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

£118m per year
21.5% totex

Engagement		**Stakeholder priority and context**	UK infrastructure is subject to a multitude of security threats, which are increasing in sophistication and persistence. The gas National Transmission System is part of Great Britain's Critical National Infrastructure (CNI), providing an essential service for society. Government sets the requirements for the appropriate levels of protection to be achieved in the national interest. Our RIIO-2 plan is to deliver the security hardening that has been mandated by Government, as efficiently as possible.			
		Topics	**Physical Security**		**Cyber Resilience**	
		Obligations	We are obliged to implement a Physical Security Upgrade Programme (PSUP) at our CNI sites, governed by BEIS. We are obliged to comply with the arrangements for policing at gas facilities in accordance with the Counter-Terrorism Act 2008, sections 85 to 90.		We are an Operator of Essential Services and must comply with the requirements of the Network and Information Systems (NIS) Regulations 2018. The aim is to coordinate and raise overall levels of cyber security across the EU.	
		Stakeholders	Our key stakeholders for this topic are: the government through the Department for Business, Energy and Industrial Strategy (BEIS), its security agencies the Center for the Protection of National Infrastructure (CPNI) and the National Cyber Security Centre (NCSC), Ofgem (in its joint role with BEIS as Competent Authority for the NIS Regulations), HSE, other energy companies that are also Operators of Essential Services, and our upstream/downstream customers.			
		Approach	Bi-lateral meetings with BEIS e.g. setting requirements, monitoring and reporting regarding progress of the PSUP programme. Bi-lateral engagement with NIS Competent Authority regarding cyber resilience. Collaboration with NCSC & GDNs e.g. through the Energy Emergencies Executive Committee (E3C).			
		What we've heard	Stakeholders say they way we manage security threats should be a priority. We've heard (through our events) that they support the need for protection from cyber and external threats because they identify with the increasing threat to society and their own businesses. Loss of gas supply for communities and/or loss of control of critical safety systems could lead to loss of life. We work closely with government who provide assessment of the changing nature of threats and with the security agencies who provide advice on best practices for risk mitigation. There are significant restrictions on the detail we can disclose for reasons of national security. Like other Operators of Essential Services, we have been engaging during 2019 with the Competent Authority on our NIS Self Assessment and Improvement Plan. These set the focus for our near term cyber resilience mitigation actions during the remainder of RIIO-1 and set the context for our programme of work in RIIO-2.			
		Key trade-offs & how engagement influenced our plan	No trade-offs – the scope of work is to meet government requirements. Our approach to cyber resilience has been shaped by engagement with NCSC and the NIS Competent Authority. For example, acting upon feedback we have standardised our approach to the assessment of cyber risk and criticality across our IT, OT and CNI systems.			
Outputs		**Measure**	**PSUP Programme** **Type: Price Control Deliverable** **Target:** implement PSUP at designated sites	**Policing** **Type: Counter-Terrorism Act obligation** **Target:** comply with requirements, cost pass-through	**Cyber Resilience Plan** **Operational Technology** **Type: Price Control Deliverable** **Target:** Cyber resilience improvements	**Business IT Security Plan** **Information Technology** **Type: Price Control Deliverable** **Target:** Cyber resilience improvements
			Specific (confidential) output measures for PSUP programme delivery will be included in PCD agreed with Ofgem. Specified volumes of work to be delivered. Quarterly security performance reporting to BEIS, Annual Regulatory Reporting Pack to Ofgem and Annual Strategic Performance Overview report – public report on website.		Specific (confidential) output measures for cyber resilience programme delivery will be included in PCDs agreed with Ofgem. Specified volumes of work to be delivered. Subject to monitoring and audit by the Competent Authority for NIS Regulations.	
		Comparison to RIIO-1 outputs	No outputs included at start of RIIO-1 because number of sites and scope not confirmed. Subsequently, scope confirmed by BEIS and regulatory cost allowance / outputs were subject to re-opener decision by Ofgem in 2015		No outputs included at start of RIIO-1 because requirements were not yet clear. Enhanced Security re-opener process in May 2018 resulted in additional cost allowances for a defined set of schemes	
	How we will deliver	**Efficiency**	Our physical security capex plan locks in 15% cost reductions so far attained in RIIO-1. We have embedded an additional efficiency ambition so that the allowance we are requesting is £7.5m lower than our view at the time of the May 2018 reopener. We proactively identify sites where lower cost operational solutions may be deployed instead of costly physical measures and other sites where PSUP is no longer required.		Key to driving efficiency of our programme is our use of risk based assessment to determine priorities. Factors considered include: age and condition of existing systems, the network capability needed by our customers, and known vulnerabilities. We always consider least functionality options. Our RIIO-2 plan embeds innovation from our Network Innovation Allowance (scheme NGGT0114) strengthening security with our SCADA systems.	
		Innovation				
		Whole system				
		Competition	Delivery is outsourced through competitive procurement events to ensure value for money. Engineering Justification Papers (confidential) set out the costs and benefits of alternatives considered. Our cyber assessment methodology and costs have been subject to external benchmarking			
		Uncertainty	We have proposed uncertainty mechanism proposed for Physical Security, Cyber Resilience, Policing. The cyber threat landscape is rapidly evolving and it is important that we should be able to flex our response accordingly. The reopener uncertainty mechanisms should cater for changes in: the level of threat, the required response, the criticality of sites/assets/processes, and technology or supply chain capability.			
		De-carbonisation				
Totex		**Cost at RIIO-1 (annual forecast)**	£25m p.a.	£0m p.a. (Policing cost is pass-through)	£2m p.a. (note £16m annual for related OT asset classes is reported in Asset Health section)	£9m p.a. (includes 2018 enhanced security reopener scope)
		Work needed	Deliver new PSUP solutions at required sites. Typically including: high security perimeter fence, controlled access points, intruder detection, CCTV & lighting, civil works, cabling. Maintain & replace existing PSUP assets in accordance with CPNI high level security principles (first generation security assets need replaced due to age and obsolescence). Our PSUP programme is well defined (no regret) so full funding should be included in our baseline price control allowance. Comply with policing requirements of Counter-Terrorism Act 2008.		A prioritised programme of replacement or security hardening of our Operational Technology (e.g. industrial control systems, telemetry, metering, gas analysers and boundary control) for our compressor, terminal and Above Ground Installation sites. A suite of initiatives and investments to improve our ability to identify, protect, detect, respond and recover to cyber threats on our IT systems. Scope of work is informed by a risk based approach, in line with HSE Guidance, and 'defence in depth' architecture in line with IEC 62446 standard, and NIS requirements. Around 80% of our scope is well defined (no regret) so should be funded in our baseline price control allowance.	
		Cost at RIIO-2 (Annual)	**£26m p.a.**	**£0m p.a.**	**£83m p.a.**	**£9m p.a.**
		Approach to uncertainty	We propose two reopeners for our physical security plan: one at mid-period and one at the end of RIIO-2	Policing cost is pass-through	We propose that both our Cyber Resilience Plan and our Business IT Security Plan are subject to two reopeners, one at the beginning of RIIO-2 and one at mid-period.	
		Consumer benefit	• Consumers want to be able to use energy as and when they want. Our plan supports this by improving the safety and resilience of the transmission system to ride through and recover from malicious events that threaten to disrupt continuity of GB energy supplies • Consumers want us to facilitate the energy system transition whilst minimising disruption to their lives. Our plan supports this by delivering the 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 • Applying innovation to enhance the resilience of our SCADA systems is a **Consumer Value Proposition** valued at £9.2m			