

DPS Schedule 6 (Order Form and Order Schedules)

Order Form

ORDER REFERENCE:	TTSC3060
THE BUYER:	Department for Transport
BUYER ADDRESS	33 Horseferry Road, London SW1P 4DR
THE SUPPLIER:	NCC Group Security Services Limited
SUPPLIER ADDRESS:	XYZ Building, 2 Hardman Boulevard, Spinningfields, Manchester, M3 3AQ
REGISTRATION NUMBER:	04474600
DUNS NUMBER:	640711540

APPLICABLE DPS CONTRACT

This Order Form is for the provision of the Deliverables and dated 10 August 2022. It's issued under the DPS Contract with the reference number RM3764iii for the provision of Cyber Security Services.

DPS FILTER CATEGORY(IES):

Non-assured NCSC Services, Clearance: Counter Terrorist Check, Networks, Internet, Cloud, Transport

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)

DPS Ref: RM3764iii

Model Version: v1.0

- o Joint Schedule 3 (Insurance Requirements) ○ o Joint Schedule 4 (Commercially Sensitive Information)
- Joint Schedule 6 (Key Subcontractors)
 - Joint Schedule 7 (Financial Difficulties)
 - Joint Schedule 8 (Guarantee)
- Joint Schedule 10 (Rectification Plan)
- Order Schedules for RM3764iii
 - Order Schedule 4 (Order Tender)
 - Order Schedule 5 (Attachment 5 - Pricing Details)
 - Order Schedule 20 (Attachment 3 - Order Specification)
- 4. CCS Core Terms (DPS version)
- 5. Joint Schedule 5 (Corporate Social Responsibility) RM3764iii
- 6. Annexes A & B to Order Schedule 6

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: 10 August 2022

ORDER EXPIRY DATE: 31 March 2023

ORDER INITIAL PERIOD: 31 March 2023

ORDER OPTIONAL EXTENSION Optional extension of 3 additional months

DELIVERABLES

See details in Attachment 3 (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 £64,300

ORDER CHARGES

Attachment 5 Order Schedule 5 (Pricing Details)

REIMBURSABLE EXPENSES

Recoverable as stated in the DPS Contract

PAYMENT METHOD

Suppliers must be in possession of a written purchase order (PO), before commencing any work under this contract. You must quote the aforementioned PO number on all invoices, and these must be submitted directly to:

ssa.invoice@sharedservicesarvato.co.uk

or via post to:

Accounts Payable,
Shared Services arvato,
5 Sandringham Park,
Swansea Vale,
Swansea
SA7 0EA

Invoices received without the correct PO number will be returned to you and will delay receipt of payment.

BUYER'S AUTHORISED REPRESENTATIVE Commercial:

[REDACTED]
[REDACTED]
[REDACTED]

Contract Manager:

[REDACTED]
[REDACTED]
[REDACTED]

SUPPLIER'S AUTHORISED REPRESENTATIVE

[REDACTED] [REDACTED]
[REDACTED] [REDACTED]
[REDACTED]

DPS Ref: RM3764iii

Model Version: v1.0

SUPPLIER'S CONTRACT MANAGER

[REDACTED]
[REDACTED]
[REDACTED]

PROGRESS REPORT FREQUENCY

First draft report for comment by participants no later than 31/01/2022

PROGRESS MEETING FREQUENCY

Weekly update via email to raise any issues for the project going forward

KEY STAFF:

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

KEY SUBCONTRACTOR(S)

Not applicable

COMMERCIALLY SENSITIVE INFORMATION

Not applicable

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 made in the Suppliers tender response to the Social Value evaluation criteria.

For and on behalf of the Supplier:		For and on behalf of the Buyer:	
Signature:		Signature:	
Name:		Name:	
Role:		Role:	
Date:	09 /08/ 22	Date:	11/08/2022

ORDER SCHEDULE 20: ORDER SPECIFICATION

- 1.** Title
 - 1.1. To provide guidance on infrastructure cyber security considerations for roads technology.
- 2.** Purpose
 - 2.1. In 2020, the Department for Transport (DfT) supported development of the sign-posting guidance published by the Transport Technology Forum (TTF). ¹ This is a follow-on project aiming to produce cyber security infrastructure guidance to local authorities.
 - 2.2. The guidance will be based around the 12 recognised Connected Vehicle (CV) Use Cases aimed at identifying areas where authorities will need to consider cyber issues as part of the roll out of CV services.
- 3.** Background to the Contracting Authority
 - 3.1. The contracting authority is the Department for Transport (DfT). DfT is the government department responsible for the safety and security of transport across the UK, including security for UK roads.
 - 3.2. Transport Security, Resilience and Response (TSRR) Directorate with DfT leads on national security matters, ranging from counter terrorism and cyber security to planning for and responding to natural hazards or civil contingencies. The Cyber Security team is responsible for identifying and helping to counter cyber security threats in the transport sector.
- 4.** Background to Requirement/ Overview of Requirement
 - 4.1. Transport is an attractive target for malicious and disruptive attacks. There is an increasing use of technology and communications on the road network, as part of the development of edge computing systems, migration to IP and infrastructure to vehicle connectivity. This opens new threats and attack routes are not present in traditional closed technology systems. Guidance is needed to ensure mitigation

¹ <https://ttf.uk.net/news/its-cyber-sign-posting-guidance/>

of these risks is understood and properly incorporated into specification, procurement and operation practices.

- 4.2. The Connected Places Catapult (CPC) is currently working on the Manual for Smart Streets (MfSS) project, which is developing high level guidance for local authorities for the deployment of digital transport services. This guidance looks at the 12 most likely services (or uses cases) that will be delivered to road users through the employment of digital systems. It guides local authorities through the planning, specification, procurement (acquisition) and operation considerations needed to ensure resultant services offer value for money, are sustainable and interoperable with other services.
- 4.3. This project will produce cyber security infrastructure guidance to local authorities. The project will identify key themes within the Use Cases MfSS is developing. Liaison with CPC will be initiated by the client to allow the supplier to review the Use Cases that CPC is developing for this project and identify common cyber security principles for local authorities contemplating using the MfSS.
- 4.4. The identified cyber security principles developed as part of this project will be incorporated into the MfSS, therefore close collaboration with CPC will be essential.
- 4.5. The work to date on the development of MfSS can be viewed here. <https://ttf.uk.net/resources/mfss/> and the 12 Use Cases under development are.

1. MfSS: Air Quality Management

The air quality management use case is comprised of information services that support the monitoring and management of air quality. This can be achieved through air quality enforcement areas or through changes to traffic management and information policies.

2. MfSS: Transport Payment

The transport payment use case is comprised of services to support authorities in implementation and running of the integrated ticketing and other transport services payment systems in the city, region, cross region or nationally.

3. MfSS: Asset Management

The asset management use case is comprised of smart asset management utilising connected data and co-ordinated applications.

4. MfSS: EV Charging Information

The electrical vehicle (EV) charging information use case is comprised of information and management services that

support the accessibility and operation of EV charging facilities.

5. MfSS: Parking Management

The parking management use case is comprised of information services to support drivers in finding and paying for suitable parking and management to support the authority in maintaining the parking service. It also incorporates the accessibility and operation of EV charging facilities.

6. MfSS: Public Transport

The parking transport use case is comprised of information service to enable customers to discover, pay and use a DRT service, and provide the authority with key digital performance metrics.

7. MfSS: Mobility as a Service (MaaS)

Mobility as a Service, also known as MaaS, provides a platform for end-to-end customer travel experience that delivers multimodal transport choices in a seamless and integrated planning and payment ecosystem.

8. MfSS: Traffic Management

The traffic management use case is comprised of services for controlling, managing, and delivering traffic management in a data and technology driven environment, where traffic management comprises, the enforceable controls exercised by the road authorities.

9. MfSS: Road User Information

The road user information use case is comprised of service to support road users with road travel information that is relevant, timely, reliable, and easy to understand whilst supporting local transport policy incorporating connected in vehicle data.

10. MfSS: Transport Data Management

The transport data management use case is comprised of services to support Local Authorities in collecting, harvesting, analysing, fusing, managing, and making data open for all relevant users and service providers. This supports authorities to maximise the efficient and effective use of transport data. This includes the use of data from 3rd party services and probe vehicle data.

11. MfSS: Signal Control

The signal control use case is comprised of the use of connected vehicle data to support/improve traffic signal control, for example including GLOSA services.

12. MfSS: Vulnerable Road Users' Safety

The vulnerable road users' safety use case is comprised of services to improve safety for Vulnerable Road Users (VRU) including pedestrians and cyclists as well as motorcyclists

and persons with disabilities or reduced mobility and orientation. These services are considered to have a most significant impact on the various categories of VRUs (Vulnerable Road Users) which could include Human-Machine-Interface or safe integration of Nomadic Devices.

- 4.6. The supplier will, as part of this project seek to understand the ways in which new IP and edge computing technologies, and V2I services are being layered onto existing traffic control systems and comms networks impact on the application of the Use Case guidance. It will look at the migration to fibre, which is now gaining momentum across England and the challenges that the sun-setting of 2g / 3g, and PSTN / EPS services will have on edge to centre networks and the services that rely on them.
- 4.7. The provider will work closely with the team at the CPC delivering MfSS, who are aware of this procurement and stand ready to assist. Appropriate introductions will be made as required.
- 4.8. The supplier will collaborate with CPC and based on this will produce a single detailed guidance resource that sits across the MfSS Use Cases and identifies actions and considerations local authorities need to take generally when preparing to adopt them. This single detailed guidance resource produced by the supplier will support local authorities and suppliers in specifying network requirements and undertaking threat / penetration testing, that builds on NCSC (National Cyber Security Centre) and CPNI expertise. The single detailed guidance resource will provide the basis for us to work with NCSC to ensure that emerging technologies can be delivered in a way that meets local authorities and Government Connectivity obligations without unnecessarily stifling the innovation that adoption of the Use Cases outlined in MfSS offers.
- 4.9. Social Value will be applied by this project within the Equal Opportunity theme. The Cyber Industry has progress to make in many aspects of equal opportunity, including increasing opportunities for those with disabilities, women, those from BAME background and those from the LGBTQ+ community.

5. Definitions

Expression or Acronym	Definition
CCS	Crown Commercial Service
NCSC	National Cyber Security Centre
Buyer	Department for Transport
TTF	Transport Technology Forum, funded by DfT and Innovate UK
CV	Connected Vehicle
MfSS	Manual for Smart Streets
CPC	Connected Places Catapult
TTF	Traffic and Technology Forum

6. Scope of Requirement

- 6.1. The following are in scope:
- 6.2. Identify the key cyber security themes within the MfSS by applying current industry cyber security thinking and practice, and knowledge of real-world threats to the services described in each of the Use Cases
- 6.3. Develop, design and prototype guidance in a style suitable for primary consumption as a web-based resource, that users can read in association with the MfSS Use Case guidance. Work with CPC to ensure this is stylistically similar to the rest of the MfSS
- 6.4. Identify cross-modal themes and produce a single detailed guidance resource that addresses the general cyber security issues that users should consider when developing services based on each of the Use Cases. The Use Case document will be provided for the delivery of this work.
- 6.5. The following are not in scope:
- 6.6. NCSC and regulatory bodies; these organisations will be able to feed into the project and guidance through supporting the DfT.

7. The Requirement

- 7.1. The project outputs expected are as follows:

- 7.2. To identify key cyber security themes applicable to the MfSS use cases; and produce a single detailed guidance resource that shows how they may be mitigated in the design of the services MfSS describes
- 7.3. This guidance resource will be incorporated into the overall MfSS offering and should follow the web-based style adopted for MfSS, (as seen in the draft materials on the TTF website). The guidance resource shall be made available to be viewed on-line on the TTF website as part of the MfSS micro-site and as a downloadable PDF document.
- 7.4. DfT expects the project to commence with a discussion on the scope, methodology and timings of meetings and drafting of products noted in 7.5 below once the contract has been awarded.
- 7.5. The Supplier will set out their methodology and approach to working with CPC to deliver this project and provide the web based and PDF format outputs required at the beginning of the project.
- 7.6. The Supplier will work with DfT to set out a methodology for amalgamating the products of this project into the wider MfSS resources on the TTF website. The supplier will not be expected to price for or undertake activities around web hosting as this will be provided by the TTF as required. The supplier will work with DfT at the start of this project to understand what web hosting support will be required and what activities will be in or out of scope of this project
- 7.7. The Supplier must have the expertise, skills, and capabilities to undertake the project, and experience within transport and security would be beneficial. The Supplier should include CVs of the people undertaking the work, their security clearances (proof will be needed once the contract has been awarded), the time they are expected to put into the work, a list of previous relevant work and example case studies.
- 7.8. There may also be an opportunity to present the new guidance to manufacturers and operators, however this will be agreed in advance.

8. Key milestones and deliverables

8.1. The following Contract milestones/deliverables shall apply:

Milestone/Deliverable	Description	Timeframe / Delivery Date
1	Inception Meeting	Within week 1 of Contract Award
2	Draft report(s) for comments by participants.	No later than 20/01/23

3	FINAL documents (Report(s), Guidance documents) to include feedback and changes.	No Later than 31/03/23
---	--	------------------------

9. Management Information/ Reporting

- 9.1. Reporting by the Supplier will be provided as a minimum on a weekly basis and will be made available to the contract manager two working days before the contract review meetings.

10. Volumes

- 10.1. This contract is a one-off requirement via the Cyber Security Services DPS (Dynamic Purchasing System) until March 2023.

11. Continuous Improvement

- 11.1. Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.

12. Environment, Sustainability and Social Value

- 12.1. The supplier shall demonstrate how they will support the equal opportunity theme, specifically by describing how the project will tackle workplace inequality.

13. Payments and Invoicing

- 13.1. The Supplier shall provide a firm price for this work. The maximum allocated budget for the contract is £70,000 excluding VAT. Bids above this value may be discounted at the discretion of the DfT.

20% of the total evaluation score will be allocated to evaluation of the prices tendered for the specified requirement.

Prices are to be submitted via DfT's E-Sourcing portal. The portal is available using the following link:

<https://dft.app.jaggaer.com/web/login.html>

14. Quality

- 14.1. The Supplier shall state how they will ensure a quality product and provide Quality Assurance through the provision of a Quality Plan. They may provide a summary of the Quality Assurance arrangements, principles, standards and checks they will use within the project.
- 14.2. The Supplier shall have Cyber Essentials plus certification and proof will be required once the contract has been awarded.

15. Staff and Customer Service

- 15.1. The Supplier shall provide a sufficient level of resource throughout the duration of the Contract to consistently deliver a quality service.
- 15.2. The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.
- 15.3. The Supplier shall ensure that staff understand the Authority's vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.
- 15.4. The Supplier shall have two years' experience working with or on projects relating to Transport Critical National Infrastructure.
- 15.5. The Supplier shall have at least three years GDPR experience.

16. Service Levels and Performance

- 16.1. The Authority will measure the quality of the Supplier's delivery by:

KPI/SLA	Service Area	KPI/SLA description	Target
1	Progress Report	Progress reports will be supplied to the DfT project manager by phone or email (to be confirmed). This will include a summary of progress against the delivery.	Weekly
2	Risk monitoring	The Supplier will raise any concerns about the possibility of failing to meet the overall deadline and lack of relevant information to meet the requirements.	Weekly

3	Communication	The Supplier shall acknowledge any communications from the contract/project manager within 2 working days	2 working days
4	Emergencies	If there is an urgent issue, the Supplier shall make the contract manager aware of this within 2 working days.	2 working days

- 16.2. If the Supplier is unable to provide a product to the agreed quality within the specified time the Authorities reserves the right to retain payment, either in whole or in part.

17. Security and Confidentiality Requirements

- 17.1. The Supplier must be able to handle, and store classified material up to and including OFFICIAL SENSITIVE level. The project reports and guidance for government and industry will be classified at OFFICIAL SENSITIVE.
- 17.2. The Supplier should demonstrate the measures in place to keep this information secure. Specifically, in the bid document the Provider should provide detail on how they will meet the following requirements:
- 17.2.1. Information classified at OFFICIAL SENSITIVE level relating to this project should only be communicated electronically with those contacts provided by the DfT using the methods below.
- 17.2.2. The Supplier should ensure the security of the information in transit. Electronically this will involve using software (for example Egress Switch system) to encrypt the files, preferably using AES-256, or other measures that offer an equivalent level of protection.
- 17.2.3. Any passwords used to encrypt files should be complex and should be conveyed separately to the files themselves.
- 17.2.4. Any electronic files should be stored on an IT system that has access controls that only allow approved and cleared personnel with a genuine 'need to know' to access them to read and copy. The IT system should be protected by an appropriate firewall.
- 17.2.5. Once electronic files are no longer needed, they should be deleted from the IT system in a way that makes recovery unlikely, either by overwriting the storage space or eventual dilution and deterioration on a busy shared storage system.
- 17.2.6. Paper copies (including drafts and notes) and any removable electronic storage must be locked away when not in use to prevent unauthorised access. Printed material should be marked OFFICIAL

- SENSITIVE and numbered to ensure no copies are lost. Paper and printed material should be shredded when no longer needed.
- 17.2.7. If any paper copies are to be posted, advice should be sought from DfT.
- 17.2.8. Access to all material generated by this project (including source data supplied by DfT) must be on a limited and controlled basis, by persons approved by the DfT.
- 17.3. Any personal information obtained under this contract must be controlled in compliance with the Data Protection Act 2018.
- 17.4. Further information on security classification is available on the Cabinet Office website at the following addresses:
<http://www.cabinetoffice.gov.uk/sites/default/files/resources/hmg-personnel-security-controls.pdf> <https://www.gov.uk/government/publications/security-policy-framework>

18. Contract Management

- 18.1. Attendance at Contract Review meetings shall be at the Supplier's own expense.

19. Location

- 19.1. The location of the Services will be carried out at the Supplier's premises within the UK. Any anticipated travel and expenses incurred from engagement with stakeholders, or the Authority must be included in the bid price.

ORDER SCHEDULE 4: ORDER TENDER

[Redacted content]

Response	Percentage Range
U.S. should take action	75% - 95%
U.S. should not take action	5% - 25%

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

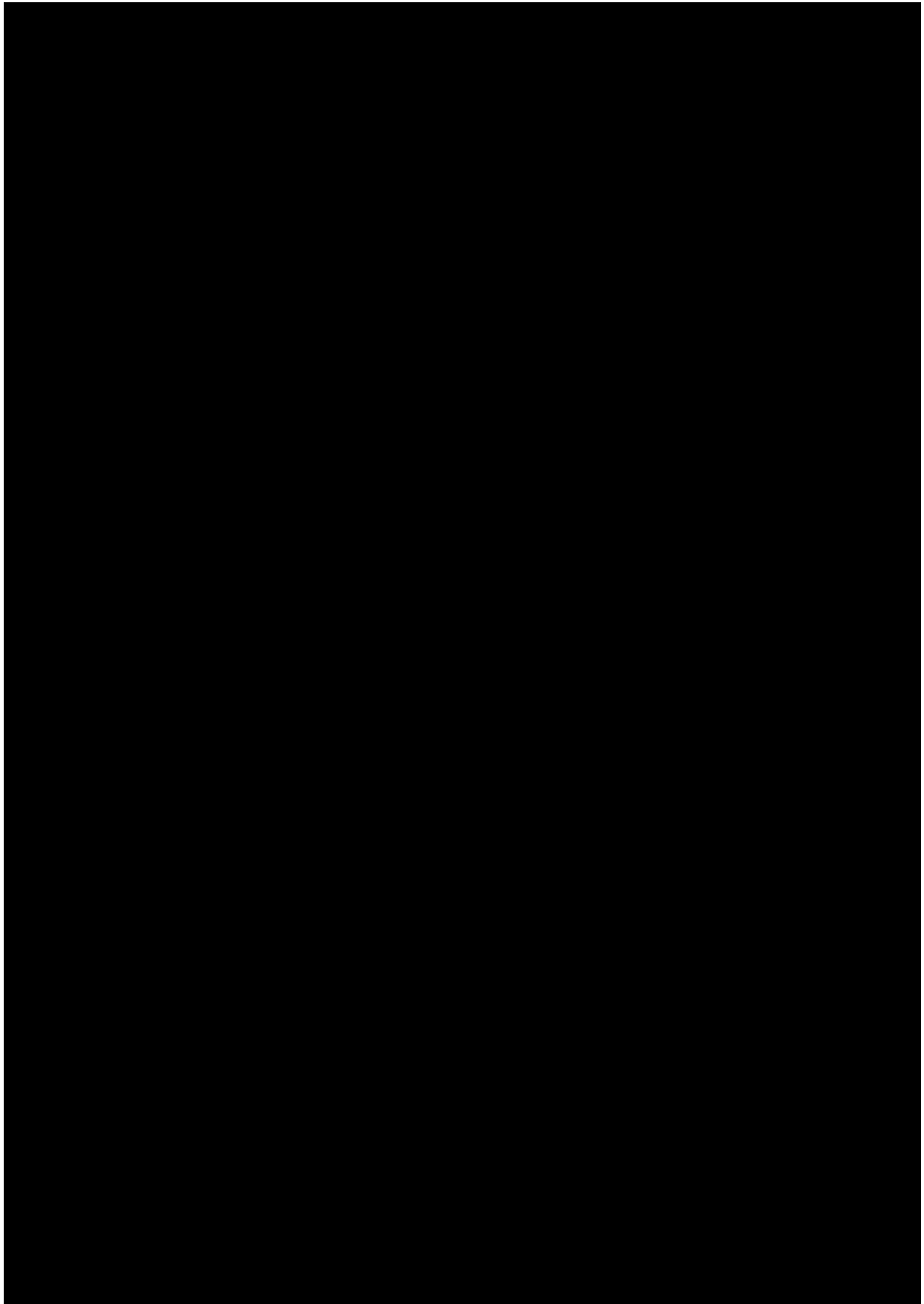
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Response	Percentage
Yes, the U.S. should take action to address climate change	95%
No, the U.S. should not take action to address climate change	5%



[REDACTED]

[REDACTED]

[REDACTED]

- | [REDACTED]
- | [REDACTED]
- | [REDACTED]
- | [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- | [REDACTED]
- | [REDACTED]
- | [REDACTED]
- | [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- I [REDACTED]
- I [REDACTED]
- I [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- I [REDACTED]

Response	Percentage
Yes, the U.S. should take action to address climate change	95%
No, the U.S. should not take action to address climate change	5%

ORDER SCHEDULE 5: PRICING DETAILS

