Framework Order Form and Call-Off Schedules

CALL-OFF REFERENCE:		ELFT_RM6017_2023
THE BUYER:		The East London NHS Foundation Trust
BUYER ADDRESS		Trust Headquarters, 9 Alie Street, London, E1 8DE
THE SUPPLIER:		Xerox (UK) Limited
SUPPLIER ADDRESS: Buildin Middlesex UB8 1DH	ng 4, Ux	dbridge Business Park, Sanderson Road, Uxbridge,
REGISTRATION NUMBER:		330754
DUNS NUMBER:		N/A
SID4GOV ID:	N/A	

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated

2023.

It's issued under the Framework Contract with the reference number RM6017 for the provision of Lot 7: Hybrid Mail, Digital and Transformational Communications.

CALL-OFF LOT(S):

Lot Number	Lot Description	Relevant (Yes / No)
3	Collection and Delivery of Letters, Large Letters and Parcels	No
4	Collection and Delivery of Letters, Large Letters and Parcels to International Destinations	No
5	Audits, Efficiency Reviews and Niche Consultancy	No
6	Business Process Outsourcing, Mailroom, Document and Data Managed Service	No
7	Hybrid Mail, Digital and Transformational Communications	Yes
8	Inbound Delivery Services	No
9	Mail Opening and Digital Scanning Services	No

10	Security Screening Services	No

CALL-OFF INCORPORATED TERMS

The following documents are incorpated into this Call-Off 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 Call-Off Special Terms and Call-Off Special Schedules.

2. Joint Schedule 1(Definitions and Interpretation) **RM6017** 3. The following Schedules in equal order of precedence:

- Joint Schedules for RM6017

 Joint Schedule 2 (Variation Form)
 O Joint Schedule 11 (Processing Data)
- Call-Off Schedules for ELFT_RM6017_2020
 - Call-Off Schedule 5 (Pricing Details) NOT USED Refer to Call-Off Schedule

Call-

(Call Off Specification) o

Off Schedule 6 (ICT Services)

Call-Off Schedule 7 (Key Supplier Staff) NOT

USED

- Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
- Call-Off Schedule 9 (Security)
- Call-Off Schedule 10 (Exit Management) NOT USED Refer to Call-Off Schedule 20 (Call Off Specification) o Call-Off
- Schedule 13 (Implementation Plan and Testing)
- Call-Off Schedule 14 (Service Levels) NOT USED Refer to Call-Off Schedule

20 (Call Off Specification) o Call-Off Schedule 15

- (Call-Off Contract Management)
- Call-Off Schedule 18 (Background Checks) Call-Off Schedule 20 (Call-Off Specification)

4. CCS Core Terms (version 3.0.6)

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

CALL-OFF SPECIAL TERMS

The following Special Terms are incorporated into this Call-Off Contract: N/A

CALL-OFF START DATE:	30 th April 2023
CALL-OFF EXPIRY DATE:	29 th April 2024
CALL-OFF INITIAL PERIOD:	1 Year
CALL-OFF EXTENSIONS:	1 Year + 1 Year (12 months each)
CALL-OFF DELIVERABLES	N/A

MAXIMUM LIABILITY

The limitation of liability for this Call-Off 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 £370,000.

REIMBURSABLE EXPENSES (LOT 5 ONLY) None

PAYMENT METHOD

On presentation of a monthly invoice to the address below with the agreed backing information.

BUYER'S INVOICE ADDRESS: EAST LONDON NHS FOUNDATION TRUST RWK PAYABLES 6765 PHOENIX HOUSE, TOPCLIFFE LANE WAKEFIELD, WF3 1WE

BUYER'S AUTHORISED REPRESENTATIVE Xerox Contract Lead for ELFT(the Buyer)

BUYER'S SECURITY POLICY

Security	Requirements by the Supplier
Data in transit protection User data transiting networks should be adequately protected against tampering and eavesdropping.	 Utilise strong cryptography as defined by NIST SP80057 to encrypt communications: Internally between Cloud Components. Between Cloud Data Centres. Between the Cloud admin portal and the Cloud. Undertake annual assessment against a recognised standard such as ISO to test the security of the communication: Internally between Cloud Components. Between Cloud Data Centres. Internally between Cloud Components. Between Cloud Data Centres. Between Cloud Data Centres. Between the Cloud admin portal and the Cloud.
Data centre security Locations used to provide cloud services need physical protection against unauthorised access, tampering, theft or reconfiguration of systems. Inadequate protections may result in the disclosure, alteration or loss of data.	Hold and maintain certification to ISO 27001.
Data at rest protection To ensure data is not available to unauthorised parties with physical access to infrastructure, user data held within the service should be protected regardless of the storage media on which it's held.	 Provide encryption facilities to ensure that no data is written to storage in an unencrypted form. Provide secure key management service providing strong cryptography as defined by the current version of NIST and FIPS standards. e.g. NIST SP800-57 Part 1'. Confirm that the encryption utilises strong cryptography as defined by the current version of NIST SP800-57. Undertake annual assessment against a recognised standard such as ISO or FIPS 140-2 to test the encryption.

Data sanitisation The process of provisioning, migrating and de-provisioning resources should not result in unauthorised access to user data.	Provide assertions regarding their data sanitisation approach.
Equipment disposal Once equipment used to	Hold certification to CSA CCM v3.0 OR ISO/IEC 27001.

deliver a service reaches the end of its useful life, it should be disposed of in a way which does not compromise the security of the service, or user data stored in the service.	
Separation between users A malicious or compromised user of the service should not be able to affect the service or data of another.	 Provide Supplier Assertions regarding their approach to user/Buyer environment separation. Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'separation between users/ Buyer environment'. Hold and maintain certification to ISO27017 for the Cloud Platform.
Governance framework The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.	 Hold and maintain certification to CSA's STAR programme OR ISO/IEC 27001. Prove that the scope of certification includes the governance framework goals set out below: A clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service. This is typically someone with the title 'Chief Security Officer', 'Chief Information Officer' or 'Chief Technical Officer'. A documented framework for security governance, with policies governing key aspects of information security relevant to the service. Security and information security are part of the service provider's financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risk. Processes to identify and ensure compliance with applicable legal and regulatory requirements.
Vulnerability management You should identify and mitigate security issues in constituent components	Hold and maintain certification to CSA CCM v3.0 OR ISO/IEC 27001, ISO/IEC 27017. Manage vulnerabilities in a manner that aligns with ISO 30111 and show ISO / CSA compliance to validate the process.

1	· · · · · · · · · · · · · · · · · · ·	
Protective monitoring You should put measures in place to detect attacks and unauthorised activity on the service	 Prove that mitigations for discovered vulnerabilities are implemented for the server-less devices, hypervisors and supporting infrastructure, within the NCSC best practice timescales set out below: 'Critical' vulnerabilities should be mitigated within 24 hours 'Important' vulnerabilities should be mitigated within 2 weeks. 'Other' vulnerabilities mitigated within 8 weeks. Hold and maintain certification to CSA CCM v3.0 OR ISO/IEC 27001 and ISO/IEC 27017 The service generates adequate audit events to support effective identification of suspicious activity These events are promptly analysed to identify potential compromises or inappropriate use of your service 	
	 The service provider takes prompt and appropriate action to address incidents 	
Incident management Ensure you can respond to incidents and recover a secure, available service	 Hold and maintain certification to CSA CCM v3.0 OR ISO/IEC 27001. Incident management processes are in place for the service and are actively deployed in response to security incidents Pre-defined processes are in place for responding to common types of incident and attack A defined process and contact route exists for reporting of security incidents by consumers and external entities Security incidents of relevance to the Service User will be reported in acceptable timescales and formats 	
Secure development Services should be designed and developed to identify and mitigate threats to their security.	management procedures. Hold and maintain certification to: a) CESG CPA Build Standard, OR b) ISO/IEC 27034, OR c) ISO/IEC 27001, OR d) CSA CCM v3.0.	
Personnel security <i>Where</i> <i>service provider personnel</i> <i>have access to your data</i> <i>and systems you need a</i> <i>high degree of confidence</i> <i>in their trustworthiness.</i>	Operate a personnel screening process that aligns with BS7858:2012 and show ISO / CSA compliance to validate the process.	
Audit information for users You should be provided with the audit records needed to monitor access to your service and the data held within it.	Record system events in near real-time to provide an audit log. Ensure that the audit logs are tamperproof. Provide a secure facility to forward / export the logs off the cloud infrastructure.	

Undertake annual assessment against a recognised standard such as ISO, CyberEssentials to test the 'auditing facility'.

SUPPLIER'S AUTHORISED REPRESENTATIVE

Associate General Counsel

CommercialGroupContracts@xerox.com

Building 4, Uxbridge Business Park, Sanderson Road, Uxbridge, Middlesex UB8 1DH

SUPPLIER'S CONTRACT MANAGER

Client

Building 4, Uxbridge Business Park, Sanderson Road, Uxbridge, Middlesex UB8 1DH

PROGRESS REPORT FREQUENCY First Working Day of each Month

PROGRESS MEETING FREQUENCY Quarterly on the first Working Day of each quarter

KEY SUBCONTRACTOR(S) – Funasset Limited Foundry House Foundry Road Taunton Somerset TA1 1JJ Company No. 02078429

COMMERCIALLY SENSITIVE INFORMATION – Supplier's Commercially Sensitive Information

Call Off Schedule 20 (Call Off Specification)

For the period of the Call Off Conttract, including any extension period and two (2) years after expiry or termination of the Call Off Contract.

SERVICE CREDITS - as per Call Off Schedule 20

ADDITIONAL INSURANCES - Not applicable

GUARANTEE - Not applicable

SOCIAL VALUE COMMITMENT - Not applicable

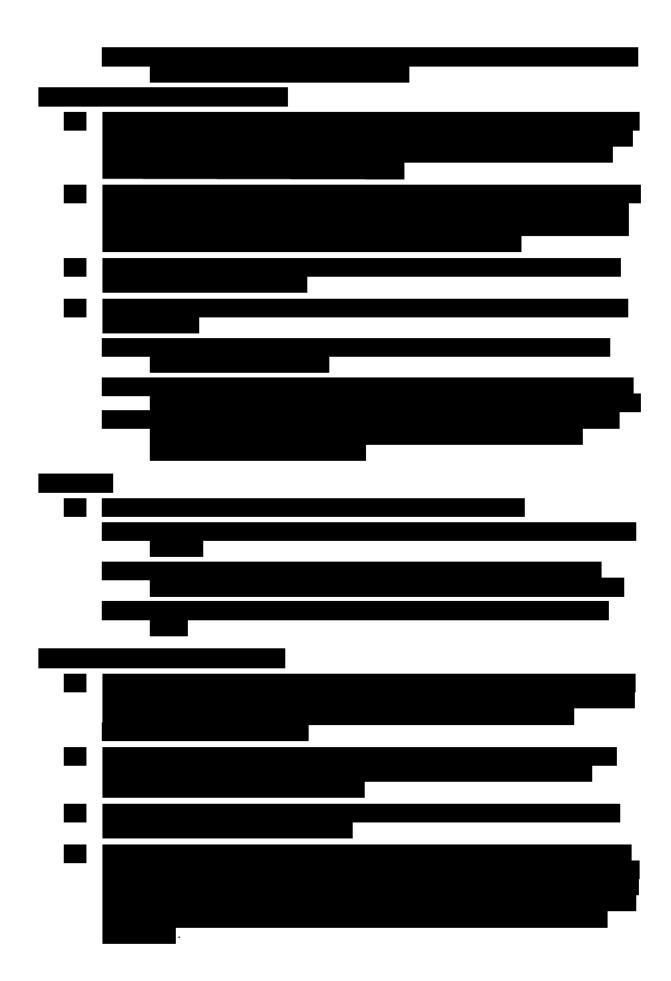
For and on behalf of the Supplier:		For and on behalf of the Buyer:	
Signature:		Signature:	- <u>SS</u>
Name:		Name:	Samanthi Gibbens

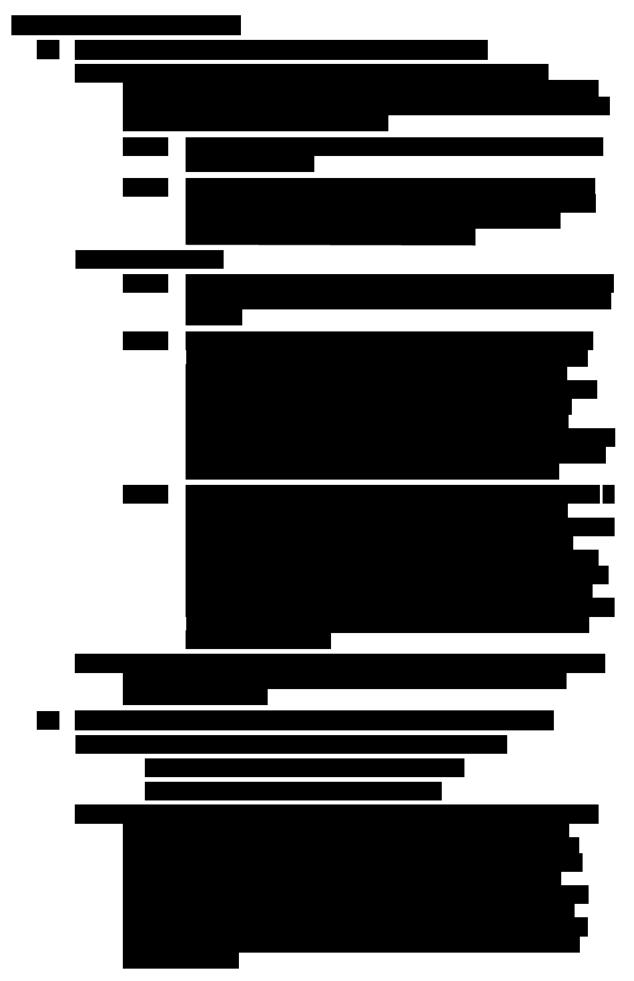
Role:	Role:	Interim Chief Finance Officer
Date:	Date:	28 th April 2023

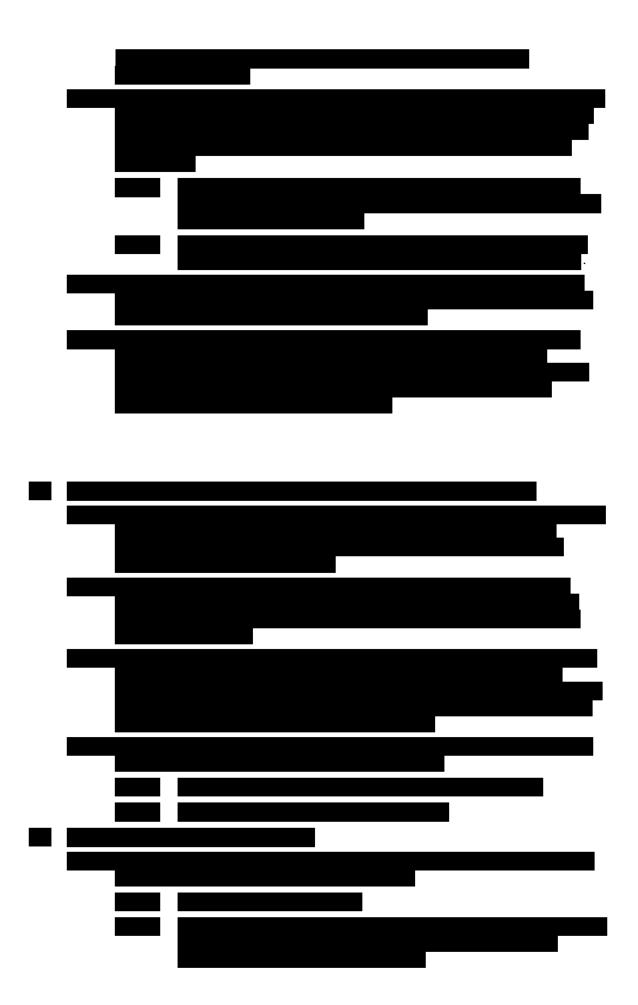


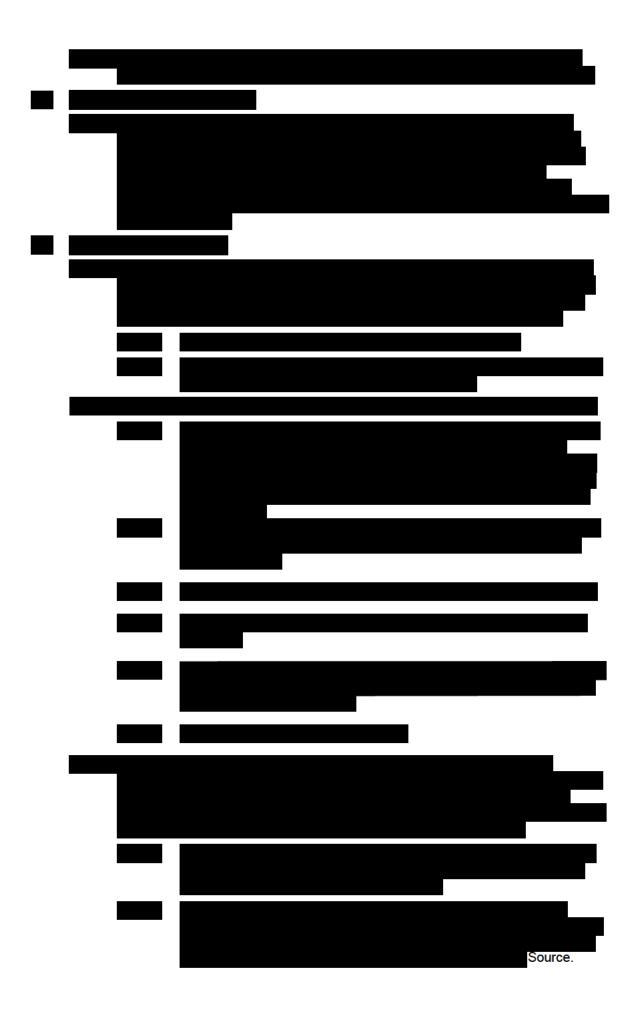


	-		

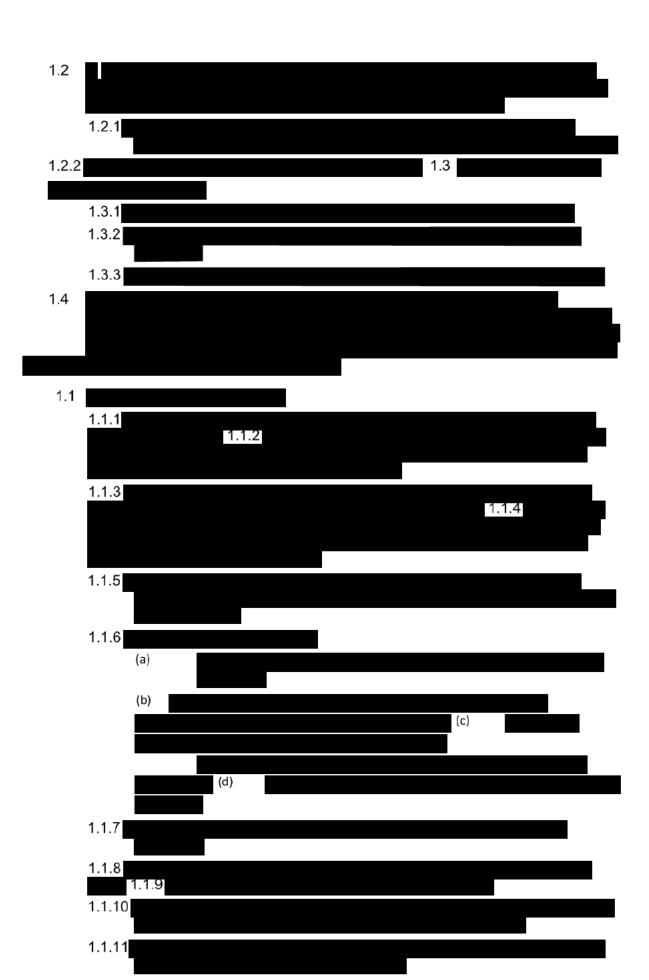


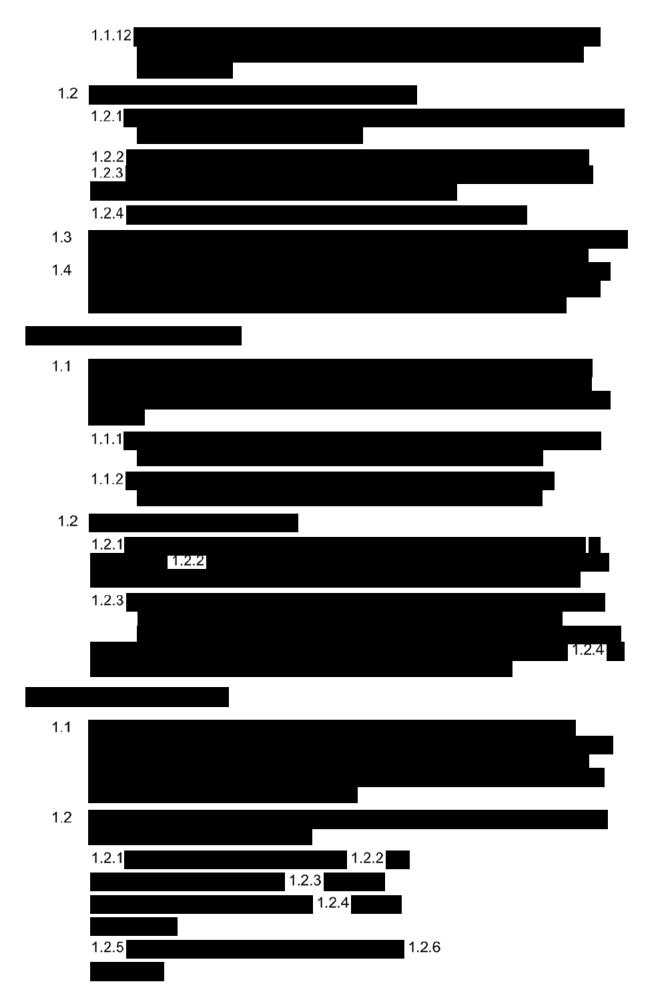


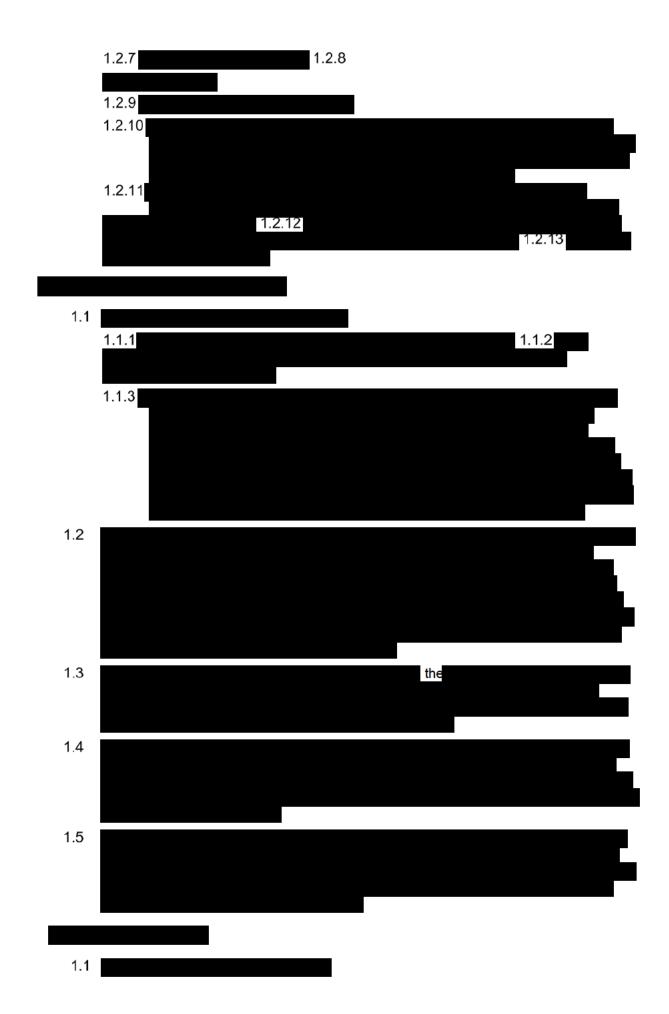


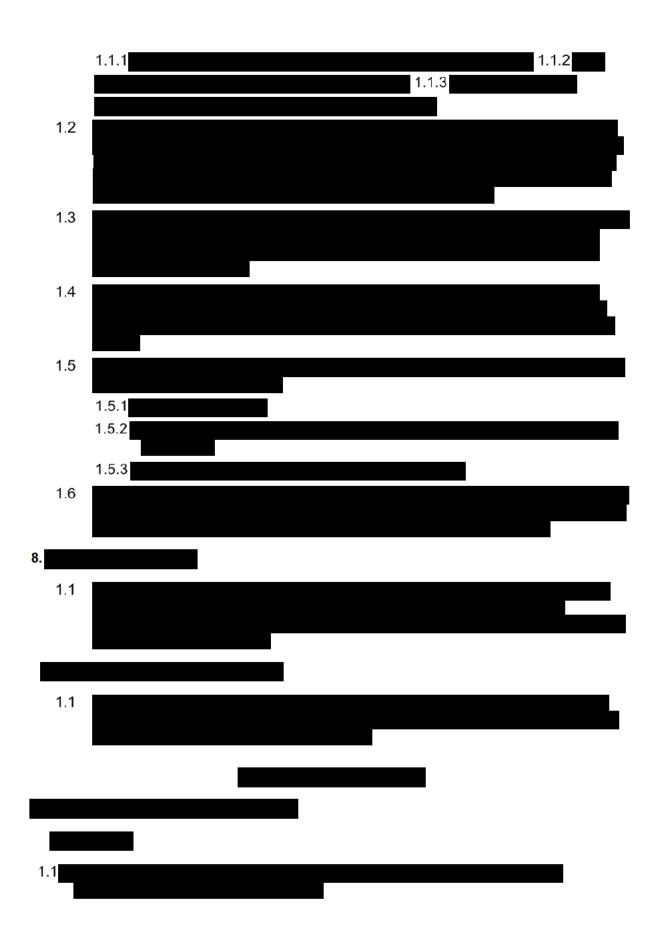


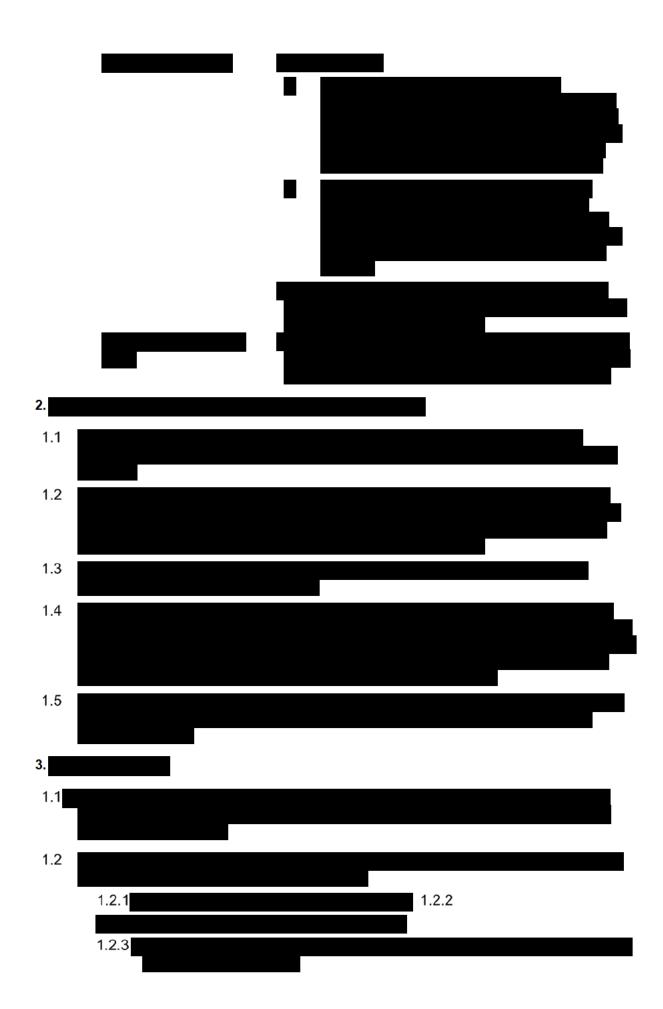
1.1		
_		

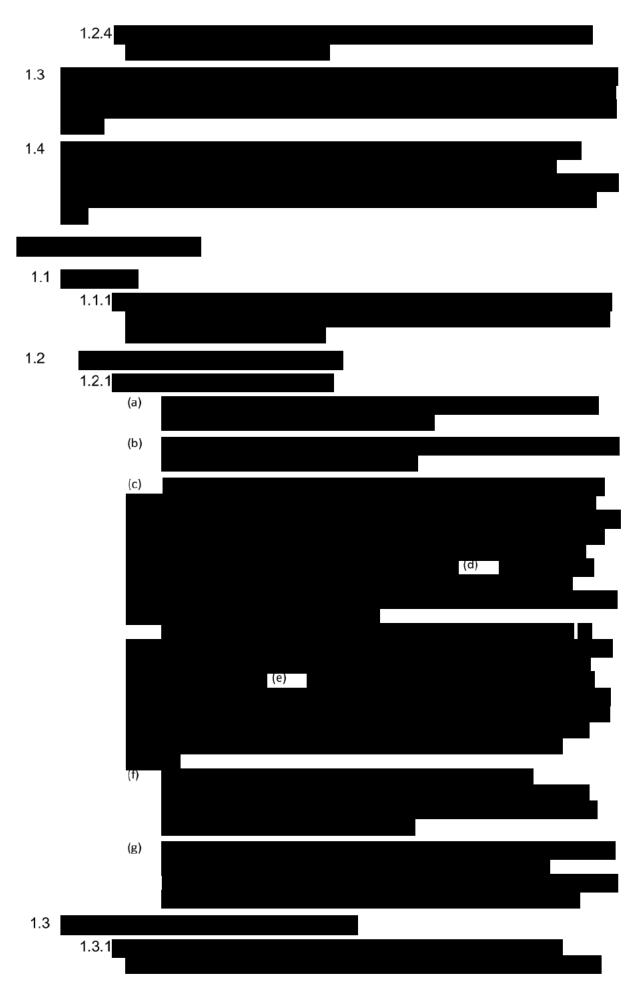


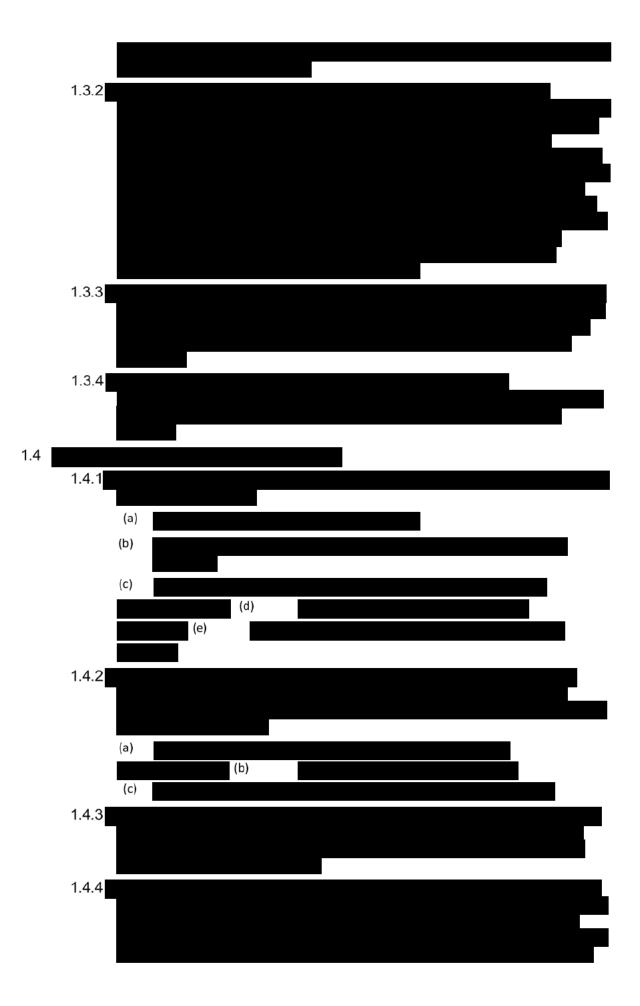


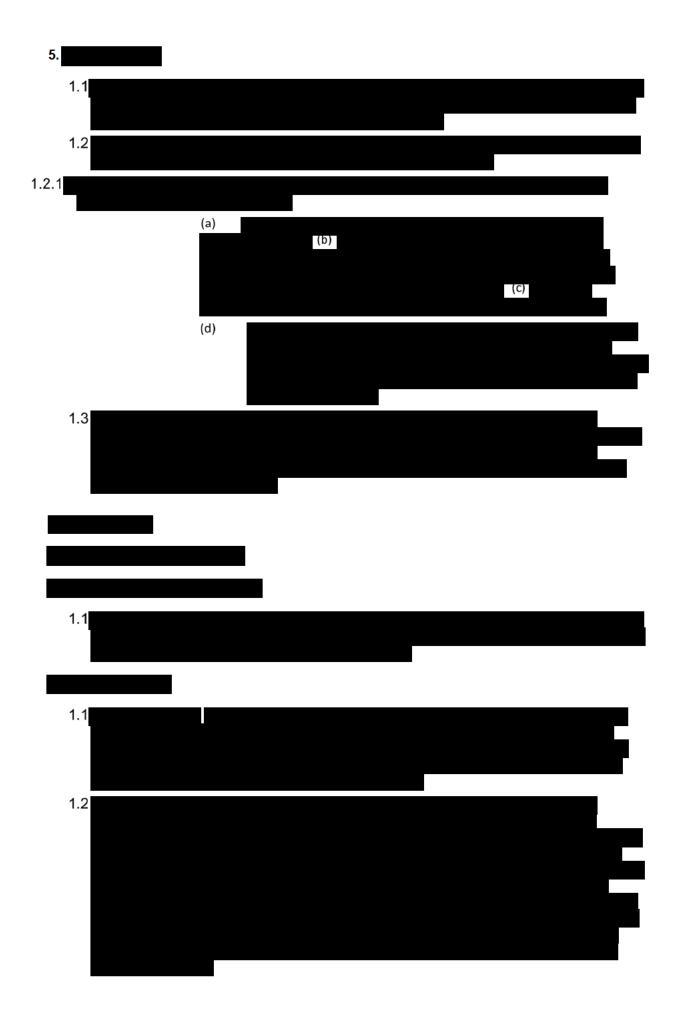


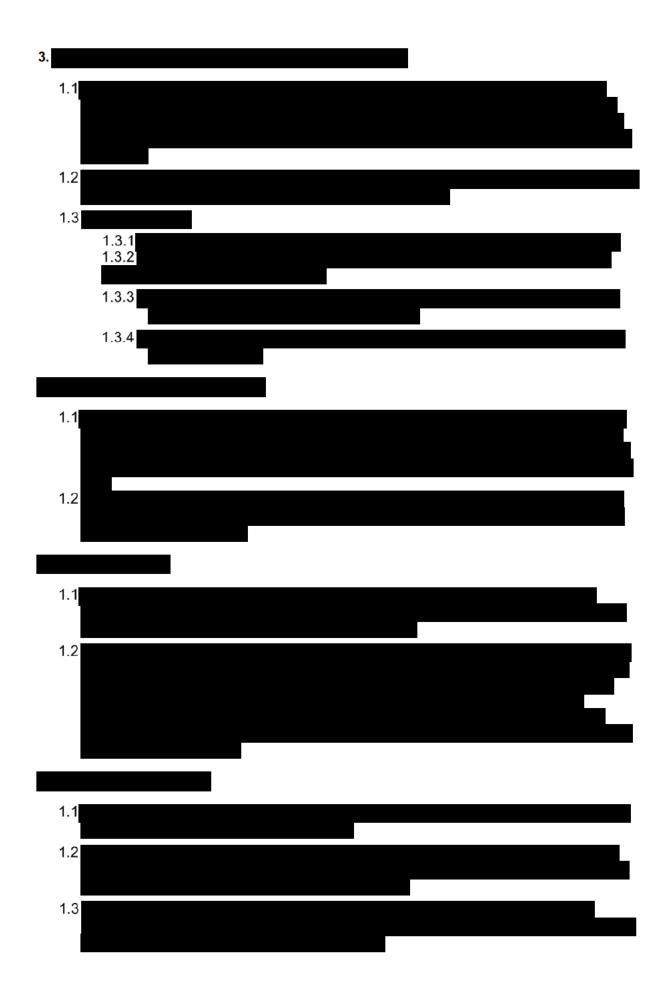


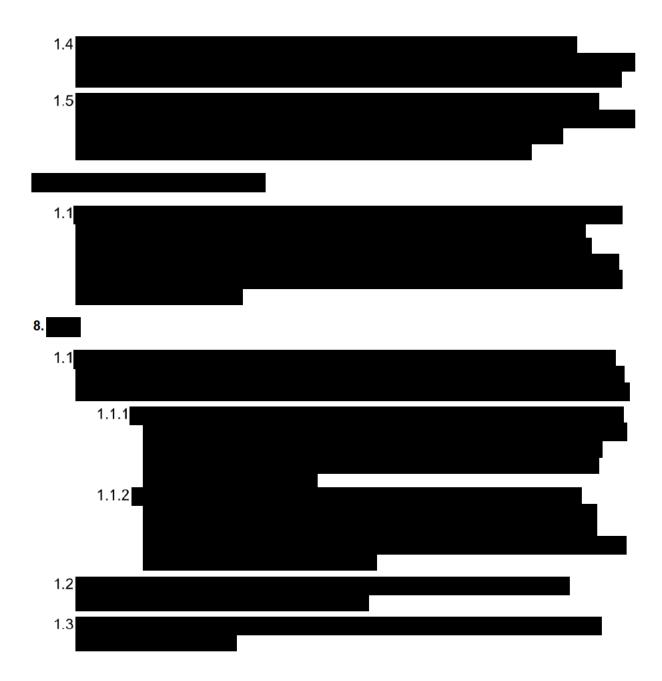




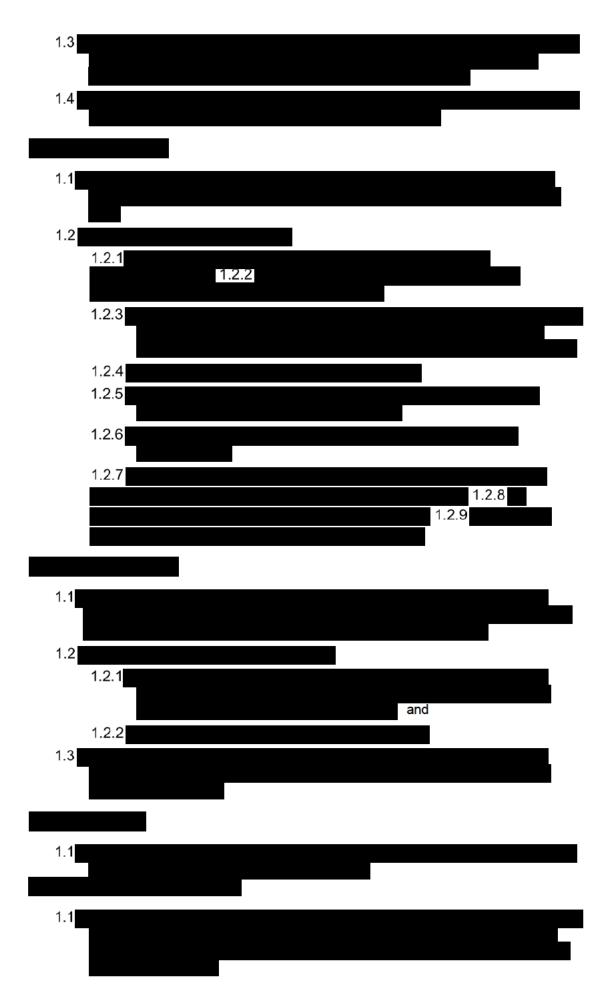


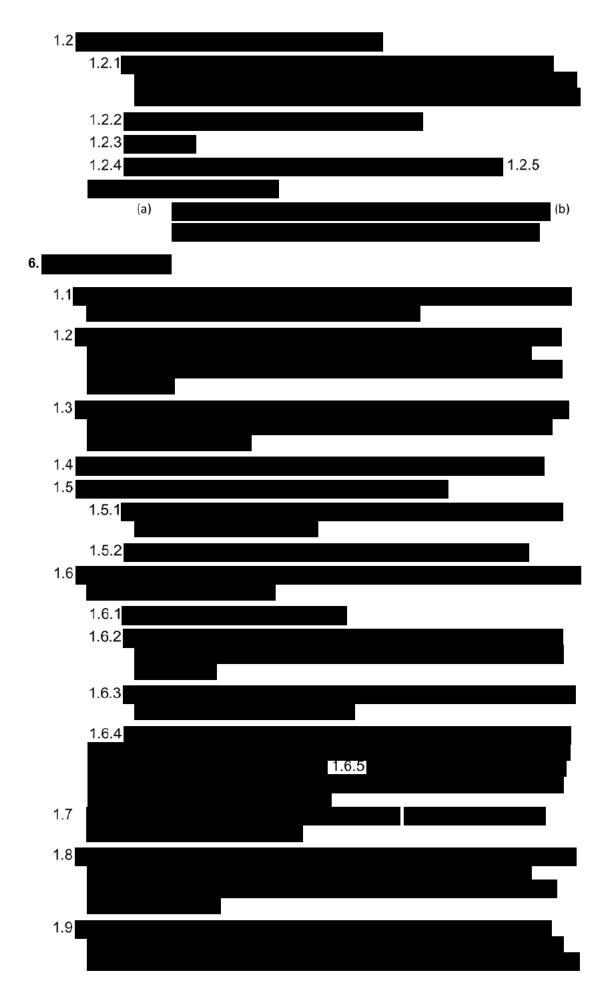


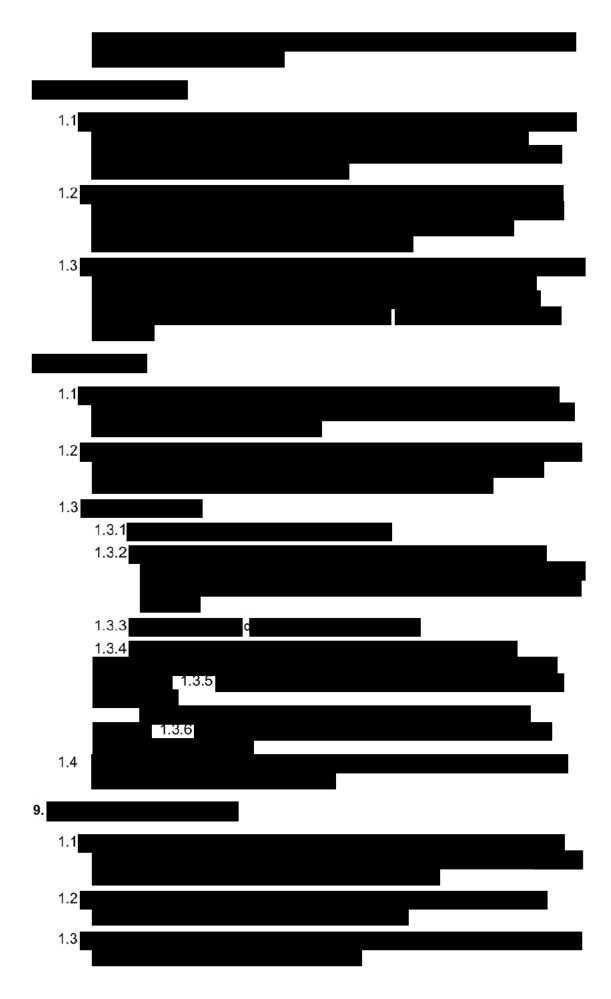


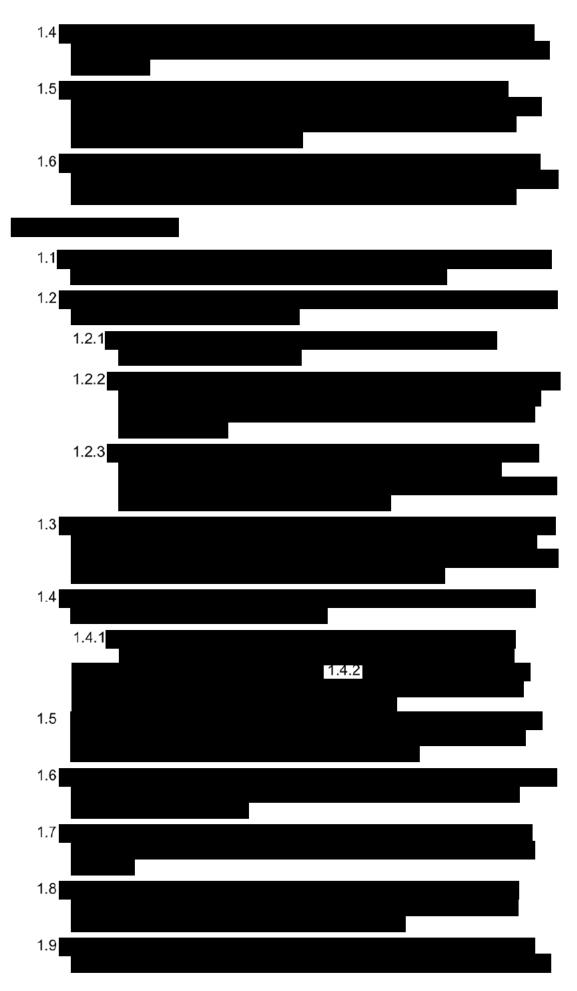


1.1			
			_
1.			
1.1			
1.2			
1.2.1	100		L
1.2.3	1.2.2		



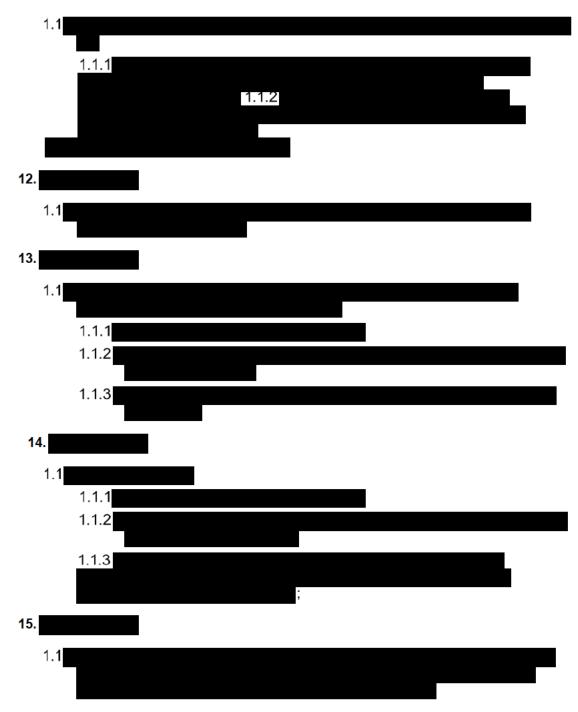






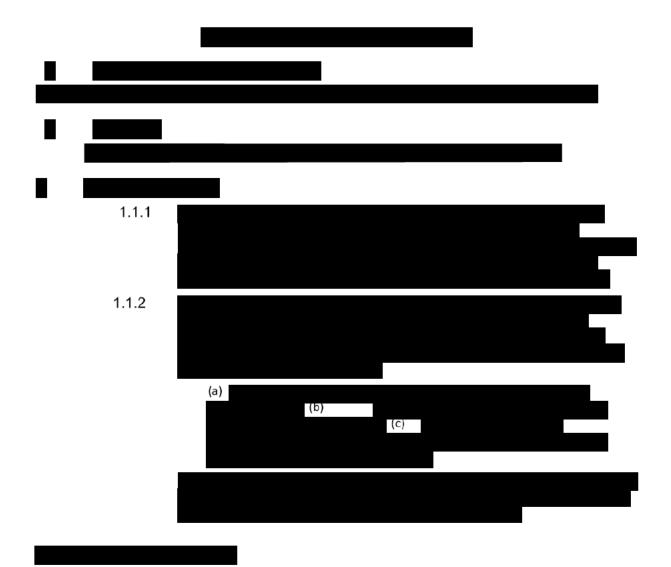


11. Risk

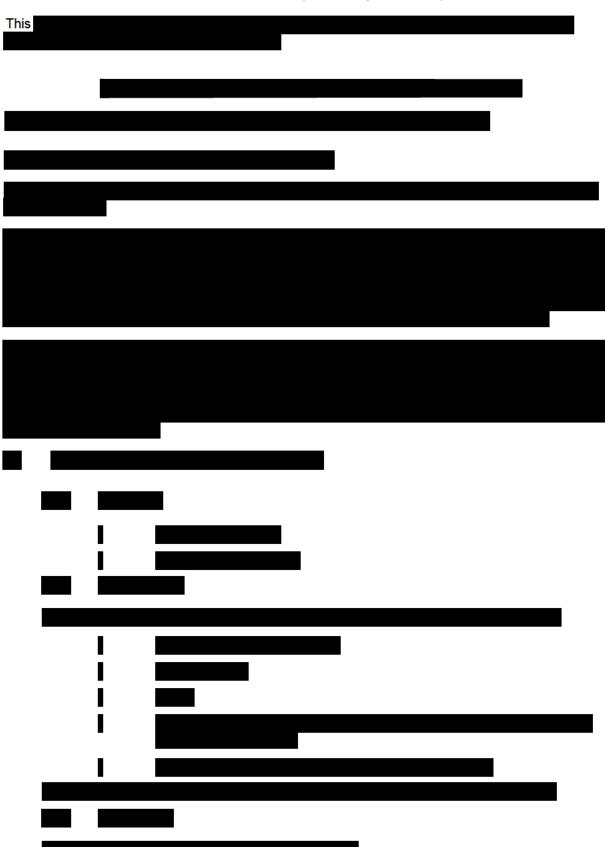


16.				
1.	.1			
]		





N/A

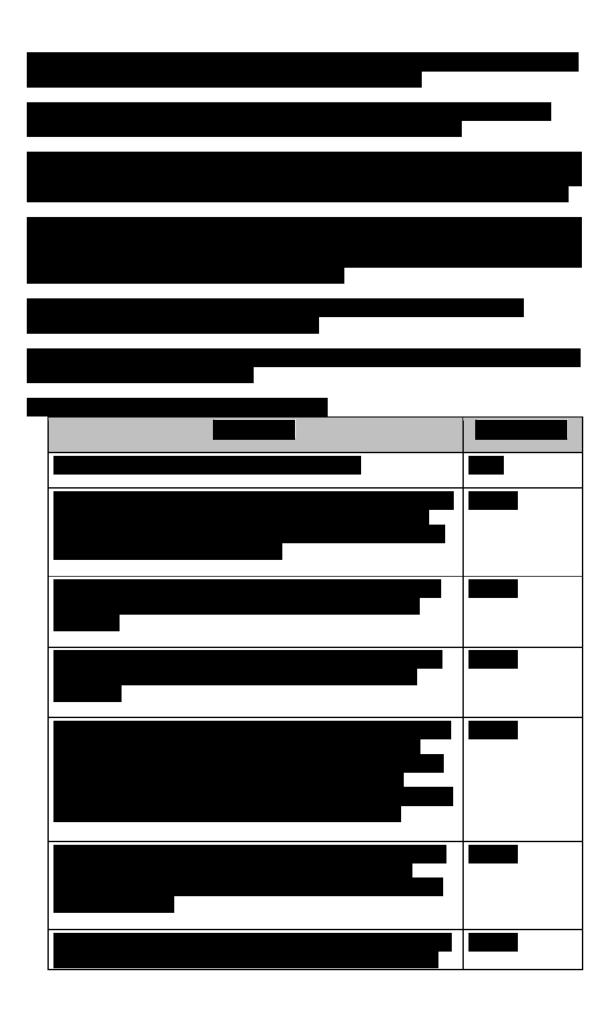


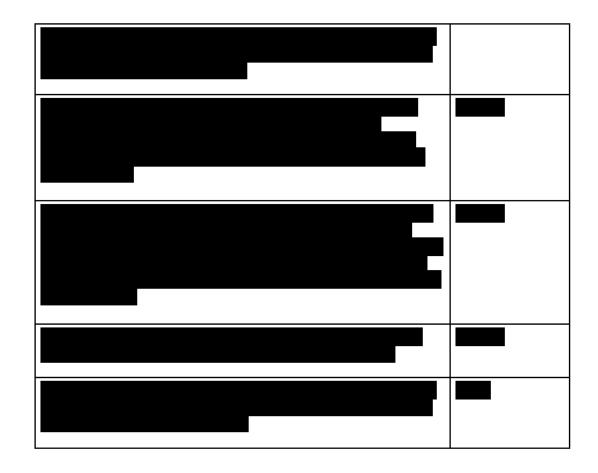
Call-Off Schedule 20 (Call-Off Specification)

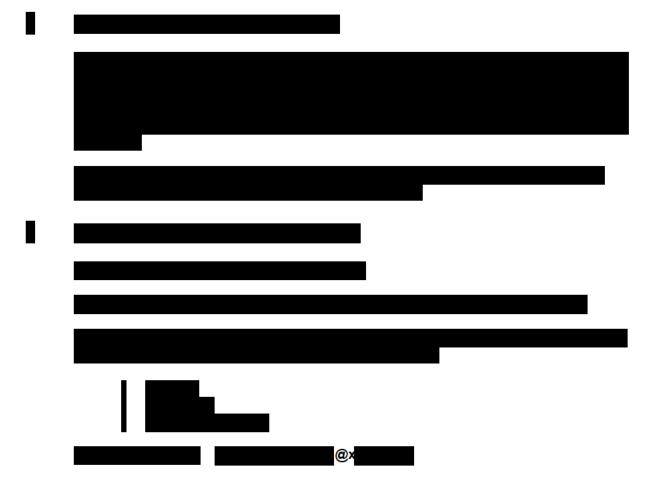
<u> </u>	

-	
_	
- 1	
	Working Day delivery

l			





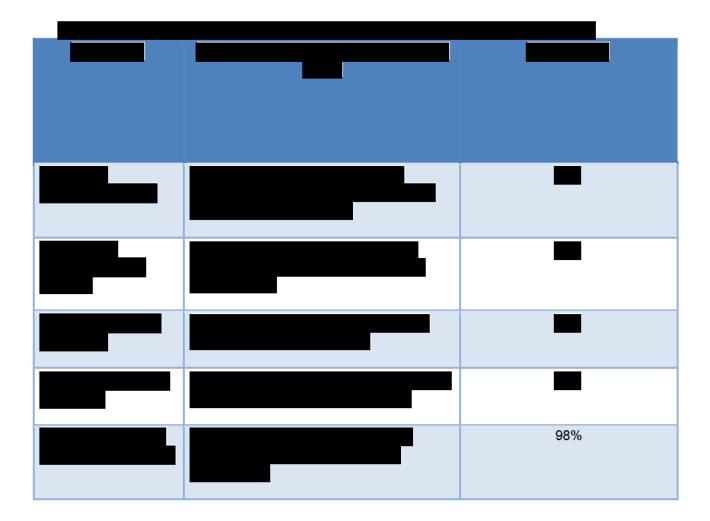


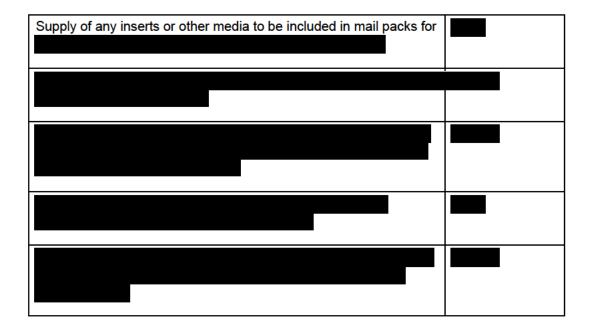
	Buyer
	-



7.5 Exceptions









	_		

		_	
	1	-	
		•	
_			
-			

1		

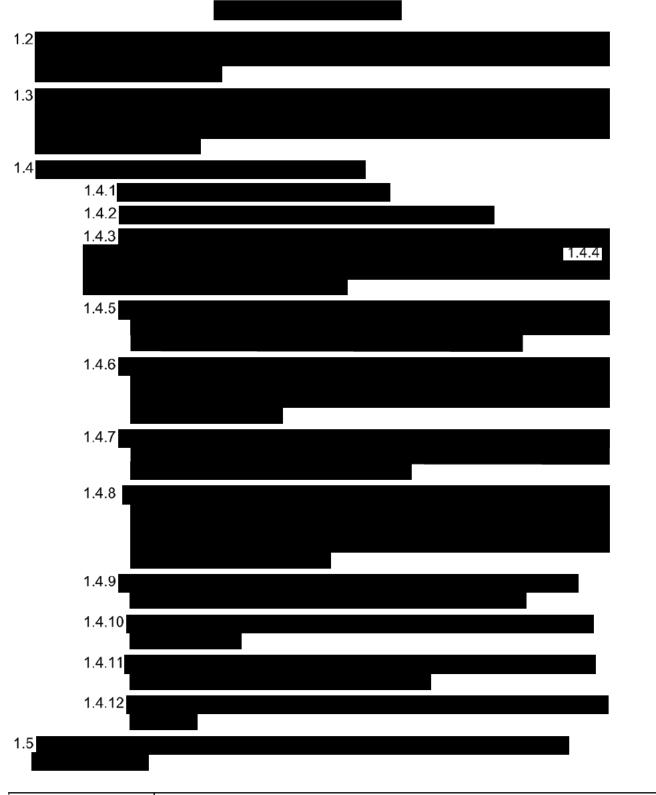




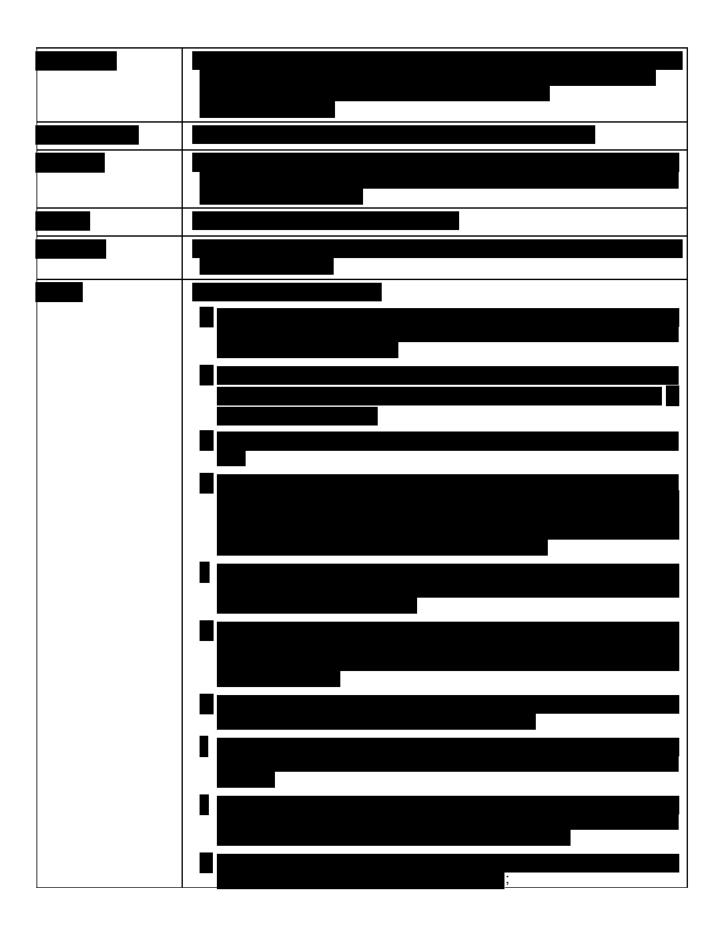


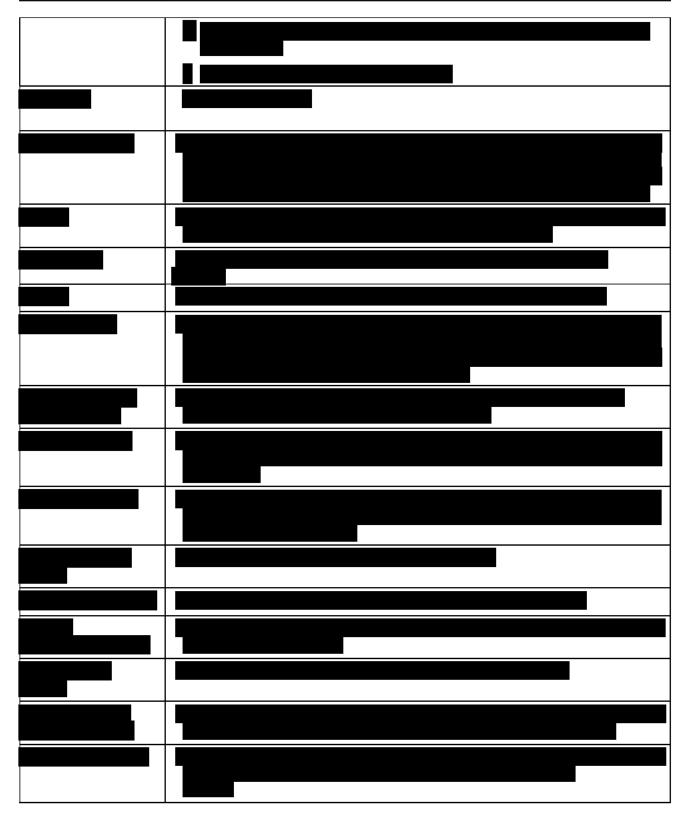


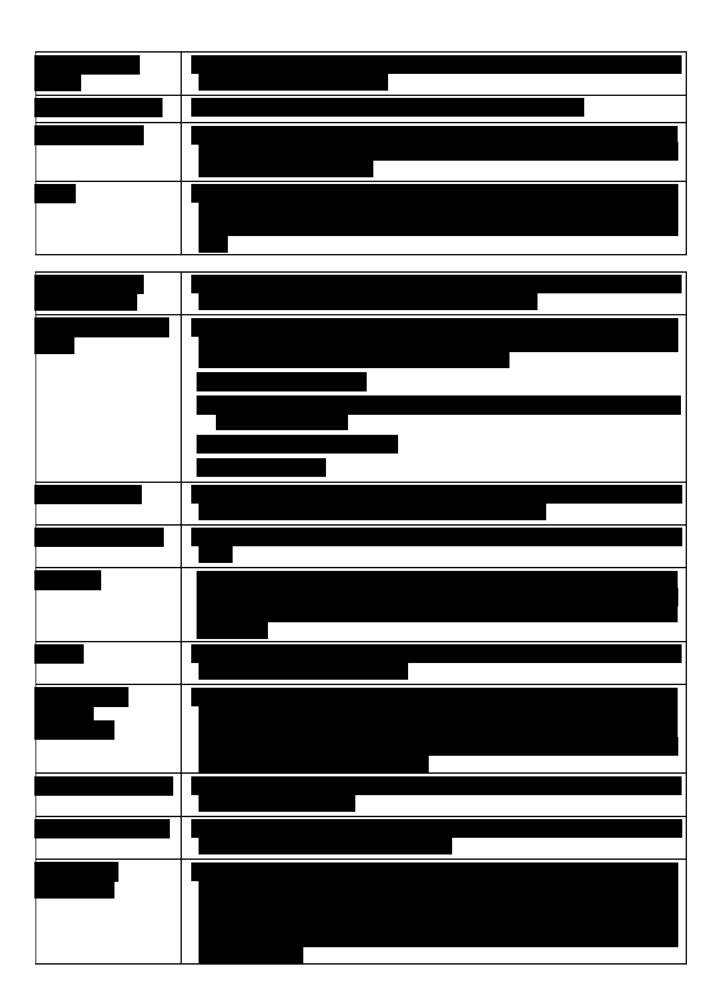


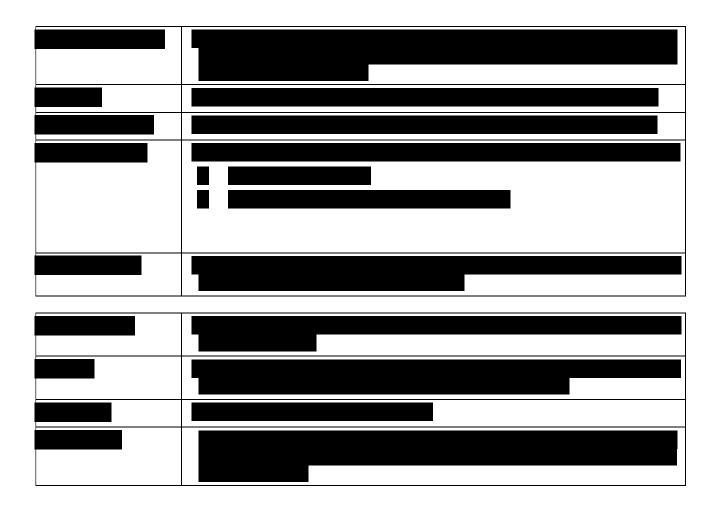


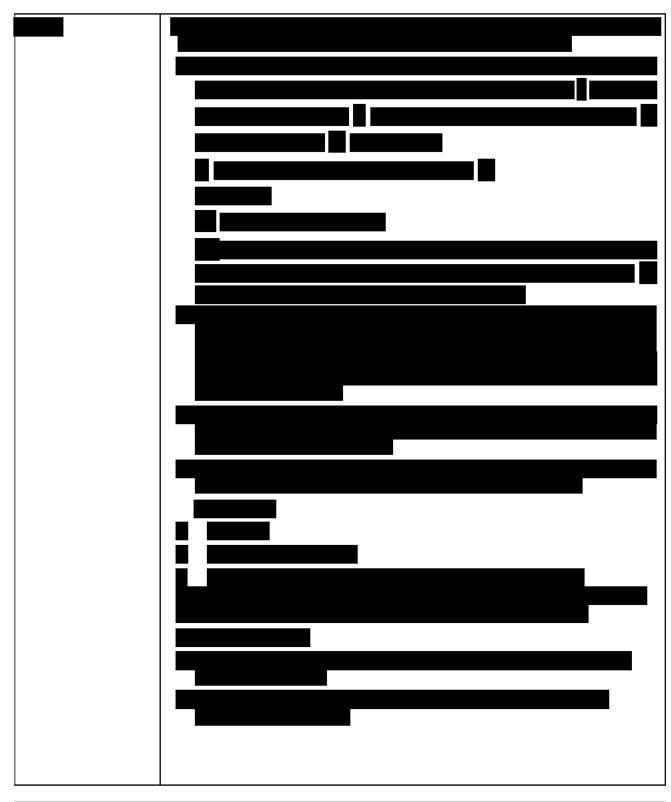








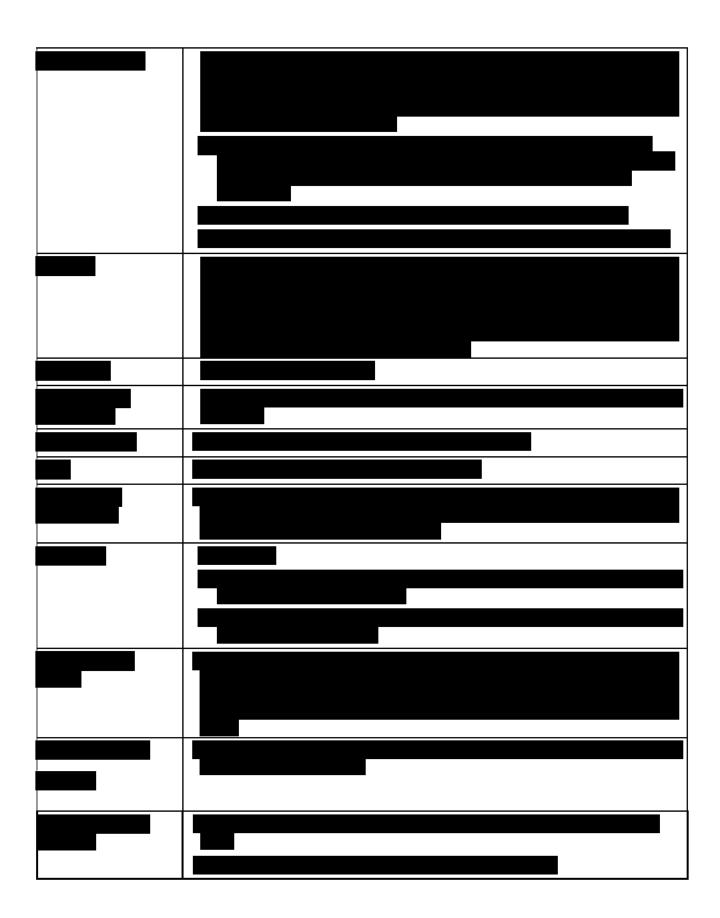


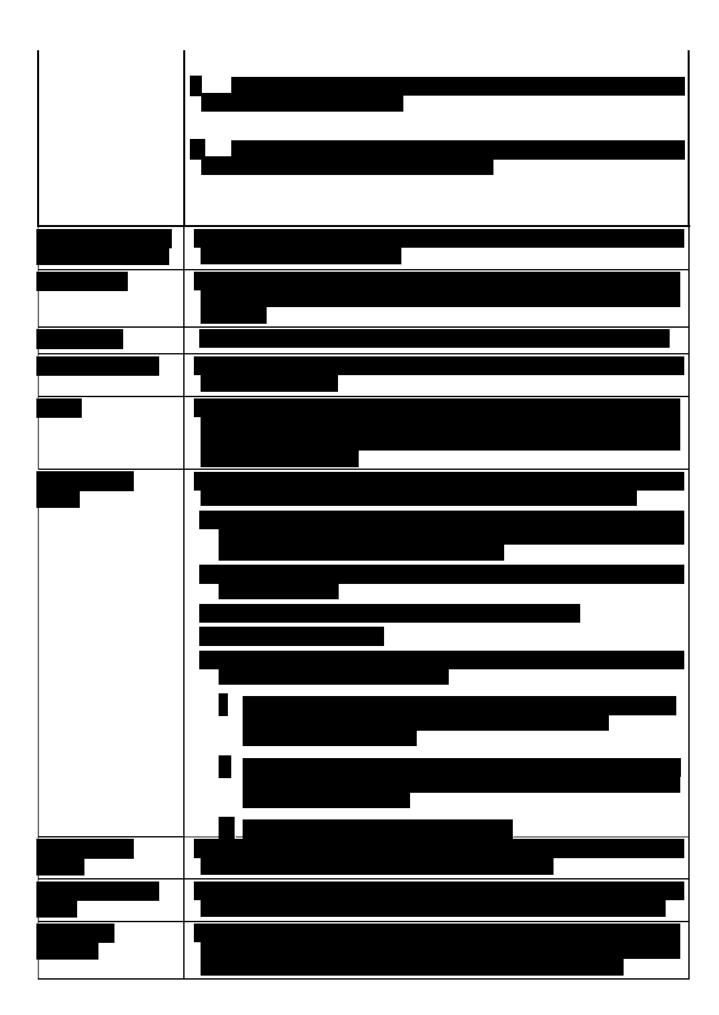


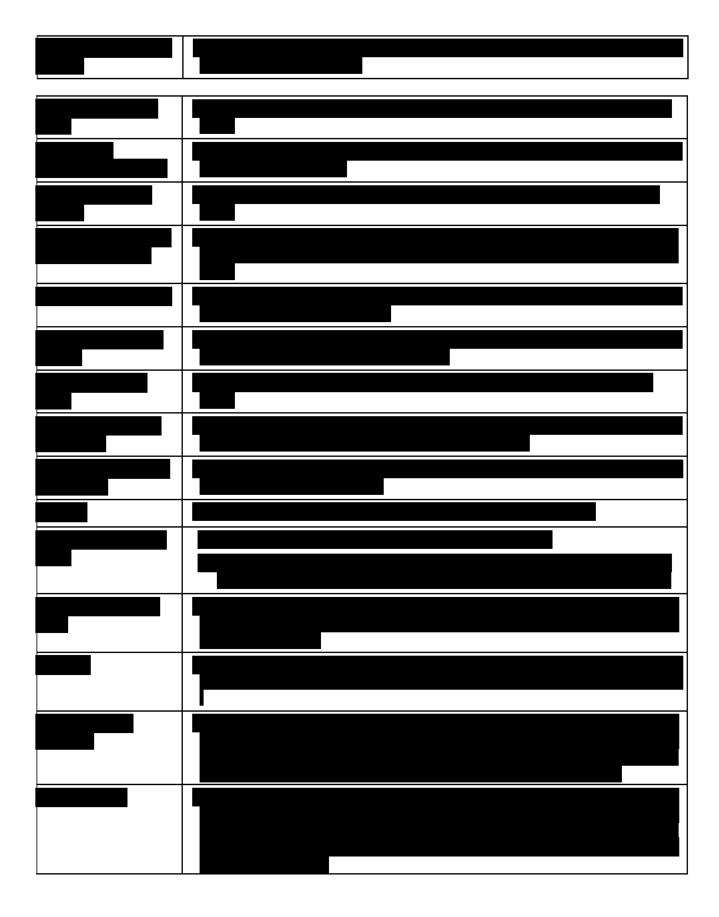
• • •

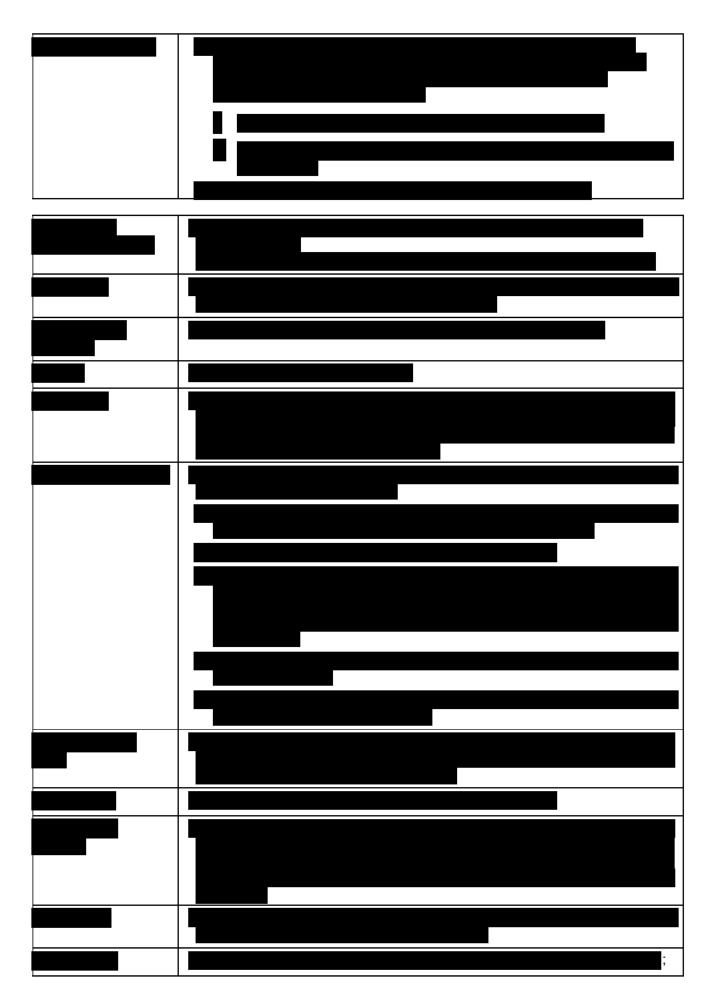


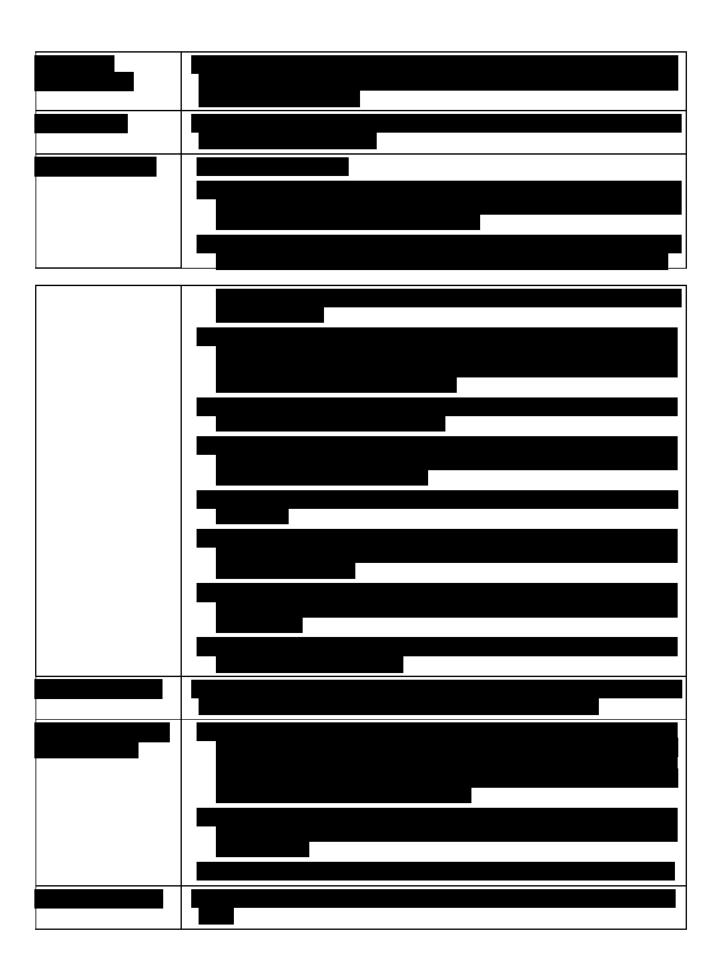
);	





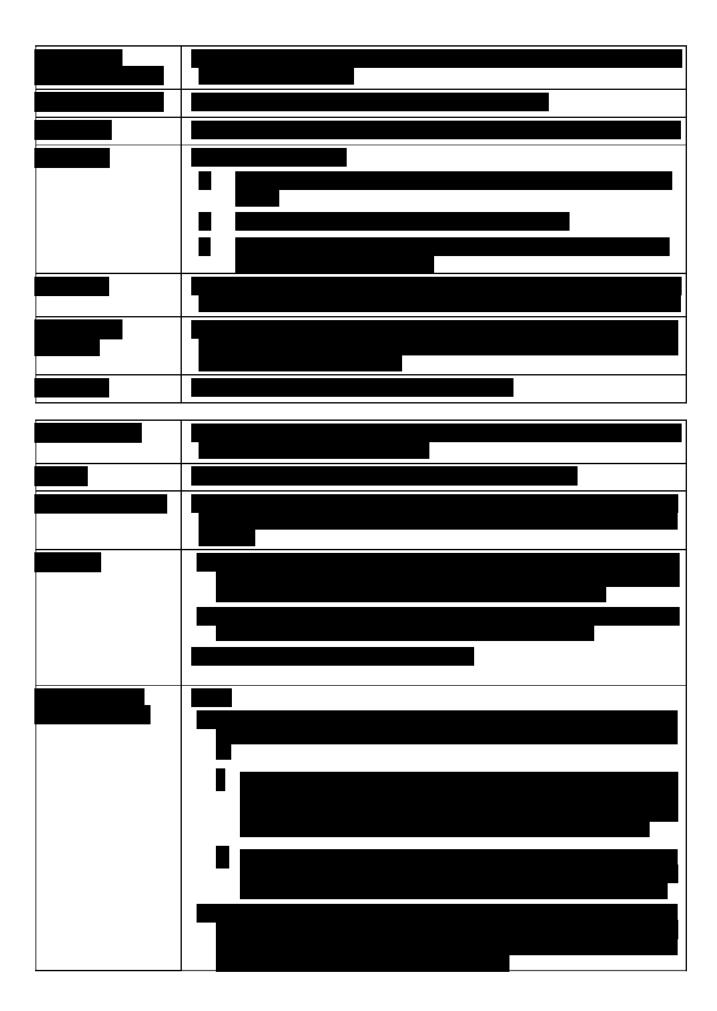


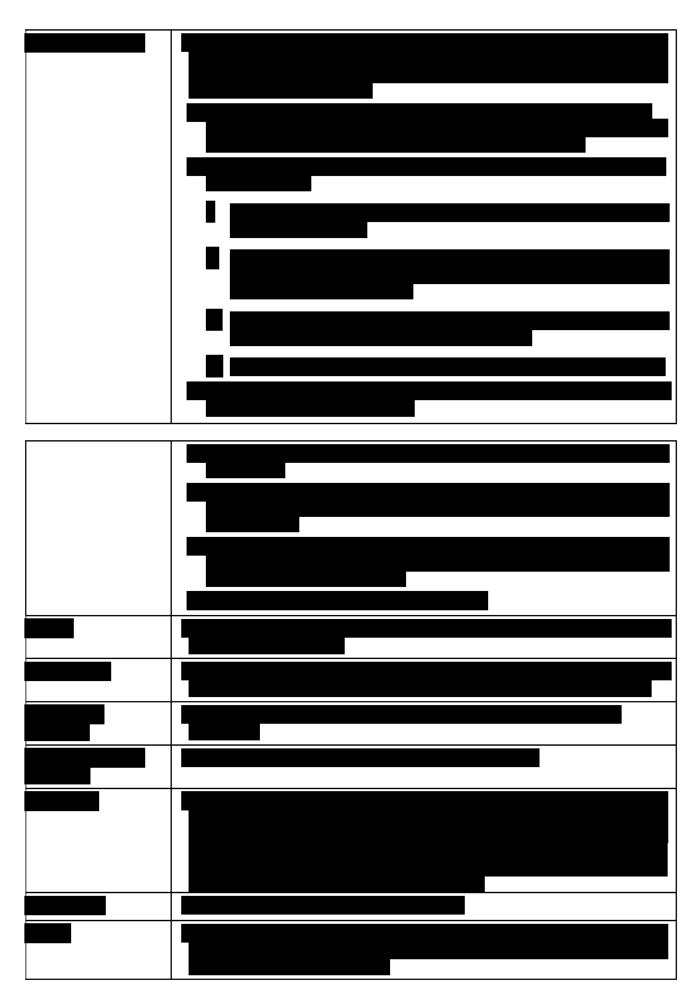


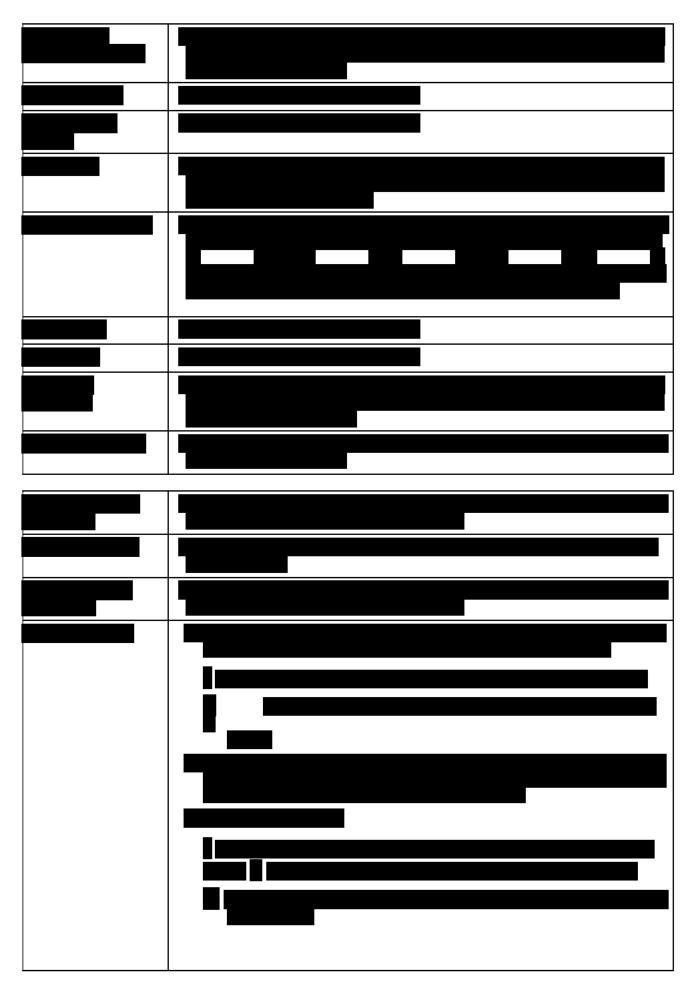


••	

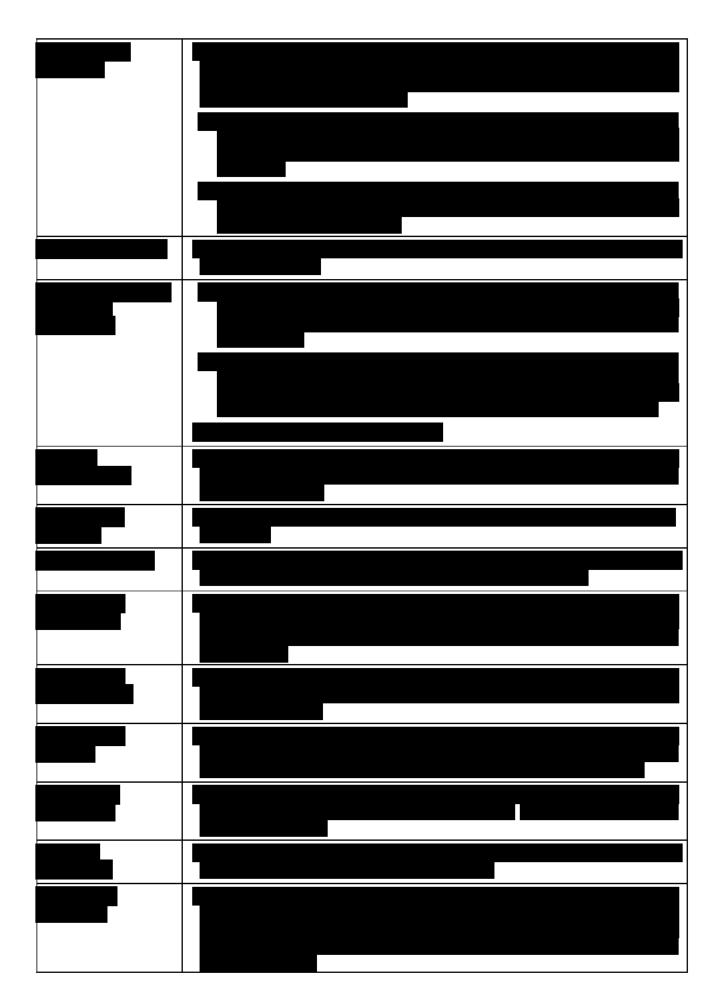


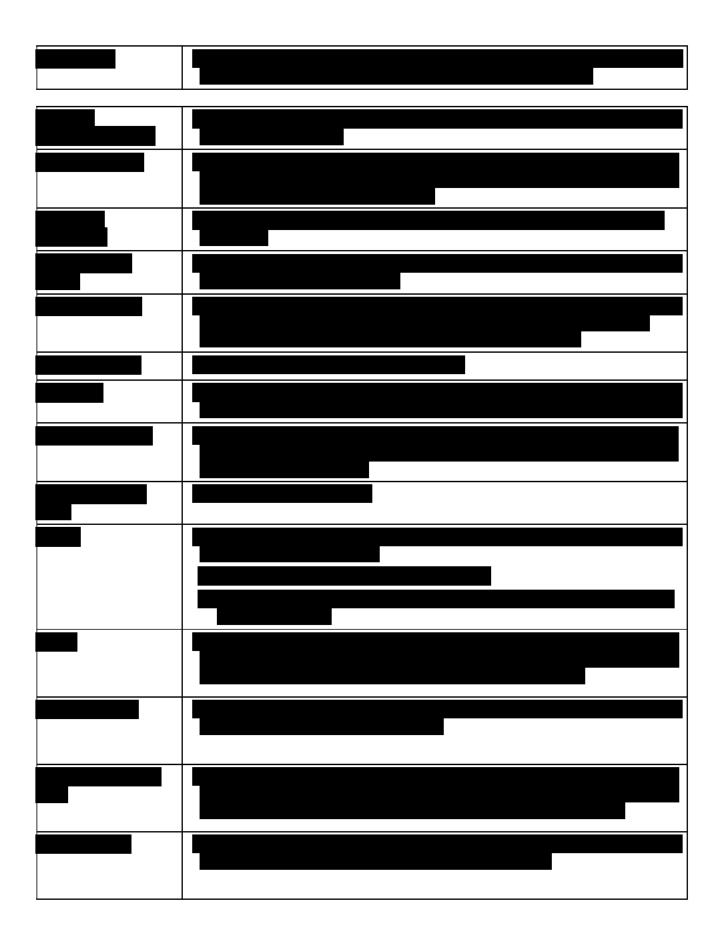


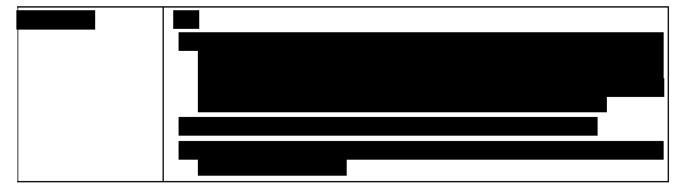


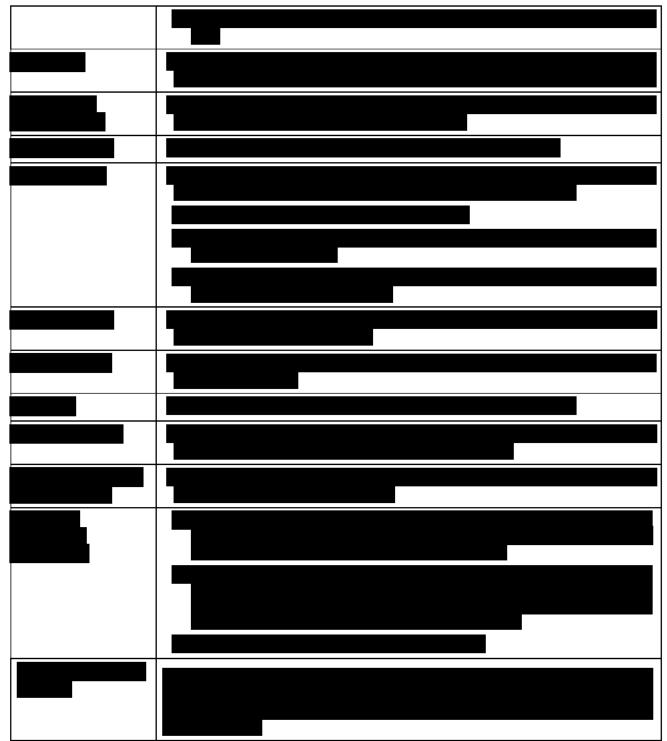


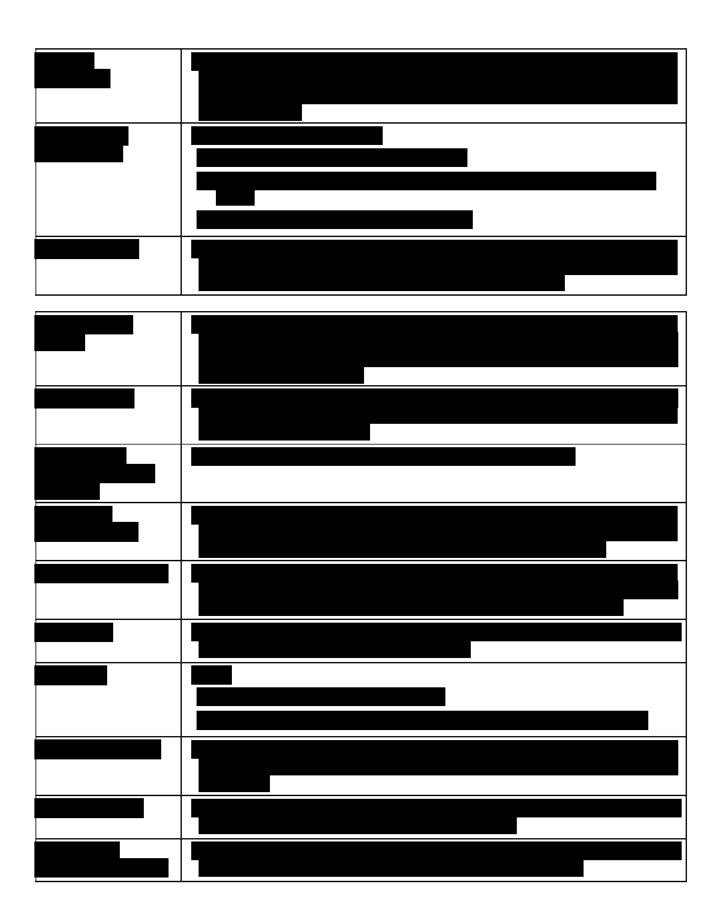
	



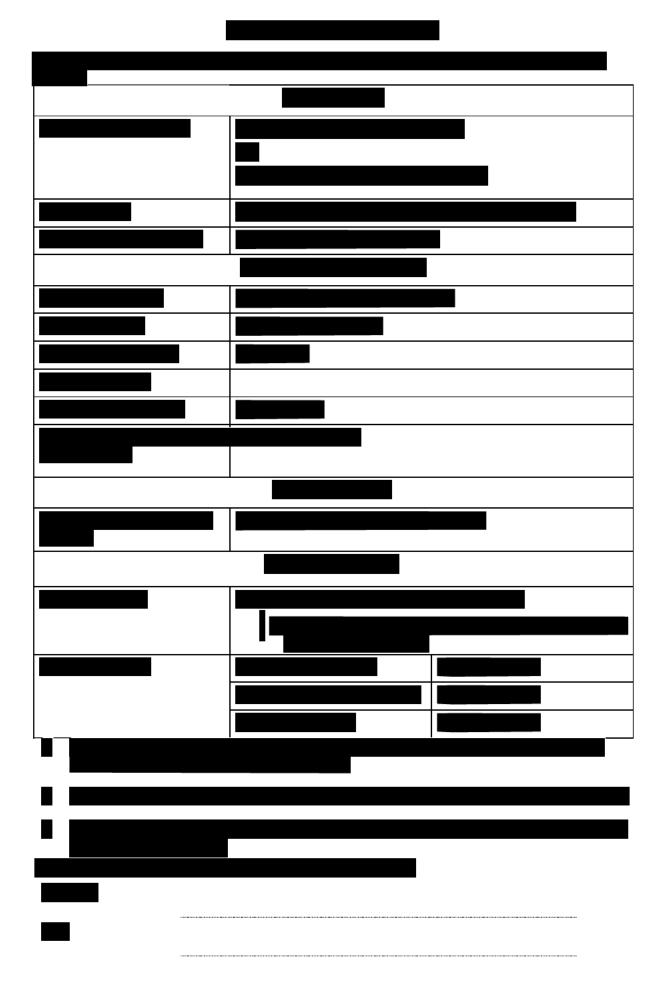








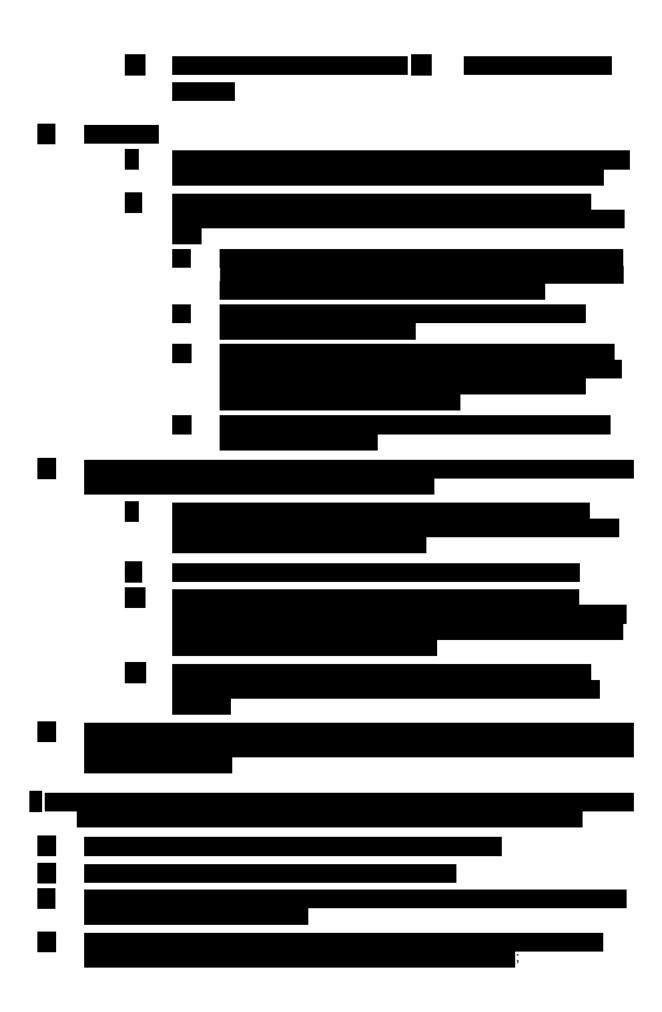


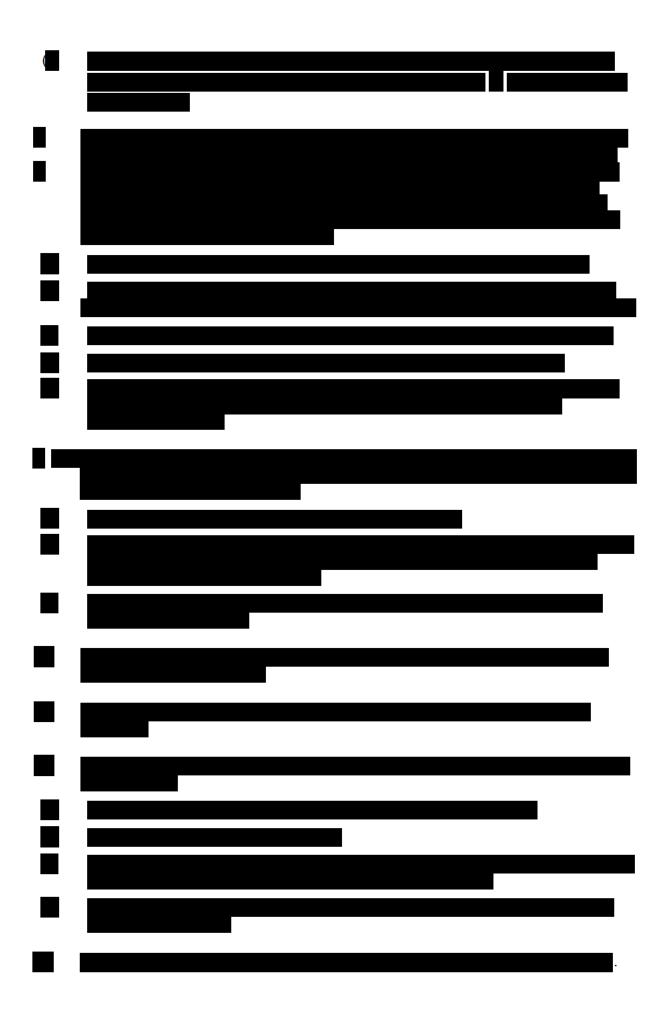


.....

.....

_			
I			
_			
_			_
- I			
-			
I			
-			
		,	

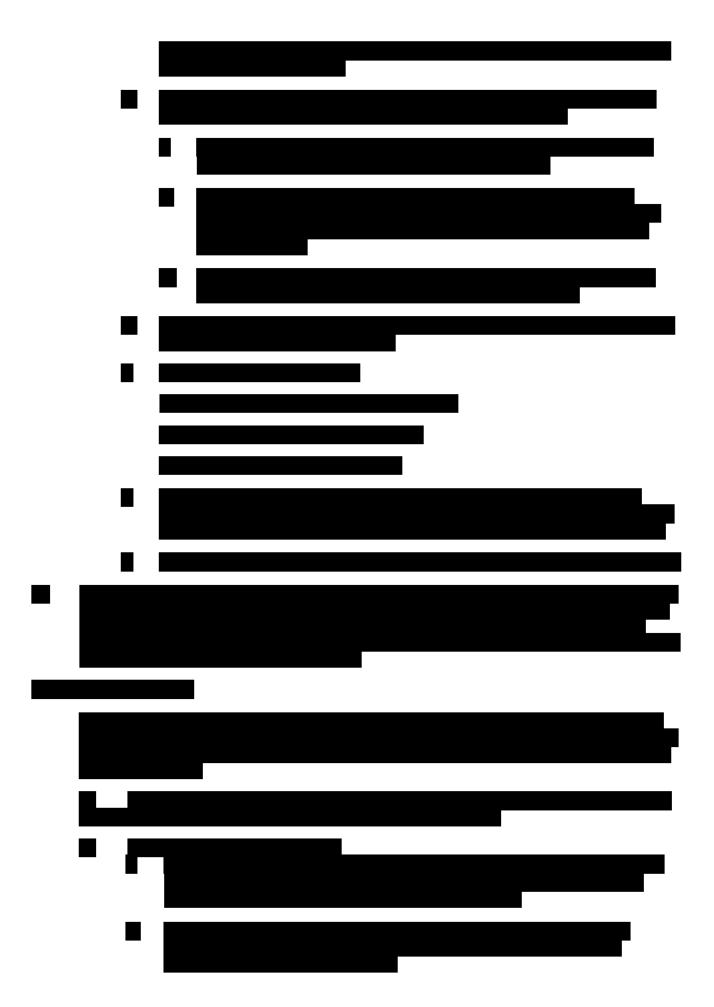


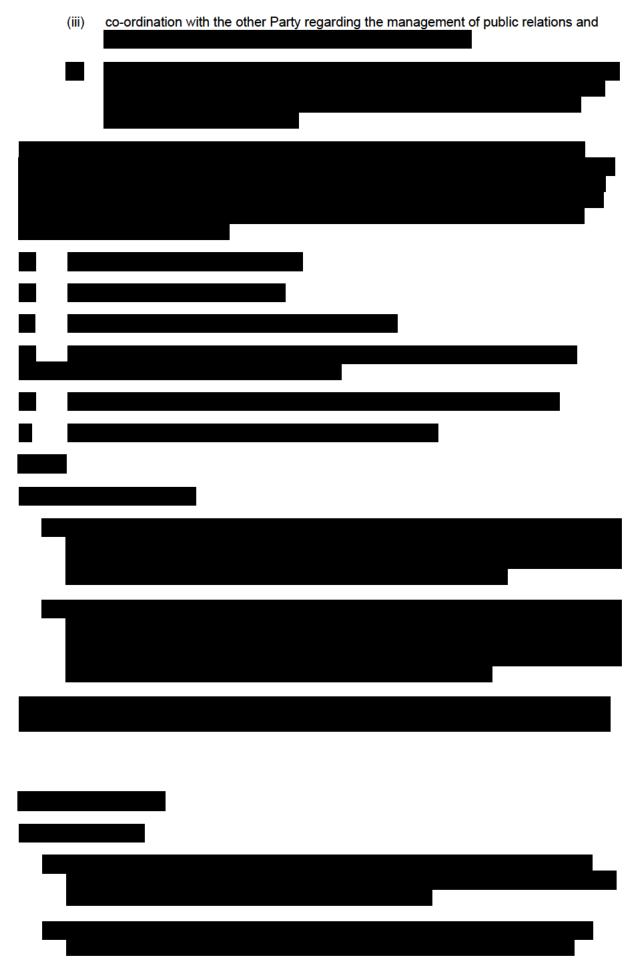


	_			
	•			
				I
_				



					,





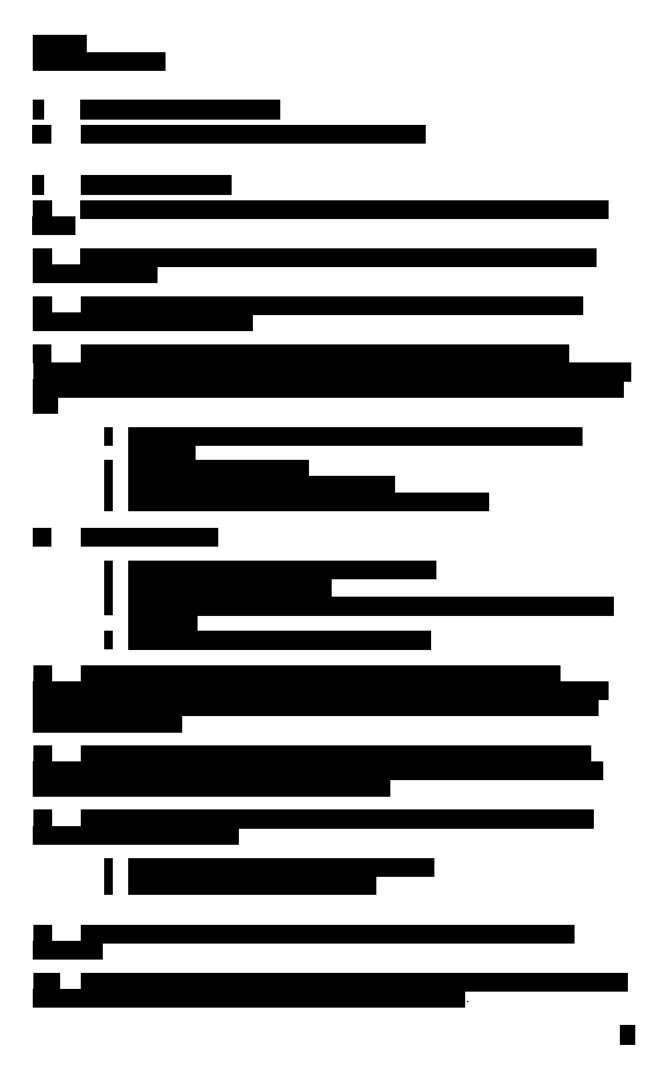
6	
-	

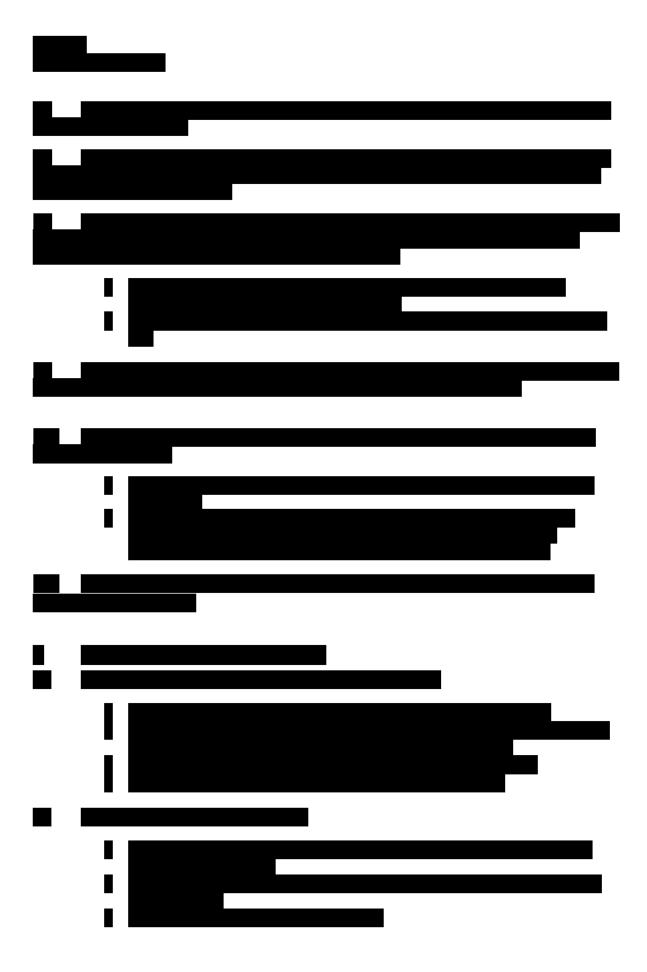
(b)			

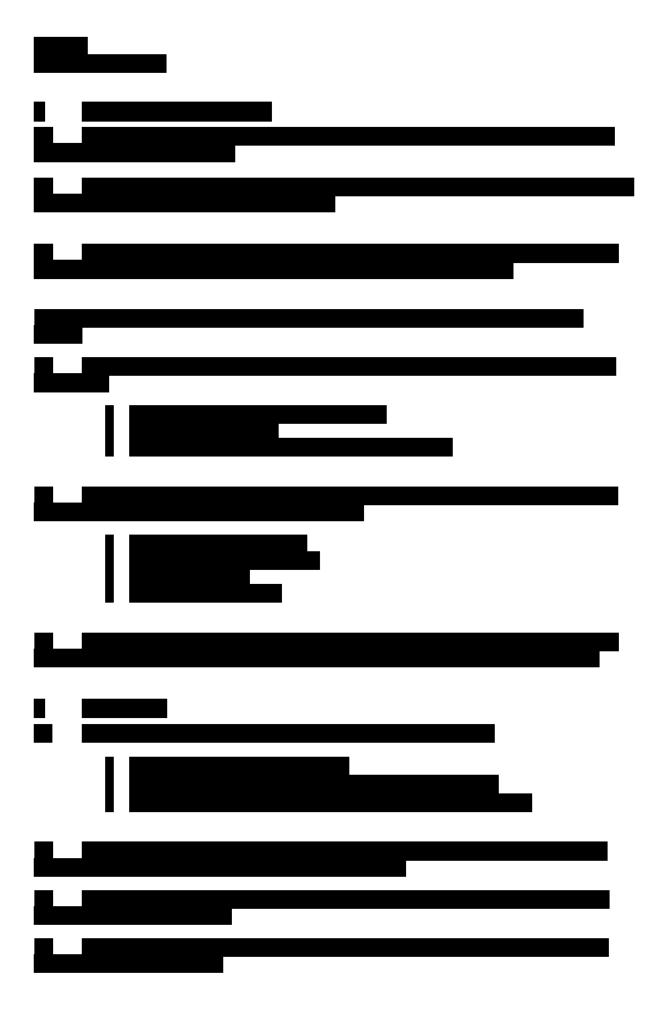


Crown Commercial Service

Core Terms







L		-
	•	
_		









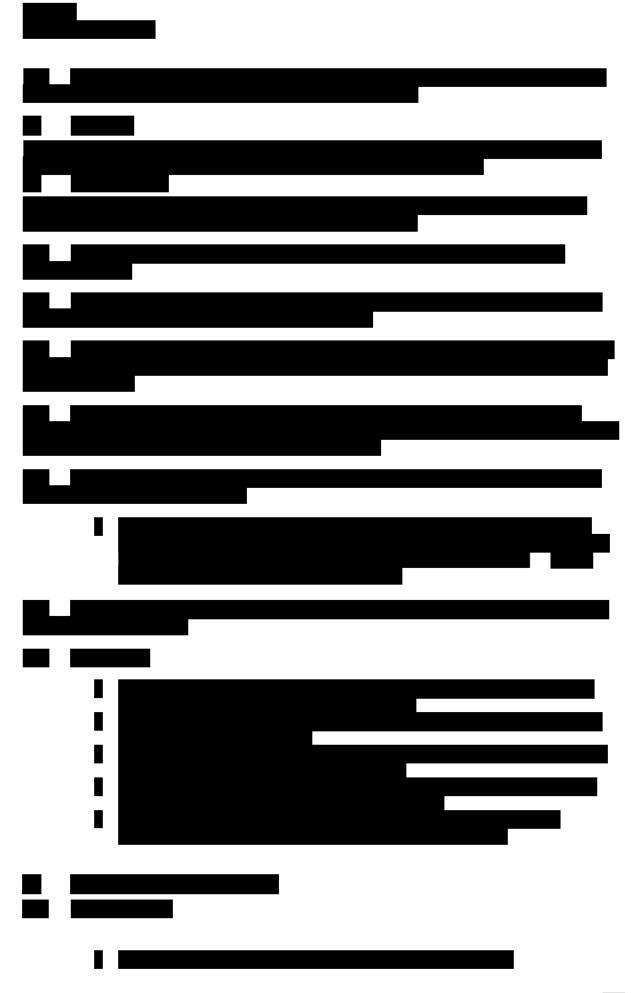






	-	

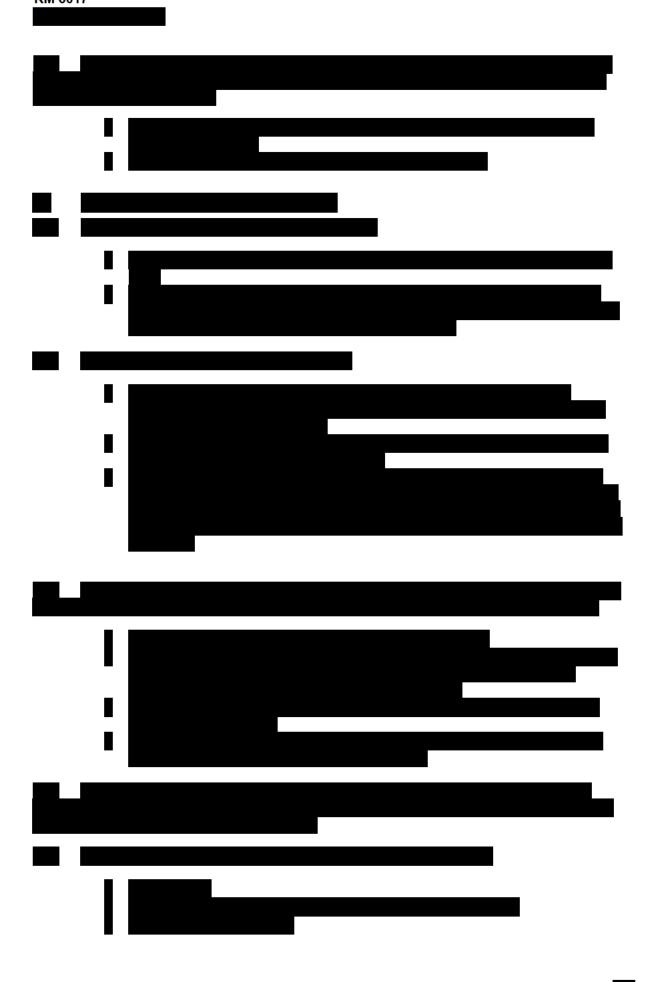
_	
_	
	I

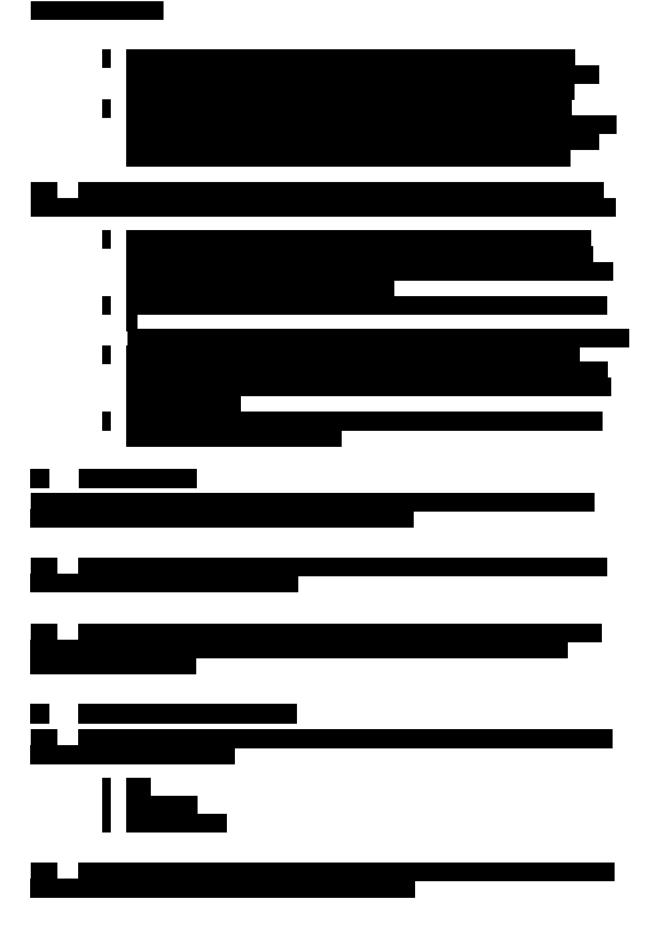




_		
ī		

RM 6017





RM 601	7			