**Invitation to Tender for**

**Refinement of Cybersecurity Procurement Language for Energy Delivery Systems**

Tender Reference Number: TRN 1401/12/2017

Deadline for Tender Responses: Wednesday 17 January 2018 1700

**Department for Business, Energy & Industrial Strategy**

Date: 1/12/17

The Department for Business, Energy & Industrial Strategy (“BEIS”) wishes to commission a project to produce Cybersecurity Procurement Language for Energy Delivery Systems

Enclosed are the following sections:

* Section 1 (page 3) Instructions on tendering procedures
* Section 2 (page 7) Specification of requirements
* Section 3 (page 18) Further information on tendering procedure
* Section 4 (page 21) Declarations and information to be provided;

Statement of Non-Collusion

Form of Tender

Conflict of Interest

Questions for tenderers

Code of Practice for Research

* Annex A: Pricing schedule
* Annex B: Code of practice for research

Please register your interest in submitting a tender for this project by emailing [Ian.Henderson@beis.gov.uk](mailto:Ian.Henderson@beis.gov.uk). This will ensure you receive immediate notification of updates to the ITT process or answers to questions raised by potential bidders.

Please read the instructions on the tendering procedures carefully since failure to comply with them may invalidate your tender. Your tender must be returned by Wednesday 17 January 2018 clearly marked as “TENDER”.

I look forward to receiving your response.

Yours sincerely,

Ian Henderson

Email: [Ian.Henderson@beis.gov.uk](mailto:Ian.Henderson@beis.gov.uk)

**Section 1**

**Instructions and Information on Tendering Procedures**

Invitation to Tender for Refinement of Cybersecurity Procurement Language for Energy Delivery Systems

Tender Reference Number: TRN 1401/12/2017

Deadline for Tender Responses: Wednesday 17 January 2018 1700

**Contents**

A. Indicative Timetable 4

B. Procedure for Submitting Tenders 4

C. Conflict of Interest 5

D. Evaluation of Responses 6

E. Terms and conditions applying to this Invitation to Tender 6

F. Further Instructions to Contractors 6

G. Checklist of Documents to be Returned 6

# Indicative Timetable

The anticipated timetable for this tender exercise is as follows. BEIS reserves the right to vary this timetable. Any variations will be published on contracts finder or circulated to all organisations who have registered an interest in notifications.

|  |  |
| --- | --- |
| **Tender Timeline** | **Date** |
| Advert and full invitation to tender issued | Friday 8 December 2017 |
| Deadline for questions relating to the tender | Monday 8January 2018 |
| Responses to questions published | Wednesday 10 January 2018 |
| Deadline for receipt of tender | Wednesday 17 January 2018 |
| Invite suppliers for bid clarification (if needed) | Friday 19 January 2018 |
| Shortlisted suppliers invited to make a presentation to the steering board. | ~ Friday 2 February 2018 |
| All suppliers alerted of outcome | ~ Friday 2 February 2018 |
| Contract award on signature by both parties | ~ Friday 2 February 2018 |
|  |  |
| Contract start date | ~ Monday 5 February 2018 |

The contract is to be for a period of 2 months unless terminated or extended by the Department in accordance with the terms of the contract.

# Procedure for Submitting Tenders

The maximum page limit for tenders is 10 pages (excluding declarations).

Please send 2 hard copies of your tender to Ian Henderson, Energy Cyber Security, 1, Victoria Street, London, SW1H 0ET by Wednesday 17 January 2018 and **email** your proposal **after** the deadline to [Ian.Henderson@beis.gov.uk](mailto:Ian.Henderson@beis.gov.uk).

For questions regarding the procurement process please contact Ian Henderson, [Ian.Henderson@beis.gov.uk](mailto:Ian.Henderson@beis.gov.uk)

Tenders will be received up to the time and date stated. Please ensure that your tender is delivered not later than the appointed time on the appointed date. The Department does not undertake to consider tenders received after that time. The Department requires tenders to remain valid for a period indicated in the specification of requirements.

BEIS shall have the right to disqualify you from the procurement if you fail to fully complete your response, or do not return all of the fully completed documentation and declarations requested in this ITT. BEIS shall also have the right to disqualify you if it later becomes aware of any omission or misrepresentation in your response to any question within this invitation to tender. If you require further information concerning the tender process, or the nature of the proposed contract, email [Ian.Henderson@beis.gov.uk](mailto:Ian.Henderson@beis.gov.uk). All questions should be submitted by Monday 8 January 2018; questions submitted after this date may not be answered. Should questions arise during the tendering period, which in our judgement are of material significance, we will publish these questions with our formal reply by the end of Wednesday 10 January 2018 and circulate – unnamed - to all organisations that have expressed an interest in bidding. All contractors should then take that reply into consideration when preparing their own bids, and we will evaluate bids on the assumption that they have done so.

You will not be entitled to claim from the Department any costs or expenses that you may incur in preparing your tender whether or not your tender is successful.

# Conflict of Interest

The Department’s standard terms and conditions of contract include reference to conflict of interest and require contractors to declare any potential conflict of interest to the Secretary of State.

For research and analysis, conflict of interest is defined the presence of an interest or involvement of the contractor, subcontractor (or consortium member) which could affect the actual or perceived impartiality of the research or analysis.

Where there may be a potential conflict of interest, it is suggested that the consortia or organisation designs a working arrangements such that the findings cannot be influenced (or perceived to be influenced) by the organisation which is the owner of a potential conflict of interest. For example, consideration should be given to the different roles which organisations play in the research or analysis, and how these can be structured to ensue maintain an impartial approach to the project is maintained.

The process by which this is managed in the procurement process is as follows:

1. **During the bidding process, organisations may contact BEIS to discuss whether or not their proposed arrangement is likely to yield a conflict of interest.** Any responses given to individual organisations or consortia will be published on contract finder (in a form which does not reveal the questioner’s identity). Any organisation thinking of submitting a bid, should share their contact details with the staff member responsible for this procurement, to ensure they receive an update when any responses to questions are published.
2. **Contractors are asked to sign and return Declaration 3 (page 24) to indicate whether or not any conflict of interest may be, or be perceived to be, an issue.** If this is the case, the contractor or consortium should give a full account of the actions or processes that it will use to ensure that conflict of interest is avoided. In any statement of mitigating actions, contractors are expected to outline how they propose to achieve a robust, impartial and credible approach to the research.
3. **When tenders are scored, this declaration will be subject to a pass/fail score**, according to whether, on the basis of the information in the proposal and declaration, there remains a conflict of interest which may affect the impartiality of the research.

Failure to declare or avoid conflict of interest at this or a later stage may result in exclusion from the procurement competition, or in the Department exercising its right to terminate any contract awarded.

# Evaluation of Responses

The tender process will be conducted to ensure that bids are evaluated fairly and transparently, in accordance with agreed assessment criteria. Further details are provided in the specification.

# Terms and conditions applying to this Invitation to Tender

The Department’s Standard Terms and Conditions of Contract will apply to this contract. These can be downloaded from Contracts Finder.

# Further Instructions to Contractors

The Department reserves the right to amend the enclosed tender documents at any time prior to the deadline for receipt of tenders. Any such amendment will be numbered, dated and issued by Wednesday 10 January 2018. Where amendments are significant, the Department may at its discretion extend the deadline for receipt of tenders.

The Department reserves the right to withdraw this contract opportunity without notice and will not be liable for any costs incurred by contractors during any stage of the process. Contractors should also note that, in the event a tender is considered to be fundamentally unacceptable on a key issue, regardless of its other merits, that tender may be rejected. By issuing this invitation the Department is not bound in any way and does not have to accept the lowest or any tender and reserves the right to accept a portion of any tender unless the tenderer expressly stipulates otherwise in their tender.

# Checklist of Documents to be Returned

* Proposal (maximum 10 pages)
* Annex A – pricing schedule
* Declaration 1: Statement of non-collusion
* Declaration 2: Form of Tender
* Declaration 3: Conflict of Interest
* Declaration 4: Questions for tenderers
* Declaration 5: Code of Practice

**Section 2**

**Specification of Requirements**

Invitation to Tender for Refinement of Cybersecurity Procurement Language for Energy Delivery Systems

Tender Reference Number: TRN 1401/12/2017

Deadline for Tender Responses: Wednesday 17 January 2018 1700

**Contents**

1. Introduction and summary of requirements 8

2. Background 8

3. Aims and Objectives 10

4. Methodology 11

5. Outputs Required 12

6. Ownership and Publication 12

7. Quality Assurance 13

8. Timetable 13

9. Challenges 13

10. Ethics 14

11. Working Arrangements 14

12. Required Skills 14

13. Consortium Bids 14

14. Budget 15

15. Evaluation of Tenders 15

# Introduction and summary of requirements

Since the launch of the Energy Cyber Security Programme in 2013 the Department of Business, Energy and Industrial Strategy (BEIS) Energy Cyber Security Team and the National Cyber Security Centre (NCSC) have focused efforts on collaboration with operators of Critical National Infrastructure (CNI) to ensure that they have appropriate technical advice and guidance to manage the cyber risks that they are exposed to.

The programme has identified the need to address vulnerabilities across the supply chain, specifically the products, vendors and integrators of operational technology and network and information systems that underpin the operation of energy delivery systems.

There is currently no UK-centric procurement language/reference document available that is structured in a format that can be easily used when procuring a single asset type (e.g. RTU, relay), a full control system or support infrastructure (e.g. entire substation, HVDC system, communications services). Demand for this work has long been recognised by industry but to date no agreement has been reached across companies on an effective approach.

BEIS therefore wishes to appoint a supplier to develop Cybersecurity Procurement Language for Energy Delivery Systems[[1]](#footnote-1)

The supplier will develop industry endorsed cybersecurity procurement language to help bridge the gap between the detailed technical guidance and the high level principles that are currently available. The supplier will produce principles-based procurement language that can be used in contracts to improve cyber security of the product or service. It should address the key asset areas procured by energy network operators (primarily gas and electricity) and should be understandable by non-cyber security experts.

BEIS is working with the Energy Networks Association (ENA) Cyber Security Group to deliver this work. It is expected that the supplier will work collaboratively with the operators that make up this group and stakeholders across the supply chain. The supplier will lead industry workshops and review internal/external standards or guidance available to develop useful, comprehensive procurement language. Though the work should focus primarily on the gas and electricity sectors, the supplier will also be required to consider and demonstrate how the learnings and outcomes can also be applied to other energy sectors.

# Background

Cyber threats to the energy sector pose economic and national security risks, threatening a key BEIS objective to ensure consumers have secure, affordable and clean energy. Addressing these threats is critical for our economy, national security and household budgets. Improving cyber security will help ensure that the UK has a secure and resilient energy system, which is amongst our most Critical National Infrastructure (CNI), underpinning all our essential services; the disruption of which could affect public safety and public health.

Since the launch of the Energy Cyber Security Programme in 2013 the BEIS Energy Cyber Security Team and the NCSC have focused efforts on collaboration with operators of energy CNI to ensure that they have appropriate technical advice and guidance to manage the cyber risks that they are exposed to. The programme has identified that operators in the sector have difficulty managing the risks that originate from within the companies that supply their operational technology and network and information systems.

Operators have little or no direct control over those risks and as a single customer have limited leverage to drive improvement. To date, supply chain risks have received limited attention from BEIS and NCSC, compared to the risks that are in direct control of the operators; it is therefore an area where Government aims to do more.

The supply chain refers to the providers of software, hardware and services to the operators of Critical National Infrastructure. It also includes the vendors that supply products and the systems integrators that bring together subsystems. The supply chain for CNI operators tends to be very complex, employing bespoke solutions and often involving hundreds of different companies.

Early indications are that vendors have varying approaches to the cyber security of the products and services that they provide. Therefore, there is a significant risk that an impact to the provision of an essential service can be brought about by compromising products, vendors or integrators that are procured and used by CNI operators.

Vulnerabilities in supply chain and procurement processes are a means by which malicious code, compromised equipment and support services and can enter the Operational Technology (OT) systems operated across the energy sector. Establishing an accessible set of baseline security requirements for procurement is one action that can help drive cyber security improvements across the supply chain.

The required output from this work will be a standard suite of procurement language that can be incorporated into procurement processes. The availability of this will help to ensure that cybersecurity is implemented throughout the testing, manufacturing, delivery, installation, and support phases of the product life cycle, improving overall reliability and reducing cybersecurity risks across the energy sector.

The Network and Information Security Directive (NISD) will be transposed in May 2018. This is the first cyber security specific regulation that CNI operators will be subject to as ‘operators of essential services.’ NISD will not place formal requirements on suppliers and so this work will help address cyber risks linked to suppliers. However, the NCSC principles that will feed into this regulation will be available in January 2018 and should be considered in the work.

# Aims and Objectives

International standards already exist that address the issue of consistent cyber security procurement language (e.g. DHS Cybersecurity Procurement Language for Energy Delivery Systems and Control Systems, IEC 62443, etc.). The supplier will undertake a comprehensive review of these existing standards/guidance and determine how to create procurement language that is UK centric and structured in a format that is easily accessible when procuring a single asset type or infrastructure area.

In addition to assessing this existing external procurement language, the supplier will meet with operators of energy delivery systems (primarily gas and electricity Distribution Network Operators) and assess the language used in their own internal procurement processes and standards. To develop a holistic overview the supplier will meet with relevant vendors and also consider how the learnings and outcomes can be applied to other energy sectors such as downstream oil.

By undertaking a comprehensive review of a broad range of procurement languages, the supplier will develop a set of requirements. They will then produce a set of principles-based procurement language statements for relevant asset types (see Section 4 - Methodology) that can easily be adopted by operators for use in future procurement activities, as outlined by the diagram below:

**Deliverable:**

**Procurement Language that can be inserted into a procurement contract**

**High Level Guidance and Principles**

e.g.

* NCSC principles
* DHS NCCIC Strategies

**Detailed Language**

e.g.

* DHS Procurement Language
* IEC 62443
* EPRI Procurement Methodology

Supplier to bridge the gap between the high level principles and the deep technical guidance currently available – i.e. some ‘reusable procurement language’ that a buyer can ideally copy and paste into a contract, designed to improve cyber security of the procured product or service. It should include a series of statements for each asset area that can be incorporated into contracts to address cyber security vulnerabilities across the procurement process.

[Not intended to be inserted into a procurement contract]

[Not intended to be inserted into a procurement contract]

**Procurement**

**Language**

**Increasing Technical Detail**

**Behavioural / Process Changes**

The final deliverable will be industry endorsed cybersecurity procurement language that:

* Bridges the gap between the detailed technical guidance (e.g. IEC 62443) and the high level principles produced by government entities and industry groups (e.g. NCSC and DHS guidance).
* Is principles-based and designed to be easily integrated into contracts to improve cyber security of the product or service.
* Addresses the key asset areas procured by energy network operators (primarily gas and electricity) but also recognises that many of principles will be relevant to generator or transmission operators, for example.
* Is understandable by non-cyber security experts.

# Methodology

The supplier will analyse Department for Homeland Security (DHS) Cybersecurity Procurement Language for Energy Delivery Systems, relevant parts of the draft IEC 62443 and any other standards or guidance that already exist to address the issue of consistent cyber security procurement language.

They will also document observations arrived at through individual and group sessions with members of the ENA Cyber Security Group and other parties deemed relevant, supported by consultation with selected ICS vendors. This will include reviewing the language used in operator’s own internal procurement processes and standards. These sessions will also be used to further define the scope that the final procurement language principles will cover.

Using this research the supplier will then produce a suite of procurement language that, at a minimum, addresses the following operational technology/asset areas and capabilities that are commonly procured by operators:

* Core Control Systems (e.g. Distribution Management Systems (DMS)) and datacenters.
* Industrial Control System (ICS) communications (central sites and field).
* Substations equipment (including IEC 61850 deployments).
* Connection of third-parties at the DMS and substation levels.
* Cybersecurity monitoring and incident response for an ICS environment.
* Lifecycle management and on-going support/maintenance (where supported by vendor).

*[Bidders are free to suggest in their responses other relevant asset and capabilities areas used by energy delivery systems that they feel will enhance the quality and adoption of the delivered reference document.]*

# Outputs Required

The final deliverable will be a report that consists of:

1. Procurement language statements that a buyer can copy and paste into a contract, designed to improve cyber security of the procured product or service.
2. An explanation of the methodology and how procurement language statements were developed.
3. An executive summary explaining how the document can be used.

# Ownership and Publication

As the outcome of this work is a product for industry use, a steering board will be assembled to ensure the work delivered meets the end user’s requirements.

The Steering Board will consist of members from:

* ENA Cyber Security Group
* BEIS Energy Cyber Security
* National Cyber Security Centre

The Steering Board will monitor and track progress on a regular basis, review the quality at major project milestones and the final deliverable. An example project process could be:

|  |  |  |
| --- | --- | --- |
| **Project Milestone** | **Outcome** | **Payment Milestone\*** |
| Meet with all DNOs and review available internal standards | Develop draft principles | N/A |
| Review existing external procurement language |
| ENA Workshop | Develop/refine draft principles | 20% |
| Vendor Workshop | Develop/refine draft principles |
| Submit draft principles | Stakeholders to review draft for peer review. | 20% |
| Submit final draft principles and procurement language statements and approval by the Steering Board | Final document | 60% |

\* Pending quality review by Steering Board.

*[Bidders are free to propose their own project milestones]*

BEIS, the procurer has ultimate responsibility for signing off the work and will be assessing the quality of the final document with the input of the Steering Board. BEIS will look to perform quality assurance checks throughout the project and will expect the supplier to provide/participate in the following:

* Regular project meetings with team leader (preferably on a monthly basis)
* Monthly progress reports highlighting new findings, spend to date and any issues.
* A draft copy of the report/guidance to be provided to BEIS two weeks before the final deliverable deadline.
* A final copy of the report/guidance agreed by the team leader prior to release. This will be provided in both hard and soft copy format.
* A final presentation of findings, recommendations and guidance to be given subsequent to the delivery of the final report.

# Quality Assurance

Once BEIS and the steering board have approved the final draft, the finished work will be published on the ENA Publications website and will be managed by the ENA.

All outputs listed in Section 5 will be owned by BEIS and should be made accessible and suitable by the supplier for publication on the ENA Publications website.

The exceptions to this are where:

* The intellectual property rights to an output (or part of an output) are owned by someone other than the supplier. Suppliers should state in their tender if this is the case and indicate whether the third party copy righted materials can be redacted.
* Data is commercial in confidence.

If these exceptions apply to any part of the outputs, suppliers should indicate this in their proposal alongside any approaches to resolving these. Where applicable, suppliers can provide optional costs for obtaining rights to data or outputs. These will be agreed before BEIS lets the contract.

Unless the above exceptions have been stated in a proposal, all outputs from a research project will assumed to be owned by BEIS. The outputs, raw data and tools developed in the research cannot therefore be used for suppliers for purposes other than our work.

# Timetable

The technical study will be conducted between 29 January 2018 and 31 March 2018. As part of the tender response the supplier should provide a more detailed breakdown of timings; suggested dates and timescales for different aspects of the project.

# Challenges

There may be a number of challenges conducting this project. Suppliers must consider how these and any other challenges will be addressed through the project delivery.

# Ethics

All applicants will need to identify and propose arrangements for initial scrutiny and on-going monitoring of ethical issues. The appropriate handling of ethical issues is part of the tender assessment exercise and proposals will be evaluated on this as part of the ‘addressing challenges and risks’ criterion.

We expect contractors to adhere to the following GSR Principals:

1. Sound application and conduct of social research methods and appropriate dissemination and utilisation of findings
2. Participation based on valid consent
3. Enabling participation
4. Avoidance of personal harm
5. Non-disclosure of identity and personal information

# Working Arrangements

The successful contractor will be expected to identify one named point of contract through whom all enquiries can be filtered. A BEIS project manager will be assigned to the project and will be the central point of contact.

# Skills and experience

BEIS would like you to demonstrate that you have the experience and capabilities to undertake the project, specifically ICS cyber security, operational technology (OT) and the procurement of related products and services. Deep knowledge of the gas and electricity networks is also required. Your tender response should include a summary of each proposed team members experience and capabilities.

Contractors should propose named members of the project team, and include the tasks and responsibilities of each team member. This should be clearly linked to the work programme, indicating the grade/ seniority of staff and number of days allocated to specific tasks.

Contractors should identify the individual(s) who will be responsible for managing the project.

# Consortium Bids

In the case of a consortium tender, only one submission covering all of the partners is required but consortia are advised to make clear the proposed role that each partner will play in performing the contract as per the requirements of the technical specification. We expect the bidder to indicate who in the consortium will be the lead contact for this project, and the organisation and governance associated with the consortia.

Contractors must provide details as to how they will manage any sub-contractors and what percentage of the tendered activity (in terms of monetary value) will be sub-contracted.

If a consortium is not proposing to form a corporate entity, full details of alternative proposed arrangements should be provided in the Annex. However, please note the Department reserves the right to require a successful consortium to form a single legal entity in accordance with Regulation 28 of the Public Contracts Regulations 2006.

The Department recognises that arrangements in relation to consortia may (within limits) be subject to future change. Potential Providers should therefore respond in the light of the arrangements as currently envisaged. Potential Providers are reminded that any future proposed change in relation to consortia must be notified to the Department so that it can make a further assessment by applying the selection criteria to the new information provided.

# Budget

The budget for this project is £40,000 excluding VAT.

Contractors should provide a full and detailed breakdown of costs (including options where appropriate). This should include staff (and day rate) allocated to specific tasks.

Payments will be linked to delivery of key milestones. Payment will be linked to the quality of the output rather than just its delivery.

Milestones can be adjusted and agreed with the contractor based on the tender response/details. Please advise in your tender response how this breakdown reflects your usual payment processes:

In submitting full tenders, contractors confirm in writing that the price offered will be held for a minimum of 60 calendar days from the date of submission. Any payment conditions applicable to the prime contractor must also be replicated with sub-contractors.

The Department aims to pay all correctly submitted invoices as soon as possible with a target of 10 days from the date of receipt and within 30 days at the latest in line with standard terms and conditions of contract.

# Evaluation of Tenders

Contractors are invited to submit full tenders in the form of a project proposal of no more than 10 pages, excluding declarations. Tenders will be evaluated by the Steering Board. Shortlisted contractors will be invited to make a 45 minute proposal presentation followed by 15 minute Q&A with the Steering Group (in person) shortly after the shortlisting process.

BEIS will select the bidder that scores highest against the criteria and weighting listed below:

* **Conflict of interest:** pass/fail.
* **Methodology:** Ability of the design to deliver the project objectives
* **Skills and expertise:** Demonstration of experience and capabilities of proposed team members

BEIS will select the bidder that scores highest against the criteria and weighting listed below:

**EVALUATION CRITERIA AND SCORING METHODOLOGY**

|  |  |  |
| --- | --- | --- |
| Criterion | Description | Weighting |
| **01** | **Methodology** | **60%** |
| 01-1 | Demonstrate understanding of requirements | 30% |
| 01-2 | Proposed Methodology | 10% |
| 01-3 | Milestones, Deliverables and Timescales | 5% |
| 01-4 | Identification of Risks, Challenges and Assumptions | 15% |
| **02** | **Skills and Expertise** | **40%** |
| 02-1 | Company experience | 10% |
| 02-2 | Project Team skills, expertise and experience | 30% |
|  | | **100%** |

# Scoring Method

# Tenders will be scored against each of the criteria above, according to the extent to which they meet the requirements of the tender. The meaning of each score is outlined in the table below.

The total score will be calculated by applying the weighting set against each criterion, outlined above; the maximum number of marks possible will be 100. Should any contractor score 1 in any of the criteria, they will be excluded from the tender competition.

|  |  |
| --- | --- |
| **Score** | **Description** |
| 1 | Not Satisfactory: Proposal contains significant shortcomings and does not meet the required standard |
| 2 | Partially Satisfactory: Proposal partially meets the required standard, with one or more moderate weaknesses or gaps |
| 3 | Satisfactory: Proposal mostly meets the required standard, with one or more minor weaknesses or gaps. |
| 4 | Good: Proposal meets the required standard, with moderate levels of assurance |
| 5 | Excellent: Proposal fully meets the required standard with high levels of assurance |

**Structure of Tenders**

Contractors are strongly advised to structure their tender submissions to cover each of the criteria above. Complete the price schedule attached at Annex A, specifying the daily rates (ex-VAT) you will charge for each level of your staff.

**Bid Clarification**

The Department reserves the right to award the contract based on applicants’ written evaluation only if one candidate emerges from the evaluation stage as significantly stronger than the others.

BEIS may invite all suppliers for bid clarification if they feel bid clarification should be carried out.

**Feedback**

Feedback will be given in the unsuccessful letters or emails.

**Section 3**

**Further Information on Tender Procedure**

Invitation to Tender for Refinement of Cybersecurity Procurement Language for Energy Delivery Systems

Tender Reference Number: TRN 1401/12/2017

Deadline for Tender Responses: Wednesday 17 January 2018 1700

**Contents:**

A. [Definitions](#_Definitions) 19

B. [Data security](#_Data_security) 19

C. [Non-Collusion](#_Non-Collusion) 20

# Definitions

Please note that references to the "Department" throughout these documents mean The Secretary of State for Energy and Climate Change[[2]](#footnote-2) acting through his/her representatives in the Department for Energy & Industrial Strategy.

The Freedom of Information Act 2000 (“FOIA”) and the Environmental Information Regulations 2004 (“EIR”) apply to the Department. You should be aware of the Department’s obligations and responsibilities under FOIA or EIR to disclose, on written request, recorded information held by the Department. Information provided in connection with this procurement exercise, or with any contract that may be awarded as a result of this exercise, may therefore have to be disclosed by the Department in response to such a request, unless the Department decides that one of the statutory exemptions under the FOIA or the exceptions in the EIR applies. If you wish to designate information supplied as part of this response as confidential, of if you believe that its disclosure would be prejudicial to any person’s commercial interests, you must provide clear and specific detail as to the precise information involved and explain (in broad terms) what harm may result from disclosure if a request is received, and the time period applicable to that sensitivity. Such designation alone may not prevent disclosure if in the Department’s reasonable opinion publication is required by applicable legislation or Government policy or where disclosure is required by the Information Commissioner or the First-tier Tribunal (Information Rights).

Additionally, the Government’s transparency agenda requires that tender documents (including ITTs such as this) are published on a designated, publicly searchable web site. The same applies to other tender documents issued by the Department (including the original advertisement and the pre-qualification questionnaire (if used)), and any contract entered into by the Department with its preferred supplier once the procurement is complete. By submitting a tender you agree that your participation in this procurement may be made public. The answers you give in this response will not be published on the transparency web site (but may fall to be disclosed under FOIA or EIR (see above)). Where tender documents issued by the Department or contracts with its suppliers fall to be disclosed the Department will redact them as it thinks necessary, having regard (inter alia) to the exemptions/exceptions in the FOIA or EIR.

# Data security

The successful tenderer must comply with the Data Protection Act (DPA) 1998 and any information collected, processed and transferred on behalf of *The Department*, and in particular personal information, must be held and transferred securely**. Contractors must provide assurances of compliance with the DPA and set out in their proposals details of the practices and systems they have in place for handling data securely including transmission between the field and head office and then to *BEIS***. Contractors will have responsibility for ensuring that they and any subcontractor who processes or handles information on behalf of *The Department* is conducted securely. The sorts of issues which must be addressed satisfactorily and described in contractors’ submissions include:

* procedures for storing both physical and system data;
* data back-up procedures;
* procedures for the destruction of physical and system data;
* how data is protected;
* data encryption software used;
* use of laptops and electronic removable media;
* details of person/s responsible for data security;
* policies for unauthorised staff access or misuse of confidential/personal data;
* policies for staff awareness and training of DPA;
* physical security of premises.
* How research respondents will be made aware of all potential uses of their data.

# Non-Collusion

No tender will be considered for acceptance if the contractor has indulged or attempted to indulge in any corrupt practice or canvassed the tender with an officer of BEIS. Section 4 contains a "Statement of non-collusion" (declaration 1); any breach of the undertakings covered under items 1 - 3 inclusive will invalidate your tender. If a contractor has indulged or attempted to indulge in such practices and the tender is accepted, then grounds shall exist for the termination of the contract and the claiming damages from the successful contractors. You must not:

* Tell anyone else what your tender price is or will be, before the time limit for delivery of tenders.
* Try to obtain any information about anyone else's tender or proposed tender before the time limit for delivery of tenders.
* Make any arrangements with another organisation about whether or not they should tender, or about their or your tender price.

Offering an inducement of any kind in relation to obtaining this or any other contract with the Department will disqualify your tender from being considered and may constitute a criminal offence.

**Section 4**

**Declarations to be submitted by the Tenderer**

Invitation to Tender for Refinement of Cybersecurity Procurement Language for Energy Delivery Systems

Tender Reference Number: TRN 1401/12/2017

Deadline for Tender Responses: Wednesday 17 January 2018 1700

**Contents**

Declaration 1: Statement of non-collusion 22

Declaration 2: Form of Tender 23

Declaration 3: Conflict of Interest 24

Declaration 4: Questions for tenderers 26

# Declaration 1: Statement of non-collusion

To: The Department for Business, Energy & Industrial Strategy

1. We recognise that the essence of competitive tendering is that the Department will receive a bona fide competitive tender from all persons tendering. We therefore certify that this is a bona fide tender and that we have not fixed or adjusted the amount of the tender or our rates and prices included therein by or in accordance with any agreement or arrangement with any other person.

2. We also certify that we have not done and undertake not to do at any time before the hour and date specified for the return of this tender any of the following acts:

1. communicate to any person other than the Department the amount or approximate amount of our proposed tender, except where the disclosure, in confidence, of the approximate amount is necessary to obtain any insurance premium quotation required for the preparation of the tender;
2. enter into any agreement or arrangement with any other person that he shall refrain for submitting a tender or as to the amount included in the tender;
3. offer or pay or give or agree to pay or give any sum of money, inducement or valuable consideration directly or indirectly to any person doing or having done or causing or having caused to be done, in relation to any other actual or proposed tender for the contract any act, omission or thing of the kind described above.

3. In this certificate, the word “person” shall include any person, body or association, corporate or unincorporated; and “any agreement or arrangement” includes any such information, formal or informal, whether legally binding or not.

……………………………………………………………………………….….

Signature (duly authorised on behalf of the tenderer)

……….………………………………………………………………………….

Print name

…………………………………………………………….…………………….

On behalf of (organisation name)

…………………………………………………………………….…………….

Date

# Declaration 2: Form of Tender

To: The Department for Business, Energy & Industrial Strategy

1. Having considered the invitation to tender and all accompanying documents

(including without limitation, the terms and conditions of contract and the Specification) we confirm that we are fully satisfied as to our experience and ability to deliver the goods/services in all respects in accordance with the requirements of this invitation to tender.

2. We hereby tender and undertake to provide and complete all the services required to be performed in accordance with the terms and conditions of contract and the Specification for the amount set out in the Pricing Schedule.

3. We agree that any insertion by us of any conditions qualifying this tender or any unauthorised alteration to any of the terms and conditions of contract made by us may result in the rejection of this tender.

4. We agree that this tender shall remain open to be accepted by the Department for 8 weeks from the date below.

5. We understand that if we are a subsidiary (within the meaning of section 1159 of (and schedule 6 to) the Companies Act 2006) if requested by the Department we may be required to secure a Deed of Guarantee in favour of the Department from our holding company or ultimate holding company, as determined by the Department in their discretion.

6. We understand that the Department is not bound to accept the lowest or any tender it may receive.

7. We certify that this is a bona fide tender.

…………………………………………………………………………........

Signature (duly authorised on behalf of the tenderer)

…………………………………………………………………………………

Print name

………………………………………………………………………….

On behalf of (organisation name)

………………………………………………………………………….

Date

# Declaration 3: Conflict of Interest

I have nothing to declare with respect to any current or potential interest or conflict in relation to this research (or any potential providers who may be subcontracted to deliver this work, their advisers or other related parties). By conflict of interest, I mean, anything which could be reasonably perceived to affect the impartiality of this research, or to indicate a professional or personal interest in the outcomes from this research.

Signed …………………………………….

Name …………………………………….

Position …………………………………….

***OR***

I wish to declare the following with respect to personal or professional interests related to relevant organisations\*;

* X
* X

*Where a potential conflict of interest has been declared for an individual or organisation within a consortia, please clearly outline the role which this individual or organisation will play in the proposed project and how any conflict of interest has or will be mitigated.*

* X
* X

Signed …………………………………….

Name …………………………………….

Position …………………………………….

Please complete this form and return this with your ITT documentation - Nil returns **are** required.

**\*** These may include (but are not restricted to);

* A professional or personal interest in the outcome of this research
* For evaluation projects, a close working, governance, or commercial involvement in the project under evaluation
* Current or past employment with relevant organisations
* Payment (cash or other) received or likely to be received from relevant organisations for goods or services provided (Including consulting or advisory fees)
* Gifts or entertainment received from relevant organisations
* Shareholdings (excluding those within unit trusts, pension funds etc) in relevant organisations
* Close personal relationship or friendships with individuals employed by or otherwise closely associated with relevant organisations

***All of the above apply both to the individual signing this form and their close family / friends / partners etc.***

If your situation changes during the project in terms of interests or conflicts, you must notify the Department straight away.

A DECLARATION OF INTEREST WILL NOT NECESSARILY MEAN THE INDIVIDUAL OR ORGANISATION CANNOT WORK ON THE PROJECT; BUT IT IS VITAL THAT ANY INTEREST OR CONFLICT IS DECLARED SO IT CAN BE CONSIDERED OPENLY.

# Declaration 4: Questions for tenderers

In some circumstances the Department is required by law to exclude you from participating further in a procurement. If you cannot answer ‘no’ to every question in this section it is very unlikely that your application will be accepted, and you should contact us for advice before completing this form.

Please state ‘Yes’ or ‘No’ to each question.

|  |  |
| --- | --- |
| **Has your organisation or any directors or partner or any other person who has powers of representation, decision or control been convicted of any of the following offences?** | **Answer** |
| 1. conspiracy within the meaning of [section 1](http://www.lexisnexis.com:80/uk/legal/search/runRemoteLink.do?langcountry=GB&linkInfo=F%23GB%23UK_ACTS%23section%251%25sect%251%25num%251977_45a%25&risb=21_T12077301839&bct=A&service=citation&A=0.2630909849289865) or 1A of the Criminal Law Act 1977 or article 9 or 9A of the Criminal Attempts and Conspiracy (Northern Ireland) Order 1983 where that conspiracy relates to participation in a criminal organisation as defined in Article 2 of Council Framework Decision 2008/841/JHA; |  |
| 1. corruption within the meaning of [section 1](http://www.lexisnexis.com:80/uk/legal/search/runRemoteLink.do?langcountry=GB&linkInfo=F%23GB%23UK_ACTS%23section%251%25sect%251%25num%251889_69a%25&risb=21_T12077301839&bct=A&service=citation&A=0.774070316337072)(2) of the Public Bodies Corrupt Practices Act 1889 or [section 1](http://www.lexisnexis.com:80/uk/legal/search/runRemoteLink.do?langcountry=GB&linkInfo=F%23GB%23UK_ACTS%23section%251%25sect%251%25num%251906_34a%25&risb=21_T12077301839&bct=A&service=citation&A=0.24433813672949012) of the Prevention of Corruption Act 1906; where the offence relates to active corruption; |  |
| 1. the offence of bribery, where the offence relates to active corruption; |  |
| 1. bribery within the meaning of section 1 or 6 of the Bribery Act 2010; |  |
| 1. fraud, where the offence relates to fraud affecting the European Communities’ financial interests as defined by Article 1 of the Convention on the protection of the financial interests of the European Communities, within the meaning of: |  |
| 1. the offence of cheating the Revenue; |  |
| 1. the offence of conspiracy to defraud; |  |
| 1. fraud or theft within the meaning of the [Theft Act 1968](http://www.lexisnexis.com:80/uk/legal/search/runRemoteLink.do?langcountry=GB&linkInfo=F%23GB%23UK_ACTS%23num%251968_60a_Title%25&risb=21_T12077301839&bct=A&service=citation&A=0.35766330215827113), the Theft Act (Northern Ireland) 1969, the Theft Act 1978 or the Theft (Northern Ireland) Order 1978; |  |
| 1. fraudulent trading within the meaning of [section 458](http://www.lexisnexis.com:80/uk/legal/search/runRemoteLink.do?langcountry=GB&linkInfo=F%23GB%23UK_ACTS%23section%25458%25sect%25458%25num%251985_6a%25&risb=21_T12077301839&bct=A&service=citation&A=0.5972529271560607) of the Companies Act 1985, article 451 of the Companies (Northern Ireland) Order 1986 or section 993 of the Companies Act 2006; |  |
| 1. fraudulent evasion within the meaning of section 170 of the [Customs and Excise Management Act 1979](http://www.lexisnexis.com:80/uk/legal/search/runRemoteLink.do?langcountry=GB&linkInfo=F%23GB%23UK_ACTS%23num%251979_2a_Title%25&risb=21_T12077301839&bct=A&service=citation&A=0.22540552446837803)  [or section 72 of the Value Added Tax Act 1994](http://www.lexisnexis.com:80/uk/legal/search/runRemoteLink.do?langcountry=GB&linkInfo=F%23GB%23UK_ACTS%23num%251994_23a_Title%25&risb=21_T12077301839&bct=A&service=citation&A=0.9838628229561671); |  |
| 1. an offence in connection with taxation in the European Union within the meaning of section 71 of the Criminal Justice Act 1993; |  |
| 1. destroying, defacing or concealing of documents or procuring the execution of a valuable security within the meaning of [section 20](http://www.lexisnexis.com:80/uk/legal/search/runRemoteLink.do?langcountry=GB&linkInfo=F%23GB%23UK_ACTS%23section%2520%25sect%2520%25num%251968_60a%25&risb=21_T12077301839&bct=A&service=citation&A=0.5036676212568264) of the Theft Act 1968 or section 19 of the Theft Act (Northern Ireland) 1969; |  |
| 1. fraud within the meaning of section 2, 3 or 4 of the Fraud Act 2006; or |  |
| 1. making, adapting, supplying or offering to supply articles for use in frauds within the meaning of section 7 of the Fraud Act 2006; |  |
| 1. money laundering within the meaning of section 340(11) of the Proceeds of Crime Act 2002; |  |
| 1. an offence in connection with the proceeds of criminal conduct within the meaning of section 93A, 93B or 93C of the Criminal Justice Act 1988 or article 45, 46 or 47 of the Proceeds of Crime (Northern Ireland) Order 1996; or |  |
| 1. an offence in connection with the proceeds of drug trafficking within the meaning of section 49, 50 or 51 of the Drug Trafficking Act 1994; or |  |
| 1. any other offence within the meaning of Article 45(1) of Directive 2004/18/EC as defined by the national law of any relevant State. |  |

# Declaration 5: Code of Practice[[3]](#footnote-3)

I confirm that I am aware of the requirements of the BEIS Code of Practice[[4]](#footnote-4) for Research and, in the proposed project, I will use my best efforts to ensure that the procedures used conform to those requirements under the following headings[[5]](#footnote-5):

Responsibilities

Competence

Project planning

Quality Control

Handling of samples and materials

Facilities and equipment

Documentation of procedures and methods

Research/work records

I understand that BEIS has the right to inspect our procedures and practices against the requirements of the Code of Practice, and that I may be asked to provide documentary evidence of our working practices or provide access and assistance to auditors appointed by BEIS.

(There is some flexibility in the application of the Code of Practice to specific research projects. Contractors are encouraged to discuss with BEIS any aspects that cause them concern, in order to reach agreement on the interpretation of each requirement.)

**Annex A: Pricing Schedule**

**Part A – Staff/project team charges**

|  |  |
| --- | --- |
| Set up Costs – please specify |  |
|  |
| Expenses |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **\*Grade/level of staff** | **Daily rate**  **(ex VAT)** | **No. days offered over course of contract** | **Tasks to be undertaken on this project** | **Total price offered per staff member** |
|  | £ |  |  | £ |
|  | £ |  |  | £ |
|  | £ |  |  | £ |
|  | £ |  |  | £ |
|  | £ |  |  | £ |
| **Sub-total** | | |  | **£** |

[\*Suppliers should also include sub-contractors]

**Part B – Non-staff/project team charges**

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **No. of items** | **Price per item**  **(ex VAT)** | **Total price per offered** |
|  |  | £ | £ |
|  |  | £ | £ |
|  |  | £ | £ |
|  |  | £ | £ |
|  |  | £ | £ |
| **Sub-total** | | | **£** |

**Part C – Full price offered**

|  |  |
| --- | --- |
| **Sub-total (Part A + Part B)** | **£** |
| **VAT** | **£** |
| **TOTAL (Sub-total + VAT)** | **£** |

**Annex B: Code of Practice for Research**

**CODE OF PRACTICE FOR RESEARCH**

***Issued by the Department for Energy & Industrial Strategy***

The Department has developed this Code of Practice from the Joint Code of Practice issued by BBSRC; the Department for Environment, Food and Rural Affairs (Defra); the Food Standards Agency; and the Natural Environment Research Council (NERC) which lays out a framework for the proper conduct of research. It sets out the key aspects of the research process and the importance of making judgements on the appropriate precautions needed in every research activity.

The Code applies to all research funded by BEIS. It is intended to apply to all types of research, but the overriding principle is fitness of purpose and that all research must be conducted diligently by competent researchers and therefore the individual provisions must be interpreted with that in mind.

***PRINCIPLES BEHIND THE CODE OF PRACTICE***

Contractors and consortia funded by BEIS are expected to be committed to the quality of the research process in addition to quality of the evidence outputs

The Code of Practice has been created in order to assist contractors to conduct research of the highest quality and to encourage good conduct in research and help prevent misconduct,.

Set out over 8 responsibilities the code of practice provides general principles and standards for good practice in research.

Most contractors will already have in place many of the measures set out in the

Code and its adoption should not require great effort.

***COMPLIANCE WITH THE CODE OF PRACTICE***

All organisations contracting to the Department (including those sub-contracting as part of a consortium) will be expected to commit to upholding these responsibilities and will be expected to indicate acceptance of the Code when submitting proposals to the Department.

Contractors are encouraged to discuss with BEIS any clauses in the Code that they consider inappropriate or unnecessary in the context of the proposed research project. The Code, and records of the discussions if held, will become part of the Terms and Conditions under which the research is funded.

Additionally, BEIS may conduct (or request from the Contractor as appropriate) a formal risk assessment on the project to identify where additional controls may be needed.

***MONITORING OF COMPLIANCE WITH THE CODE OF PRACTICE***

Monitoring of compliance with the Code is necessary to ensure:

* Policies and managed processes exist to support compliance with the Code
* That these are being applied in practice.

In the short term, BEIS can require contractors to conduct planned internal audits although BEIS reserve the right to obtain evidence that a funded project is carried out to the required standard. BEIS may also conduct an audit of a Contractor’s research system if deemed necessary.

In the longer term it is expected that most research organisations will assure the quality of their research processes by means of a formal system that is audited by an impartial and competent third party against an appropriate internationally recognised standard that is fit for purpose.

A recommended checklist for researchers can be found on the UK Research Integrity Office (UKRIO) website at http://www.ukrio.org/what-we-do/code-of-practice-for-research

***SPECIFIC REQUIREMENTS IN THE CODE OF PRACTICE***

***1. Responsibilities***

All organisations contracting to the Department (including those sub-contracting as part of a consortium will be responsible for the overall quality of research they conducted. Managers, group leaders and supervisors have a responsibility to ensure a climate of good practice in the research teams, including a commitment to the development of scientific and technical skills.

The Principal Investigator or Project Leader is responsible for all the work conducted in the project including that of any subcontractors. All staff and students must have defined responsibilities in relation to the project and be aware of these responsibilities.

***2. Competence***

All personnel associated with the project must be competent to perform the technical, scientific and support tasks required of them. Personnel undergoing training must be supervised at a level such that the quality of the results is not compromised by the inexperience of the researcher.

***3. Project planning***

An appropriate level of risk assessment must be conducted to demonstrate awareness of the key factors that will influence the success of the project and the ability to meet its objectives. There must be a written project plan showing that these factors (including research design, statistical methods and others) have been addressed. Projects must be ethical and project plans must be agreed in collaboration with BEIS, taking account of the requirements of ethical committees[[6]](#footnote-6) or the terms of project licences, if relevant.

Significant amendments to the plan or milestones must be recorded and approved by BEIS if applicable.

***4. Quality Control***

The organisation must have planned processes in place to assure the quality of the research undertaken by its staff Projects must be subjected to formal reviews of an appropriate frequency. Final and interim outputs must always be accompanied by a statement of what quality control has been undertaken.

The authorisation of outputs and publications shall be as agreed by BEIS, and subject to senior approval in BEIS, where appropriate. Errors identified after publication must be notified to BEIS and agreed corrective action initiated.

***5. Handling of samples and materials***

All samples and other experimental materials must be labelled (clearly, accurately, uniquely and durably), and retained for a period to be agreed by BEIS. The storage and handling of the samples, materials and data must be as specified in the project plan (or proposal), and must be appropriate to their nature. If the storage conditions are critical, they must be monitored and recorded.

***6. Documentation of procedures and methods***

All the procedures and methods used in a research project must be documented, at least in the personal records of the researcher. This includes analytical and statistical procedures and the generation of a clear audit trial linking secondary processed information to primary data.

There must be a procedure for validation of research methods as fit for purpose, and modifications must be trackable through each stage of development of the method.

***7. Research/work records***

All records must be of sufficient quality to present a complete picture of the work performed, enabling it to be repeated if necessary.

The project leader is accountable for the validity of the wok and responsible for ensuring that regular reviews of the records of each researcher are conducted[[7]](#footnote-7)

The location of all project records, including critical data, must be recorded. They must be retained in a form that ensures their integrity and security, and prevents unauthorised modification, for a period to be agreed by BEIS

A recommended checklist for researchers can be found on the UK Research Integrity Office (UKRIO) website at http://www.ukrio.org/what-we-do/code-of-practice-for-research

1. Energy Delivery Systems comprise the sensors and actuators used for monitoring and controlling energy delivery processes, the computer-based systems that analyze and store data and the communication pathways and networks that interconnect the various computer systems – *DOE/DHS Cybersecurity Procurement Language for Energy Delivery (April 2014)* [↑](#footnote-ref-1)
2. The Invitation to Tender is issued for the Secretary of State for Energy and

   Climate Change, as the new office of Secretary of State for Business,

   Energy and Industrial Strategy has yet to be constituted as a corporation sole.

   It is expected that rights and liabilities of the Secretary of State for Energy and

   Climate Change, including this Invitation to Tender, will in due course be transferred to

   the Secretary of State for Business, Energy and Industrial Strategy by an

   Order in Council under section 2 of the Ministers of the Crown Act 1975. [↑](#footnote-ref-2)
3. Please note that this declaration applies to individuals, single organisations and consortia. [↑](#footnote-ref-3)
4. The Code of Practice is attached to this ITT as Annex B [↑](#footnote-ref-4)
5. Please delete as appropriate [↑](#footnote-ref-5)
6. Please note ethical approval does not remove the responsibility of the individual for ethical behaviour. [↑](#footnote-ref-6)
7. Please note that this also applies to projects being undertaken by consortia. [↑](#footnote-ref-7)