23. I want you to protect the transmission system from cyber and external threats

What is this stakeholder priority about?

UK infrastructure is subject to many security threats, that are increasing in sophistication and persistence. These threats include terrorism, criminality and vulnerability in information technology (IT) and operational technology (OT) systems. Our network is part of Great Britain's Critical National Infrastructure (CNI) and appropriate protection from threats is therefore essential to underpin the safety, security and reliability of the nation's energy supply. The UK Government sets the requirements for the appropriate levels of physical and cyber resilience that are to be achieved in the national interest.

What have you told us?

You say that the way we manage security threats should be a priority. We understand this is because you identify with the increasing threat both to society and to your own businesses. You recognise that disruption to the gas network and to your energy supplies would have immediate, direct and adverse consequences for you.

What will we deliver?

- Our RIIO-2 plan is to deliver the security hardening that has been mandated by the government, as efficiently as possible. This will improve the safety and resilience of the transmission system to ride through and recover from accidental or malicious events such as cyber-attack, which otherwise threaten to disrupt continuity of GB energy supply.

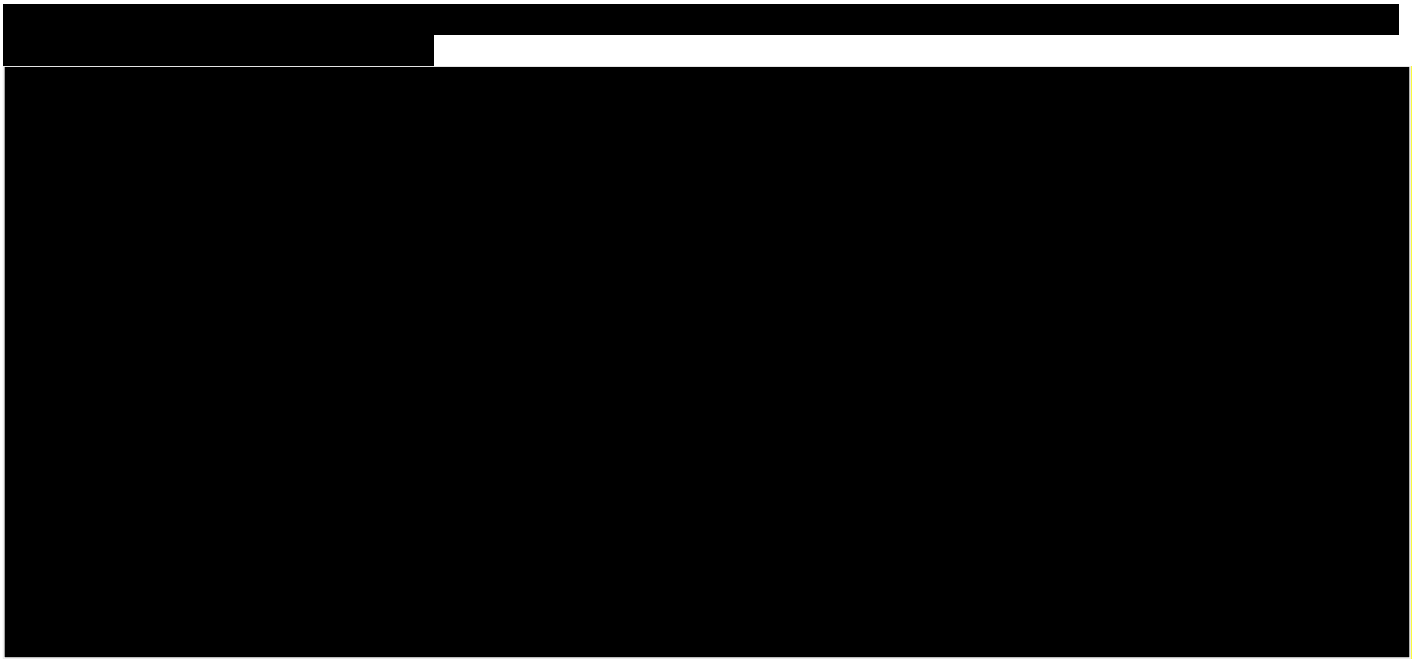
- We will deliver a strategic long-term programme to replace key operational technology used for the safety and control of critical systems. This work is driven by age and obsolescence as well as cyber resilience and the programme will extend through RIIO-3 and beyond.

- This is an area of significantly increasing expenditure driven by the growing level of threat and by new legislation steering the action that we must take to protect the network. Our plan includes £123.4m per year (21% of our RIIO-2 total costs) for this priority. We propose that funding for this known scope of work is included within our base revenue. Our plan does not include any provision for unforeseen costs that may arise from future changes in security requirements or in response to actual security events. We propose that uncertainty mechanisms allow us to adjust our scope and costs during RIIO-2 in response to changing circumstances.

What efficiencies have we included in our plan?

- Our physical security capex plan locks in 15% cost reductions so far attained in RIIO-1.

- Our operational technology capex plan incorporates efficiencies of around 30% through improved delivery contract strategies and bundling of work to maximise volume discounts from the supply chain.



1. What is this stakeholder priority about?

This priority is about protecting our network from threats that could otherwise disrupt continuity of GB energy supply, with serious consequences for society. We rely on industrial control systems to control and protect processes ranging from valves to compressor machinery. Loss or compromise of these systems could pose a serious safety risk – for example, failure to contain gas could result in fire or explosion with a knock-on impact on adjacent assets and facilities.

Our key activities and costs covered in this chapter include:

- strategic capability to monitor, detect, respond and recover from malicious threats
- Enhancing cyber security resilience
- delivery of the Physical Security Upgrade Programme (PSUP)
- policing at gas facilities as required by the Counter-Terrorism Act, 2008
- response to actual or new threats that emerge during RIIO-2.

We have consciously included our asset replacement costs for operational technology and enhanced physical security in this chapter rather than in chapter 22. We have done this because protection from threats is the primary cost driver and we expect specific RIIO-2 outputs to be attached to this work, separate to the NARMs asset health outputs.

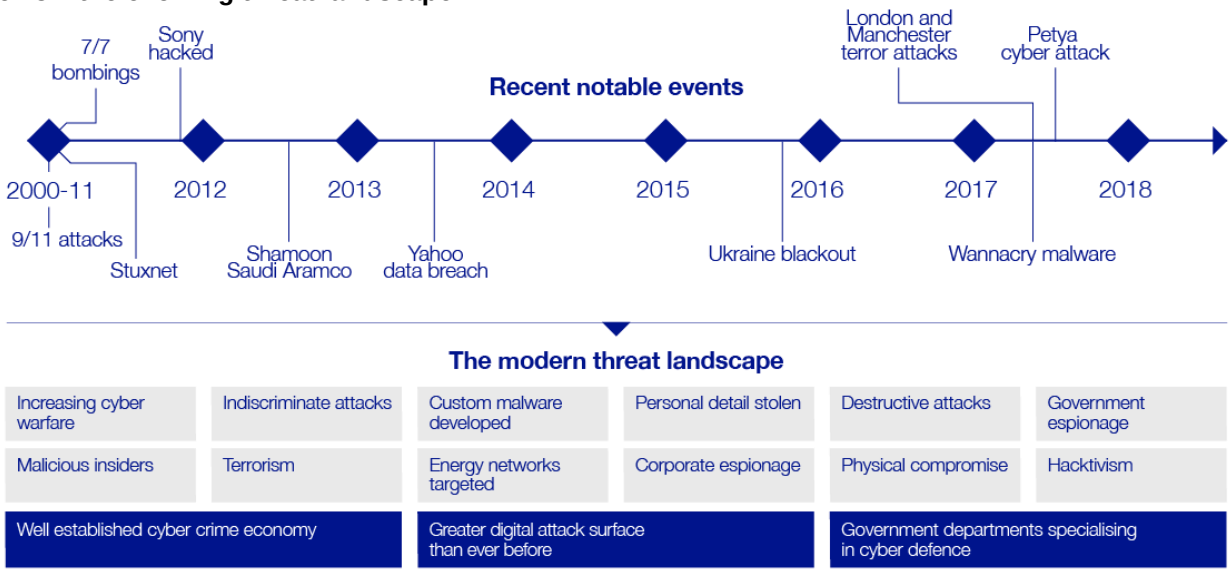
Evolving threat

The network was designed with sound engineering and safety considerations at the forefront, rather than with a mindset of protection from malicious threats. As threats emerged we mitigated them through a programme of physical security hardening at our sites leading up to the 2012 London Olympics, and this work has continued throughout the current price control.

Cyber security threat is the risk to computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide. The danger to energy systems is increasing due to the rapid digitisation of energy assets and the convergence of information technology (IT) systems (used for data-centric computing) with operational technology (OT) systems (used to control industrial processes and equipment).

The cyber threat landscape is evolving rapidly, and security experts think that, for every major cyber-attack in the public domain, four more major attacks are not reported. The energy sector has experienced a significant increase in the volume of reported attacks since the Iranian Natanz nuclear facility was attacked by ‘Stuxnet’ malware in 2010. Since then, Ukrainian energy companies have experienced attacks in 2015, 2016 and 2017. In 2017, there were reports that Saudi Arabia’s national oil company had suffered an attack on the safety computer systems designed to prevent disaster at its critical infrastructure facilities.

Figure 23.2 the evolving threat landscape



Security services process

Elements of our network are classified as critical national infrastructure (CNI). This means loss or compromise would have a major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life.

The UK Government, in conjunction with the Centre for the Protection of National Infrastructure (CPNI) and the National Cyber Security Centre (NCSC), set requirements for the appropriate levels of physical and cyber resilience to be achieved in the national interest. We work closely with these agencies to identify the most efficient way to meet these requirements, which call for significant operating and capital expenditure.

Some of our assets are co-located with those of other energy companies and it is important that we work closely with these and other operators of essential services to achieve joined-up protection across the energy industry. When considering the impact of any loss of gas transmission supply, the consequential impact on the electricity transmission network and market must also be considered; gas is our largest primary fuel source for electricity generation, typically accounting for around 40% of electricity production.

Mitigating cyber threats – the NIS Regulations, 2018

Heightened awareness of cyber threats is underlined in the UK Government's National Cyber Security Strategy[60] and through the launch in October 2016 of the NCSC[61]. The NCSC provides a single point of contact for expertise and guidance in the prevention of, and response to, cyber security incidents.

The requirements for a co-ordinated response across network companies have been established through the Security of Network and Information Systems (NIS) Regulations 2018[62]. The NIS Regulations aim to minimise the risk of cyber-attack and the resulting impact on UK CNI, the economy and consumers. This is in keeping with the NIS Directive[63] aiming to co-ordinate and raise overall levels of cyber security across the European Union (EU).

The NIS Regulations apply to a defined list of operators of essential services (OES), each with a relevant 'competent authority' (CA) supporting and monitoring compliance. We are a designated OES and within the energy sector the CA role is jointly held by the Department for Business, Energy and Industrial Strategy (BEIS) and Ofgem.

[60] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
[61] https://www.ncsc.gov.uk/
[62] http://www.legislation.gov.uk/uksi/2018/506/pdfs/uksi_20180506_en.pdf
[63] https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Mitigating physical threats – the Physical Security Upgrade Programme

The Secretary of State initiated the Physical Security Upgrade Programme (PSUP) and it is now governed by BEIS. It is a national programme to enhance physical security at CNI sites. Requirements arising from this programme have been a key driver of our activity both before and during the current regulatory period. This will continue through RIIO-2. We follow standards and guidelines for good practices endorsed by BEIS and CPNI[64].

2. Our activities and current performance and learnings from RIIO-1

Strategic capability to monitor, detect and respond to threats

Our shared-service corporate teams manage how we handle security threats. They work with the lines of business to understand how threats may affect business performance and to devise a balanced security strategy to mitigate these risks.

We have adopted a security standard based on five core principles[65] to drive a coordinated approach across personnel, physical, cyber and information security:

IDENTIFY what is important

PROTECT with appropriate risk-based controls

DETECT incidents and events, automate detection where possible

RESPOND to incidents and events

RECOVER what is important in line with agreed timescales and levels of business criticality

During the RIIO-1, period it has been a key focus to develop the capability of our organisation in line with the above principles. Training, awareness and the right security culture across our teams are as important for risk reduction as headline expenditure on hardware and software measures. Our people are our most important defence. All our operational personnel interfacing with operational technology undertake mandatory cyber security training. [redacted].

Enhancing cyber security resilience

A major cyber security breach of business, operational technology, and/or critical national infrastructure systems/data is one of the key operational risks monitored by the National Grid Board. It receives quarterly cyber security updates and board members have received cyber security training. We've included scenarios of cyber security breach and reasonable worst-case examples in our executive committee risk workshops.

In recent years, we have completed a series of assessments against the five principles to assess the level of our security and identify capability gaps and risks in line with the evolving threat landscape. We've worked closely with the security services to conduct these, as well as third party specialists and external auditors. The outcome of these assessments has driven the focus of our targeted risk mitigation activities in RIIO-1 and shaped our long-term strategy for RIIO-2 and beyond.

The three principal areas of our cyber security spending in RIIO-1, stemming from our targeted risk mitigation activities, are:

- data centres
- cyber security programmes 1 and 2
- NGGT specific cyber investments.

These three programmes have been funded during RIIO-1 through a re-opener uncertainty mechanism described below.

Enhanced security costs reopener

Ofgem provided a reopener uncertainty mechanism to adjust allowances for actual/planned enhanced security costs when those costs became more certain. As a result of our application in the May 2018 re-opener window our allowances for enhanced security costs were adjusted by £63.4m. These adjustments relate to the three key risk mitigation activities described above, for which additional output measures and reporting requirements have been established. For further information, refer to the reopener publications[66].

[64] https://www.cpni.gov.uk/protecting-my-asset
[65] https://www.nist.gov/cyberframework
[66] https://www.ofgem.gov.uk/publications-and-updates/informal-consultation-riio-1-price-control-reopeners-may-2018

Enhancing physical security resilience - Physical Security Upgrade Programme (PSUP)

We have been delivering enhanced physical security measures since before the RIIO-1 period, with expenditure ramping up from around 2010. During this time, we have worked very closely with the government to assist its assessments of the criticality of sites and evaluation of the most appropriate security solutions. It has been essential for us to be flexible about planning and delivering work due to changes in threat, priority or required response.

Our PSUP work is being delivered in phases. Security solutions for the phase one sites were completed by 31 March 2018, with all sites now being monitored by our alarm-receiving centre. Phase two work is ongoing and scheduled for completion by 31 March 2021, while phase three work is proposed for delivery during RIIO-2. The typical scope of a PSUP solution includes a mixture of the following physical elements:

- high security perimeter barrier, with substantive foundations and anti-burrow cills
- various controlled access points (e.g. vehicle gates, pedestrian access)
- intruder detection
- high technology closed circuit television and lighting systems
- power cabling and ducting
- on-site asset and building protection (e.g. transformers, switchgear, control rooms)
- on-site communications infrastructure (cabling, transmitters, receivers)
- two-way 24/7 communications to the central alarm-receiving centre.

Across our programme to date we have achieved capex efficiencies of around 15% and we are now forecast to complete our in-flight RIIO-1 work approximately in line with the 2015 allowance.

The May 2018 re-opener also considered potential adjustments to allowances to reflect work no longer required and future PSUP work at shared site locations where our assets are alongside those of other network companies such as gas distribution networks. The outcome of this process highlighted that, with our current methods, it would not be possible to deliver this additional work in the RIIO-1 period at a cost that Ofgem considers to be efficient for consumers. No further adjustment was made to our RIIO-1 allowances at that time. Ofgem will assess our efficient costs as part of the RIIO-1 close-out process.

In response to this challenge, we are re-evaluating our delivery model and targeting delivery of the shared sites with our phase three work in the RIIO-2 period. We have incorporated an £8m efficiency target in our RIIO-2 forecast compared to our view at the time of the May 2018 re-opener. We are reviewing our contracting approach and delivery methods needed to achieve this ambition and aim to update our cost efficiency evidence for inclusion in our December 2019 final RIIO-2 plan.

Policing costs

The Counter-Terrorism Act 2008, sections 85 to 90, governs the arrangements for policing at gas facilities. The security requirements and associated costs are set by the government and are outside our control. Because of this, our policing costs are recovered via a cost pass-through uncertainty mechanism.

Physical security – summary of current performance

In summary, the enhanced physical security we have delivered to date includes:

- security at our highest priority sites, which has been protected in line with government requirements
- enhanced security [redacted]
- working closely with the UK Government to assist their assessments of the appropriate security response in the national interest.

The key benefits delivered for consumers include:

- significant reduction in the risk of security breaches that could have severe societal consequences for GB consumers
- identifying sites where lower cost operational solutions can be deployed in place of costly physical measures and other sites where PSUP is no longer required, to make sure resources are directed efficiently
- 15% cost efficiencies in solution delivery during the programme so far.

3. What are our stakeholders telling us?

The direction of our plan meets your expectations

You've told us that the way we manage security threats should be a priority. We understand this is because you identify with the increasing threat to society and your own businesses. You recognise that disruption to the network and to energy supplies

would have direct, adverse consequences for you. There is a close interdependence between the work we do to protect the network from external threats, to enable consumers to use energy as and when they want (chapter 22) and to keep the gas system safe (chapter 21).

In 2017, we carried out public attitudes research in conjunction with [redacted] and found that the survey group (around 2,000 representative UK domestic consumers) placed a high priority on developing resilience to cope with a terrorist or cyber-attack.

At our shaping the future engagement events in autumn 2017 and our future needs of the network events in summer 2018, we explored your attitudes to security threats. Feedback included:

"Agree 100% with the critical need to protect the transmission system against cyber and external threats…" [redacted]

"Cyber security is very important to us" [redacted]

"Outputs need to include cyber security and this needs to be funded" [redacted]

In autumn 2018, the independent stakeholder user group looked at how we are developing the physical and cyber security elements of our business plan. The group noted that the measures we take are mandated by government and the security services. To protect national security, the government restricts what we can say publicly about our current level of resilience and the specific measures we will take in the future to reduce vulnerability. For these reasons, it is not appropriate for us to engage the group or wider stakeholders on the detail of our plan and the substance of it can't be influenced by customer or consumer preferences. Our approach is therefore to build the confidential detail of our plan with government agencies, while providing transparency about the process that we follow. In its role as economic regulator, Ofgem protects consumers by scrutinising our costs to ensure that only efficiently incurred costs are allowed.

We also engage other networks to ensure learning from best practice, and with our US business to ensure efficiency and innovation from a group level can be applied to our activities.

The detail of our plan is driven by government agency requirements

The key stakeholders whose requirements have shaped our plan for dealing with external threats are the government (BEIS), its security specialists (CPNI and NCSC), Ofgem (in its role as Competent Authority for the NIS Regulations) and the Health and Safety Executive (HSE). We collaborate on best practices across the National Grid Group where we own gas and electricity transmission and distribution networks across the north eastern United States. Working closely with our US colleagues helps us to gain more powerful insights in our 24/7 analysis and management of global security information and event data.

We take a strategic, risk-based approach to cyber security and its impact on gas network resilience. This is consistent with voluntary best practices advised by the US National Institute of Standards and Technology[67] and mandatory requirements now introduced in the UK through the NIS Regulations. We are working with Ofgem and BEIS in their joint role as NIS Competent Authority, and with the HSE, to assess our existing cyber protection capability and confirm further work to protect against threats.

We use a risk assessment methodology and evaluate current capability against the criteria set out in the Cyber Assessment Framework provided by the NCSC. The framework is a systematic method intended to meet the requirements of both the NIS Regulations and wider CNI needs. The assessment is done, and we have developed an improvement plan of tactical actions for the rest of the RIIO-1 period. The work included in our RIIO-2 plan is part of our longer-term strategic investment plan for cyber resilience. We are talking to the NIS Competent Authority to agree the scope and priorities, and we will update our plan as required during 2019.

In its 2018/19 business plan[68], the HSE reflects an increased focus on the emerging risks of cyber security and it has recently updated its operational guidance[69] on cyber security for industrial automation and control systems. This is specifically relevant to us because we operate these systems for major hazard risk reduction and continuity of gas supplies, and our planned RIIO-2 cyber resilience activities are in line with latest HSE guidance:

[67] https://www.nist.gov/cyberframework
[68] http://www.hse.gov.uk/aboutus/strategiesandplans/businessplans/plan1819.pdf
[69] http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf

"Operators subject to both health and safety and NIS legislation should carry out risk assessment(s) that cover both major accident and loss of essential services consequences and then use the highest risk to determine the countermeasures to be applied."

The requirement for physical security at our operational sites has been reviewed in 2005, 2009, 2010/11, 2014 and 2017. At each review we worked closely with BEIS to decide how many sites required enhanced protection. The resources we commit and the work we will carry out in the RIIO-2 period will continue this programme. Where our assets are co-located with other parties, such as gas distribution networks, we work with them to ensure an efficient, joined-up approach. While much of the government's focus at the start of RIIO-1 related to physical security, it has shifted to cyber security as we head toward RIIO-2.

4. Our proposals for RIIO-2 and how they will benefit consumers

Our mission is:

"We protect our people, our premises, and digital systems with the objective of maintaining trust in National Grid services.

We take our responsibilities as an operator of essential services (OES) seriously. Our proposals to protect the gas system from cyber and external threats in the RIIO-2 period are:

- to continue to take proportionate measures to protect the integrity of the network in line with best practice, government and HSE requirements
- to strengthen the ability of the gas transmission system to cope with and recover from malicious events that threaten GB energy supplies
- to deliver the cyber resilience improvements agreed with the Competent Authority for the NIS Regulations
- to deliver physical security upgrades at the sites required by BEIS, ensuring that all our PSUP solutions remain compliant with CPNI high level security principles
- to comply with our legislative requirements (the Counter-Terrorism Act 2008)
- to monitor and report our performance and adapt our plans and delivery as circumstances change
- to pursue greater cost efficiency, deploying innovation and best practice where we can

Outputs

In this section we provide a short description of the proposed RIIO-2 work in each of the key areas:

- cyber resilience – operational technology
- cyber resilience – information technology
- physical security upgrade programme (PSUP)
- policing.

We have set out further details of the business plan proposals for each area in the accompanying engineering justification reports. These reports explain in greater depth the drivers for the activity, the options considered (including 'do nothing'), and the analysis of costs and benefits. We have used further templates to set out our proposed outputs in the form of price control deliverables and, where appropriate, our proposals for the design of uncertainty mechanisms.

Our 'protect from threats' priority maps to Ofgem's output category: 'Maintain a safe and resilient network.' In the following table we have summarised the proposed outputs, the relationship to uncertainty mechanisms and additional supporting information.

Table 23.3 outputs summary 'protect from threats'

PCD name	Business plan proposal - what the PCD measures	Related UM	Supporting info
1. **Cyber resilience**	Delivery of cyber security enhancements to reduce the risk of events which could have a severe impact on GB consumers. Upfront allowance & Totex incentive sharing applies for known work with defined outputs.	UM_1	National Grid UK Cyber Security Strategy (Annex A23.01) Gas Transmission and Gas System Operator NIS Self-Assessments (Annexes A23.03 and A23.04) Gas Transmission and Gas System Operator draft NIS Improvement Plans (Annexes A23.05 and A23.06) Justification Paper –NGGT Cyber Resilience (Information Technology) (Annex A23.02)

			Operational Technology and Cyber Resilience Justification Paper (Annex A23.07)
2. **Physical security**	Delivery of physical security enhancements to reduce the risk of events which could have a severe impact on GB consumers. Upfront allowance & Totex incentive sharing applies for known work with defined outputs	UM_2	Enhanced Physical Site Security Asset Health Justification Report (Annex A23.08) Enhanced Physical Site Security Major Project Justification Report (Annex A23.09)

How do our RIIO-2 proposals benefit consumers?

Our plan to protect from threats delivers benefits for industrial and domestic consumers:

Consumer priorities	How does our plan support this?
"I want to use energy as and when I want"	- We improve the safety and resilience of the network to ride through and recover from malicious events that threaten to disrupt continuity of GB energy supplies.
"I want you to facilitate delivery of a sustainable energy system"	- Our plan delivers security enhancements that the government has identified as being in the national interest. This reduces the risk of actual events that could have severe societal consequences for GB consumers.
"I want an affordable energy bill"	- Including uncertainty mechanisms involving the security agencies to monitor and adjust our delivery during RIIO-2 will ensure our effort and expenditure continues to be directed at maximising consumer benefit even when circumstances change.

5. How will we deliver?

To manage our cyber and physical security programmes we will regularly monitor potential interactions with network developments. For example, if assets become more or less important as we review network capability or as customer activity changes (for example, disconnections) we will re-prioritise our work.

Through our portfolio planning process, we have confirmed that the proposed cyber resilience operational technology scope is deliverable as part of our longer-term programme that will continue through RIIO-3. The necessity to balance system access outages with maintaining secure supplies, limits how many sites we can work on simultaneously. Our delivery programme is part of an enduring, sustainable, asset replacement cycle that fits with the economic optimal average asset life of 15 years.

The programme of work will be subject to competitive procurement events to ensure we achieve value for money. With upfront funding we'll be able to interest the supply chain in a longer term, larger portfolio of work, and drive efficient delivery. We plan to grow our in-house cyber delivery capability by recruiting eight more people so that we achieve the right balance between internal expertise and outsourcing.

Our RIIO-2 plan embeds innovation from our Network Innovation Allowance (scheme NGGT0114) strengthening security with our Supervisory Control and Data Acquisition (SCADA) systems.

We will continue to focus on applying innovation to drive efficiency in delivery our work.

6. Risk and uncertainty

The threat landscape has changed significantly during RIIO-1, particularly in relation to cyber security. Our close work with the security agencies has helped us to a good understanding of the work we need to deliver in RIIO-2 to meet current government requirements. We consider this known work to be 'no regret'. It constitutes around 80% of the scope in this part of our RIIO-2 plan. The key assumptions underpinning our approach are set out in chapter 31.

We propose that in relation to the known work, where the outputs and costs are sufficiently clear, base revenue funding should be included in our RIIO-2 price control allowance for the full scope of this

planned work. We should be strongly incentivised to deliver this work efficiently in the interests of consumers.

We are working with the NIS Competent Authority to confirm our RIIO-2 scope informed by our NIS self-assessment and NIS improvement plans.

We believe the regulatory framework must allow for our outputs and costs to be adjusted in the RIIO-2 period as circumstances change and we support Ofgem's proposal to include uncertainty mechanisms in RIIO-2 for physical security and cyber resilience. In our response to Ofgem's RIIO-2 framework consultation, we made suggestions for how the uncertainty mechanisms could be improved, learning from RIIO-1 experience. Our proposals are summarised in the table below and further details are set out in chapter 29.

It should be noted that there are important interactions across the whole of our business plan. For example, elements of our asset resilience and cyber resilience programmes of work will also bring important safety and reliability benefits. The scope of work we have included in this chapter is consistent with the categories of work in the RIIO-1 enhanced security costs and/or it goes far beyond previous business as usual activity. We expect these areas of work to have their own RIIO-2 outputs, monitoring and reporting regimes.

Table 23.4 uncertainty mechanisms

UM name	Type	Business plan proposal – what the UM addresses	Frequency
1. **Cyber resilience**	Reopener Upfront allowance & Totex incentive sharing applies for known work with defined outputs.	There is some uncertainty above our baseline scope and costs for cyber resilience work in RIIO-2. An ongoing adjustment mechanism avoids security works being over or underfunded in RIIO-2.	Process undertaken annually May or may not result in required changes
2. Physical security	Reopener Upfront allowance & Totex incentive sharing applies for known work with defined outputs.	Scope and cost of physical security work that is in consumer interests in RIIO-2. Ongoing adjustment mechanism to avoid us being over or underfunded for physical security works in RIIO-2.	Process undertaken annually May or may not result in required changes
7. New threat vector	Reopener	Bespoke UM proposal relating to new threat vectors - "unknown unknowns". Concept to be developed further through future iterations.	Only triggered in exceptional circumstances, so that we can respond to stakeholder requirements.
9. **Policing cost associated with Counter-Terrorism Act 2008**	Pass through	Policing costs cannot be controlled by NGGT or predicted, therefore treated as pass-through.	Annual

7. Our proposed costs for RIIO-2

Our proposed total expenditure to meet this stakeholder priority is summarised in the tables below. Our cyber resilience – operational technology costs include:

[redacted]

[redacted]

[redacted]

*It should be noted that in relation to the above work, some 80% of the costs would be incurred for replacement of these systems on grounds of age and obsolescence even if additional cyber resilience requirements did not apply. Our operational technology capex costs incorporate efficiencies of around 30% through improved delivery contract strategies and bundling of work to maximise volume discounts from the supply chain. These systems have asset lives of up to 15 years.

Our cyber resilience – information technology costs reflect NGGT's allocation of common services and systems shared with National Grid Electricity Transmission and National Grid Electricity System Operator. These include:

- [redacted] capex for secure data centres in keeping with the strategic approach approved by Ofgem in the 2018 enhanced security reopener
- [redacted] totex for security hardening of hardware and software systems, provision of 24/7 cyber security monitoring, training and recruitment of cyber skilled personnel. These costs are incurred through our coporate teams.

Our physical security costs reflect:

- [redacted] capex for new Physical Security Upgrade Programme (PSUP) solutions
- [redacted] capex to commence asset replacement of our first generation enhanced security installations as they reach end of life (this programme will extend into RIIO-3). These assets typically have asset lives of 7 or 15 years
- [redacted] opex includes 24/7 alarm monitoring, routine maintenance and fault repairs representing NGGT's allocation of a common service shared with NGET and a third party
- [redacted] opex for policing costs as dictated by the Counter-Terrorism Act and treated as cost pass-through

No provision for unforeseen costs that may arise from future changes in security requirements, as these would be handled by uncertainty mechanisms.

Our physical security capex costs lock in the 15% efficiency so far attained in RIIO-1. We have incorporated £8m efficiency ambition compared to our view at the time of our May 2018 reopener submission.

[redacted]

Business plan data templates

Our business plan is accompanied by a set of spreadsheet business plan data templates (BPDT) in a format required by Ofgem. We have provided the table below to show you how our protect from threats activity costs feed into the BPDTs. This table is not yet included. At the time of writing Ofgem is still working on the detail of the physical security and cyber resilience BPDT to reflect the proposed RIIO-2 framework.

8. Next steps

We wish to discuss with Ofgem the detailed content and regulatory treatment for the various elements that make up this part of our plan. Ofgem intends to hold workshops in 2019 and publish further guidance for the development of our cyber resilience plans. In tandem, further guidance is expected from the NIS Competent Authority for development of our NIS strategic investment plan. We expect this engagement will result in refinements to our RIIO-2 work plan and costs for presentation in our final RIIO-2 business plan.