# DPS Schedule 6 (Order Form and Order Schedules)

## Order Form

| | |
|---|---|
| ORDER REFERENCE: | **CS20512** |
| THE BUYER: | **Department for Business, Energy and Industrial Strategy (BEIS)** |
| BUYER ADDRESS | **1 Victoria Street, London, SW1H 0ET** |
| THE SUPPLIER: | **PA Consulting Services Limited** |
| SUPPLIER ADDRESS: | **10 Bressenden Place<br>London<br>SW1E 5DN** |
| REGISTRATION NUMBER: | **00414220** |
| DUNS NUMBER: | **211000617** |

DPS SUPPLIER REGISTRATION SERVICE ID: N/A

APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated 2nd February 2021 It's issued under the DPS Contract with the reference number RM3764iii for the provision of Cyber Security Services.

DPS FILTER CATEGORY(IES):
**NCSC Assured Services, Chemicals, Reference: 7738**

ORDER INCORPORATED TERMS
The following documents are incorporated into this Order Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Order Special Terms and Order Special Schedules.
2. Joint Schedule 1 (Definitions and Interpretation) RM3764iii
3. The following Schedules in equal order of precedence:

    - Joint Schedules for RM3764iii
        - Joint Schedule 2 (Variation Form)
        - Joint Schedule 3 (Insurance Requirements)
        - Joint Schedule 4 (Commercially Sensitive Information)

- Joint Schedule 7 (Financial Difficulties)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)

---

- Order Schedules for RM3764iii

  - Order Schedule 7 (Key Supplier Staff )
  - Order Schedule 8 (Business Continuity and Disaster Recovery)
  - Order Schedule 9 (Security)
  - Order Schedule 22 (Secret Matters)

4. CCS Core Terms (DPS version)
5. Joint Schedule 5 (Corporate Social Responsibility) RM3764iii

No other Supplier terms are part of the Order Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

ORDER SPECIAL TERMS
The following Special Terms are incorporated into this Order Contract:
None

ORDER START DATE: 10th February 2021

ORDER EXPIRY DATE: 31st March 2021

ORDER INITIAL PERIOD: 7 weeks

ORDER OPTIONAL EXTENSION: None

DELIVERABLES - As per specification CS20512 below

## Introduction

BEIS is the Lead Government Department (LGD) responsible for overall effectiveness of the safety and security regime for the UK's chemical industry, and within this role we work with partners across central government, industry and regulators to provide high standards of security at the designated Critical National Infrastructure (CNI) chemical sites in the UK.

The chemicals sector was designated as a national infrastructure sector in 2015 and 11 sites, operated by 10 companies, were identified as CNI in 2016. More recently a further 6 sites have been identified as CNI, making a current total of 17 sites, operated by 15 companies.

## Background to the Requirement

The chemicals sector was originally designated CNI based on the risk to life due to a malicious release of Toxic Liquified Gas (TLG) which can cause mass fatalities. Any risk, analysis, planning and strategy will need to be based on this requirement.

The processes or measures the LGD introduces must be consistent, repeatable, and reproducible across the x17 chemicals CNI operators to ensure that Governance can be undertaken both in monitoring and tracking resilience.

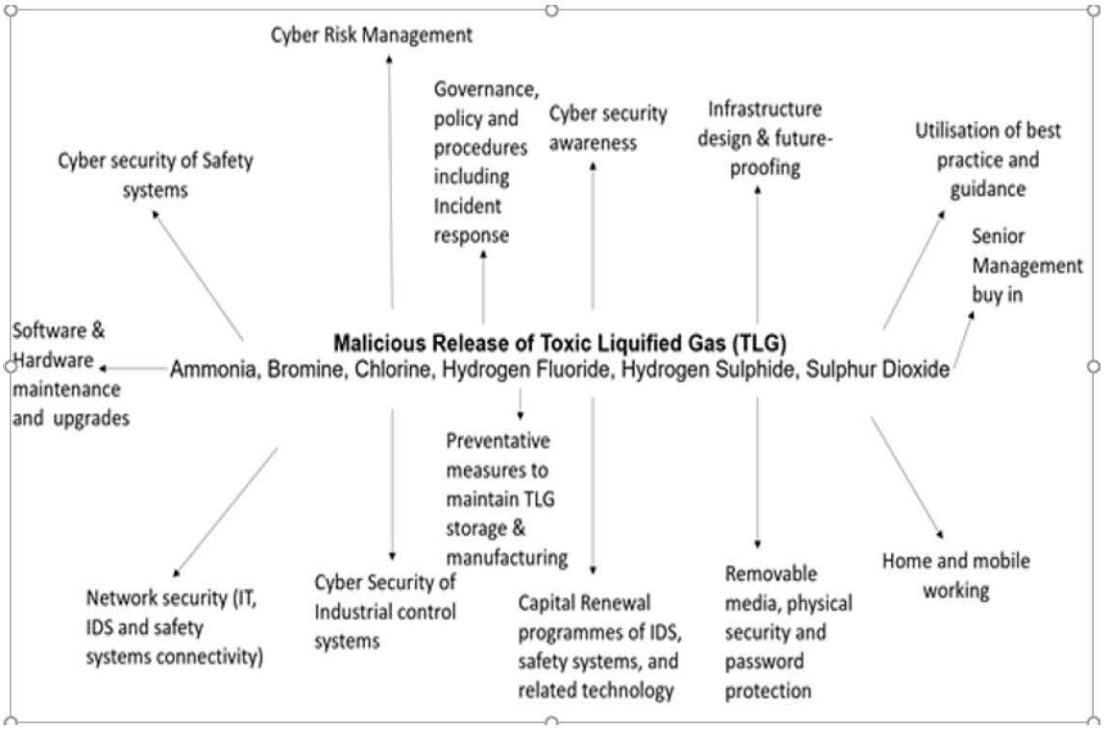
This is especially important now that there are x6 new CNI operators, which do not have any assessments or audits undertaken to date.

It is expected the chemicals cyber security maturity assessment process will sit alongside the protective security strategy as highlighted in figure 1 which both these processes should feed into the Chemicals CNI & Resilience Security Strategy and SSRP which is refreshed annually as part of the Cabinet Offices National Security Risk Assessment (NRSA) process.

The personnel and protective security maturity assessment process was developed several years ago, however limited progress has been made (which we are revising the methodology) and currently the BEIS chemicals cyber security assessment methodology does not exist

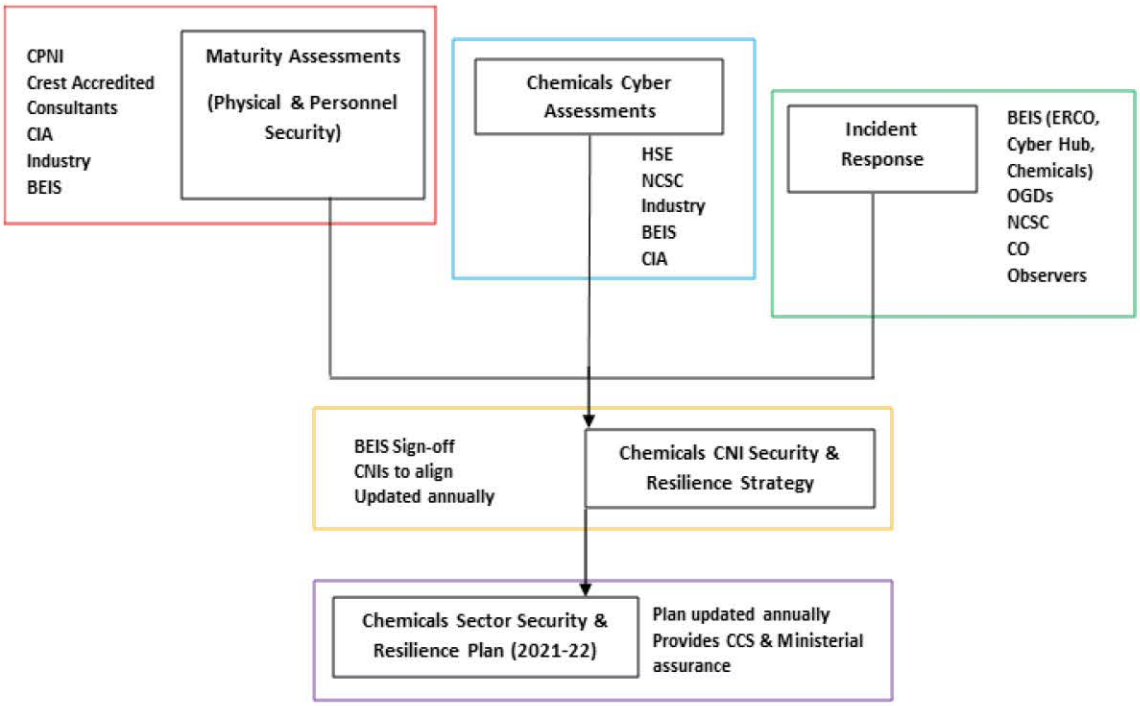
Operating within these parameters the chemicals cyber resilience strategy may have the following pillars to develop the Cyber LGD assessment process as shown in figure 2.

## Figure 1



The overall strategy is intended to produce a **chemical cyber assessment process** as shown below in figure 2:

## Figure 2




**Existing evidence (to be reviewed Documentation will be provided upon receipt of the successful expert supplier)**

- Project Langdale: (x10 site specific reports and x1 summary report)

  In 2018 BEIS commissioned NCC group to undertake cyber security reviews of 9 CNI site operators, focussing specifically on assessing the potential risk of a cyber-attack resulting in a loss of containment. The site-specific reports were sent to the participating site operators, although the findings have not been consistently reviewed and considered. It is clear the analysis and prescribed recommendations are not intuitive for industry to undertake. **Further guidance and support are needed to ensure the department as the LGD can be assured that the risks are As Low As Reasonably Practicable (ALARP).**

- Actica cyber security study of Safety Instrumented Systems (SIS) (currently WIP x5 site specific reports and x1 summary report)

  The Safety Instrument System (SIS) study was undertaken by Actica consultants during 2020 to further assess the risks associated of a cyber-attack of the Emergency Shut Down systems (ESDs) at 5/17 sites. The site-specific reports have been shared with the assessed chemical sites and industry feedback has been sought.

- NCSC UK CNI Cyber Risk Review: Findings report for the chemical sector (Amber report 2018)

  The document highlights some general recommendations which could be applied in the chemical CNIs; however, there is a caveat that no specific analysis have been undertaken at the x11 original CNI sites.

It is understood that the Amber report has been shared with the Chemicals Sector Resilience Liaison Group (CSRLG) members, although no resilience discussions or methodological measures have been undertaken.

- Chemicals CNI Security Resilience Strategy document

  This document is intended as an industry and Government collaborative strategy to raise the standards of protective security by a pre-defined date using an audit and Risk Management process (security maturity assessments) developed by CPNI. Protective security encompasses physical, personnel and general cyber security measures.

  Out of the 11 original CNI, 10 operators have so far signed up to raise their protective security standards, however no CPNI protective security maturity assessment has been undertaken since the original assessment in 2019. BEIS are currently developing a process to revise the process and undertake assessments.

- HSE OG86

  Work is underway to foster information sharing with the HSE to understand their auditing programme over the next 2 years. This will require a BEIS/HSE data sharing agreement to use this information for cyber assurance. Analysis is needed to identify which relevant parts of the auditing documentation satisfies LGD cyber assurance and what are the gaps.

## Aims and Objectives

a) Analyse documents in Background to the Requirement section above, distilling the information to specific discussion points and actions which can be facilitated through workshops to assess findings and a means of tracking cyber security improvements.

b) Commissioning new analysis to collect evidence from the new x6 CNIs to develop a cyber assessment profile of each new chemical site operator.

c) Utilise any other information and best practice which can be used to develop an effective analysis and contribute to the cyber security maturity assessment process.

d) Utilising (a), (b) and (c) to develop a LGD cyber security maturity assessment process which forms the overarching BEIS LGD security strategy (figure 2).

e) Produce material for at a minimum of 4 cyber workshops pitched at 2-3 hours each.

f) Identify gaps in analysis and understand and identify any future work.

g) Identify who the stakeholders are and identify the most efficient and cost-effective way to consult with them.

h) Analyse the OG86 process and distil the relevant information requirements for use as the BEIS LGD for cyber security assurance.

i) Produce suitable outputs as described in specific requirement section below to a very high quality

## Specific Requirements

The successful bidder will provide a kick-off meeting at the project start-up (with appropriate slides and other documents) to identify:

(i) How the project will be delivered in the tight time scales (to set the pace)
(ii) Project plan i.e. discuss Gantt chart, identify how risks will be managed etc.
(iii) Utilisation of evidence and best practise
(iv) Introduce the team on both sides
(v) Identify the frequency of progress meetings
(vi) Discuss how stakeholder engagement will take place
(vii) Articulate what the outputs will look like i.e. number of reports, spreadsheets etc.
(viii) AOB

Part 1: **Analyse current evidence base, identify gaps and distil information into key findings and recommendations**

(ix) Analyse documentation in section 4
(x) Distil information into key findings, areas of improvement and gap analysis
(xi) Utilise the information to produce a plan and strategy to undertake workshops to: (1) discuss findings; (2) identify how it will be facilitated; (3) develop a process to monitor and track progress and improvements (4) Determine how many workshops are required and duration
(xii) Analyse the findings and correlate with figure 1 (as guidance) to develop a risk register, using expert analysis, evidence gaps and identify any further assessments required.
(xiii) Utilise best practice, any relevant standards, documentation and industry expertise to build the analysis

Part 2: **Develop a cyber evidence base for Six new chemicals CNI operators**

(xiv) Utilise the findings from part 1 to develop an evidence base for the new CNI operators to ensure that the findings are consistent with part 1. This is expected to require consultation with CNI stakeholders, desk top studies and other evidence collection requirement.
(xv) Analyse the findings, correlate with part 1 and figure 1 to develop a risk register, identifying expert analysis, evidence gaps and any further assessments required.
(xvi) Utilise best practice, any relevant standards, documentation and industry expertise to build the analysis
(xvii) Identify evidence gaps and any further work needed.

Part 3: **HSE OG86 analysis and Security Maturity Assessment process**

Utilising Part 1 and part 2

(xviii) Analyse the information requirements from OG86 and provide recommendations how BEIS could use the inspection reports as part of the BEIS LGD cyber security assurance process. We understand that although it is aligned to the CAF the information requirements are too detailed especially when inspectors populate the proforma.

(xix) Currently OG86 does not use metrics to assess risk, experts are encouraged to develop this as discuss with HSE in collaboration with BEIS.

(xx) Identify any information gaps and correlate the distilled OG86 audit into the risk register developed in parts 1 and parts 2.

(xxi) Integrate analysis and findings into the security assurance process/methodology and identify how it can fit into the overall security auditing process highlighted in figure 2.

The successful bidder 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.

BEIS would like bidders to demonstrate the key roles within the team, including the lead contact, alongside the skills and expertise they would bring to this project

The successful bidder will 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.

## Timetable

All deliverables must be received by BEIS by 31 Mar 2021; however, project timelines are at the discretion of the supplier subject to discussion with BEIS project manager (at the kick off meeting), and as long this deadline is met.

Payments will be linked to delivery of key milestones. The indicative milestones and phasing of payments are as follows:

**Payments Terms**

1st stage: at the end Feb 2021 (40% of the total project costs)

2nd stage: 31st March 2021 (60% of the total project costs)

**Milestones**:

1st stage: Draft outputs from specific requirement section above (number of reports and spreadsheets need to be agreed at kick off)

2nd stage: Draft outputs from section 6 (number of reports and spreadsheets need to be agreed)

## Terms and Conditions

Bidders are to note that any requested modifications to the Contracting Authority Terms and Conditions on the grounds of statutory and legal matters only, shall be raised as a formal clarification during the permitted clarification period.

## Schedule of Processing, Personal Data and Data Subjects

The Supplier shall only process in accordance with the instructions as advised below and comply with any further written instructions with respect to processing by the Contracting Authority. Any such further written processing instructions required by the Contracting Authority shall be incorporated into this Schedule and shall be the subject of a formal amendment to this Contract.

1. The contact details of Contracting Authority Data Protection Officer are Email: dataprotection@beis.gov.uk
2. The contact details of the Suppliers Data Protection Officer are: REDACTED, email: REDACTED @paconsulting.com
3. The Supplier shall comply with any further written instructions with respect to processing by Contracting Authority. Any such further instructions shall be incorporated into this Schedule.

| | |
|---|---|
| Description | Mini Competition against an existing Framework Agreement. |
| Subject matter of the Processing | Chemical industry Critical National Infrastructures (CNIs) Cyber-security vulnerability assessment Project.<br>The processing of names and business contact details of staff of both Contracting Authority and Contractor will be necessary to deliver the services exchanged during the course of the Contract, and to undertake Contract and performance management.<br>The Contract itself will include the names and business contact details of staff of both the Contracting Authority and the Contractor involved in managing the Contract. |
| Duration of the processing | Processing will take place from the Start Date of the Contract. The Contract will end on 31 March |
| Nature and purposes of the processing | BEIS are processing your personal data for the purposes of the tender exercise, or in the event of legal challenge to such tender exercise.<br>Legal basis of processing<br>The legal basis for processing your personal data is processing as necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, such as the exercise of a function of the Crown, a Minister of the Crown, or a government department; the exercise of a function conferred on a person by an enactment; the exercise of a function of either House of Parliament; or the administration of justice.<br>Recipients<br>Your personal data will be shared by us with other Government Departments or public authorities where necessary as part of the tender exercise and may share your data if required to do so by |

| | |
|---|---|
| | law, for example by court order or to prevent fraud or other crime.<br>The nature of processing will include the storage and use of names and business contact details of staff of both the Contracting Authority and the Supplier as necessary to deliver the services and to undertake the Contract and performance management. The Contract itself will include the names and business contact details of staff of both the Contracting Authority and the Supplier involved in managing the Contract. |
| Type of Personal Data | Names and contact details of employees involved in preparing and submitting the bid; Names and contact details of employees proposed to be involved in delivery of the contract.<br>Names, contact details, age, qualifications, and experience of employees whose CVs are submitted as part of the bid. |
| Categories of Data Subject | Staff (including volunteers, agents, and temporary workers), Contracting Authority / clients, /suppliers |
| Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data | Provide the Contracting Authority with a complete and uncorrupted version of the Personal Data in electronic form (or such other format as reasonably required by the Contracting Authority and erase from any computers, storage devices and storage media that are to be retained by the Supplier the expiry of the Contract and Contractor retention period. The Supplier will certify to the Contracting Authority that it has completed such deletion.<br>Where Personal Data is contained within the Contract documentation, this will be retained in line with the Department's privacy notice found within the Procurement Documents. |

GDPR Questionnaire

The Supplier agrees that during any term or extension it shall complete and return the attached questionnaire as advised below.

Note: the Contracting Authority also reserves the right to amend or increase these frequencies, as it deems necessary to secure assurance with regards to compliance. The Contracting Authority requires such interim assurances to ensure that the Supplier is still compliant with the needs of the GDPR Act due to the implications of a breach. The Supplier shall complete and return the questionnaire to the contact named in the Contract on the anniversary of the commencement of the Contract.
The Supplier agrees that any financial burden associated with the completion and submission of this questionnaire at any time, shall be at the Suppliers cost to do so and will not be reimbursable.

GDPR Assurance Questionnaire May1

MAXIMUM LIABILITY
The limitation of liability for this Order Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is a maximum of £89,975.00ex VAT

BID RESPONSE AND ORDER CHARGES
See Annex A

REIMBURSABLE EXPENSES
Recoverable as stated in the DPS Contract

PAYMENT METHOD
The Supplier shall submit an invoice within 28 days of supplying the Supplies and or performing Services to the satisfaction of the Contracting Authority. The invoice shall show the amount of VAT payable and bear the Purchase Order number. Save where an invoice is disputed, the Contracting Authority shall pay the Contractor within 30 days of receipt of an invoice via BACS payment.

- 1st stage: at the end Feb 2021 (40% of the total project costs)
- 2nd stage: 31st March 2021 (60% of the total project costs)

If you have a query regarding an outstanding payment please contact our accounts payable section either by email to finance@services.uksbs.co.uk or by telephone 01793-867204 between 09:00 and 17:00 Monday to Friday

BUYER'S INVOICE ADDRESS:
finance@services.uksbs.co.uk
UKSBS, Queensway House, West Precinct, Billingham, TS23 2NF

BUYER'S AUTHORISED REPRESENTATIVE

Core Services Procurement
professionalservices@uksbs.co.uk
Polaris House, North Star Avenue, Swindon, SN2 1FF

BUYER'S ENVIRONMENTAL POLICY
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/675134/beis-environmental-policy-2018.pdf

BUYER'S SECURITY POLICY
https://www.gov.uk/government/publications/civil-nuclear-cyber-security-strategy

SUPPLIER'S AUTHORISED REPRESENTATIVE
REDACTED
PA Partner in Charge
REDACTED@paconsulting.cm

SUPPLIER'S CONTRACT MANAGER
REDACTED
PA Partner in Charge
REDACTED@paconsulting.com

PROGRESS REPORT FREQUENCY
Weekly with the Project Manager

PROGRESS MEETING FREQUENCY
Weekly with the Project Manager and fortnightly with the team.

KEY STAFF
REDACTED
PA Partner in Charge
REDACTED
PA Assignment Manager

KEY SUBCONTRACTOR(S)
**Not Applicable**

COMMERCIALLY SENSITIVE INFORMATION
All information contained in Annex A

SERVICE CREDITS
Not applicable

ADDITIONAL INSURANCES
Not applicable

GUARANTEE
Not applicable

SOCIAL VALUE COMMITMENT

The Supplier agrees, in providing the Deliverables and performing its obligations under the Order Contract, that it will comply with the social value commitments in Order Schedule 4 (Order Tender)]

| **For and on behalf of the Supplier:** | | **For and on behalf of the Buyer:** | |
|---|---|---|---|
| Signature: | REDACTED | Signature: | REDACTED |
| Name: | REDACTED | Name: | REDACTED |
| Role: | Member of PA's Management Group<br>9 Feb 2021 | Role: | Deputy Director, Chemicals, Bioeconomy & Plastics<br>9 Feb 2021 |

# Annex A – Bid response and Order Charges

REDACTED

AW5.2 Price Schedule
REDACTED