allow them to assess our business plans in this area.

The investments outlined within this chapter are consistent with and complimentary to those in chapter 9 *We will provide a safe and reliable network.*

2. Track record and implications for T2

Investments in this chapter are split into five categories that improve our ability to identify, detect, protect, respond to and recover from threats. These categories are:

2.1 Extreme weather
2.2 Physical security
2.3 Cyber security
2.4 Operational Telecommunications (OpTel)
2.5 Black Start.

Costs and outputs in the T1 period

Our performance in T1 and the learning we take forward into our T2 plan is outlined below;

Table 10.2 Costs and outputs for the T1 period

Category	Target	Forecast	T1 allowance (£m)	Forecast cost for T1 (£m)
Extreme weather	45-55 sites	49 sites	145.4	124.57
Physical security	25 sites	33 sites	289	259.39
Cyber security (information technology)	n/a	n/a	5.8	17.92
Cyber security (operational technology)	n/a	n/a	n/a	48.79
OpTel	Control telephony at 300 sites	Control telephony at 300 sites	69	43.37
Black Start	n/a	n/a	n/a	n/a

We have delivered our planned investments efficiently and developed alternate solutions which reduced the threat (avoiding mitigation measures) and delivered more cost-effective solutions where appropriate. Further detail on these can be found within ‘Innovation in the T1 period’ below.

For **extreme weather**, we took a flexible approach to flood protection due to potential changing requirements. By developing site specific solutions as and when investment was required, we made sure that:

- only sites which had a risk of flooding were targeted for investment, and
- mitigation solutions could be adapted to site specific needs.

Site solutions were developed using guidance provided by the Energy Networks Association through their Engineering Technical Report (ETR) 138 ‘Resilience to Flooding of Grid and Primary Substations’, in conjunction with the local Environment Agency and provide a coordinated energy sector response to the threat of flooding. Our investments in the T1 period and those planned in the T2 period protect from low probability, high impact events. However, events such as that at Whaley Bridge in August 2019 and the widespread flooding in northern England in November 2019, show that these investments are critical in protecting substations from flooding and the resulting impact on consumers.

Our plans to protect sites from **physical attack** changed through the T1 period as determined by the Physical Security Upgrade Programme (PSUP). The PSUP is a government mandated initiative to protect the UK’s most essential infrastructure. The Centre for the Protection of National Infrastructure (CPNI) work alongside the Department of Business, Energy and

Industrial Strategy (BEIS) to combine their privileged access to information and threat intelligence to analyse and inform risk assessments. They specified the security measures we implemented.

Our physical security plans and associated allowances were managed using two re-openers; one in 2015 and one in 2018. The final agreed targets were to deliver security enhancements to 25 sites, for which we received allowances of £289m. We are forecast to deliver enhanced site security to 33 sites by the end of the T1 period. This is due to starting work on sites earlier in the T1 period, which have later been removed from the PSUP list, in conjunction with BEIS, because of a change in threat or requirements.

We did not request allowances to manage the threat of **cyber-attack** on our Operational Technology (OT) in the T1 period. At that time, we managed our cyber security at a global IT level addressing more 'established' means of cyber-attack on IT systems, for which £5.8m allowances were received for Electricity Transmission. Due to the increased threat and introduction of new requirements, we plan to invest a total of £17.92m on IT cyber resilience. This is an allocation to NGET from our IT shared service.

We actively monitor cyber threats 24/7 and use threat intelligence from specialist agencies to inform our cyber strategy and investment plans. We have been flexible to meet new cyber requirements and mitigate risks as they arose. This includes the emerging threat against OT, for which there are now requirements to protect. This has resulted in forecast expenditure of £48.79m in the T1 period. We are currently trialling solutions and vendors in preparation for our T2 cyber investments. By being agile in the T1 period, we have responded to new threats and developed long-term strategies on how to maintain a network resilient to cyber threats.

Our **Operational Telecommunications (OpTel)** network is made up of optical fibres that run on our overhead line network connecting our substations and electricity control rooms. It is essential infrastructure for the daily operation of the network and plays a vital role in the communications required to protect the network from threats. In the T1 period, we have completed the replacement of telecoms assets at 300 substations and migration of legacy services commenced prior to the T1 period. We have implemented a new telecoms network management control centre and replaced legacy end of life control telephony.

We did not receive any specific allowances for **Black Start** in the T1 period. As part of our standard performance, we have managed our assets to an agreed level to maintain security of supply and therefore any costs that support our T1 Black Start preparedness were covered by our asset maintenance expenditure.

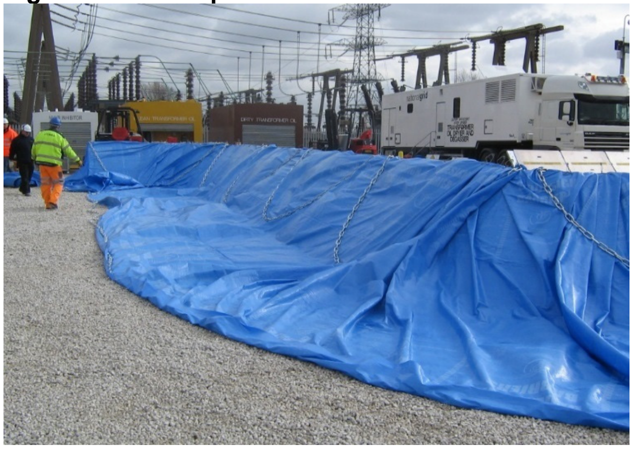
Further information on our T1 performance can be found within the relevant Investment Decision Packs (IDP) and other requested plans as follows:

NGET_A10.04 – Business IT Security Plan (Confidential)
NGET_A10.05 – Extreme weather
NGET_A10.06 – Physical security (Confidential)
NGET_A10.07 – Black Start
NGET_A10.08 – OpTel refresh
NGET_A10.09 – Cyber Resilience Plan (Confidential)

Innovation in the T1 period

We have delivered our T1 plans using innovative approaches where possible. One example of which is on extreme weather. We have worked with the Environment Agency when developing site specific flood solutions in the T1 period to identify whether we can deliver joint offsite environmental solutions such as flood diversion. These solutions remove or reduce the risk to National Grid sites and drive further value for consumers by delivering more cost-effective investment. We have continued to use removable flood barriers, that can be shared between sites, where possible, to further mitigate the need for investment to protect from tidal and river flooding. These barriers have been utilised many times throughout the T1 period, including at one of our sites during the 2019 dam incident in Whaley Bridge. Figure 10.3 below gives an example of these barriers in use.

Figure 10.3 Example removable flood barrier use



We have also coordinated our threat protection activities, for example by combining the delivery of weather and physical resilience works to deliver more efficiently.

Whole system approach

Whilst we play a key role in ensuring a resilient electricity network, considerations and plans must be made across the whole system in this area. Our approach to physical security and weather resilience is guided by BEIS and provides a coordinated sector response to these threats, by defining critical and priority sites and threat mitigations. On cyber, we have engaged with the other TO's to share our view on threats, risk against assets and required mitigation for OT both within the T1 and T2 periods. This encourages a consistent approach to risk mitigation and allows us to understand where we can work together to deliver joint solutions or share best practice and learning going forward. More information on this engagement is provided within annex NGET_A10.01 Engagement log.

Learning for T2

Our experience on weather resilience and physical security during the T1 period has provided us with credible cost data and has informed our delivery approach for the T2 period, enabling us to build proven efficiencies into our T2 proposals. Our T2 investment to protect from [redacted]

External threats have the potential to change significantly in a short period of time. We must be flexible in how we manage and mitigate threats to keep our network protected. The need to adapt plans on a regular basis is a key learning from the T1 period and this is reflected in our request to include uncertainty mechanisms within the T2 period across the topics outlined in this chapter.

3. What our stakeholders are telling us

Our stakeholders want a continuous supply of electricity and want as little disruption as possible. They understand the threats we face and the impact that those threats could have on our network reliability. They want us to manage these threats in a way that is informed by relevant specialists and is appropriate and proportionate to the level of risk on our network. The Energy Research Partnership (ERP) report on the future resilience of the UK electricity system states:

“There is a growing trend of society and business becoming increasingly reliant upon new technology, broadband and communication; all requiring electrical energy and ultimately leading to an increased interdependency between sectors. Furthermore, the world is changing; from climate change including extreme weather events, through to an increase in malicious intent to affect networks.” *(ERP, November 2018.)*

With the growing business and societal reliance on electricity, we must protect the network from existing threats and also deliver a network that provides future resilience beyond the T2 period. The investments we have planned will build the foundations for future resilience by addressing immediate threats, enhancing our capability to monitor and respond to incidents and conducting further research into future requirements for resilience. One key area of investment on network resilience is our OpTel network. OpTel is vital to providing overall network resilience and the capabilities to effectively monitor the network for threats and respond to them efficiently.

We are engaging with our stakeholders on the topic of resilience via established industry forums including the CIGRE Power Systems Resilience Group. The messages we are hearing highlight challenges in determining appropriate levels of resilience for the future. These challenges are consistent with those summarised in the ERP report on future resilience.

Stakeholders want us to focus on ensuring we are effectively protected from the threat of cyber-attack. Cyber-attacks have grown in both sophistication and frequency throughout the T1 period. They are now used throughout the world as a means of political attack and warfare. The threat against OT has increased and has been evidenced by several notable attacks globally including the 2015 attack against the Ukraine electricity distribution network. This attack resulted in several outages that caused approximately 225,000 consumers to lose power supply. The Government’s National Cyber Security Strategy recognises the threat against OT as follows:

“The rapid implementation of connectivity in industrial control processes in critical systems, across a wide range of industries such as energy, mining, agriculture and aviation, has created the ‘industrial internet of things’. This is simultaneously opening up the possibility of devices and processes, which were never vulnerable to such interference in the past, being hacked and tampered with, with potentially disastrous consequences.” *(National Cyber Security Strategy 2016-2021)*

We have informed and consulted stakeholders where possible

We are unable to engage widely on our cyber security and physical security plans due to their sensitive nature. Our stakeholders understand the challenge with engaging on this topic and have told us that they want us to engage with the few stakeholders who have the knowledge or authority to inform our business plans to ensure our level of investment is appropriate and proportionate to the risks we face. We have provided further detail on the specific feedback received from the workshop and consultation in our engagement log.

We have also conducted willingness to pay research on Black Start, which concluded that consumers would be willing to pay more for faster response times in the event of a total system shutdown. More information on this can be found within annex NGET_A6.04 Willingness to pay report.

We are also engaging with the Scottish TOs and DNOs who have similar risks, to help create a view of the whole electricity system and approach to risk mitigation. We have also shared best practice across the National Grid Group including Gas Transmission, NGESO and our US business.

We have worked with government and specialist agencies to develop our plans

We have engaged with government and relevant specialist agencies to ensure our plans meet those requirements and are proportionate to the risk we face. For each threat area, these stakeholders include:

Weather – BEIS and Environment Agency
Physical security – BEIS and CPNI
Cyber security – Ofgem and BEIS (as NIS Competent Authority – see below) and the National Cyber Security Centre (NCSC)
Black Start – BEIS
Optel – CPNI

The need for the significant increase in cyber security investment when compared with the T1 period is driven by new regulations and the increasing cyber threat. The Network and Information Systems (NIS) Regulations were implemented in May 2018. They aim to increase the overall level of cyber security across operators of essential services in the EU. We have worked with the NIS Competent Authority (a joint role held by Ofgem and BEIS) to ensure our plans reflect the investment required to meet these new regulations. This approach has been agreed and is consistent with all other parties governed by these regulations. We provide as supporting documents to this submission the two cyber documents requested by Ofgem in their Sector Specific Methodology Decision. These are:

1) Annex NGET_A10.04 Business IT Security Plan, and;
2) Annex NGET_A10.09 Cyber Resilience Plan.

These documents have been structured to meet our requirements under both RIIO-2 Business Plan guidance and the NIS Regulations.

We have also provided our previous NIS submissions to further support our business plans. These are:

1) Annex NGET_A10.02 NIS Improvement Plan
2) Annex NGET_A10.02A NIS Self-Assessment

A summary of our engagement activities and outcomes is provided in table 10.4 below, alongside what trade-offs have been made and how stakeholders have influenced the plan. The engagement log contains detailed information on our engagement approach and outcomes. This can be found in annex NGET_A10.01 Engagement log.

Table 10.4 Summary of our engagement

	Engagement on protecting the network from external threats
Purpose and approach	We have engaged with a variety of stakeholders through different methods and forums to understand general stakeholder views on resilience and protection from threats as well as specific requirements under this topic. To understand specific requirements and guidance which we were expected to follow, we engaged with stakeholders as follows: • **CPNI and BEIS** – bilateral and continuous engagement throughout the T1 period to inform our PSUP risk position and action required. • **NIS Competent Authority (BEIS and Ofgem) and the NCSC** – bilateral meetings, specific NIS focused workshops and industry engagement within the Energy Emergencies Executive Committee to inform cyber risk position and required works. • **BEIS and industry parties** – through the Black Start Task Group to contribute to the discussion and proposal of a Black Start standard. • **BEIS and industry parties** – through the ETR138 working group to understand T2 guidance on protection from surface water flooding and BEIS's expectations for network companies to comply.

	Engagement on protecting the network from external threats
What stakeholders told us	General stakeholder views gained through our engagement are outlined within the supporting stakeholder engagement log for this topic annex NGET_A10.01 Engagement log. Due to the confidential and/or sensitive nature of our plans, stakeholders have told us to engage with relevant specialists where possible to develop and agree appropriate solutions. These relevant specialists have proposed that we: 1. implement the revised standards set out in Engineering Technical Report (ETR) 138 (requirements for site flood protection) by the end of the T2 period. See annex NGET_A10.10 Extreme weather assurance letter 2. implement required levels of physical security on designated PSUP sites 3. implement agreed cyber security enhancements in line with NIS Regulation guidance 4. ensure rapid restoration in a Black Start scenario in line with BEIS proposals.
Key trade-offs and how engagement influenced our plans	• We have prioritised OT cyber enhancement works on several sites within the T1 period to implement appropriate levels of security on our more critical sites. This allows us to drive efficiencies, trial available solutions and adapt our longer-term plans to protect all sites if the threat or requirements change within the T2 period. We consider this appropriate in the short term to both protect our sites and meet NIS requirements. • We currently do not plan to protect all sites at risk of surface level flooding. Our estimates have been based on learning from sites requiring work within the T1 period. We expect some sites within flood risk zones to have appropriate landscape or infrastructure in place which reduces this threat. We also expect alternate solutions such as offsite environmental solutions to be a possibility. • Our key stakeholders have had a major influence on our T2 business plans, our engagement has informed what we do when protecting against cyber-attack, physical attack and extreme weather. • We commissioned Frontier Economics to carry out assurance of how our stakeholder engagement had been reflected within our July draft business plan. They assessed how well the logic between stakeholder evidence and business plan actions had been documented, and identified gaps or areas of improvement. Frontier note that overall, the stakeholder engagement on this topic is challenging given that security plans often cannot be shared with stakeholders due to confidentiality. However, the stakeholder engagement on this topic appears to be comprehensive and well-designed and that we have clearly attempted to provide stakeholders with a necessary level of knowledge to express informed views. One piece of feedback received and addressed within our business plan was 'On physical security, it could be made clearer in the business plan that action around the Physical Security Upgrade Programme is a government mandated requirement, and is not driven by the views of wider stakeholders'. Within the engagement log, we have provided an overview of all the feedback received from Frontier on our engagement and provided detail on how this has been addressed within our business plans.
How we've responded to the Independent Stakeholder Group and Challenge Group	• Due to the nature of the investments within this chapter, the **Independent Stakeholder Group** and **RIIO-2 Challenge Group** have not been able to provide a great deal of feedback on the detail of our plans, but have influenced our approach and guiding principles. • We have, however, welcomed feedback on this chapter, have clarified points about which were unclear and provided additional detail on our OpTel and cyber investments in response to feedback received.

4. Our proposals for the T2 period

Our proposals to mitigate the threat of extreme weather are similar to investments made in the T1 period, however, with a wider scope as a result of updated ETR138 requirements and the need to address threats such as erosion and climate change. Our physical security proposals address security at [redacted] commissioning in the T2 period in line with existing PSUP requirements.

Our plans to enhance cyber security form a significant part of our expenditure in this area. This represents an increase on T1 costs due to a step change in threat against OT and the need to follow the guidance under the new NIS Regulations. Due to the level of uncertainty around longer-term cyber investment, we have separated our T2 cyber proposals into two categories for both of the cyber plans being submitted.

1. **Baseline request** – known and measurable solutions to existing threat, with high confidence in cost
2. **Uncertainty** – expected expenditure to be requested via a reopener within the T2 period

Our uncertainty category accounts for expected expenditure where we know there is a risk that needs to be mitigated, however, the solution or costs have not yet been fully developed. It also includes investments that are planned later within the T2 period. These are not included in our baseline request due to expected changes to the cyber threat and our need to be flexible with our business plans. We also acknowledge that our forecast uncertainty expenditure may change between now and the planned reopeners due to potential change in threat or requirements.
Our Black Start plans include investment to improve the performance of key assets to achieve the proposed BEIS restoration target.
We will invest to safeguard the OpTel network [redacted]

[redacted]

Our proposals provide a direct benefit by enhancing our resilience to incidents that threaten the security of supply of electricity to end consumers. They will enable us to better protect our assets and infrastructure and more effectively and efficiently respond to incidents as they occur. In conjunction with the initiatives outlined in chapter 9 *We will provide a safe and reliable network*, these proposals ensure that consumers continue to receive a secure supply of electricity that is becoming increasingly critical to their everyday lives. Table 10.5 below outlines how what stakeholders are telling us links to the proposals we are making and the consumer benefit of these proposals.

Table 10.5 Our proposals for the T2 period

Stakeholder feedback	Our proposals	Output type	T2 Baseline (£m)	Consumer benefit
Requirement from BEIS for all network companies to implement the revised standards set out in Flood Resilience Engineering Technical Report 138 by the end of RIIO T2.	**Extreme weather:** Protect our sites from surface level flooding and better understand how we protect from weather-related threats in the long term. We will enhance flood protection on a proposed 100 sites as well as addressing increasing erosion incidents and developing a long-term climate change strategy.	PCD	59.81	All sites at risk of surface level flooding will be protected by the end of the T2 period, protecting end consumers from loss of supply because of substation flooding.
CPNI/BEIS requirement to implement required levels of Physical Security on all designated PSUP sites.	**Physical security:** Continue to meet our PSUP requirements at all designated sites. We will enhance physical security on [redacted] commissioning within the T2 period.	PCD	44.63	All PSUP sites will be protected from physical attack, reducing the risk of loss of supply to consumers because of a physical security incident.
Formal legislation for all operators of essential services to implement agreed cyber security enhancements in line with NIS Regulation guidance. Final risk reduction based plan to be agreed with the NIS Competent Authority.	**Cyber security:** Enhanced cyber security and capabilities to a level agreed with the NIS Competent Authority. Implementation of investments across OT and Information Technology environments aligned to the NIS Cyber Assessment Framework.	PCD	16.84 (IT) 167.54 (OT)	Many cyber-attacks purposely aim to cause disruption such as loss of electricity supply. Effective protection and enhanced capabilities to respond to incidents minimises the impact on consumers if a cyber incident was successful.
Maintain a network resilient to external threats within the T2 period and beyond.	**OpTel:** Highly resilient and cyber secure operational telecoms infrastructure, essential for the safe and reliable operation of the system, supporting physical security management and Black Start capabilities. We will **replace 1,850km of fibre-wrap**, which has reached end of life, and telecoms equipment at **274 sites.**	PCD	241.02	Provides ongoing overall system resilience by enabling communication and operation activities during and following incidents arising from system incidents and external threats.
Ensure rapid restoration in a Black Start scenario to meet requirements of proposed BEIS restoration standard.	**Black Start:** Enhanced system and people capabilities to ensure an efficient and effective response in a Black Start scenario. We will install **high performance LVAC systems at** [redacted] and **resolve technical limitations on** [redacted].	PCD	22.19	Allows for a faster restoration of supply of electricity to end consumers in the event of a Black Start scenario.

5. The justification for our proposals

Our proposals will be delivered by the activities outlined within this chapter, which we have ensured meet the relevant requirements and guidance available for each threat area. The solutions that have been selected have been through a robust process which considers various options to deliver the required output, with Cost-Benefit Analysis (CBA) being conducted where possible at this stage. Lessons learnt have been captured from previous investment and incorporated into future projects. The proposed expenditure is efficient and has been subject to unit cost comparisons, cost audits and benchmarking where appropriate.

We have provided our view of our less certain costs under the cyber uncertainty category to ensure these proposals can be further developed and allowances requested once these costs and solutions can be well justified. The proposed reopener mechanisms will also ensure allowances can be adjusted appropriately should requirements change in the T2 period.

Key drivers

There are two key drivers for all the investments included within this chapter, these are:

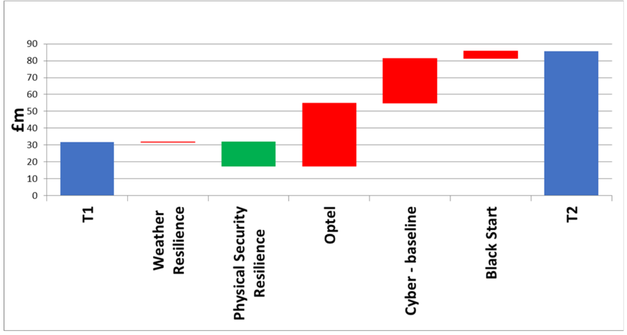
1. **change in threat**
2. **change in requirements.**

Most importantly, we must ensure that the network is adequately protected from the threats we face and ensure that any impact on end consumers is minimal. To help assist with this, there is legislation and guidance in place to ensure appropriate levels of security and capability exist. The legislation and guidance that we are following for each threat category are listed below:

Extreme weather – ETR138 (guidance on flood protection) and request from BEIS that this is implemented within the T2 period.
Physical security – PSUP (BEIS requirements advised by CPNI to apply to all CNI sites on the PSUP list).
Cyber security – NIS Regulations (Ofgem and BEIS governed legislation)
Black Start – Proposed BEIS standard (to be introduced into legislation or industry code)
OpTel – Industry standards (guidelines adopted by NGET, consistent with other TOs)

The impact that this legislation and guidance has on our expenditure in comparison to our actual capex expenditure in the T1 period is illustrated in figure 10.6. This graph has been provided in response to a request from the RIIO-2 Challenge Group. The figure compares annualised capex expenditure for the first six years of the T1 period with our proposed T2 investments. The main increase in expenditure is as a result of enhancing our cyber security and the refresh of the OpTel network. This is due to new cyber threats and requirements which have emerged throughout the T1 period and our OpTel assets (which were commissioned in the 1990s) reaching end of life. Due to the significant progress made in protecting the network from physical attack within the T1 period, there is a net reduction in physical security expenditure, with extreme weather expenditure remaining flat in the T2 period. Figure 10.6 does not include forecast investment of c£200m, primarily in extreme weather, physical security and cyber in the last two years of the T1 period which would result in annualised expenditure of £62m. Cyber expenditure in the remainder of the T1 period is in response to NIS regulations and helps to prepare for delivery of our T2 investments.

Fig 10.6 Change in capex expenditure from T1 to T2



Increasing consumer and economical reliance on a constant flow of electricity as demonstrated through the ERP report findings, and through our own engagement with stakeholders, drives a need for higher levels of resilience across the whole network. The need for greater resilience on our network is driving our investment in Black Start and OpTel, as well as consideration of other whole system solutions.

Consideration of options

All of our proposed investments have undergone options assessment, considering different options available to mitigate the threats we face. The options considered for all investments included the options to;

1. **do nothing**
2. **defer investment to T3 or beyond.**

As there was a need to address priority threats within the T2 period, the majority of options considered related to timing, value of investment or level of protection or capability applied. Consideration of these options ensured we are taking an approach that is proportionate to the risk against our network. In all cases, we are taking an approach to protect our most critical or vulnerable assets and sites to ensure maximum benefit. This option will be deliverable and ensures we are not investing more than necessary for consumers, whilst still meeting the guidance and requirements available. In some cases, this has led us to phase investment across the T2 and T3 periods. We have also conducted Cost-Benefit Analysis (CBA) where appropriate to compare options. Further information on our options assessment and CBA for individual investments can be found within the supporting Investment Decision Packs and cyber plans.

We have commissioned external technology specialists, see annex NGET_A10.08A Wavestone report, to conduct a review of future requirements of our OpTel network and consider cost effective ways of delivering this service in the future. Key findings from this review conclude that that current performance should be maintained or enhanced and requirements for such can only be met by a dedicated fibre-optic based solution, supporting our proposed outputs in this area.

Due to new requirements to protect OT from cyber-attack, we have split our proposed costs into a baseline allowance request and a reopener within the T2 period. The split of our investments was informed by our options assessment, with the 'baseline' representing a view of the projects we have high confidence in the required solution and costs. Those investments included within the 'uncertainty' category are either planned later in the T2 period, do not yet have mature solutions available or would benefit from solutions being trialled prior to deciding on an appropriate route. This approach helps to drive efficiencies and value for money for consumers as we will only request allowances where we have a high degree of confidence in costs and appropriateness of solutions.

Outputs to be delivered

To achieve the appropriate levels of security and resilience in line with requirements and guidance, that are proportionate to the risk we face, we propose the activities and outputs outlined in table 10.7 below.

Table 10.7 Proposed activities for the T2 period

Proposals	Activities	Volume/capacity
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
Proposals	**Activities**	**Volume/capacity**
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Cost justification

Our baseline expenditure is efficient and can be split into two categories based on how they have been forecast:

1. Costs based on T1 performance and actual costs, existing tenders etc.
2. Requirements for works are new and therefore we have conducted benchmarking where possible.

Our plans for **extreme weather** and **physical security** are based on existing requirements for which we have delivered programmes of investment within the T1 period. Our costs have been based on historic spend, building in efficiencies where possible for T2. T1 PSUP costs have been subject to independent technical and value for money audits and align with comparable Gas Transmission benchmarks. The majority of costs passed technical and value for money audits with no issues, with a small percentage of costs referred to Ofgem for their review. All these works in T2 will be competitively tendered.

The majority of our T2 expenditure on physical security will be on [redacted] sites requiring security measures to be in place, resulting **£24.4m** investment. The remaining **£3m** is to be spent on ongoing maintenance activities. The remaining **£17.2m** of costs outlined within our cost table are ongoing opex costs for managing the physical security on a day to day basis.

The majority of our **cyber security** investments are in response to new threats and requirements. For this reason, our costs have been supported by external benchmarking and tenders where possible. In late 2019, we conducted benchmarking on our approach, methodology and costs for the investments included within our Business IT Security Plan. This concluded that we were within range on cost and level of capability when compared to utilities worldwide. Further information about our benchmarking activities against our key cyber investment areas can be found within annexes NGET_A10.04 Business IT Security Plan, NGET_A10.09 Cyber Resilience Plan and NGET_A10.11 Cyber Benchmarking (Gartner).

Where we have not been able to provide sufficient justification for our costs, these have not been included within our baseline allowance request. Further research into viable options and assessment of costs for chosen solutions will be completed prior to requesting adjustments to allowances within the T2 re-openers.

Black Start costs are based on efficiently incurred costs for LVAC asset replacement in the T1 period, and standard times for maintenance and testing activities.

Our **OpTel** costs are based on learning and experience from OpTel and associated projects during the T1 period, and efficiently incurred costs for the deployment of Optical Path Ground Wire (OPGW) during our T1 overhead line refurbishment plan. Our OpTel costs incorporate planned efficiencies from aligning OpTel and overhead line refurbishment work in the T2 period and are phased to deliver capacity at the point when it is required.

Benchmarking and efficiency

Gartner conducted a benchmarking exercise, see annex NGET_A10.11 Cyber Benchmarking (Gartner), on our cyber resilience methodology and business plans. This demonstrates our proposed cyber investments are aligned to market costs for equivalent capabilities based on scale, scope, geography and complexity. Our plans have not changed as a result of this benchmarking since October 2019. Our physical security costs have been subject to a value for money audit within the T1 period and are comparable to Gas Transmission benchmarks. The remainder of our costs are informed by historical costs and efficiencies from the T1 period.

We are also making stretching commitments to future efficiencies, applying a **£3m productivity commitment** to improve the productivity of our people by 1.1% year on year. Further detail is provided in Chapter 14 – *Our total costs and how we provide value for money*.

BAU Innovation

The NIS Regulations are driving cyber investment in the T2 period. This has enabled us to engage with the NIS Competent Authority and implement enhancements to our cyber security within the T1 period. [redacted] We will continue to utilise options for delivery on physical security and flood protection as used within the T1 period, aligning these investments to minimise impact and drive efficiencies.

Enabling whole systems

As mentioned previously, cyber security on OT is a fairly recent need and therefore we have not yet explored all options for whole system solutions in this area. We have engaged with the Scottish TOs to understand where this will be possible as the risk to OT spans the entire network. We will expand our engagement to other network companies and consider opportunities to develop whole system solutions. The decision to allow for re-opener opportunities within the T2 period also allows us to engage further and develop whole system solutions in this area.

How we will deliver on cyber security

We are currently working with the NIS Competent Authority to develop and agree strategic plans for how to improve our cyber-security within the T2 period. Our investments will focus on [redacted] These plans are being developed using a risk-based methodology to ensure we are prioritising our most critical risks and systems.

[redacted]

Our detailed justification of our business plans for this chapter are included within the following annex documents:

A10.04 – Business IT Security Plan (Confidential)
A10.05 – Extreme weather
A10.06 – Physical security (Confidential)
A10.07 – Black Start
A10.08 – OpTel refresh
A10.09 – Cyber Resilience Plan (Confidential)

6. Our proposed costs for the T2 period

Our proposed expenditure in T2 is detailed in table 10.8 below. Further justification on how these costs have been benchmarked, and how our operational expenditure has been assessed as efficient is detailed within Chapter 14 *Our total costs and how we provide value for money*.

Table 10.9 shows the cyber uncertainty costs which are not included in our baseline submission but are included for transparency of our current view of T2 re-opener value.

Table 10.8 – Proposed baseline costs for the T2 period*

Baseline cost	21/22	22/23	23/24	24/25	25/26	Total T2	Annual T1	Annual T2	Subject to native competition	Internal historical benchmarks	External benchmarks	Subject to UM
Extreme weather	4.30	8.76	14.28	16.15	16.33	59.81	15.57	11.96	✓	✓		✓
Physical security	4.27	3.48	4.47	27.85	4.57	44.63	32.42	8.93	✓	✓	✓	✓
Cyber security (IT)	5.30	6.41	5.13	0.00	0.00	16.84	2.24	3.37	✓	✓	✓	✓
Cyber security (OT)	33.61	38.62	40.90	30.24	24.17	167.54	6.09	33.51	✓	✓	✓	✓
OpTel	26.71	42.47	66.39	48.22	57.23	241.02	5.42	48.20	✓	✓		
Black Start	4.39	4.39	4.47	4.47	4.47	22.19	n/a	4.44	✓	✓		✓
Supporting IS investment	0.52	0.67	0.64	0.53	0.51	2.86	0.17	0.57				
Total	**79.09**	**104.80**	**136.28**	**127.46**	**107.28**	**554.90**	**61.91**	**110.98**	**Cost certainty: High confidence**			
Pension allocation						**1.08**						

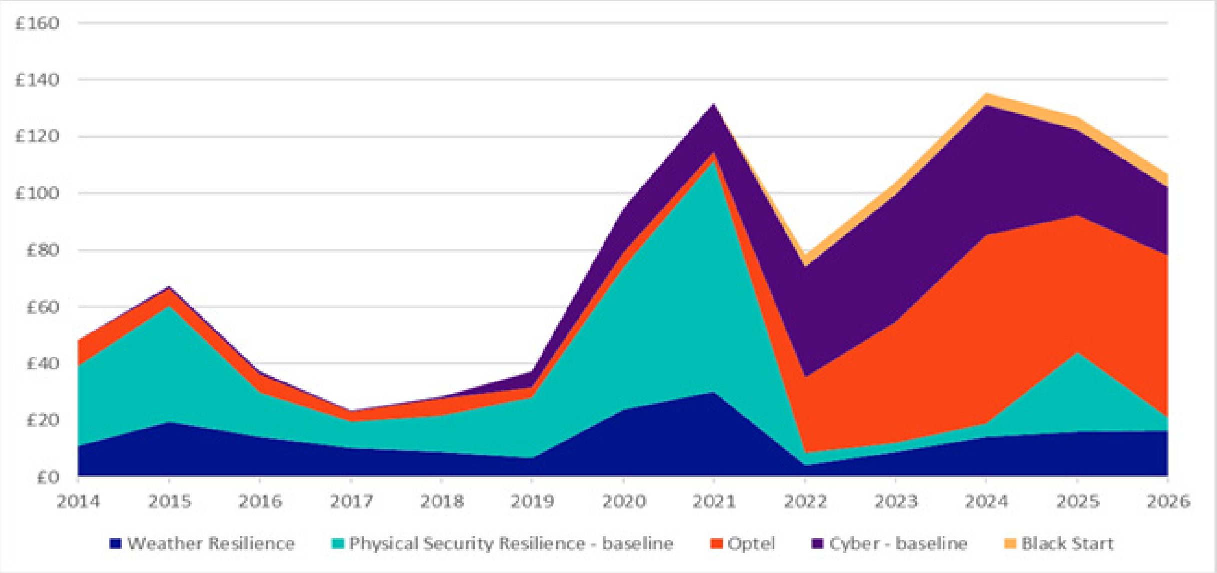
*Business Plan Data Table References: Extreme weather – C2.24, Physical security – D4.4a, D4.4b, OpTel – C2.25, Cyber Security (IT) –D4.8b, Cyber Security (OT) – D4.8a, Black Start – C2.12

Table 10.9 – Other potential expenditure for the T2 period

Other potential expenditure	Totex (£m)	Not in baseline due to…	Covered by UM
Cyber Security (Information Technology)	12.56	Costs for years 3 & 4 of our plan have not been included to account for likely change in cyber threat. This allows for projects to be delivered later in our T2 plan to be subject to further development and take advantage of newer solutions available within the T2 period.	Proposed uncertainty mechanisms for cyber security
Cyber Security (OT)	364.38	We are continuing to develop our cyber plans for the T2 period with the completion of some trial works within the T1 period. This allows us to test solutions and vendors for works to be requested through a T2 re-opener when the scope, solution and costs are more certain.	Proposed uncertainty mechanisms for cyber security

The figure below shows the baseline spend across the T1 period and proposed T2 expenditure for this topic.

Figure 10.10 Expenditure profile across the T1 and T2 period



Within the T2 period, we will be investing more in the areas of Black Start, cyber security and ensuring a resilient OpTel network. We are making these investments to ensure an approach in which there are several layers of defence from threats. This means that if an attacker was able to break a control, they would not necessarily be able to gain access to the information/data they seek or cause the disruption intended.

Our cyber security enhancements on OT are co-ordinated with our asset replacement and maintenance programme to drive efficiencies where possible and minimise any disruption to customers and end consumers. For the avoidance of doubt, the cyber investments in this chapter are above and beyond our general asset maintenance and IT investments.

7. How we will manage risk and uncertainty

We have no control over the nature of external threats, how they change and how quickly they change. In line with historic trends, we can expect that they will become more frequent and sophisticated in nature. We will manage the risk they pose by monitoring threats and having flexible business plans that we can adjust or reprioritise.

To ensure we can deliver the protection needed and that consumers only pay for what is necessary, we are proposing the following approach to managing risk and uncertainty:

- Baseline allowances for investments with known and deliverable outputs.
- Uncertainty mechanisms to account for uncertain costs or solutions, as well as potential changes to requirements in the T2 period.

The uncertainty mechanisms we are proposing will allow us to address new and emerging threats, respond to the latest threat mitigation guidance and meet new requirements as they arise. This will ensure that we can constantly assess the threats against the network and take the required action (as agreed with relevant authorities) to effectively protect the network and continue to deliver a secure supply of electricity to end consumers. We summarise the proposed uncertainty mechanisms in table 10.11 below.

Table 10.11 – Proposed uncertainty mechanisms for the T2 period

Topic	Why it is needed	Mechanism	Frequency
Extreme weather	Potential change to requirements outlined in ETR138 due to change in flood risk or extreme weather threat.	Re-opener	Once within the T2 period
Physical security	Potential change to physical security Upgrade Programme (PSUP) requirements or site-specific requirements. This may result in more or less sites requiring site security enhancements.	Re-opener	Twice within the T2 period (mid-way and end)
Cyber security	Change in threat, advance in technology, new requirements, greater certainty about appropriate solutions, reprioritisation of deliverables required.	Re-opener	Twice within the T2 period (at the start and mid-way) *
Black Start	Potential change in BEIS requirements.	Re-opener	Once within the T2 period.
Ensuring a resilient electricity network	Potential requirements resulting from ongoing engagement with stakeholders about applying enhanced levels of overall resilience to the network. This could also address enhanced resilience to new threats not currently addressed within T2.	Re-opener	Once within the T2 period.

*Within their Sector Specific Methodology Decision, Ofgem stated that there would be two re-openers for works included within the Cyber Resilience Plan (OT) and one re-opener for works included within the Business IT Security Plan (Information Technology). The threats we face are constantly evolving [redacted] For this reason, we consider it appropriate to also allow for a second re-opener for the uncertainty within our Business IT Security Plan.

We understand that it may be Ofgem's intention only to allow the first re-opener for OT if network companies chose not to submit their business plans in December 2019. Given the evolving cyber landscape on OT, we have provided a proposal for investments in which we have high confidence in scope, cost and deliverability with a view of required projects for which we are not currently seeking allowances.

The work we are completing to enhance OT cyber resilience within the T1 period will enable us to be in a more informed position at the first T2 re-opener opportunity to request allowances for these works. We therefore request that Ofgem allow network companies that have provided business plans in December 2019 to have use of the first re-opener within the T2 period. We expect a re-opener mechanism to take the form of a one-off submission to Ofgem within a defined scope of investment, that will be assessed and result in an agreed adjustment to allowances within the T2 period.

Probability and impact

The probability of requiring the use of a re-opener varies between topics. We consider it very likely that we will be requesting adjustment to allowances through the cyber re-openers in the T2 period. As the cyber NIS Regulations are relatively new, we expect to have frequent ongoing engagement with the NIS Competent Authority. This engagement will help us to keep up to date with their view of cyber risk, whilst also being informed by other sources and monitor delivery of our investments. We expect that this engagement will inform changes required to both our IT and OT cyber plans throughout the T2 period and subsequently inform adjustments requested to allowances through the available re-openers.

We do acknowledge that Ofgem have proposed that the Business IT Security Plan and the Cyber Resilience Plan should have separate regulatory treatment, with the Cyber Resilience Plan managed on a 'use it or lose it' basis. For this reason, we propose that the Cyber Resilience Plan is reviewed at the end of the T2 period to take account for any changes to plans and allowances through the re-openers.

On topics like extreme weather and physical security, requirements are clear and the threat is not expected to change quickly or significantly. The use of these re-openers is less likely but we consider them necessary in ensuring that changes to requirements can be addressed in a timely and efficient manner if required.

We are also proposing a re-opener mechanism that covers the need to enhance resilience of the electricity network. The electricity sector will experience significant change over the next ten years, with electricity increasingly used to decarbonise other sectors (e.g. transport and heat), leading to an increasing dependence on electricity, requiring greater resilience. Through ongoing engagement with stakeholders on future network resilience, we will continue to progress our focus on resilience measures and solutions. Further detail on how we plan to manage uncertainty can be found within the relevant Investment Decision Packs and also annex NGET_ET.12 Uncertainty mechanisms.

Next steps

We welcome questions from Ofgem on our proposals and propose ongoing engagement with Ofgem, CPNI, BEIS, and the NIS Competent Authority.