DPS Schedule 6 (Order Form Template and Order Schedules)

Order Form

ORDER REFERENCE:	TRGA3311
THE BUYER:	**Department for Transport**
BUYER ADDRESS	Great Minster House 33 Horseferry Road Westminster London SW1P 4DR
THE SUPPLIER:	**Dionach Limited**
SUPPLIER ADDRESS:	Unipart House Garsington Road Oxford OX 4 2PG
REGISTRATION NUMBER:	03908168
DUNS NUMBER:	23-917-8804

APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated 20th September 2023.
It's issued under the DPS Contract with the reference number RM3764iii for the provision of Cyber Security Services.

DPS FILTER CATEGORY(IES):
GovAssure – NCSC Assured

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 6 (Key Subcontractors)
        - Joint Schedule 10 (Rectification Plan)
        - Joint Schedule 11 (Processing Data)

    - Order Schedules for RM3764iii
        - Order Schedule 1 (Transparency Reports)
        - Order Schedule 4 (Order Tender)
        - Order Schedule 5 (Pricing Details)
        - Order Schedule 7 (Key Supplier Staff)
        - Order Schedule 8 (Business Continuity and Disaster Recovery)
        - Order Schedule 9 (Security)
        - Order Schedule 10 (Exit Management)
        - Order Schedule 15 (Order Contract Management)
        - Order Schedule 20 (Order Specification)

4. CCS Core Terms (DPS version)
5. Joint Schedule 5 (Corporate Social Responsibility) RM3764iii
6. Annexes A & B to Order Schedule 6
7. Order Schedule 4 (Order Tender) as long as any parts of the Order Tender that offer a better commercial position for the Buyer (as decided by the Buyer) take precedence over the documents above.

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:	25th September 2023
ORDER EXPIRY DATE:	24th September 2024
ORDER INITIAL PERIOD:	12 months
ORDER OPTIONAL EXTENSION	12 months

DELIVERABLES

See details in Order Schedule 20 (Order Specification)

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 £41,800.

ORDER CHARGES

The year 1 charges for this contract are fixed at £41,800 excluding VAT. The total value of this contract can be increased to £100,000, however DfT are not obligated to spend this full amount.

REIMBURSABLE EXPENSES
Recoverable as stated in the DPS Contract

PAYMENT METHOD
The payment method for this Call-Off Contract is BACS.

BUYER'S INVOICE ADDRESS:
Invoices will be sent to:

Shared Services Arvato

5 Sandringham Park

Swansea Vale

Swansea

SA7 0EA

Alternatively, electronic Invoices can be issued to:

ssa.invoice@sharedservicesarvato.co.uk

Please see Annex C for additional information.

BUYER'S AUTHORISED REPRESENTATIVE
[redacted]
Head of Cyber and Information Security
[redacted]

BUYER'S ENVIRONMENTAL POLICY
Is contained in Annex A

BUYER'S SECURITY POLICY
Is contained in Annex B

SUPPLIER'S AUTHORISED REPRESENTATIVE
[redacted]
Account Manager
[redacted]
Unipart House, Garsington Rd, Oxford OX4 2PG

SUPPLIER'S CONTRACT MANAGER
[redacted]
Account Manager
[redacted]
Unipart House, Garsington Rd, Oxford OX4 2PG

PROGRESS REPORT FREQUENCY
Weekly

KEY STAFF

[redacted]
GovAssure Assessor
[redacted]
Unipart House, Garsington Rd, Oxford OX4 2PG

[redacted]
GovAssure Assessor
[redacted]
Unipart House, Garsington Rd, Oxford OX4 2PG

[redacted]
GovAssure Assessor
[redacted]
Unipart House, Garsington Rd, Oxford OX4 2PG

KEY SUBCONTRACTOR(S)
Not applicable

COMMERCIALLY SENSITIVE INFORMATION
Not applicable

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:	[redacted]	Signature:	[redacted]
Name:	[redacted]	Name:	[redacted]
Role:	CEO	Role:	Procurement Business Partner
Date:	22 September 2023	Date:	23rd September 2023

Annex A – DfT Environmental Policy

Policy statement

DfT is committed to protecting the environment, reducing pollution and whole life carbon in our procurements and continually improving our environmental performance.

Scope

This policy applies to the Department for Transport central department. Any DfT arms-length bodies or executive agencies may use this policy or apply their own.

Description

DfT's operational activities and the individual activity of its staff affect the environment.
The aim of this policy is to inform our interested parties including staff, contractors, suppliers and the public that DfT is committed to reducing any negative environmental impacts produced by our activities, products and services.

Our policy is to continually improve our environmental performance by:

- • reducing our greenhouse gas emissions from energy use
- • reducing waste and maximising reuse and recycling
- • reducing our greenhouse gas emissions from business travel
- • controlling how much water we use
- • reducing how much paper we use
- • protecting our biodiversity and ecosystems
- • adapting to climate change
- • reducing the carbon impact of our construction projects through innovative methods, cleaner materials and more efficient design

Delivery and monitoring

We will:

- fulfil our compliance obligations in relation to the environment
- meet or exceed the terms of the government's policy on the environment
- set targets to reduce our environmental footprint and protect the environment

• collate, monitor, and analyse data to measure performance against our targets
• prepare for policy changes and tighter targets
• encourage staff, contractors and suppliers to reduce their impact on the environment when providing services and products to us and within their own organisations
• report progress against our targets quarterly to a senior performance board
• report our environmental performance openly and transparently through our annual report and accounts

Although the Department is responsible for the environmental performance of DfT, we expect all staff, contractors and suppliers involved in DfT's business to share this responsibility.

Annex B – Security Policy

Information and cyber security policy

1. Introduction

The Department for Transport Central (DfTc) Information & Cyber Security Policy Framework provides an overview of Digital Services suite of Information Security policies. The policies set out the minimum requirements for information security which the Department, its delivery partners and third party suppliers must comply.

2. Purpose

The purpose of this policy is to demonstrate the management board's commitment to Information Security and to support the overarching policy principles to which all subordinate policies and controls must adhere to. It explains the responsibilities that various functions, roles and individuals have for ensuring the confidentiality, integrity and availability of information.

3. Objectives

The aim of this policy is to enable and maintain effective information security through implementing supporting policies, standards and controls to protect information assets processed or stored by and on behalf of DfTc.
The key objectives of the Departmental Information & Cyber Security Policy Framework are the preservation of confidentiality, integrity, and availability of systems and information. These three pillars compose of the Confidentiality, Integrity, Availability triad:

- **Confidentiality** - Access to information shall be restricted to those authorised users with a legitimate business need and appropriate authority to view it.
- **Integrity** – Data and information are to be complete and accurate with all management systems operating correctly.

- **Availability** - Information shall be readily available to those authorised to view it as and when it is needed.

This objective can be achieved through safeguarding the Confidentiality, Integrity and
Availability of DfTc Assets and all information it collects, stores, transfers and process for clients, staff and partners in accordance with legislation, regulation and contractual obligations.

4. Scope

DfTc's Information & Cyber Security Policy Framework shall apply to all data, information, information systems, networks, applications, devices, locations used to store, process, transmit or receive information and staff within DfTc, its primary delivery partners and third-party suppliers.
Never-the-less the scope shall be based on and remain compliant with the mandatory requirements set out within the Minimum Cyber Security Standard.

5. Overarching Principles

DfTc is committed to protecting the security of its information and information systems against breaches of confidentiality, failures of integrity or interruptions to the availability.
In order to meet this intent, DfTc will adopt the overarching principles below:

- ensure that senior management provides clear direction to imbed information security within all DfTc's strategic objectives to deliver secure and successful services
- ensure compliance with legal, statutory, regulatory or contractual obligations related to information security
- establish a management framework to initiate and control the implementation and operation of information security
- implement human, organisational, and technological security controls to preserve the confidentiality, availability and integrity of its information systems
- develop and maintain policies, procedures and guidelines to meet government standards for information security, reflecting industry best practice
- ensure robust risk management processes are in place to identify potential threats, vulnerabilities and controls to reduce the risks to an acceptable level
- ensure that staff and contractors understand their responsibilities in relation to information security
- ensure information security is an integral part of information systems throughout its lifecycle (from concept to disposal/termination)
- ensure access to information and information assets is granted on the need to know principle
- ensure policy and controls on remote working practices and the use of removable media for legitimate business purposes are in place and documented

- ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses
- keep up to date on latest cyber security threats and trends through various reliable sources and apply good working practices
- continuously review and improve DfTc's information security controls to minimise and prevent compromise to information systems
- establish information security education, training and awareness initiatives, ensuring that all users conduct mandatory information security awareness training
- ensure that information security is implemented and operated in accordance with this policy and other supporting, policies, procedures or standards
- ensure independent reviews of information security policy and associated controls are performed internally and using services of an external/third party reviewer annually

6. Responsibilities for Information Security

Overall responsibility for information security and assets shall rest with the Business.
Heads of Departments shall ensure that information security within their business area shall promote good information and cyber security practices and ensure that staff adhere to DfTc's Information & Cyber Security Policies Framework.
The Senior Information Risk Owner is responsible for the direction of information risk at board level and takes the lead in the departments strategic approach for managing risks, supported by the Head of Information & Cyber Security.
Head of Information and Cyber Security will be the owner for all Information & Cyber Security Policies within DfTc.
On a day-to-day basis the Digital Assurance Manager shall be responsible for organising and managing information and cyber security; ensuring the department is abreast of all related security policies and good working practices.
Digital Services has overall responsibility for creating, updating, reviewing (annually) and disseminating the suite of Information & Cyber Security Polices as well as providing staff training and awareness on Information & Cyber Security.
Line Managers shall be responsible for ensuring that staff, contractors and third party users are aware of and apply:

- The information security policy suite
- Their personal responsibilities for information security
- Who to ask for further advice on information security matters

Users are responsible for complying with the terms of this policy and all DfTc policies, procedures, regulations and legislation governing the information and systems they access.

7. Compliance and Breach of Policy

DfTc shall conduct and maintain cyber security compliance and assurance activities on the subordinate polices to effectively manage information risks and ensure cyber security objectives and the requirements of the policy are met.
All staff shall abide by the security policies of the Department. Staff shall remain responsible for both the security of their immediate working environments and for security of the data, information assets, systems and devices they use, ensuring that their confidentiality and integrity are not breached, and their proper availability is maintained. Failure to do so may result in disciplinary action.
If you have any questions or concerns about this policy, please discuss them with your line manager.

8. Review and Development

This Information & Cyber Security Policy Framework shall be owned, maintained, reviewed and updated by Information and Assurance team. The suite of Information Security Policies shall be owned, maintained, reviewed and updated by Digital Services. This review shall take place annually or in response to changes in service, technology. Reviews will account for changes to legislation and regulations.

9. Associated Documentation

This overarching policy provides direction for all DfTc information security policies, standards and controls which underpin it.

DfTc's Information Security Policy Framework is underpinned by a suite of Information & Cyber Security policies. Details of which can be found within the table below in **Appendix A**.

All staff, users, and any third parties authorised to access the DfTc network or information systems are required to familiarise themselves with these supporting policies and to adhere to them.

Appendix A: associated documentation

Policies supporting this framework include (this is not an exhaustive list):

Policy	**Summary**
Acceptable Use Policy	The Acceptable Use Policy (AUP) aims to protect all users of DfTc equipment and data and minimise risk by providing clarity on the behaviours expected and required by DfTc Staff, Agents, Service Providers, Contractors and Consultants. It sets a framework on how to conduct DfTc's business to meet legal, contractual, and regulatory requirements and defines how individuals must behave in order to comply with this policy.
Information Security Governance Framework	The purpose of this policy is to demonstrate the management board's commitment to Information Security. It sets out a framework of governance and accountability for

	information security management across DfTc and forms the basis of DfTc's Information Security Management System (ISMS). This incorporates all policies, standards and procedures that are required to protect DfTc's data and information.
Information and Cyber Security Policy Framework	The purpose of this policy is to support the overarching policy principles to which all subordinate policies and controls must adhere to. It explains the responsibilities that various functions, roles and individuals have for ensuring the confidentiality, integrity, and availability of information. It includes a set of policies for information and cyber security which are defined, approved by management, published, communicated, and understood by staff, partners, and external parties.
Privilege Account Policy	This policy details the measures that must be in place for the management of privileged accounts which operate across the Department for Transport central (DfTc) estate.
Information Risk Management Policy (Medium)	This policy details the importance of creating a culture that actively manages risk, how the Department wishes to embed risk management into decision making and the risk appetite of the Department. It also details the various roles and responsibilities of individuals, the requirements for recording risks and the departmental risk process.
Information Risk Management Framework (Medium)	The risk management framework enables DfTc to apply the principles and best practices of risk management to improving the security of its systems and critical infrastructure within desired levels across DfTc in line with strategy and risk appetite to achieve its objectives.
Information Asset Policy	This policy sets out DfTc's approach to managing data within information assets in accordance with their classification and value. It explains the concept of an Information Asset and defines the role of the Information Asset Owner who is responsible for each Information Asset. This policy also sets out the primary responsibilities of an Information Asset Owner for managing the risks to personal data and business critical information held within a department.
Joiner, Movers, Leavers Policy	This policy outlines the security requirements associated with any individuals who join, move within, work for, or leave the DfTc.
Secure Configuration Policy	This policy provides guidelines for applying effective, secure, and reliable configuration management techniques, whether in test, development, or production environments.

	Outlines rules for computer network access, determines how policies are enforced and lays out some of the basic architecture of the company security/network security environment.
Patch Management Policy	This policy is comprised of a set of steps and procedures aimed towards managing and mitigating vulnerabilities within the DfTc environment through a regular and well-documented patching process.
Vulnerability Management Standard	This standard sets out the requirement to identify and address technical vulnerabilities quickly and effectively, reducing the likelihood of them being exploited, which could result in security breaches and damage to DfTc reputation.
Managed Device Policy	This policy provides guidance to staff who intend to use their own smartphones, tablets, laptops, and desktop PCs to access work information and services.
Bring Your Own Device Policy (BYOD)	This policy sets out requirements for the use of personally owned devices for work purposes to ensure systems and data are accessed and used appropriately, legally, and securely and staff clearly understand their responsibilities when using BYOD.
Password Policy	This policy defines the standard for creation and management of strong passwords.
Removable-Media Policy	This policy establishes the principles and working practices that are to be adopted by staff of the Department for Transport Central (DfTc) in relation to the use of removable media for data transfer. It also details the measures that must be in place to ensure the controlled use of removable media devices where a valid business case for its use has been provided.
Overseas Working Policy	This policy outlines the principles and working practices that are to be adopted by all staff posted outside of the United Kingdom whilst working for DfTc.
Supplier Assurance Framework/Policy	This policy sets out the requirements when engaging with third-party suppliers who have access to any DfTc information assets. It provides guidance on identifying and managing risks through assessments and monitoring third party compliance with business standards.
Access Control Policy	This policy outlines the requirements for the management of access control to minimise potential exposure from unauthorised access to resources and ensure that only authorised individuals have access to networks, systems and applications, to preserve and protect confidentiality, integrity and availability.

Account Management Policy	The purpose of this policy is to establish the requirements and processes to protect, monitor, and audit account access and reduce the compromise of user accounts by reducing the attack surface.
Authentication Policy	This policy sets out the principles and responsibilities for the identification and authentication of users and devices for accessing DfTc data and/or services to protect against a security breach by verifying that each user is who they claim to be and restricting access to authorised users.
Information Security Exception Policy	This policy explains how an exception request for deviation from the normal or non-compliance to any cyber security polices and standards can be requested, and the required process for effective management of exceptions to mitigate risk.

Annex C – Invoicing Procedures

1 You should not provide goods or services without receipt of a valid Purchase Order

2 The contract specification will set out the timing of invoices

3 It is important that invoices contain the correct information, or they will be returned to you. Invoices should be submitted in a timely manner after the despatch of goods or provision of services. Be aware that the following data must be included on every invoice:

- Business unit (e.g., DFT)
- Valid Purchase Order (PO) number relevant to the goods/services being invoiced. The PO number must be in the format 8000XXXXXX or 450XXXXXX. This will be found on the Purchase Order you receive
- Quantities / prices (as applicable) consistent with those on the original PO
- Clear and detailed text describing the goods or services

4 We would expect to contract with your legally registered company name (legal entity) but can incorporate a 'trading as' name in our finance system if required. Any communication received (such as invoices) from the 'trading as' entity will need to make clear reference to the legal entity or delays in payment may occur

5 Do not undertake new work or supply goods or services in excess of the original Purchase Order Value.

6 All invoices or credit notes must be an original document

7 If an incorrect Purchase Order number or no Purchase Order number is quoted, the invoice will be returned to you. You will be able to handwrite the correct Purchase Order numbers on the invoices that are returned, however it is preferable that you change it on your system and reissue to ensure any future invoices are referenced correctly

8 You must identify the business unit the invoice or credit note relates to e.g., DFT

9 E-invoices must not include profanities, as these will also be blocked by Arvato email security filters and may delay/stop the invoice being received

10 If an invoice needs to be withdrawn for any reason, you will need to send a credit note. Credit notes should quote the Purchase Order number and your original invoice reference along with details of what the credit note applies to, particularly if it is not for the full value of the invoice

11 Any correspondence or enquiry sent to the designated email address for invoices/credit notes which is not an original document will be deleted, with no action being taken

12 Unless we specify otherwise, payment will be made by BACS no later than 30 days of receipt of a valid invoice. We will aim to pay you within 10 days.

Transmission of Invoices

13 All invoices and/or credit notes will either need to be sent electronically as an attachment to an email or as a hard copy document through the post to the designated address listed below:

Email: ssa.invoice@sharedservicesarvato.co.uk

Postal Address: Shared Services Arvato
5 Sandringham Park
Swansea Vale

SA7 0EA

14 If an original invoice and/or credit note is sent electronically, then the same document must not be sent as a hard copy through the post and vice versa

15 All e-invoices and/or credit notes must be sent in a PDF format. Any documents that are received and are not in a PDF format will be deleted with no action being taken.

16 A 10Mb maximum file size per email is applicable

17 If the e-invoice is encrypted, this could result in the invoice being blocked by Arvato email security filters

18 Shared Services Arvato cannot be responsible for any e-invoice until it has been received. Responsibility for ensuring the e-invoice is received by Arvato in a timely manner lies with the supplier

How to Notify a Change

19 If you change important information, such as your organisation's contact or bank details, you need to provide written official confirmation. Please notify Shared Services Arvato as soon as possible:

Tel: 0344 892 0343

Email: support@sharedservicesarvato.co.uk (Please do not email original invoices/credit notes to this email address)

Postal Address:

Shared Services Arvato
5 Sandringham Park
Swansea Vale SA7 0EA

Enquiring about progress of payments

20 All supplier invoices and payment enquiries must be directed to Shared Services Arvato. If you contact the relevant business unit directly, they will direct you to Shared Services Arvato

21 For all payment and invoice queries you will need to contact the Shared Services Arvato Service and Support Desk directly on 0344 892 0343. When calling you should quote the Purchase Order number, your vendor account number (if known) and the business unit you are invoicing e.g., DFT

22 You should ask for your communication to be logged on a "service ticket" along with your contact details. This will allow all issues relating to your query to be logged under a unique reference number

23 You should quote the service ticket number in any follow up conversations

24 If Shared Services Arvato has the invoice but cannot release it for payment, you are required to take appropriate action to ensure it can be paid

25 If the invoice has not been received by Shared Services Arvato, the responsibility is on you to get the invoice to Shared Services Arvato. If you are sending invoices to anyone other than Shared Services Arvato, please change your customer invoicing address to Shared Services Arvato

26 If a response from Shared Services Arvato is required, one will be provided to you within 10 working days

27 If you have any remittance queries, these should be discussed with Shared Services Arvato:

Tel: 0344 892 0343

Email: support@sharedservicesarvato.co.uk (Please do not email original invoices/credit notes to this email address)

28 You must also ensure that a statement is sent to Shared Services Arvato monthly to aid prompt payment of invoices (email and postal address as above)