Introduction

This document has been produced by National Grid to support Ofgem in their public consultation on the notice of adjustment to allowances submitted by National Grid on 8th May 2018. The notice was submitted to Ofgem in accordance with Special Condition 7D of the Electricity Transmission Licence and Special Condition 6D of the Gas Transmission Licence and is in relation to 'Enhanced Security Costs' as defined by the licences. This covers;

'costs incurred, or expected to be incurred, by the licensee for the purpose of implementing any formal recommendation or requirement of the Secretary of State to enhance the security of any of the IT systems required to operate the licensee's Transmission System'[1].

The content of the notice submitted to Ofgem is strictly confidential and cannot be published; therefore this document provides a public overview of the need and requirements for National Grid's enhanced security plans. It will also provide a high-level overview of the proposed allowance adjustment and how National Grid has ensured all investments within the notice effectively meet known requirements.

Since the start of the RIIO T1 period (2013/14 – 2020/21), requirements for enhanced security investments have evolved and become more clearly defined. This has enabled National Grid to determine the appropriate solutions for these requirements; solutions which were uncertain at the time of submitting RIIO T1 Business Plans.

At the time of RIIO T1 Final Proposals, Ofgem understood that some requirements for the eight year RIIO period were uncertain. Accordingly, RIIO arrangements included a number of uncertainty mechanisms, providing the opportunity to review uncertain costs in defined areas so that evolving needs could be efficiently addressed. One of the uncertainty mechanisms for the Gas and Electricity System Operators covers 'Enhanced Security costs'; the notice was submitted by National Grid on 8th May 2018 within these terms. The notice details investments designed to enhance the security and resilience of National Grid's IT Systems within the RIIO T1 period.

National Grid's notice to Ofgem describes specific investments to enhance the security of the IT systems critical to operating gas and electricity transmission systems. These investments meet National Grid's current known requirements for IT security and prepare National Grid to respond to future threats and new requirements as they emerge. This proposed adjustment to allowances equates to a total value of £125.25m (09/10 prices) which covers enhancements to Data Centres (£84.80m) and cyber security (£40.45m). The specific requirements and solutions related to these investments have emerged or become more clearly defined within the RIIO T1 period.

[1] NGET licence definition of 'Enhanced Security Costs'

The need for enhanced security

Since 2013, significant changes have occurred in the security environment. There have been several notable global cyber-attacks which have demonstrated the capacity of would-be-attackers and the potential impact of a successful attack.

National Cyber Security Centre (NCSC) Chief Executive Ciaran Martin has recognised the threat, saying that interference *"has included attacks on the UK media, telecommunication and energy sectors"*[2].

Cyber-attacks have made a step change from causing disruption, to being designed to cause major widespread sabotage and destruction. This has increased the responsibility of National Grid, as an owner and operator of Critical National Infrastructure (CNI) in particular, to ensure it has the right security measures in place.

This threat has also been confirmed by the UK Government through increased investment in Cyber Security (demonstrated within the first two National Cyber Security Strategy documents) and the creation of the NCSC in 2017.

Requirements for enhanced security

It is important that National Grid protects those IT systems needed to operate the essential services they provide. This need has been recognised more widely by EU Government bodies, demonstrated by the introduction of EU-wide legislation requiring operators of essential services (including National Grid) to enhance the security of their networks and information systems.

The Network and Information Systems (NIS) Directive was transposed into UK law in early May 2018 and provides additional requirements for National Grid to enhance the security and resilience of their networks and IT systems. To help companies prepare for the Directive's requirements, the NCSC has provided guidance material which will help towards the achievement of 14 high-level security principles. These principles outline a set of requirements through an outputs based approach which National Grid will need to meet in complying with the new legislation.

The NIS Directive sets out four top-level objectives which will be realised through implementation of the set of security principles. These objectives are;

Objective A: Managing security risk

Objective B: Protecting against cyber attack

Objective C: Detecting cyber security events

Objective D: Minimising the impact of cyber security incidents

Sector-specific guidance for the energy sector is expected to be made available in autumn 2018. In the absence of energy sector specific guidance, National Grid is working to implement investments which will help achieve the key aim of the NIS Directive. This will ensure the security benefits resulting from compliance with the NIS Directive are achieved as soon as possible. National Grid

[2] Ciaran Martin, CEO of the NCSC, The Times Tech Summit, 15th November 2017

believes that they should not wait until energy sector guidance is made available, if at all, given the importance of the issue. This approach has been re-enforced in discussions between National Grid and UK Government.

National Grid has engaged with stakeholders including the Department for Business, Energy and Industrial Strategy (BEIS) and the NCSC to ensure alignment with Government when working towards the common goal of minimising the impact of cyber-attack on energy consumers and society.

Government expectations of National Grid as a 'provider of essential service' under the NIS Directive are that they take the steps appropriate to protect those IT systems essential for the operation of the transmission networks.

National Grid engaged with the NCSC prior to the Directive's introduction and was advised that their investments will help support the security of its CNI systems in line with the Directive.

National Grid has also engaged with external specialists in IT security to better understand the risks and vulnerabilities present within National Grid's IT systems, property, processes and people. This has enabled National Grid to establish a clear set of requirements ensuring appropriate action to minimise known risks and vulnerabilities. The investments outlined within National Grid's notice meet these requirements.

National Grid's notice of adjustment to allowances

The investments detailed in National Grid's notice ensure action is taken in response to the existing cyber threat. They also represent preparation for future threats.

These investments are all in response to guidance published by UK Government, together with recommendations made by external IT security specialists who have assessed National Grid's systems to identify key threat areas in order to best target investment. All future investments outlined in the notice will align to the guidance provided in the NIS Directive.

National Grid applies the industry-recognised approach of 'defence in depth', ensuring a layered approach to security. This ensures that the enhanced security investments cover technical, physical, people and process elements of security. Protecting the CNI systems also involves ensuring that business systems have robust controls and monitoring in place.

The benefits of the investments made to enhance the security of National Grid's IT systems will be realised through a reduced risk of failure or compromise as a result of a cyber-attack and will reduce any impact on UK consumers. As a result of these investments National Grid have improved capabilities to better defend systems from attack, detect suspicious traffic on its networks and respond to attacks against IT systems.

Conclusion

National Grid's enhanced security investments are critical to ensure that the IT systems required in operating transmission systems are effectively protected. These investments meet requirements more clearly defined since the beginning of the RIIO T1 period in 2013.

These investments create and improve National Grid's capability to protect its IT systems. By moving forward with the initiatives in the notice provided to Ofgem, National Grid has taken action to protect IT systems and the critical services they support. These investments ensure alignment with new legislation such as the NIS Directive, established to protect consumers and critical national infrastructure from the impact of cyber-attack.

The notice submitted to Ofgem covers all current known requirements, based on the latest information available. The investments completed and proposed within the notice will meet existing requirements for enhanced security of IT systems.