Simon Wood
Environment, Health & Safety
Specialist

37-39 High Holborn
London
WC1V 6AA

Direct telephone: 020 7269 7607
UKPIA switchboard: 020 7269 7600
Email: simon.wood@ukpia.com

10th April 2022

NIS Regulation Team
Department for Digital, Culture, Media & Sport
4th Floor - area 4/48
100 Parliament Street
London
SW1A 2BQ

Response to the Consultation on Proposal for legislation to improve the UK's cyber resilience

UK Petroleum Industry Association (UKPIA) represents the eight main oil refining and marketing companies operating in the UK. The UKPIA member companies – bp, Essar, Esso Petroleum, Petroineos, Phillips 66, Prax Refining, Shell, and Valero – are together responsible for the sourcing and supply of petroleum products meeting over 85% of UK inland demand, accounting for a third of total primary UK energy.

The refining and downstream sector currently lies at the heart of the UK economy, providing a secure supply of affordable energy for transport and buildings whilst supplying feedstocks for the petrochemicals sector and specialised non-energy products such as lubricants, bitumen, and graphite for use in electrodes.

The UK downstream sector is also currently the largest hydrogen-producing sector in the UK, responsible for almost half of UK production.

Response to the consultation

Question 1. Do you agree that managed services should be brought into the scope of NIS Regulations? [YES/NO]

Question 2. Do you agree with the examples of managed services proposed to be within or out of scope of the NIS Regulations, provided in Annex 1? [YES/NO]

Question 3. IF NO AT Q2. Please explain the reasons for your answer:

Member response
UKPIA agrees with the criteria and nature of the managed services that are proposed for inclusion within the scope of the NIS Regulations.

Question 4. Do you agree that the range of managed services brought into scope of NIS legislation should be defined by the following characteristics?

A. They are supplied to a client by an external supplier [YES/NO]
B. They involve regular and ongoing service management of data, IT infrastructure, IT networks and/or IT systems [YES/NO]
C. They are categorised as business to business (B2B) rather than business to consumers (B2C) services [YES/NO]
D. Their provision relies on the provider's own network and information system [YES/NO]

Question 5. IF NO AT A - D IN Q4: Please explain the reasons for your answer

Member response
UKPIA has no comments.

Question 6. Do you agree that the definition of managed services subject to regulatory obligations under NIS should be narrowed further? [YES/NO]

Question 7. How effective do you believe each of the government's proposed options for narrowing the definition of managed services will be?

- Have privileged access or connectivity to a customer's data, IT infrastructure, IT networks and/or IT systems
- Perform essential or sensitive functions
    - Very effective
    - Somewhat effective
    - Not at all effective
    - Don't know

Question 8. Please explain why you believe each of the proposed options to be effective or ineffective.

Member response
UKPIA believes that a narrower definition of managed services would limit the scope and reduce the number of entities involved. UKPIA also considers this to be a sensible approach in the first instance. This is because of the digital interconnectivity of the value chains of the businesses involved in the Downstream Oil Sector. However, once the system is implemented and reached a mature state, it may then be worth considering a widening of the scope to include more entities as without doing so could have an adverse impact on the UK's Cyber resilience.

Question 9. If VERY EFFECTIVE at Q7B please include specific essential or sensitive functions which you think should be included within a definition of managed services.

Member response
UKPIA has no comment to this question.

Question 10. Please suggest any further options for characteristics which could be applied to defining managed services.

Member response
UKPIA has no comment to this question.

Question 11. Do you think that the exemption for digital service provider small and micro-businesses should be modified to enable a small number of critical providers to be brought under scope of NIS Regulations? [YES / NO]

Question 12. Please explain your answer.

Member response
UKPIA believes that an exemption for digital service provider small and micro-businesses should be modified to enable a small number of critical providers to be brought under scope of NIS Regulations. This is because of the digital interconnectivity of the value chains of the businesses involved in the Downstream Oil Sector. However, once the system is implemented and reached a mature state it may then be worth considering a widening of the scope to include more entities. This would strengthen the UK's Cyber resilience.

Question 13. Are there any other comments you would like to make about this measure?

Member response
UKPIA has no comment to this question.

Question 14. Do you agree with the Government's proposal to specify a two-tier supervisory regime for providers of digital services? [YES/NO]

Question 15. Do you agree with the Government's proposal to define the factors that the ICO should take into consideration as part of the two-tier supervisory regime? [YES/NO]

Question 16. Do you agree that further guidance on supplier-customer cyber resilience cooperation is necessary, particularly as part of a supervisory regime for the most critical digital service providers? [YES/NO]

Question 17. How effective do you believe each of the government's proposed options for factors would be in ensuring the digital services most critical to the UKs resilience are captured?

A. The criticality of the customers supplied

B. The level of dependence of the customer on the service
C. The level of connectivity and access to the customers network
D. Market reach (e.g. average annual number of clients supported by a service)
E. Scale (e.g. annual staff headcount of a service)
F. Financial
G. Concentration in the market
H. The likely consequences for national security

Very effective
Somewhat effective
Not at all effective
Don't know

Question 18. Please explain why you believe the proposed options to be effective or ineffective.

Member response
UKPIA has no comment to this question.

Question 19. Do you have any suggestions for alternative factors that should be considered?

Member response
UKPIA has no comment to this question.

Question 20. Are there any other comments you would like to make about this measure?

Member response
UKPIA has no comment to this question.

Question 21. Do you agree with the UK government having power to amend certain elements of the NIS Regulations and the UK version of the Commission Implementing Regulation 2018/151 through secondary legislation? [YES/NO]

Question 22. Do you agree with the safeguards and limitations proposed in this document? [YES/NO]

Question 23. IF NO AT Q22: Which safeguards do you consider to be inappropriate for this proposal?

Member response
UKPIA has no comment to this question.

Question 24. Are there any other safeguards or limitations that you feel that the government should consider?

Member response
UKPIA welcomes the proposal ensuring a requirement to both consult and produce impact assessments, before utilising delegated powers to amend certain

elements of the NIS regulations, is safeguarded. However, there is a danger that since impact assessments are formulated by DCMS and tend to use a range of government-based assumptions which may be subject to significant bias and may result in inappropriate impact assessment conclusions occurring. This may have the undesired effect of providing an opportunity for the abuse of the delegated power which the safeguards should specifically aim to avoid. Therefore, suitable provisions also need to be included to ensure that impact assessments are created in partnership with industry, operators and affected parties so that any impact assessment then includes the true impact costs.

For example, the reporting cost of the impact assessment makes assumptions about the median hourly wage paid to legal professionals, IT professionals and board members. These may appear grossly undervalued versus true market costs of people working in these type of job roles, the result being an underestimated impact assessment.

Question 25. Are there any areas of the NIS Regulation in the UK which you think should not be included in the delegated power? [YES/NO]

Question 26. IF YES AT Q25: What area(s) should not be included and why should it not be updated using secondary legislation?

Member response
UKPIA has no comment to this question.

Question 27. Are there any other comments you would like to make about this measure?

Member response
UKPIA has no comment to this question.

Question 28. Do you agree with the government's proposal for a delegated power that would allow the government to amend the NIS Regulations to expand the scope of the NIS framework? [YES/NO]

Question 29. IF NO AT Q28: Please explain your answer.

Member response
UKPIA has no comment to this question.

Question 30. Do you agree that this measure should contain safeguards and limitations? [YES/NO]

Question 31. IF YES AT Q30: What safeguards and limitations do you think should be in place?

Member response
UKPIA welcomes the measure safeguarding the views of interested and affected parties, ensuring that they are considered when developing national policy. This will ensure that the policy is relevant, appropriate and effective. However, UKPIA is concerned that the safeguard, to only 'consider' views may enable delegated powers to be inappropriately used. It is therefore suggested this safeguard should be expanded to ensure that both: 1. a minimum % of affected parties views are received as part of that consultation; and 2. that any significant objections (for example >30% of consulted parties) to the proposed amendments would prevent delegated powers being allowed to push through scope changes.

Question 32. Do you agree that there are benefits in additional sectors (such as those examples listed in the rationale section) being designated under NIS? [YES/NO]

Question 33. If YES AT Q32: What benefits do you see in additional sectors being designated under NIS?

Member response
UKPIA has no comment to this question.

Question 34. Are there any other comments you would like to make about this measure?

Member response
UKPIA believes that careful consideration and allowances need to be made for the selection of a competent authority for any new industry sector. Measures should ensure that where an organisation or facility which is already included as a NIS operator (through existing NIS scope) it is not subjected to additional regulatory burden from the expansion or scope / introduction of an additional competent authority. For example, if the scope were to increase to include chemicals manufacturing organisations, and those facilities or organisation were already considered a NIS operator under existing energy thresholds. Provisions should therefore be made to ensure consistency and efficiency ensuring an operators cyber resilience is assessed as a whole, by a single competent authority (CA). UKPIA believes that a single CA for the assessment of the entire facility / organisation under NIS should be identified as the responsible regulator. Our concern is that industry may be presented with the situation where the same cyber security management system is assessed by two different CAs. This has

the potential for different interpretations and would be overly burdensome for the affected organisations for no net benefit to the risks being managed.

Question 35. Do you agree that the government should be granted the power to designate critical dependencies? [YES/NO]

Question 36. Please provide any suggestions for changes or an alternative approach that would allow for the designation of critical dependencies.

Member response
UKPIA has no comment to this question.

Question 37. Are there any additional safeguards that you think are necessary?

Member response
UKPIA has no comment to this question.

Question 38. Are there any other comments you would like to make about this measure?

Member response
UKPIA has no comment to this question.

Question 39. Do you agree with expanding incident reporting duties to include incidents that do not affect continuity? [YES/NO]

Question 40. Please explain your answer.

Member response
Such an expansion to incident reporting duties will result in: • Increased burden (potentially substantial) on essential service providers. • A potentially very difficult, costly or complex solution required to assess incidents and report them. • Potentially an unenforceable regulation. • Intangible benefits in terms of reducing risk to essential services at a cost to UK industry. • Reduced competitiveness versus conducting business in non-UK nations. • Reduced budgets for cyber protective measures as a consequence of reporting costs escalating – i.e., potentially directly reducing cyber resilience overall. UKPIA believes that the impact assessment for incident reporting figure quantifying the cost per incident report as £59.54 is grossly underestimated. It is our view that this number is fundamentally flawed in a number of ways. By way of simple example, it estimates the median legal professional rate as ~£25 per hour, yet according to the government's own guideline figures for solicitor rates

(https://www.gov.uk/guidance/solicitors-guideline-hourly-rates) the true number should be in the region of £218-512 per hour.

The same £59.54 figure also vastly underestimates the number of people involved, the wage of those individuals and the complexity/cost of implementing/maintain systems to detect and trigger reporting.

UKPIA believes that the true cost to industry of incident reporting based on the existing NIS provisions is therefore significantly higher. For example, if the true cost to industry is in the region of £2000-5000 per reportable incident, then the cost of reporting incidents under NIS for ~2480 reportable incidents quoted would be expected to be in the range of ~£5M-12M. This is significantly more than the low end of ~£79k suggested in the impact assessment. If the open-ended expansion of reporting duties proposed under this consultation is adopted, the true cost to operators of additional reporting duties has the potential to spiral considerably. This will place a significant financial risk and burden on operators.

We would be grateful if DCMS would give further consideration to the overall negative impact of the cost of reporting on the UK's cyber resilience. Negative impacts may be caused by operators having to expend or divert funds to meet additional reporting duties. This will be especially evident when the scope of these additional reporting duties for incidents do not impact service provision directly rather than for incidents with a potential to impact a service provision.

It is noted the consultation impact assessment confirms that "there is very little understanding" of how organisations detect and manage incidents. It also indicates that DCMS does not fully understand what these incidents look like or how many incidents there will be. This is a concern as the impact assessment does not include any realistic account for true cost to industry by proposing such an expansion. Similarly, the assessment indicates that the true cost to both competent authorities and NCSC has not been possible to quantify or included within the impact assessment.

UKPIA believes that the work stream DCMS says is planned to further understand reportable incidents needs to be completed. Only then can DCMS complete a full true impact assessment before considering any expansion to reporting duties within the NIS regulations.

Question 41. Do you agree with the below proposal for the additional incident reporting requirement? [YES/NO]
"Any incident which has a significant impact on the availability, integrity, or confidentiality of networks and information systems, and that could cause, or threaten to cause, substantial disruption to the service."

Question 42. Please explain your answer.

Member response
UKPIA believes that the definition is too vague and subject to interpretation, the result being that: • A CA has the ability set overly burdensome thresholds without consequence or benefit. • The burden on organisations of meeting such an increased reporting requirement may be both substantial and not consummate with the risk. • The complexity with attempting to understand if an incident that 'could' threaten disrupt a service is open to interpretation and will either result in no tangible increase in reporting rate, create overly onerous & costly reporting duties or create an increase in subjective disputes where a CA opinion may differ to operator opinion. The NIS already requires operators to have sufficient systems / management systems in place to detect, respond and recover from any cyber incidents with potential to disrupt services. Reporting of such incidents therefore provides no real reduction of risk to the service but will almost certainly increase costs, complexity and regulatory risk for operators.

Question 43. Please provide any alternative suggestions for how the additional incident reporting requirement could be defined?

Member response
UKPIA would suggest no additional reporting requirements are defined – i.e no change.

Question 44. What factors do you feel are most important in assessing whether an incident has the potential to impact the continuity of the service?

Member response
It is suggested that the scope of incident reporting should be limited to only equipment with a direct NIS duty as it is now. I.e. only implement reporting for those computing or networking equipment directly in the scope of equipment involved in providing the essential service provision. It is already a requirement of NIS that operators understand the scope of this equipment and deploy appropriate countermeasures accordingly. Considering incidents beyond this scope of equipment would be open ended, it would then become be both difficult and expensive to implement while potentially impossible to enforce for reasons given in previous responses above.

Question 45. Are there any other comments you would like to make about this measure?

Member response
When considering the potential global footprint of several NIS operators the proposed measure introduces the following issues: • The potential for competing / conflicting regulations which an operator may not be able to meet. • The potential for regulatory burden to be significant with multiple nations regulators investigating potentially the same incident. • The potential burden on an organisation may be significant and costs incurred across multiple nations. UKPIA believes that the cost/benefit analysis, in support of the increased reporting requirement, should also factor in that both CA and operators will face increased costs. It is also concerning that a separate section of the proposal suggests that the CA will be adopting a full cost recovery model. This is somewhat of a contradiction as the cost is in fact solely incurred by operators only. Operators pay the cost of providing increased reporting, they also incur the cost of the CA in receiving these incident reports. Industry then also incurs the cost of a CA assessing a reporting organisation. The beneficiary of this cost is the competent authority with increased threat intelligence awareness. This is not the same as a more cyber resilient industry or service provision as a result the burden of cost is inappropriate and held solely by industry. Additionally certain NIS industries/operators operate on UK soil to the overall advantage of the UK. For instance, by providing better UK services, security, regulatory oversight, employment opportunities and development of UK skills. UKPIA believes that further consideration should be made of any expansion of NIS regulations which would make it more expensive to conduct that service on UK soil versus conducting that similar business within other nations.

Question 46. Do you agree that the current cost recovery mechanism (invoice-based) needs to be changed? [YES/NO]

Question 47. Please explain your answer.

Member response
It is fair that the regulator would recover their costs for time spent working on a specific incident or advising industry. Therefore, it is fair to expect that the number of hours companies see charges for is proportionate, risk and performance based, and that requirements are efficiently brought to conclusion. Cost recovery should be fair, transparent and accountable.

Question 48. How should the government best fund regulatory oversight of the NIS regulations?

Member response
UKPIA believes that national bodies delivering regulatory oversight under legislation such as the Health and Safety Executive and Environmental Agencies cost recovery mechanisms are good examples for DCMS to consider.

Question 49. How effective do you believe each of the government's proposed options for how competent authorities should recover their costs from companies will be?

- Option 1: Remove the limitation in the legislation and expand cost recovery to all regulatory activities
- Option 2: Introduce a 'hybrid' cost recovery model, which allows competent authorities to both recover costs on an estimated/projected basis (through monthly/quarterly/annual fees), and to recover exact costs through invoices
    - Very effective
    - Somewhat effective
    - Not at all effective
    - Don't know

Question 50. Please explain your answer.

Member response
UKPIA believes that either cost recovery option would be appropriate.

Question 51. Do you have any concerns about the burden that this proposal would place on regulated organisations, in light of other regulations they may be subject to? [YES/NO]

Question 52. Please explain your answer.

Member response
UKPIA has no comment to this question.

Question 53. Please provide any other suggestions you may have for other options for how competent authorities should recover their costs from companies.

Member response
UKPIA has no comment to this question.

Question 54. Are there any other comments you would like to make about this measure?

Member response
UKPIA has no comment to this question.

Thank you for the opportunity to respond to the consultation.

Yours sincerely,

Simon Wood
Environment, Health and Safety Specialist