PR24

NORTHUMBRIAN WATER living water | ESSEX&SUFFOLK WATER living water

A3-09 PHYSICAL AND CYBER SECURITY

NES23

TABLE OF CONTENTS

1. INTRODUCTION

This enhancement case includes three investments in physical and cyber security that are needed to meet new standards introduced in 2022 and 2023 – physical security at 30 water sites (£18.5m); physical security at 2 large wastewater sites (£13.3m); and e-CAF cyber security requirements (£8.0m).

We own and manage a complex network of assets to provide our customers with safe, clean drinking water and treat sewage to protect the environment. To provide this service, we store hazardous chemicals, employ thousands of people in offices and operational sites, and have sites considered critical to the UK National Infrastructure.

We must comply with the legal requirements of the Security and Emergency Measures Direction 2022 (SEMD), enabling legislation under Section 208 of the Water Industry Act 1991. Obligations introduced by Defra in 2022 under SEMD include:

- Revised alternative water supply planning requirements to a minimum of 1.5% of the total domestic population for the first 120 hours after an incident.
- Revised CNI classification/methodology leading to increased numbers of CNI-designated assets.

We have already met these requirements for robust alternative water supplies, as well as the legal requirements for CNI sites designated before the 2022 SEMD and require no new enhancement funding for these. Our enhancement case includes investment to meet the physical security requirements for **water sites newly designated under SEMD 2022**, which has not previously been funded through enhancement expenditure.

The DWI completed a detailed assessment of the investments proposed to improve security at 30 CNI sites and they have written to us confirming their support for these schemes (see Annex A).

In addition to the new requirements for water sites, the 2022 SEMD also required us to identify security risks to our wastewater sites. This review showed that there are two high-risk and high-consequence sites that will now be designated under the Control of Major Accident Hazards (COMAH) Regulations 2015. Before the 2022 SEMD, we did not have any sites designated under COMAH. Our enhancement case includes investment to meet the physical security requirements for **wastewater sites newly designated under SEMD 2022 and COMAH**, which have not previously been funded through enhancement expenditure.

The Government's National Cyber Security Centre (NCSC) acknowledges that cyber threats to Critical National Infrastructure (CNI) companies are increasing rapidly. Before 2020, the Network Information Systems Directive (NIS-D) introduced regulatory compliance measures to ensure appropriate enhancements were made to cyber security for all water companies in relation to the production and delivery of clean water services.

We have invested significantly in cyber security since 2020, and this means that by 2025 we will have appropriate levels of control to minimise our cyber security risk across all areas of our business (that is, not just clean water) and will meet the requirements of legislation including NIS-D. We already meet the standards set under the Cyber Assessment Framework by the NCSC.

However, the Drinking Water Inspectorate (DWI) wrote to all companies with a new expectation to meet enhanced cyber security standards from 31 March 2028 – the "e-CAF". This new standard means further improvements in six of the contributing outcomes. In a subsequent letter from Ofwat, we were instructed to include enhancement investment **to meet these new e-CAF standards** in our business plan.

As part of our ongoing business continuity planning, we will also continue identifying opportunities to increase resilience with the necessary investments through base allowances.

1.1. SUMMARY OF COSTS

We summarise the enhancement capex and opex for these investments in Table 1 below. As requested in Ofwat's letter of 5th July 2023, we have included investment for meeting new cyber security standards in lines CW3.132 and CW3.133. We have no requirement for enhancement costs to meet the existing target (lines CW3.126-126), and there is no separate business case for this.

TABLE 1: COST BREAKDOWN BY OPEX AND CAPEX

Table line (from CW3)	2025-30 Cost (£m)	CW3 line reference
Security - SEMD; enhancement water capex	16.099	CW3.121
Security - SEMD; enhancement water opex	1.742	CW3.122
Additional line 2; enhancement water capex	0.921	CW3.132
Additional line 2; enhancement water opex	7.108	CW3.133
Table line (from CWW3)	**2025-30 Cost (£m)**	**CWW3 line reference**
Security - SEMD; enhancement wastewater capex	12.036	CWW3.170
Security - SEMD; enhancement wastewater opex	1.226	CWW3.171

2. NEED FOR ENHANCEMENT INVESTMENT

a) Is there evidence that the proposed enhancement investment is required (ie there is a quantified problem requiring a step change in service levels)? This includes alignment agreed strategic planning framework or environmental programme where relevant.

b) Is the scale and timing of the investment fully justified, and for statutory deliverables is this validated by appropriate sources (for example in an agreed strategic planning framework)?

c) Does the proposed enhancement investment or any part of it overlap with activities to be delivered through base, and where applicable does the company identify the scale of any implicit allowance from base cost models?

d) Does the need and/or proposed enhancement investment overlap or duplicate with activities or service levels already funded at previous price reviews (either base or enhancement)?

e) Is the need clearly identified in the context of a robust long-term delivery strategy within a defined core adaptive pathway?

f) Where appropriate, is there evidence that customers support the need for investment (including both the scale and timing)?

g) Is the investment driven by factors outside of management control? Is it clear that steps been taken to control costs and have potential cost savings (eg spend to save) been accounted for?

In this section, we look at the need for enhancement investment in more detail. Section 2.1 looks at the requirement for water sites newly designated by SEMD 2022, Section 2.2 looks at the requirement for wastewater sites newly designated by SEMD 2022 and COMAH, and Section 2.3 looks at the requirement to meet the new enhanced e-CAF cyber security standards.

For all of these investments, there is a clear statutory driver with requirements that must be met during 2025-30. These enhancements do not overlap with activities to be delivered through base, and we fully meet the previous legal standards – with no new enhancement expenditure required. We can show clearly that these are not the same investments in either physical or security that have been funded through enhancement expenditure at previous price reviews (and we have met the standards for which previous enhancement expenditure was allowed).

These standards are not part of a long-term pathway, as they are short-term requirements. However, our long-term strategy (NES_LTDS) assumes that there will continue to be a similar level of investment in future periods to meet increasing standards. There are no clear trigger points for adaptive pathways, and the evidence is not yet clear how improving technology will affect cyber security (as both the risks and the technology available to tackle this are likely to increase).

Section 2.4 looks at evidence from customer engagement for their support for investments in physical and cyber security. In practice, the requirements for the scale and timing are statutory requirements and we have limited scope to change these.

These investments are entirely driven by factors outside of our control, as they relate to new statutory requirements. We have met existing standards, and have proactively improved our security to meet part of the new standards (through base expenditure) before these have been set as requirements.

2.1. PHYSICAL SECURITY AT WATER SITES

The Security and Emergency Measures (Water and Sewerage Undertakers and Water Supply Licensees) Direction 2022 (SEMD) is the principal general direction issued by the Secretary of State and Welsh Ministers under Section 208 of the Water Industry Act 1991 (the Act). Undertakers and licensees must maintain a water supply and sewerage system in the interests of national security or mitigate the effects of any civil emergency.

SEMD Section 3 stipulates the following as a general duty on water companies:

"The company must, in complying with this Direction, have regard to any relevant guidance, procedures, requirements, best practice and any risks, including long term risks, relating to civil emergencies and national security".

Paragraph 7 of the SEMD sets out the specific regulatory requirement for us to identify security risks. We must:

(a) *identify and assess any security risks (including long-term risks) to the provision of its water supply or sewerage functions, including security risks that may arise through dependencies on external suppliers and;*
(b) *put in place measures to avoid or, if this is not possible, mitigate those risks.*

In response to the regulatory changes in 2022 and the subsequent Defra CNI Criticalities review, we carried out a security risk assessments of all CNI sites. We did this by applying Defra's Protective Security Guidance 2022 (PSG) to all sites. This is supported by detailed CNI advice and product specifications provided by the National Protective Security Authority (NPSA).

We carried out a detailed assessment of the CNI functions that appear on the Defra Critical National Infrastructure Knowledge Base (CNIKB) in 2022. We used a security risk assessment of each CNIKB function to identify and assess security risk (SEMD para 8). The results of this detailed survey and risk assessment work led to determining vulnerable and contamination points at each site. We then needed to implement measures to avoid or mitigate these risks and the impact of a security event SEMD para 8(c).

Based on this review, we now have **30 assets designated as CNI** in response to SEMD 2022 – compared to just 2 before the review. The changes in 2022 also required NWL to review the provisions for alternative water provision where we concluded that our existing arrangements were sufficient to meet the updated standards.

This enhancement case sets out the schemes that are needed to comply with the CNI security requirements set out in PSG Section 8. These are statutory investments that we must make in order to comply with our duties. This comprises:

- Funding to install specific measures to ensure appropriate security at the 28 sites that have not previously held CNI status (these sites have not had any previous funding).
- Funding to address new vulnerable and contamination points at 2 sites which were previously designated as CNI. These additional points were identified under the new regulatory guidance, and are an increase in standards.

Defra has set a clear expectation that all CNI-designated assets will be fully compliant by 2030, and investment will be phased and delivered throughout AMP8. We will continue to return CNI audit returns as part of the DWI SEMD submission to meet SEMD Paragraph 18 (1), showing an annual picture of CNI compliance.

Failure to comply with the security direction will result in enforcement action. Enforcement options available to the DWI include:

- Serving an enforcement order under section 18 of the Act, provisional or final dependent on the severity of the non-compliance and the risk to water supplies.
- Accepting an undertaking under section 19 of the Act when appropriate in place of an enforcement order, if the steps proposed will ensure compliance.
- Imposing a financial penalty under section 22A of the Act on a water undertaker or water supply licensee.

We have not included any other process functions where there is a lesser risk or no vulnerability or possible contamination of the final water from this enhancement case. Where sites have existing security measures, these have been considered and factored in as an existing layer of security to mitigate the required security enhancement and avoid unnecessary cost.

We have risk assessed the threats and considered the likely attack methodologies taking into account the adversaries, actions they would likely take, and the assets that are either attractive or vulnerable. We have considered the crime patterns in our region, the assets' locations and accessibility. This work has led us to discount attack methods such as vehicles as a weapon (VAW) and unmanned aerial vehicles (UAVs). We are not seeking funding for countermeasures for this type of threat.

As compliance across our Water infrastructure has already been funded and achieved throughout previous AMPs, we are not seeking additional funding to meet the Water UK Security Standards, version 4.3, January 2023.

As part of their **price review guidance**, DWI expects us to follow the approach outlined above and identify SEMD expenditure in our PR24 business plan.

Link to our Long-Term Strategy

This investment is needed as part of the 'miscellaneous' investment area under our Long Term Strategy (LTS) core pathway. This investment is required to ensure a total of 30 sites (28 newly designated and two existing) meet their security requirements. This is a low / no-regret investment because it must meet statutory requirements in 2025-30 and builds upon the work and investment made in previous AMPs. We have already made provision for the revised alternative water planning requirements and no further investment is required for AMP8.

We are legally required to deliver this investment under the Security and Emergency Measures (Water and Sewerage Undertakers and Water Supply Licensees) Direction 2022 (SEMD). Therefore, we consider this investment necessary in 2025-30 to deliver our LTDS. Future investment may be needed if further sites are identified as CNI, and this assessment will follow in line with SEMD.

DWI position

We submitted our proposals to the Drinking Water Inspectorate (DWI) who issued a letter for support for them on the 25th August 2023. That letter (presented in Annex A) stated:

'The Inspectorate has completed its detailed assessment of the scheme proposed by Northumbrian, Essex and Suffolk Water to increase the security to the required standards to facilitate compliance with the Security and Emergency Measures Direction 2022 at 30 CNI Sites (and associated assets as applicable). A summary of the outcome of our assessment of this scheme is attached.

Based on the information submitted by the company, the Inspectorate supports the need for this scheme, and the supported scheme shall be included by the company in its Final Business Plan' DWI, August 2023

The letter provides in-principle support for the sites and schemes identified. Subsequent assurance of the final cost estimates for these same investments and locations led to a small adjustment of the expected costs from the c.£15.5m estimate we originally provided to the DWI which is referenced in the letter.

Links to data tables

This business case relates to the following lines in the data tables:

- CW3
    - Security - SEMD; enhancement water capex
    - Security - SEMD; enhancement water opex
    - Security - SEMD; enhancement water totex

2.2. PHYSICAL SECURITY AT WASTEWATER SITES

In 2.1, we describe the SEMD regulations and the requirement to identify security risks to providing our water supply and sewerage functions.

In response to the SEMD changes in 2022, we carried out a security risk assessment of most of our wastewater asset base. We applied Defra's Protective Security Guidance 2022 (PSG) to all sites. This is supported by product specifications provided by the National Protective Security Authority (NPSA).

Based on this review, we identified **two high-risk and high-consequence sites** that will also now become designated under the Control of Major Accident Hazards (COMAH) regulations[1]. This is because of the expansion of the treatment capacity and biogas storage on these sites. We had no COMAH-designated sites before the review. Where sites had existing security measures, we considered these and factored them in as an existing layer of security to mitigate the required security enhancement and avoid unnecessary costs.

We have risk assessed the threats and considered the likely attack methodologies taking into account the adversaries, actions they would likely take, and the assets that are either attractive or vulnerable. We have considered the crime patterns in our region, the assets' locations and accessibility. This work has led us to discount attack methods such as vehicles as a weapon (VAW) and unmanned aerial vehicles (UAVs). We are not seeking funding for countermeasures for this type of threat.

Link to our Long-Term Strategy

This investment is needed as part of the 'miscellaneous' investment area under our Long Term Strategy (LTS) core pathway. This investment is required to ensure the two sites meet their COMAH and SEMD requirements. This is a low / no-regret investment because it must meet statutory requirements in 2025-30 and builds upon the work and investment made in previous AMPs. We are legally required to deliver this investment under the COMAH regulations. Therefore, we consider this investment necessary in 2025-30 to deliver our LTS.

Links to data tables

This business case relates to the following lines in the data tables:

- CWW3
    - Security - SEMD; enhancement wastewater capex
    - Security - SEMD; enhancement wastewater opex

[1] See: https://www.hse.gov.uk/comah/index.htm

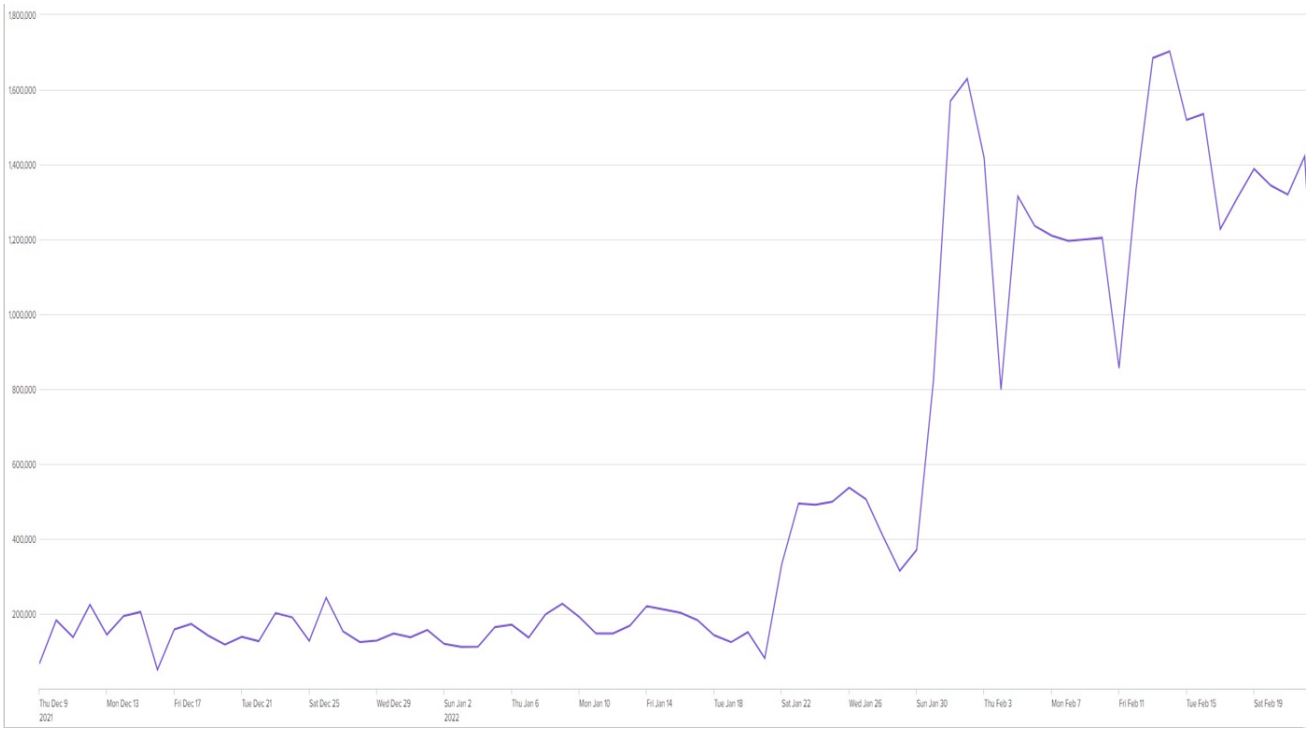
- Security - SEMD; enhancement wastewater totex

2.3. CYBER SECURITY

Cyber security risks are increasing for all UK CNI companies.

For example, during the days leading up to the Russian invasion of the Ukraine we saw an almost tenfold (200,000 to 1,800,000) number of scans against our firewall coming from Moscow IP addresses. Many other CNI companies who were also monitoring this activity saw similar results, indicating that CNI companies are a target for hostile foreign sources.

FIGURE 1: RECORDED SCANS AGAINST OUR FIREWALL, DEC 21 TO FEB 22



As well as hostile foreign states, the proliferation of ransomware developed and distributed by cyber criminals has had a significant impact on numerous businesses, many of which are within the CNI. It is imperative that cyber security capability continues to be enhanced to mitigate against this increasing and constantly evolving threat to protect our business, our customers, and the UK as a whole.

As documented in the Government's impact assessment of the Network and Information Systems Regulation 2018:

"The main expected benefits (of enhancing cyber security) are a reduction in the level and scale of cyber security breaches. This has benefits for the companies controlling the networks, other organisations operating on the network and the wider economy where breaches would otherwise disrupt everyday activity."

A cyber-attack could lead to significant negative impacts across our business, and could potentially affect every measure and outcome for our water and wastewater services. This includes the following:

- Disruption to water services
- Poisoning of water (changes to chemical levels)
- Disruption to wastewater services
- Pollution incidents
- Disruption to traditional IT systems (Customer service impact)
- Loss or theft of Customer or Employee data
- Financial theft and fraud
- Intellectual property or commercial data theft (causing greater harm to the UK economy)
- Regulatory requirement (GDPR, NIS)

In response, we have been investing since 2020 across all three domains (people, process, and technology) of cyber security to manage our risk appropriately. Our priority is to implement security controls across the entire business to protect all our systems, all our customers and all our employees.

Despite current and past investment the increased threat to the water sector has resulted in the DWI issuing a notice on 23rd June 2023 to improve security even further by stating:

We wrote to you on 4 October 2022 to advise you of work that NCSC had undertaken on the Cyber Assessment Framework (the CAF). The work involved the modelling of historic breaches and additional breaches since the original target profile was published in 2018, to determine what changes would be required to the CAF to reflect resilience against moderate capability attacks as opposed to the current position which achieves resilience against limited capability attacks. This resulted in the development of the enhanced CAF (the "e-CAF").

Therefore, we are writing to advise you that further to the existing target to meet the sector specific profile (the "SSP") for the CAF by 31 March 2025, there is an additional milestone to ultimately achieving full compliance with the CAF, to meet the enhanced CAF profile for the sector by 31 March 2028. For awareness, this means further improvements in six of the contributing outcomes, which all move from amber to green:

Operators of Essential Services, OESs, should now start developing improvement plans aimed at achieving this milestone. The nature of cyber security, moving at a fast pace, means that this target comes some weeks after the submission of proposals for NIS schemes for consideration by the Inspectorate for support in company's business plans for PR24.

The new enhancements require 35 metrics across 6 contributing factors to be fully achieved. These are set out in Table 2 below.

TABLE 2: CONTRIBUTING FACTORS AND METRICS FOR E-CAF

B2.c Privileged User Management
• Privileged user access to your essential function systems is carried out from dedicated separate accounts that are closely monitored and managed. • The issuing of temporary, time-bound rights for privileged user access and / or external third-party support access is in place. • Privileged user access rights are regularly reviewed and always updated as part of your joiners, movers and leavers process. • All privileged user access to your networks and information systems requires strong authentication, such as multi-factor (MFA) or additional real-time security monitoring. • All privileged user activity is routinely reviewed, validated and recorded for offline analysis and investigation.
B4.a Secure By Design
• You employ appropriate expertise to design network and information systems. • Your networks and information systems are segregated into appropriate security zones, e.g. operational systems for the essential function are segregated in a highly trusted, more secure zone. • The networks and information systems supporting your essential function are designed to have simple data flows between components to support effective security monitoring. • The networks and information systems supporting your essential function are designed to be easy to recover. • Content-based attacks are mitigated for all inputs to operational systems that affect the essential function (e.g. via transformation and inspection).
B4.b Secure Configuration
• You have identified, documented and actively manage (e.g. maintain security configurations, patching, updating according to good practice) the assets that need to be carefully configured to maintain the security of the essential function. • All platforms conform to your secure, defined baseline build, or the latest known good configuration version for that environment. • You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented. • You regularly review and validate that your network and information systems have the expected, secure settings and configuration. • Only permitted software can be installed. • Standard users are not able to change settings that would impact security or the business operation. • If automated decision-making technologies are in use, their operation is well understood, and decisions can be replicated.

C1.a Monitoring Coverage

- Monitoring is based on an understanding of your networks, common cyber attack methods and what you need awareness of in order to detect potential security incidents that could affect the operation of your essential function. (e.g. presence of malware, malicious emails, user policy violations).
- Your monitoring data provides enough detail to reliably detect security incidents that could affect the operation of your essential function.
- You easily detect the presence or absence of IoCs on your essential functions, such as known malicious command and control signatures.
- Extensive monitoring of user activity in relation to the operation of essential functions enables you to detect policy violations and an agreed list of suspicious or undesirable behaviour.
- You have extensive monitoring coverage that includes host-based monitoring and network gateways.
- All new systems are considered as potential monitoring data sources to maintain a comprehensive monitoring capability.

C1.c Generating Alerts

- Logging data is enriched with other network knowledge and data when investigating certain suspicious activity or alerts.
- A wide range of signatures and indicators of compromise is used for investigations of suspicious activity and alerts.
- Alerts can be easily resolved to network assets using knowledge of networks and systems. The resolution of these alerts is performed in almost real time.
- Security alerts relating to all essential functions are prioritised and this information is used to support incident management.
- Logs are reviewed almost continuously, in real time.
- Alerts are tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms.

C1.e Monitoring Tools & Skills

- You have monitoring staff, who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and performance.
- Monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process.
- Monitoring staff follow process and procedures that address all governance reporting requirements, internal and external. Monitoring staff are empowered to look beyond the fixed process to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data.
- Your monitoring tools make use of all logging data collected to pinpoint activity within an incident.
- Monitoring staff and tools drive and shape new log data collection and can make wide use of it.
- Monitoring staff are aware of the operation of essential functions and related assets and can identify and prioritise alerts or investigations that relate to them.

We must meet these new standards by 2028, so there are no choices to make about the scale and phasing of investment. This does not overlap with any investment in base expenditure, which funds us to meet the existing standards of cyber security.

Due to our proactive approach to investment in cyber security since 2020, we are already on target to achieve these areas in line with the previous "amber" status requirements (this was the requirement under CAF). We are also well placed to achieve the new "green" status on some of the less challenging targets. We have reviewed the gaps and have identified where additional investment is required to achieve the legislative target by 2028.

We used the Government's 14 high-level security principles to help identify these gaps. The NCSC has developed these principles and we are expected to comply with them.

TABLE 3: UK GOVERNMENT'S 14 HIGH LEVEL SECURITY PRINCIPLES

Objective A. Managing security risk - Governance - Risk management - Asset management - Supply chain	**Objective B.** Defending systems against cyber attack - Service protection policies and procedures - Identify and access control - Data security - System security - Resilient networks and systems - Staff awareness and training
Objective C. Detecting cyber security events - Security monitoring - Anomaly detection	**Objective D.** Minimising the impact of cyber security incidents - Response and recovery planning improvements - Impact on the natural environment by prevention of pollution events caused by compromised sites and assets

Our enhancement investment will not be used to replace existing controls such as firewalls, anti-malware software, or mobile device management. It will also not replace any of the enhancements we have made already in the current peiod.

Instead, this ensures compliance with the new e-CAF, and so mitigate the additional risks that the NCSC have identified since they published their original target profile in 2018.

Link to our Long-Term Strategy

This investment is needed as part of the investment areas proposed under our Long Term Strategy (LTS) core pathway. This is a low / no-regret investment because it must meet statutory requirements in 2025-30 and builds upon the work and investment made in previous AMPs.

We are legally required to deliver this investment under the Network Information Systems Directive[2]. Therefore, we consider this investment necessary in 2025-30 to deliver our LTS. We are likely to need more investment in the future, and our long-term delivery strategy assumes this will continue at the current rate in future price review periods.

Links to data tables

This business case relates to the following lines in the data tables:

- CW3
    - Additional line 1; enhancement water capex
    - Additional line 1; enhancement water opex

As requested in Ofwat's letter of 5th July 2023, we have included investment for meeting new cyber security standards in lines CW3.130 and CW3.131.

Discussion with DWI

We discussed our cyber security proposals with the Drinking Water Inspectorate (DWI) on 24 August 2023, and they agreed that our proposal made sense and appeared pragmatic in terms of achieving the e-CAF. We uploaded the completed plan to the DWI on 15 September – their agreed deadline – for their review. Given the timing of this request, we expect that the DWI will review the need for specific investments and options in more detail after our business plan has been submitted to Ofwat.

2.4. CUSTOMER SUPPORT FOR THE NEED

These investments are statutory, and do not provide additional services for customers. In our pre-acceptability research, we asked customers about which areas of investment in our proposed "must do" and "preferred" plans mattered most to them. "Introducing new security measures at critical sites to ensure services aren't interrupted" was presented as a "must do" area of the plan in both the North East and Essex and Suffolk (**enhancements and other service area summaries**, NES43).

Security measures ranked last of the 14 areas of investment presented for research participants in the North East, and second last of the 11 areas presented in Essex and Suffolk. Participants also ranked this area last for the areas which required investment (**enhancements and other service area summaries**, NES43).

[2] See: **https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018**

However, customers also ranked some of the potential service impacts as high priority (pollution incidents and water quality) or medium priority (supply interruptions) in our triangulation of priorities (**prioritisation of common PCs**, NES44).

Since these are statutory requirements, we included this in our “must do” plan for customers – and cannot remove this from our plan in 2025-30 or delay these investments. Customers supported our preferred plan in our Affordability and Acceptability research, including these investments.

3. BEST OPTION FOR CUSTOMERS

a) Has the company considered an appropriate number of options over a range of intervention types (both traditional and non-traditional) to meet the identified need?

b) Has a robust cost–benefit appraisal been undertaken to select the proposed option? Is there evidence that the proposed solution represents best value for customers, communities and the environment over the long term? Is third-party technical assurance of the analysis provided?

c) In the best value analysis, has the company fully considered the carbon impact (operational and embedded), natural capital and other benefits that the options can deliver? Has it relied on robustly calculated and trackable benefits when proposing a best value option over a least cost one?

d) Has the impact (incremental improvement) of the proposed option on the identified need been quantified, including the impact on performance commitments where applicable?

e) Have the uncertainties relating to costs and benefit delivery been explored and mitigated? Have flexible, lower risk and modular solutions been assessed – including where forecast option utilisation will be low?

f) Has the scale of forecast third party funding to be secured (where appropriate) been shown to be reliable and appropriate to the activity and outcomes being proposed?

g) Has the company appropriately considered the scheme to be delivered as Direct Procurement for Customers (DPC) where applicable?

h) Where appropriate, have customer views informed the selection of the proposed solution, and have customers been provided sufficient information (including alternatives and its contribution to addressing the need) to have informed views?

We have considered a range of options, including some non-traditional solutions. We have reviewed and assessed our existing protective measures, assessed risks, and identified detailed needs for components of our security. In many cases, there are very limited options for tackling specific needs, with some of these being specified by guidance.

Our option assessment included looking at the carbon impacts of options, but in practice we have selected the least cost option. We have looked at uncertainties about cost and benefit delivery.

There are no options for third party funding for security. We considered our physical security investments for Direct Procurement for Customers (DPC) but it falls far below the size threshold. New cyber security requirements arrived in July 2023, after we had completed our DPC assessment, but these investments also fall far below the size threshold.

We have not discussed security options at our sites with customers, as these are specific legal requirements (and we cannot share the precise options with customers in any case). However, we include our customer evidence in Section 3.4.

3.1. PHYSICAL SECURITY AT WATER SITES

Our above-ground assets are categorised according to defined criteria in the agreed National Standards (which we described in Section 2). Defra engaged all water companies in a national piece of work (the 'CNI Criticality Review') from June 2021. This assessed CNI sites based on a functional approach, rather than the previous site-based approach. Asset dependency and cross-sector interdependency were also added into the consideration of critical national infrastructure resilience.

After Defra set new CNI criteria, we appraised all our assets within the scope of the Defra Criticalities review. Our security team collaborated with internal network analysis, water resources, and supply strategy teams to identify potential new CNI sites. A copy of our approach to this assessment is held within the Defra Criticality Review work plan (we do not share this here, as this is sensitive information). An important element of this work was to ensure that only the most critical sites were put forward to Defra for cross-referencing interdependencies with other CNI sectors and assessment.

Some sites such as enhanced reservoirs and wastewater assets that were already subject to prescribed additional security measures are still not in the scope for CNI categorisation. We have not included these sites within this enhancement case.

On completing its CNI Criticality Review, Defra determined that 32 of NW's operational sites met the updated CNI criteria.

After analysing these 32 sites, we consulted further with Defra. Following this consultation process, Defra confirmed that there would be a reduction in the number of CNI sites to a total of 30. Defra agreed that we own 30 entries on the Critical National Infrastructure Knowledge Base (CNIKB).

Our security team carried out a desktop survey and security risk assessment work to determine the additional security measures needed at each of these 30 sites. Each site was reviewed as part of a desktop analysis of critical processes and functions. We used criteria within the Protective Security Guidance (PSG) Section 8 to compile a list of Vulnerable Points (VP) and Contamination Points (CP). We can provide an example of this assessment on request (again, this information is sensitive).

We carried out detailed surveying of sites, including engagement with site owners and process experts, to confirm the desktop analysis outputs and understand site-specific security risks and incidents. We used the results to identify the final list of process functions and assets for possible additional security protection.

Our security team reviewed and assessed the existing protective measures (physical, electronic, access control, verification) for condition and compliance. We used this data to mitigate potential new security measures needed around VP/CP assets to introduce the layered security options approach. There are many different requirements at different sites (such as increasing the security of access points, e.g. fences, gates, doors, windows or installing electronic security systems that can be remotely monitored, e.g. electronic alarm systems, electronic fences, CCTV, etc.).

We carried out Security Risk and Threat Assessments for each site to identify security risks using national crime reporting criteria to establish an Immediate Risk Value. We then weighed this against existing legacy protective measures and prioritised to allow for the consideration of risk acceptance and possible 'do nothing' options for risks that have minimal impact or are highly unlikely to occur, thus reducing costs. Further scrutiny confirmed that only the additional security measures to protect the VP/CP were captured and included in costs.

We carried out cost analysis for each VP/CP point on all 30 CNIKB assets and functions, to count the number of component security parts required across each CNI site. This included a comparison with existing measures compliant with WUKSS Cat2 Option 1.

The options and costings we have captured are heavily informed by our 2015-20 (AMP6) experience delivering compliance with the Water UK Security Standards (WUKSS), where we needed to install similar security levels at several of our water asset sites. Our AMP6 experience highlighted the financial benefits of fencing and site security solutions over providing security to every VP and CP.

Our options for protection are limited to those detailed in WUKSS, as these options are considered as proven in achieving compliance. WUKSS Cat2 Option1 is the National Protective Security Authority's (NPSA) preferred option and has been selected as appropriate to protect vulnerable and contamination points. The WUKSS Security control grid options are detailed in Annex 2 (of the WUKSS).

The NPSA's preferred layered approach (that is, fenceline and specific asset protection) conforms to the VP and CP protection principles detailed in PSG Section 8. Alternative protection options are considered only where WUKSS Cat2 Option 1 is inappropriate for practical, operational, or aesthetic reasons.

Option 1 within WUKSS is the NPSA 'preferred method for new build' and, therefore, has been chosen based on this as the least cost option to develop enhanced security control measures. This option has been scrutinised as part of the survey process and costed in a way that would make us fully compliant.

We have fully considered the carbon impact of delivering this option. Rated security equipment that has passed the NPSA and LPCB tests and is certified for use on CNI assets are typically hard structures, and so we cannot avoid a carbon impact. We considered natural barriers and topography that could be used as supplementary barriers to protect against some risks and screen high-value targets. Trees and ditches, for example, can be used to deter hostile vehicles or narrow

lines of attack. However, following security assessments, there was no need to address any additional risk of hostile vehicles at our sites and so we have not selected any options that use this type of deterrent.

We considered options for asset screening through planting, but ultimately these do not meet the hard security measures needed for compliance. We note that there are security and biodiversity advantages to using natural resources to reduce sightlines from beyond the perimeter around key structures and attractive or vulnerable targets. Screening works to hide assets but also works with engineering design to force adversaries into a position where they can be monitored. For example, to gain sight of a target, adversaries must move into a location that can be monitored or outfitted with detection technology. These options require careful consideration, as planting should not provide a hiding place for adversaries, which would have the opposite effect.

We considered the incremental impact of our security investments on performance commitments. These do support some risk reduction, as poor or no security can put water quality at risk (due to deliberate or accidental actions of someone who should not have had access to the asset). Poor security can also create risks of supply interruptions or lower capacity due to asset damage, and potentially pollution incidents from compromised assets. However, as these incidents remain very infrequent, there is no impact in practice on our performance commitments.

We considered the uncertainties relating to costs and benefit delivery. These measures would support compliance with the legal requirements, but it remains uncertain if increased security standards might be required in future reviews. The cost of security products is very reliant on the cost of steel at the point of manufacture, and so we expect our cost estimates to be vulnerable to real price effects on materials and labour rates. We mitigate this risk for all our expenditure together (see **A3 – costs**, NES04).

We have not included enhancement expenditure for alternative water provision in our business plan. However, should the large-scale loss of water supply occur, we have adopted industry best practice for a large-scale incident – that is, the use of rapid deployment static tanks as the most effective response capability. We already have a significant capacity in this regard and to meet increased requirements stipulated by Defra WSR, we will increase the number of rapid deployment assets in-line with the increased requirements under SEMD without needing further enhancement funding.

TABLE 4: SUMMARY OF COSTS (£M)

Solution	NW	ESW	TOTEX	CAPEX	OPEX
Materials costs	£5.674	£4.883	£10.557	£10.557	£0.00
Contract overheads	£1.544	£1.329	£2.873	£2.873	£0.00
Project overheads	£0.647	£0.557	£1.204	£1.204	£0.00
Risk @ 10%	£0.787	£0.677	£1.464	£1.464	£0.00
Maintenance	£0.936	£0.806	£1.742	£0.00	£1.742
TOTAL	**£9.588**	**£8.252**	**£17.840**	**£16.098**	**£1.742**

3.2. PHYSICAL SECURITY AT WASTEWATER SITES

Our above-ground assets are categorised according to defined criteria in the agreed National Standards (which we described in Section 2).

We reviewed and assessed security risk across the entire wastewater asset base using the Water UK Security Standards section 5 and 6. We used this site security risk assessment methodology to categorise the security control level of each of the sites.

We need to make improvements just for the two highest risk sites, which we assessed as having a security category of CAT2H and are within the COMAH thresholds. All other wastewater sites are not in scope of this enhancement case.

Our security team reviewed and assessed the existing protective measures (physical, electronic, access control, verification) for condition and compliance. We used this data to mitigate potential new security measures needed around assets to introduce the layered security options approach. There are many different requirements at different sites (such as increasing the security of access points, e.g. fences, gates, doors, windows or installing electronic security systems that can be remotely monitored, e.g. electronic alarm systems, electronic fences, CCTV, etc.).

We conducted Security Risk and Threat Assessments for each site to identify security risks using national crime reporting criteria to establish an Immediate Risk Value. We then weighed this against existing legacy protective measures and prioritised to allow for the consideration of risk acceptance and possible 'do nothing' options for risks that have minimal impact or are highly unlikely to occur, thus reducing costs. Further scrutiny confirmed that only the additional security measures to protect the assets were captured and included in costs.

We carried out a cost analysis to count the number of component security parts required across each site. This included a comparison with existing measures compliant with WUKSS Cat2 Option 1.

The options and costings we have captured are heavily informed by our 2015-20 (AMP6) experience delivering compliance with the Water UK Security Standards (WUKSS), where we needed to install similar security levels at several of our water asset sites. Our AMP6 experience highlighted the financial benefits of fencing and site security solutions over providing security to every building and function.

Our options for protection are limited to those detailed in WUKSS, as these options are considered as proven in achieving compliance. WUKSS Cat2 Option1 is the National Protective Security Authority's (NPSA) preferred option and has been selected as appropriate to protect vulnerable and contamination points.

The NPSA's preferred layered approach (fence line and specific asset protection) conforms to the VP and CP protection principles detailed in PSG Section 8. We only considered alternative protection options where WUKSS Cat2 Option 1 is inappropriate for practical, operational, or aesthetic reasons.

Option 1 within WUKSS is the NPSA 'preferred method for new build' and, therefore, has been chosen based on this as the least cost option to develop enhanced security control measures. This option has been scrutinised as part of the survey process and costed in a way that would make us fully compliant.

We have fully considered the carbon impact of delivering this option. Rated security equipment that has passed the NPSA and LPCB tests and is certified for use on CNI assets are typically hard structures, so we cannot avoid a carbon impact. We considered natural barriers and topography that could be supplementary barriers to protect against some risks and screen high-value targets. Trees and ditches, for example, can be used to deter hostile vehicles or narrow lines of attack. However, following security assessments, there was no need to address any additional risk of hostile vehicles at our sites, so we have not selected any options that use this type of deterrent.

We considered options for asset screening through planting, but ultimately, these do not meet the hard security measures needed for compliance. We note that there are security and biodiversity advantages to using natural resources to reduce sightlines from beyond the perimeter around key structures and attractive or vulnerable targets. Screening works to hide assets but also works with engineering design to force adversaries into a position where they can be monitored. For example, to gain sight of a target, adversaries must move into a location that can be monitored or outfitted with detection technology. These options require careful consideration, as planting should not provide a hiding place for adversaries, which would have the opposite effect.

We considered the incremental impact of our security investments on performance commitments. These do support some risk reduction, as poor or no security can increase the risk of pollution incidents (due to deliberate or accidental actions of someone who should not have had access to the asset). Poor security can also create lower capacity risks due to asset damage and potential pollution incidents from compromised assets. However, as these incidents remain very infrequent, there is no impact in practice on our performance commitments.

We considered the uncertainties relating to costs and benefit delivery. These measures would support compliance with the legal requirements, but it remains uncertain if increased security standards might be required in future reviews. The cost of security products is very reliant on the cost of steel at the point of manufacture, and so we expect our cost estimates to be vulnerable to real price effects on materials and labour rates. We mitigate this risk for all our expenditure together (see **A3 – costs**, NES04).

TABLE 5: SUMMARY OF COSTS (£M)

Solution	NW	ESW	TOTEX	CAPEX	OPEX
Materials costs	£7.428	£0.000	£7.428	£7.428	£0.000
Contract overheads	£2.492	£0.000	£2.492	£2.492	£0.000
Project overheads	£1.022	£0.000	£1.022	£1.022	£0.000
Risk @ 10%	£1.094	£0.000	£1.094	£1.094	£0.000
Maintenance	£1.226	£0.000	£1.226	£0.000	£1.226
TOTAL	**£13.262**	**£0.000**	**£13.262**	**£12.036**	**£1.226**

3.3. CYBER SECURITY

To identify options for investment, we explored the NIST Cyber Security Framework controls[3] – "identify, protect, detect, respond, and recover". We identified areas where good practice enhancements could be made to provide pragmatic levels of mitigation for the predicted threat.

- **Identify** Understanding the environment is essential to managing cybersecurity risks. This includes all digital and physical assets and their interconnections, including understand the risks and exposure.
- **Protect** The appropriate safeguards and controls to prevent, limit or contain the impact of a potential cybersecurity event.
- **Detect** The appropriate measures to quickly identify cybersecurity events. Continuous monitoring solutions to detect anomalous activity and other threats. Visibility to anticipate a cyber-incident and have all information at hand to support an appropriate response.
- **Respond** The ability to contain an incident and respond quickly.
- **Recover** Appropriate activities to restore services following a cybersecurity event.

We developed our options and their associated costs through preliminary market engagement and pricing, which we expect to be refined over time as the requirement is finalised. These costs remain uncertain as these requirements were so close to the end of the business plan process – and we might see changes in the market compared to our early market engagement.

We have collated costs to enhance our security in line with the e-CAF based on all the above criteria. We know that we must remain flexible and able to adapt quickly to new threats and changes in technology and therefore we will carry out further optioneering of solutions and services as part of the individual projects as and when they start.

Table 4 summarises our enhancement investment proposal. The table is collated based on costs to enhance our cyber defenses using today's technology and today's prices. The areas for enhancement are areas we believe need investment to cope with the changes to the e-CAF.

[3] See: https://www.nist.gov/cyberframework

TABLE 7: SUMMARY OF SECURITY CONTROLS AND THEIR ASSOCIATED COSTS

Security enhancement	Solution	Capex (£m, five years)	Opex (£m, five years)	Totex (£m, five years)
Detect	OT Anomaly Detection expansion	0.199	0.514	0.713
	Increased SIEM Ingest	-	1.036	1.036
Prevent	PLC security management	0.500	2.625	3.125
	OT Vulnerability Management	0.030	0.450	0.480
	OT data encryption in transit	0.142	0.234	0.376
	Cyber industrial automated risk analysis	0.050	0.500	0.550
Respond, test, govern and comply	Additional internal resource	-	0.985	0.985
	Supply chain security governance and governance	-	0.764	0.764
TOTAL		**0.921**	**7.108**	**8.029**

We have carried out an initial market engagement process to determine a set of investments to meet the required legislation but recognise that some of the solutions may change as new threats emerge and technology advances over the next few years. We summarise some of the investments based on our current assumptions of enhanced investment below.

Detect: These solutions are to promptly identify cyber-attacks and systems compromise, so as to reduce, or potentially eliminate the impact to our customers.

- **OT anomaly detection and OT Asset management (C1A, C1c, C1e)**. As part of our 2020-25 programme, we are investing significantly in a solution to monitor OT (or Operational Technology) assets and identify anomalous behavior across our highest profile sites. Our current investment is not as broad as the new e-CAF requires and as such we would invest further in this platform to extend the offering to wider reaches of our infrastructure as directed.
- **SIEM ingestion increase (C1A, C1c, C1e).** We currently ingest security data such as alerting from numerous sources into a cloud-based solution called a Security Information and Event Management (SIEM) platform. This information is monitored 24/7 by our managed Security Operations Centre where security incidents un unusual behavior are monitored around the clock. To meet new standards, we would need to ingest more data into the SIEM to provide better alerting and visibility across a broader and more diverse estate. Our estimated ingest would grow from 150Gb per day to 250Gb per day.

Prevent: These proposed solutions are proportionate security measures to help protect essential services and systems from cyber-attack.

- **PLC protection (B2c, B4a, B4b).** OT Defender technologies provides zero-trust device level security for both new and legacy OT assets. PLCs operated by water companies are supplied by several manufacturers but lack secure and deployable and secure password tools across a common interface. They also lack multi-factor capabilities. As a result of this, passwords are either shared or not used and no audit capability is available. We have a fully costed solution that would ensure that all changes to any PLC are both authorised and authenticated, while providing a full audit trail of both successful and blocked changes. This is a requirement for e-CAF compliance, but it is becoming more essential in any case as the technology advances and PLCs are replaced with ip enabled technology which allows remote access.
- **Vulnerability Management (C1A, C1e).** Vulnerability Management platforms are commonplace in IT networks but not so much within OT networks. They scan the network and use I.O.C.s to provide knowledge about where the biggest risks lie so they can be appropriately managed. Our costs are based on estimates that we currently have for deploying vulnerability management on the IT estate.
- **OT data encryption in transit (B4a, B4b).** Secure design and configuration means that it will be imperative to implement encryption of data going across corporate and third party networks (O2 MPLS, 3rd party cellular). This means implementing VPN concentrators and other changes to the network to support this.
- **Cyber industrial automated risk analysis.** This is an automated OT&ICS risk assessment and risk management solution designed to quantify OT cyber risk, provide compliance reporting to security standards such as NIS-D, and ensure effective security mitigation and investment planning to effectively reduce cyber risk within the OT estate. This type of solution helps identify priorities for investment in a changing threat landscape to ensure customer money is spent wisely on mitigating controls.

Respond and recover, identify and govern: These resources will help us govern our systems as well as ensuring we have the capabilities to respond and recover promptly in line with Government advice that companies should start preparing for ‘when’ a cyber-incident happens, not ‘if’.

- **Additional internal resource (C1e).** We need skilled resources to correctly manage our new tools. A significant element of the e-CAF requires appropriate skilled resource to be able to monitor, identify, investigate, and report on vulnerabilities, events, and incidents. In addition to this, the changes to the OT network technology over the period to a more connected/IP-based infrastructure means that the scope of cyber risk that falls under NIS-D will expand significiantly. This means we need three new roles (two OT security operations, and one OT security governance role). We have carried out external benchmarking for salaries for two roles, at a cost of around £197,100 per year for three roles.
- **Supply chain security governance and assurance**. We must make sure our own environment is secure - but our supply chain for security measures is just as important. Following conversations with NCSC, DWI, DEFRA

and other interested parties, the NIS-D is likely to introduce elements of enhancing supply chain security assurances during 2025-30. This would fall in line with the European NIS-2. As such we need mechanisms to ensure our supply chain is secure. 'Security Scorecard' is one of several information security companies that rates cybersecurity postures of corporate entities through completing scored analysis of cyber threat intelligence signals for the purposes of third-party management and risk management. Insurance companies also use these products to provide them with cyber risk information. We have asked potential suppliers to provide costs for providing security risk insights for around 100 key suppliers within our NIS-D supply chain (and our costs are based on information from suppliers). In addition to this, we will need an additional role in our procurement team to manage the cyber security tooling and interaction with our NIS-D supply chain to ensure compliance (our costs are based on externally benchmarked salaries).

We have estimated these costs based on estimates to deploy today. However, we know that these costs will vary over time, and we will thoroughly explore and implement these costs based on the risk and technology at the time of implementation. Although the solutions used may vary, the outcome and areas requiring investment will not.

In the long-term, the cyber security environment remains extremely dynamic – this is not similar to traditional water company investment, and there are many uncertainties. For example:

- Technology changes quickly and new technology presents new threats.
- Security solutions may disappear or merge with other solutions.
- The threat landscape changes very quickly depending upon areas outside of our control. This could be anything from cyber criminals inventing new malicious software, to cyber conflict from the other side of the world resulting in our water systems being attacked by hostile foreign states.
- The threat will change in line with foreign state investment, malicious and mischievous members of the public, IT savvy members of the public, terrorism, as well as new technology creating more opportunities for accidental breaches. We know that the high-tech hacking technology that was only in the hands of Governments and the intelligence services a few years ago is now in the hands of cyber criminals who have brought harm to several large organisations in recent years. This trend will continue in line with the rapid pace of technology.
- License costs can change dramatically based on the business decisions of the supplier and who our wider technology is tied into.
- The NIS Regulations will almost certainly change further during the AMP to further enhance areas such as our supply chain or to bring wastewater into scope.

Although our enhancement expenditure is about meeting regulatory requirements, we strongly believe that this alone does not make our business more cyber secure. We will continue to use our base expenditure budget to support risk reduction in other areas which fall outside of the current NIS-D framework, such as wastewater.

3.4. CUSTOMER VIEWS ON OPTIONS

We have not discussed options for either physical security or cyber security with our customers. In our customer engagement, our customers told us that they expected us to engage with experts on the ways to tackle resilience, rather than discussing options with them directly (our **Shaping Our Future** research). Our customers expect us to meet our statutory requirements.

In this case, we have selected least-cost options and have eliminated other options in the filtering stages, rather than there being choices to make between least-cost and best-value options (which might deliver wider social and environmental benefits, for example). The remaining options are technical and require specialist and detailed knowledge of the statutory requirements to make decisions – so we have made these choices through engagement with Defra and DWI, rather than asking customers about technical options, in line with our customers' expectations.

4. COST EFFICIENCY

a) Is it clear how the company has arrived at its option costs? Is there supporting evidence on the calculations and key assumptions used and why these are appropriate?

b) Is there evidence that the cost estimates are efficient (for example using similar scheme outturn data, industry and/or external cost benchmarking)?

c) Does the company provide third party assurance for the robustness of the cost estimates?

We have estimated the costs of our options based on preliminary market testing where possible, or historic unit costs where this is not possible. We describe in Section 3 how we have carried out desktop studies and site surveys to determine the most cost-effective solution, and then used actual costs from similar projects to derive total costs.

We have not been able to provide industry or external cost benchmarking on these costs. The costs for our physical security investments have been subject to third-party assurance provided by Mott MacDonald in June 2023. Mott MacDonald used cost curves from our “iMod” cost database and calculated appropriate contract overheads.

4.1. PHYSICAL SECURITY AT BOTH WATER AND WASTEWATER SITES

Our investments have been driven by the recommendations from the Security Risk Assessment and CNI survey process. We developed our cost estimates using unit cost benchmarking and forecasting of historical spending in AMP 6 for similar solutions. We have then undertaken preliminary market testing where we could.

Since this is a statutory requirement, the most cost-effective solution is selected from the range of options available using WaterUK's Security Standards V4.2 2023 (WUKSS) options grid. While the guidance is quite restrictive by defining relatively narrow outcomes to be delivered and, in most cases, a prescriptive set of ways to meet the requirement, we are expected to the options grid documented in WUKSS as this provides a complaint, protective security solution for non-CNI assets. CNI-designated assets are expected to have additional security measures that provide a layered depth of security protection with a vulnerable or contamination point at the centre of that protection. We have therefore used the Water UK options grid as a baseline security requirement and added additional security measures to harden the CNI asset base.

We will need to install new physical and electronic security solutions at the relevant sites. We completed a desktop study and site survey for each site to determine the most cost-effective solution at these. We then used actual costs from similar projects previously delivered to determine an overall cost.

Many of the proposed and considered solutions have already been installed, in some way, on our estate during AMP6 (2015 to 2020). We gathered detailed costings of these solutions and verified these with third parties through market

testing, and then extrapolated these to prepare the detailed costings for the AMP8 schemes. So, we have a high degree of confidence in the submitted costings. When schemes have both an enhancement element and a base element due to overlapping non-CNI security requirements, we only included the additional costs associated with the CNI classification in this enhancement case. And when schemes have an enhancement element and a base element due to overlapping non-COMAH security requirements, we only included the additional costs associated with the COMAH classification in this enhancement case.

We developed our costs after consulting approved suppliers. We have obtained many quotations for standard specified products, such as doors, fencing, window bars, and hatches. These were based on the standard specifications for each of these products, with the least-cost option that would achieve compliance with WaterUK Security Standards. We explored the market so that we could estimate costs for each of these security productions accurately. We then used these costs to build the CNI and COMAH enhancement case values, accurately representing 2022-23 market rates.

CNI sites generally have consistent security requirements. Typically, the most cost-effective and practical solution that meets requirements involves perimeter fencing and securing each location rather than securing each access or contamination point – such as valves.

Where VP/CP are co-located, we have included cost efficiencies where we could, with the lowest cost option selected to secure both points within the same solution. It has been further possible to improve the security of three CNIKB function assets by using the security countermeasures to protect more than one element of CNIKB, resulting in large cost savings in the implementation of a single security solution for multiple CNI functional assets and significantly reducing the total cost of the overall CNI enhancement.

As well as material costs, we have tested delivery costs against our framework (as this work will likely be carried out by one of our framework partners). This helps to make sure we have applied correct market values for delivery.

The costs generated for this enhancement case have been subject to third-party assurance provided by Mott Macdonald in June 2023. Mott Macdonald used iMod cost curves for the project and contract overheads to estimate the overheads.

Following this assurance, our subsequent analysis used iMod cost curves better suited to the specific works involved, removing possibilities such as access roads, compounds, and accommodation which won't be needed within these works. This helped to improve our estimate of costs.

4.2. CYBER SECURITY

We have developed our cyber security costs based on preliminary market testing where possible, where there are relevant suppliers already. Where we could not do this, we have estimated costs based on quotes or historic costs for similar work

(this is more difficult than for physical security, where we have installed similar measures before). For resourcing costs, we have tested the market through external benchmarking for roles (where we do not currently have comparators).

We do not have industry benchmarking for these costs, as these are a new requirement. We also do not have third party assurance for these costs yet, as these are a late requirement and our suppliers do not have costs to compare.

5. CUSTOMER PROTECTION

We have not proposed any specific price control deliverable (PCD) for SEMD or cyber security. SEMD is a legal requirement and failure to meet these requirements would result in enforcement action against us, providing a strong incentive for delivery. We are also required to provide a regular update to Defra on the progress of these schemes.

We have assessed these investments against Ofwat's criteria in **IN23/05** for PCDs. Neither our physical or cyber security investments are considered material for the purposes of setting PCDs, as they are below 1% of water and wastewater totex. As set out in IN23/05, this materiality threshold should be applied separately to these two items as these are different enhancement line groupings.

As the enhancement investment does not meet the materiality threshold, we also further considered if we needed to propose additional price control deliverables anyway – but we concluded that as there is strong oversight of project delivery from other regulators (in this case, Defra, DWI, and HSE) and this is not required under Ofwat's guidance.

Further to this assessment, it is relatively easy for Ofwat to understand and make sure that these investments are not funded twice. The investments at PR24 will fully fund the requirements to meet physical security standards for newly designated CNI and COMAH sites following SEMD 2022; and will fully fund the requirements to meet e-CAF standards as required by 31 March 2028.

We expect that there will be additional security requirements during 2025-30 that require additional investment. Where this is the case, we will use efficiencies and cost sharing to fund this within our PR24 cost allowances (unless wider circumstances meet the thresholds for existing uncertainty mechanisms and reopeners). This was our approach during AMP7, where we have already met some of the new requirements without additional funding.

There are no third-party funding or delivery arrangements for this investment.

ANNEX A: DWI LETTER

Drinking Water Inspectorate
Area 1A, Nobel House
17 Smith Square
London SW1P 3JR
Enquiries: 0330 041 6501
E-mail: DWI.Enforcement@defra.gov.uk
DWI Website: www.dwi.gov.uk

DWI reference: SEMD_NES_01

25 August 2023

Mr Andrew Beaver
Water Director
Northumbrian, Essex and Suffolk Water
Sandon Valley House
Canon Barns Road
East Hanningfield
Essex
CM3 8BD

Dear Mr Beaver

Periodic Review 2024: Northumbrian, Essex and Suffolk Water

DWI Scheme reference: SEMD_NES_01 - CNI Protective Security - New CNI Designation

Final Decision Letter – Support Proposed Scheme

The Inspectorate has completed its detailed assessment of the scheme proposed by Northumbrian, Essex and Suffolk Water to increase the security to the required standards to facilitate compliance with the Security and Emergency Measures Direction 2022 at 30 CNI Sites (and associated assets as applicable). A summary of the outcome of our assessment of this scheme is attached.

Based on the information submitted by the company, the Inspectorate **supports** the need for this scheme, and the supported scheme shall be included by the company in its Final Business Plan, subject to the caveats listed in the attachment.

Consequently, a blank section 19 Undertaking schedule template has been attached to this letter for the company's review. I would be grateful if the company could add measures as appropriate, to this template and send the completed template back to DWI.Enforcement@defra.gov.uk by 30 November 2023.

I am copying this letter to

- Paul Martin, Ofwat

Yours sincerely

Nicholas Adjei

Deputy Chief Inspector, on behalf of the Secretary of State for Environment, Food and Rural Affairs

Cc Simon Hodges, Northumbrian, Essex and Suffolk Water
Cc Simon Benton, Principal Inspector (Enforcement), Drinking Water Inspectorate
Cc Daniel Giblin, Company Liaison Inspector, Drinking Water Inspectorate
Cc Michael Wood, Principal Inspector (SEMD), Drinking Water Inspectorate

Department for Environment, Food and Rural Affairs Llywodraeth Cymru Welsh Government

Periodic Review 2024: Summary of DWI Assessment –Supported

Water Company Name: Northumbrian, Essex and Suffolk Water

DWI Scheme Reference: SEMD_NES_01

Scheme Name: CNI Protective Security

Proposal:

Increase the security at 30 CNI sites to the required standards. 28 of these sites are newly designated.

Supporting Evidence:

Risks described in the formal PR24 submission and the most recent RAG return, provided to the Drinking Water Inspectorate.

Conclusion:

The Drinking Water Inspectorate supports the delivery of this scheme in order to secure or maintain compliance with the requirements of the Security and Emergency Measures Direction, subject to the following caveats.

Caveats: No Caveats

Timescale: End March 2030

Estimated Cost: £15.5 million

Legal Instrument Required: Undertaking, under section 19(1) of the Water Industry Act 1991 (as amended).

Comment:

The Inspectorate has concluded that there is a breach, or likely breach in the next 5 years, of paragraph 7 of SEMD 2022 or relevant guidance (Emergency Planning Guidance (EPG), Protective Security Guidance (PSG) and Water UK security Standards (WUKSS).

Paragraph 7 states that the company must identify and assess any security risks to the provision of its water supply or sewerage functions. It must put in place measures to avoid or, if this is not possible, mitigate those risks.

The Inspectorate has no role in determining proportional allocation of expenditure. Where technical support from the Inspectorate is given, this should not be taken by the company to imply that the scheme will be partially or wholly funded.