The voice of the energy industry

Energy UK response to the Department of Digital, Culture, Media and Sport's Security of Network and Information Systems (NIS) Directive Consultation

30 September 2017

About Energy UK

Energy UK is the trade association for the GB energy industry with a membership of over 90 suppliers, generators, and stakeholders with a business interest in the production and supply of electricity and gas for domestic and business consumers. Our membership encompasses the truly diverse nature of the UK's energy industry – from established FTSE 100 companies right through to new, growing suppliers and generators, which now make up over half of our membership.

Our members turn renewable energy sources as well as nuclear, gas and coal into electricity for over 26 million homes and every business in Britain. Over 619,000 people in every corner of the country rely on the sector for their jobs with many of our members providing lifelong employment as well as quality apprenticeships and training for those starting their careers. The energy industry adds £83bn to the British economy, equivalent to 5% of GDP, and pays over £6bn in tax annually to HMT.

Executive Summary

Energy UK welcomes the opportunity to work with Department of Digital, Culture, Media and Sport (DCMS) via consultation response on the transposition plans for the Network and Information Systems (NIS) Directive. We and our members broadly support the proposals set out by Government in their consultation around strategies to ensure those sectors providing an essential service are prepared to meet the demands of a modern cyber-attack capability. Our members further welcome the opportunity to deepen their relationships with the National Cyber Security Centre (NCSC), Department of Business, Energy and Industrial Strategy (BEIS) and DCMS as a result of the NIS Directive's transposition into UK law.

Whilst Energy UK appreciates the difficulty of ensuring an appropriate consultation period is granted given the General Election, we and our members determine the proposals and associated timeframes to be unclear in the former and too short in the latter to realistically implement the reporting obligations and security principles set out in this consultation. Energy UK recommends a transition period be implemented to allow for appropriate implementation of the principles and reporting obligations placed on operators of essential services (OES).

We support the designated bodies of CSIRT, SPOC and Competent Authorities, with the caveat stated in the questions on the same subject below. Having said this, we have strong concerns over several aspects noted in the consultation from DCMS namely; lack of clarity around the OES thresholds and reporting obligations. Energy UK also strongly believes the penalty regime is too high and is not proportionate to the risk of disruption to the service provided by operators. Energy UK further questions the lack of consideration given to the Data Communications Company (DCC) who, through the Smart Meter Roll Out, work with a significant body of sensitive data - potentially targetable for security breach impacting millions of consumers - and so could be deemed an OES.

Energy UK strongly recommends DCMS clarifies the aspects above to ensure not only that the correct OES are aware of their obligation to comply, but they are aware of what should be reported on as a 'significant incident' and which security principles should be adhered to, so we as an industry of critical infrastructure, can better understand how best to be resilient.

For more detail about the questions posed within the consultation document please refer to the responses submitted by our members. Should you have any questions regarding this consultation response then please do not hesitate to get in touch via the details below.

Yours sincerely,

Tanisha Beebee
Policy Executive, Generation
Energy UK, Charles House
5-11 Regent Street, London, SW1Y 4LR
tanisha.beebee@energy-uk.org.uk

Response to Questions

1. Are the identification thresholds set at a level that captures the most important operators in your sector based on their potential to cause a significant disruptive effect if disrupted? YES/NO

No.

2. If not, why not? What would you change and why? Narrative response

For the electricity subsector, providing the essential service of electricity supply, it is unclear at which point the threshold designates an operator of this essential service. First, the definition of a 'common control network' requires substantially more detail. The UK energy market is made up of energy companies who tend to have more than one asset/power station site in their portfolio, of which the majority on their own generate < 2GW. Whilst these assets are separated by location, some do share common networks, be it corporate or trading and dispatch. Some are linked by firewalls and others by intranet. Whilst these linkages are not necessarily 'true control systems', an attack on one asset's network could impact another. In this vein, Energy UK seeks clarity on whether 'cumulative capacity > 2GW controlled by an individual/common control network' applies to individual, single control network sites generating over 2GW (i.e. DCS) or several sites under the same umbrella company cumulatively generating over 2GW? If the former, very few operators would be included in the scope set out by DCMS and taking this approach, would not necessarily address all the risks identified in the NIS Directive.

There is an increasing risk that the many sites below 2GW could cause a significant disruptive effect if disrupted simultaneously; therefore it may be appropriate for these sites to be included in scope, to increase their resilience. Growing on this point, Energy UK members already take cyber security incredibly seriously as their companies make up a significant portion of the UK's critical national infrastructure – for those not deemed an OES under the proposed thresholds, we hope to see a separate set of principles or guidance be created. In terms of 'Reserve Power', does this refer to stored energy or Black Start? If so, further consultation will be necessary to determine which OES will be impacted.

Energy UK seeks clarity on exactly when OES' will be notified that they fall within the identification thresholds and who will be notified in the OES. Energy UK recommends liaising with industry working groups to determine who best to inform that the NIS Directive will apply to each operator.

3. Do you agree with the government's proposed approach of adopting a multiple competent authority model? YES/NO

Yes.

4. If not, why do you believe a single competent authority model represents a better option? Do you have an alternative outside of these two models? Narrative answer.

N/A.

5. Is the proposed competent authority for your sector a suitable choice? YES/NO

No.

6. If NO, who do you believe should be the competent authority for your sector and why? Narrative answer.

Whilst Energy UK members agree that a multiple competent authority model is best as this ensures the necessary experience in the workings of this sector to aid the enforcement and support of the NIS Directive, together BEIS/NCSC with the possibility of enforcement from Ofgem could pose a complicated mix as each entity's existing responsibilities are currently quite different in the sector. Should Ofgem be delegated compliance responsibilities from the competent authority, we would ideally like to see a transition period to allow for Ofgem's learning and understanding to grow to competency level in this area.

Energy UK sees great importance in the continuation of good relationships between industry bodies, the regulator, BEIS and the NCSC fostering collaboration in policy development, and transposition of the NIS Directive should not hinder this. As such, Energy UK seeks clarity on which body will hold exactly what responsibility with regard to NIS Directive's implementation. For example, will BEIS produce guidance for implementation, but Ofgem enforce action where breaches are identified? Who will be taking 'action as a last resort?' More clarity is needed to identify which body holds which responsibility.

7. Do you believe these high level principles cover the right aspects of network and information systems security to ensure that risks will be appropriately managed? YES/NO

No.

8. If NO, can you clarify what aspects you believe are missing and recommend how we could address these? Narrative answer

The energy industry continues to work heavily with legacy operating systems. The high level security principles fail to give attention to obsolescence of legacy systems which are still in use on numerous power station sites. Several systems in use are not patchable or updatable (some run on Windows NT for example) and so extra risk management or mitigation policies should be considered and implemented to adhere to the existing systems, not covered in the high level principles.

Alternatively, Energy UK recommends that OES be given the flexibility to demonstrate other methods of protection on their ICS systems based on their own internal risk assessments and asset topologies. The guidance and principles should then be drawn on to determine the next security decision.

Energy UK supports the aspects of the principles and guidance which bare similarities to ISO27001 and other existing guidance documentation such as the NIST Cyber Security Framework, as it ensures an ongoing, joined up approach to cyber security.

Energy UK strongly recommends a draft CAF be published ahead of January 2018 to enable OES to prepare for the forthcoming security principles to which they will be required to adhere to in May 2018. In order to measure compliance, we recommend a separate consultation on the security principles to deem their appropriateness for each industry OES, as well as a draft CAF be published in 2017.

9. Do you believe these principles would impose any additional costs on designated operators, or on the sectors in scope as a whole? YES/NO

Yes.

10. If YES, what do you consider would be the anticipated resource implication on designated operators, or on the industry as a whole of meeting these principles? Are you able to elaborate on the nature of these costs? Where possible please detail any specific financial costs you consider would likely result. Narrative answer

Energy UK has received numerous recourse implication examples and individual costs associated with imposing the principles on the OES. Energy UK recommends DCMS refers to individual energy company consultation responses for specific examples of resource pressures and additional costs. In summary, some costs involve (but are not limited to); human factors such as hiring additional staff (both for security and for legal purposes), training programs and significant technical costs such as data analytics, anomaly detection, general separation firewalls and asset discovery systems among many more.

The simultaneous arrival of several regulations also increases the pressures and costs on operators to provide resources which are costly to augment from the marketplace.

11. Do you have any plans to make additional security related investments as a result of this Directive? Where possible please indicate the size of investment (in £)? YES/NO

Please see answer to question 10.

12. If YES, please provide the amount and details of what investments would be required. Narrative answer

Please see answer to question 10.

13. Do you consider these incident reporting proposals to be reasonable to ensure that serious incidents affecting the network and information systems of essential services are reported? YES/NO

No.

14. If NO, why not? Can you suggest revised incident reporting proposals that ensure serious incidents are reported? Narrative answer

Energy UK proposes that DCMS considerably clarifies what is deemed a 'serious incident'. Where some incidents take place which impact a given operating system within an OES, this may not impact electricity supply (to the Grid or consumers) and thus may not cause a 'significant impact'. The majority of incidents which do take place are not significant enough to be deemed reportable under the consultation's definitions on page 19. Whilst existing reporting platforms exist in the form of CiSP and CERT-UK, not all incidents are required to be reported on and so for clarity, Energy UK seeks a clear and concise definition or threshold of what is deemed appropriate to report.

Without such clarity and with the penalty for noncompliance set as such, the NCSC may receive an unmanageable number of incident reports. This paired with the obligation to report incidents under GDPR, Energy UK recommends further guidance is published, specifically for the energy industry on the reporting obligations for OES. This may be through the method of a simple 'minimum' information required reporting form for OES to adhere to. Energy UK also recommends that OES not face double reporting obligations from one incident under multiple existing legislations.

Energy UK recommends that the same (or similar) timeframe be established to begin reporting incidents, to that of GDPR reporting obligations. GDPR gave 2 years for implementation and a further 9 months to commence reporting and the same treatment should be allocated to OES under the NIS Directive.

Finally, Energy UK recommends that anonymity be given to protect an OES' company reputation if incidents are to be reported to the NCSC.

15. Do you consider that the proposed timeframe for providing incident reports place an undue burden on designated operators of essential services? YES/NO

No.

16. If YES, can you explain what these burdens and costs would be? Narrative answer

Energy UK does not deem the timeframe to report an issue however, at the very least, some scope should be left for exceptional circumstances should an OES be unable to report within the timeframe.

Energy UK recommends DCMS refers to individual energy company consultation responses should there be specific reporting obligation burdens and costs.

27. Do you wish to take part in the proposed targeted consultation exercise once the security and incident reporting thresholds have become clearer? YES/NO

Yes, Energy UK welcomes the opportunity to be consulted with again.

28. If YES, please provide an appropriate name, and email address for future correspondence.

Tanisha Beebee
Tanisha.Beebee@energy-uk.org.uk

29. Do you consider the proposed penalty regime to be proportionate to the risk of disruptions to operators of essential services? YES/NO

No.

30. Do you believe that the proposed penalty regime will achieve the outcome of ensuring operators take action to ensure they have the resources, skills, systems and processes in place to ensure the security of their network and information systems? YES/NO

No.

31. If you answered NO to either of these two questions, please explain how the penalty regime could be amended to address your concerns. Narrative answer

Energy companies across the supply chain have existing obligations to ensure risk management processes and security measures are in place. The NIS Directive's legal measures add to the existing obligations, especially that of GDPR of which penalties have already been set for such obligations. Energy UK notes that the penalty regime stated by DCMS is too high and is not proportionate to the risk of disruption to the service provided by operators. Energy UK recognizes that the reputational damage of an OES surpasses the need for the proposed penalty regime at this high level.

Energy UK recommends the penalty regime be based on other quantifiable indices such as number of consumers impacted or length of time with loss of supply and in this vein, more layers should be applied to the penalty regime which reflect the genuine impact rather than simply non-compliance. Energy UK considers a guidance framework be created ensuring those noncompliant OES are penalized appropriately and in proportion to the level of impact. Energy UK members welcome the opportunity to deepen their relationships with NCSC, BEIS, Ofgem and DCMS by actively gaining contact when confusions arise and to acquire guidance where needed and we believe this proactive engagement should be taken into consideration before any penalty be applied.

Fundamentally, Energy UK seeks further clarity over a potential 'double jeopardy' effect whereby one incident may fall under reporting obligations and penalty regimes from existing legislations – notably

GDPR. We hope DCMS will clarify this point and create a regime whereby only one penalty be applied.