





Department
for Environment
Food & Rural Affairs

Cyber Incident Response Partner Service

June 2021

Order Form

1. Contract Reference	ecm_61509	
2. Data	28 May 2021	
3. Buyer	Secretary of State for the Department of Environment Food and Rural Affairs Nobel House, 17 Smith Square, London SW1P 3JR	
4. Supplier	KPMG LLP 15 Canada Square, Canary Wharf, London E14 5GL OC301540	
5. The Contract	<p>The Supplier shall supply the deliverables described below on the terms set out in this Order Form and the attached contract conditions ("Conditions") and any Annexes or additional service specific terms as may be required and provided by the Supplier in the relevant Award Letter.</p> <p>Unless the context otherwise requires, capitalised expressions used in this Order Form have the same meanings as in Conditions.</p> <p>In the event of any conflict between this Order Form and the Conditions, this Order Form shall prevail.</p> <p>Please do not attach any Supplier terms and conditions to this Order Form as they will not be accepted by the Buyer and may delay conclusion of the Contract.</p>	
6. Deliverables	Goods	Not applicable

	<p>Services</p> <p>As laid out in the ITT offer dated 10th March 2021</p> <p>To be performed at Defra sites and related sites as directed and requested by the Authority.</p>
7. Specification	The specification of the Deliverables is as set out in Annex 2 and the Supplier's tender dated 10 th March 2021.
8. Term	<p>The Term shall commence on</p> <p>01 June 2021</p> <p>and the Expiry Date shall be</p> <p>31st May 2024, unless it is otherwise extended or terminated in accordance with the terms and conditions of the Contract.</p> <p>The Buyer may extend the Contract for a period of up to 24 months by giving not less than 10 Working Days' notice in writing to the Supplier prior to the Expiry Date. The Terms and conditions of the Contract shall apply throughout any such extended period.</p>
9. Charges	The Charges for the Deliverables shall be as set out in Annex 2 and the Supplier's tender dated 10 th March 2021.
10. Payment	<p>All invoices must be sent, quoting a valid purchase order number (PO Number), to:</p> <p></p> <p></p> <p>Within 10 Working Days of receipt of your countersigned copy of this letter, we will send you a unique PO Number. You must be in receipt of a valid PO Number before submitting an invoice.</p> <p>To avoid delay in payment it is important that the invoice is</p>

	<p>compliant and that it includes a valid PO Number, PO Number item number (if applicable) and the details (name and telephone number) of your Buyer contact (i.e. Contract Manager). Non-compliant invoices will be sent back to you, which may lead to a delay in payment.</p> <p>If you have a query regarding an outstanding payment please contact our Accounts Payable section either by email to</p> <p>[REDACTED]</p>	
11. Buyer Authorised Representative(s)	<p>For general liaison your contact will continue to be</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>or,</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	
12. Address for notices	<p>Buyer:</p> <p>Secretary of State for the Department of Environment, Food and Rural Affairs</p> <p>Nobel House, 17 Smith Square, London SW1P 3JR</p> <p>[REDACTED]</p> <p>[REDACTED]</p>	<p>Supplier:</p> <p>KPMG LLP 15 Canada Square, London E14 5GL</p> <p>Attention: Del Heppenstall - Partner</p> <p>[REDACTED]</p>

<p>13. Procedures and Policies</p>	<p>For the purposes of the Contract the staff vetting, security policy and other specific policies as detailed in the ITT shall apply.</p> <p>The Buyer may require the Supplier to ensure that any person employed in the delivery of the Deliverables has undertaken and holds current and valid Security Clearance.</p> <p>The Supplier shall ensure that no person who discloses that he/she has a conviction that is relevant to the nature of the Contract, relevant to the work of the Buyer, or is of a type otherwise advised by the Buyer (each such conviction a "Relevant Conviction"), or is found by the Supplier to have a Relevant Conviction (whether as a result of a police check, a Disclosure and Barring Service check or otherwise) is employed or engaged in the provision of any part of the Deliverables.</p>
<p>Signed for and on behalf of the Supplier</p>	<p>Signed for and on behalf of the Buyer</p>
<p>[Redacted Signature]</p>	<p>Name: [Redacted]</p> <p>[Redacted]</p>
<p>Date: 28/05/2021</p>	<p>Date: 1st June 2021</p>
<p>[Redacted Stamp]</p>	<p>[Redacted Stamp]</p>

Annex 1

Terms and Conditions of Contract for Services

1 Interpretation

1.1 In these terms and conditions:

“Agreement”	means the contract between (i) the Customer acting as part of the Crown and (ii) the Supplier constituted by the Supplier’s countersignature of the Award Letter and includes the Award Letter and Annexes;
“Award Letter”	means the letter from the Customer to the Supplier printed above these terms and conditions;
“Central Government Body”	<p>means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:</p> <ul style="list-style-type: none">(a) Government Department;(b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);(c) Non-Ministerial Department; or(d) Executive Agency;
“Charges”	means the charges for the Services as specified in the Award Letter;
“Confidential Information”	means all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (i) is known by the receiving Party to be confidential; (ii) is marked as or stated to be confidential; or (iii) ought reasonably to be considered by the receiving Party to be confidential;
“Customer”	means the person named as Customer in the Award Letter;
“DPA”	means the Data Protection Act 1998;
“Expiry Date”	means the date for expiry of the Agreement as set out in the Award Letter;
“FOIA”	means the Freedom of Information Act 2000;

“Information”	has the meaning given under section 84 of the FOIA;
“Key Personnel”	means any persons specified as such in the Award Letter or otherwise notified as such by the Customer to the Supplier in writing;
“Party”	means the Supplier or the Customer (as appropriate) and “Parties” shall mean both of them;
“Personal Data”	means personal data (as defined in the DPA) which is processed by the Supplier or any Staff on behalf of the Customer pursuant to or in connection with this Agreement;
“Purchase Order Number”	means the Customer’s unique number relating to the supply of the Services;
“Request for Information”	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term “request” shall apply);
“Services”	means the services to be supplied by the Supplier to the Customer under the Agreement;
“Specification”	means the specification for the Services (including as to quantity, description and quality) as specified in the Award Letter;
“Staff”	means all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any sub-contractor of the Supplier engaged in the performance of the Supplier’s obligations under the Agreement;
“Staff Vetting Procedures”	means vetting procedures that accord with good industry practice or, where requested by the Customer, the Customer’s procedures for the vetting of personnel as provided to the Supplier from time to time;
“Supplier”	means the person named as Supplier in the Award Letter;
“Term”	means the period from the start date of the Agreement set out in the Award Letter to the Expiry Date as such period may be extended in accordance with clause 4.2 or terminated in accordance with the terms and conditions of the Agreement;
“VAT”	means value added tax in accordance with the provisions of the Value Added Tax Act 1994; and
“Working Day”	means a day (other than a Saturday or Sunday) on which banks are

open for business in the City of London.

1.2 In these terms and conditions, unless the context otherwise requires:

- 1.2.1 references to numbered clauses are references to the relevant clause in these terms and conditions;
- 1.2.2 any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;
- 1.2.3 the headings to the clauses of these terms and conditions are for information only and do not affect the interpretation of the Agreement;
- 1.2.4 any reference to an enactment includes reference to that enactment as amended or replaced from time to time and to any subordinate legislation or byelaw made under that enactment; and
- 1.2.5 the word 'including' shall be understood as meaning 'including without limitation'.

2 Basis of Agreement

- 2.1 The Award Letter constitutes an offer by the Customer to purchase the Services subject to and in accordance with the terms and conditions of the Agreement.
- 2.2 The offer comprised in the Award Letter shall be deemed to be accepted by the Supplier on receipt by the Customer of a copy of the Award Letter countersigned by the Supplier within **14** days of the date of the Award Letter.

3 Supply of Services

- 3.1 In consideration of the Customer's agreement to pay the Charges, the Supplier shall supply the Services to the Customer for the Term subject to and in accordance with the terms and conditions of the Agreement.
- 3.2 In supplying the Services, the Supplier shall:
 - 3.2.1 co-operate with the Customer in all matters relating to the Services and comply with all the Customer's instructions;
 - 3.2.2 perform the Services with all reasonable care, skill and diligence in accordance with good industry practice in the Supplier's industry, profession or trade;
 - 3.2.3 use Staff who are suitably skilled and experienced to perform tasks assigned to them, and in sufficient number to ensure that the Supplier's obligations are fulfilled in accordance with the Agreement;
 - 3.2.4 ensure that the Services shall conform with all descriptions and specifications set out in the Specification;
 - 3.2.5 comply with all applicable laws; and
 - 3.2.6 provide all equipment, tools and vehicles and other items as are required to provide the Services.
- 3.3 The Customer may by written notice to the Supplier at any time request a variation to the scope of the Services. In the event that the Supplier agrees to any variation to the scope of the Services, the Charges shall be subject to fair and reasonable adjustment to be agreed in writing between the Customer and the Supplier.

4 Term

- 4.1 The Agreement shall take effect on the date specified in Award Letter and shall

expire on the Expiry Date, unless it is otherwise extended in accordance with clause 4.2 or terminated in accordance with the terms and conditions of the Agreement.

- 4.2 The Customer may extend the Agreement for a period of up to 24 months (2 x 12 month periods) by giving not less than 10 Working Days' notice in writing to the Supplier prior to the Expiry Date. The terms and conditions of the Agreement shall apply throughout any such extended period.

5 Charges, Payment and Recovery of Sums Due

- 5.1 The Charges for the Services shall be as set out in the Award Letter and as described in Annex 2 – Charges and shall be the full and exclusive remuneration of the Supplier in respect of the supply of the Services. Unless otherwise agreed in writing by the Customer, the Charges shall include every cost and expense of the Supplier directly or indirectly incurred in connection with the performance of the Services.
- 5.2 All amounts stated are exclusive of VAT which shall be charged at the prevailing rate. The Customer shall, following the receipt of a valid VAT invoice, pay to the Supplier a sum equal to the VAT chargeable in respect of the Services.
- 5.3 The Supplier shall invoice the Customer as specified in the Agreement. Each invoice shall include such supporting information required by the Customer to verify the accuracy of the invoice, including the relevant Purchase Order Number and a breakdown of the Services supplied in the invoice period.
- 5.4 In consideration of the supply of the Services by the Supplier, the Customer shall pay the Supplier the invoiced amounts no later than 30 days after verifying that the invoice is valid and undisputed and includes a valid Purchase Order Number. The Customer may, without prejudice to any other rights and remedies under the Agreement, withhold or reduce payments in the event of unsatisfactory performance.
- 5.5 If the Customer fails to consider and verify an invoice in a timely fashion the invoice shall be regarded as valid and undisputed for the purpose of paragraph 5.4 after a reasonable time has passed.
- 5.6 If there is a dispute between the Parties as to the amount invoiced, the Customer shall pay the undisputed amount. The Supplier shall not suspend the supply of the Services unless the Supplier is entitled to terminate the Agreement for a failure to pay undisputed sums in accordance with clause 16.4. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 19.
- 5.7 If a payment of an undisputed amount is not made by the Customer by the due date, then the Customer shall pay the Supplier interest at the interest rate specified in the Late Payment of Commercial Debts (Interest) Act 1998.
- 5.8 Where the Supplier enters into a sub-contract, the Supplier shall include in that sub-contract:
- 5.8.1 provisions having the same effects as clauses 5.3 to 5.7 of this Agreement; and
 - 5.8.2 a provision requiring the counterparty to that sub-contract to include in any sub-contract which it awards provisions having the same effect as 5.3 to 5.8 of this Agreement.
 - 5.8.3 In this clause 5.8, "sub-contract" means a contract between two or more suppliers, at any stage of remoteness from the Authority in a

subcontracting chain, made wholly or substantially for the purpose of performing (or contributing to the performance of) the whole or any part of this Agreement.

- 5.9 If any sum of money is recoverable from or payable by the Supplier under the Agreement (including any sum which the Supplier is liable to pay to the Customer in respect of any breach of the Agreement), that sum may be deducted unilaterally by the Customer from any sum then due, or which may come due, to the Supplier under the Agreement. The Supplier shall not be entitled to assert any credit, set-off or counterclaim against the Customer in order to justify withholding payment of any such amount in whole or in part.

6 Premises and equipment

- 6.1 If necessary, the Customer shall provide the Supplier with reasonable access at reasonable times to its premises for the purpose of supplying the Services. All equipment, tools and vehicles brought onto the Customer's premises by the Supplier or the Staff shall be at the Supplier's risk.
- 6.2 If the Supplier supplies all or any of the Services at or from the Customer's premises, on completion of the Services or termination or expiry of the Agreement (whichever is the earlier) the Supplier shall vacate the Customer's premises, remove the Supplier's plant, equipment and unused materials and all rubbish arising out of the provision of the Services and leave the Customer's premises in a clean, safe and tidy condition. The Supplier shall be solely responsible for making good any damage to the Customer's premises or any objects contained on the Customer's premises which is caused by the Supplier or any Staff, other than fair wear and tear.
- 6.3 If the Supplier supplies all or any of the Services at or from its premises or the premises of a third party, the Customer may, during normal business hours and on reasonable notice, inspect and examine the manner in which the relevant Services are supplied at or from the relevant premises subject to any confidentiality obligations the Supplier is bound to adhere.
- 6.4 The Customer shall be responsible for maintaining the security of its premises in accordance with its standard security requirements. While on the Customer's premises the Supplier shall, and shall procure that all Staff shall, comply with all the Customer's security requirements.
- 6.5 Where all or any of the Services are supplied from the Supplier's premises, the Supplier shall, at its own cost, comply with all security requirements specified by the Customer in writing.
- 6.6 Without prejudice to clause 3.2.6, any equipment provided by the Customer for the purposes of the Agreement shall remain the property of the Customer and shall be used by the Supplier and the Staff only for the purpose of carrying out the Agreement. Such equipment shall be returned promptly to the Customer on expiry or termination of the Agreement.
- 6.7 The Supplier shall reimburse the Customer for any loss or damage to the equipment (other than deterioration resulting from normal and proper use) caused by the Supplier or any Staff. Equipment supplied by the Customer shall be deemed to be in a good condition when received by the Supplier or relevant Staff unless the Customer is notified otherwise in writing within 5 Working Days.

7 Staff and Key Personnel

- 7.1 If the Customer reasonably believes that any of the Staff are unsuitable to undertake work in respect of the Agreement, it may, by giving written notice to the Supplier:
- 7.1.1 refuse admission to the relevant person(s) to the Customer's premises;
 - 7.1.2 direct the Supplier to end the involvement in the provision of the Services of the relevant person(s); and/or
 - 7.1.3 require that the Supplier replace any person removed under this clause with another suitably qualified person and procure that any security pass issued by the Customer to the person removed is surrendered,
- and the Supplier shall comply with any such notice.
- 7.2 The Supplier shall:
- 7.2.1 ensure that all Staff are vetted in accordance with the Staff Vetting Procedures;
 - 7.2.2 if requested, provide the Customer with a list of the names and addresses (and any other relevant information) of all persons who may require admission to the Customer's premises in connection with the Agreement; and
 - 7.2.3 procure that all Staff comply with any rules, regulations and requirements reasonably specified by the Customer.
- 7.3 Any Key Personnel shall not be released from supplying the Services without the agreement of the Customer, except by reason of long-term sickness, maternity leave, paternity leave, termination of employment or other extenuating circumstances.
- 7.4 Any replacements to the Key Personnel shall be subject to the prior written agreement of the Customer (not to be unreasonably withheld). Such replacements shall be of at least equal status or of equivalent experience and skills to the Key Personnel being replaced and be suitable for the responsibilities of that person in relation to the Services.

8 Assignment and sub-contracting

- 8.1 The Supplier shall not without the written consent of the Customer assign, sub-contract, novate or in any way dispose of the benefit and/ or the burden of the Agreement or any part of the Agreement. The Customer may, in the granting of such consent, provide for additional terms and conditions relating to such assignment, sub-contract, novation or disposal. The Supplier shall be responsible for the acts and omissions of its sub-contractors as though those acts and omissions were its own.
- 8.2 Where the Customer has consented to the placing of sub-contracts, the Supplier shall, at the request of the Customer, send copies of each sub-contract, to the Customer as soon as is reasonably practicable. This clause is subject to any obligations of confidentiality the Supplier is bound to adhere.
- 8.3 The Customer may, with the prior written consent of the Supplier, assign, novate, or otherwise dispose of its rights and obligations under the Agreement provided that such assignment, novation or disposal shall not increase the burden of the Supplier's obligations under the Agreement.

9 Intellectual Property Rights

- 9.1 All intellectual property rights in any materials provided by the Customer to the Supplier for the purposes of this Agreement shall remain the property of the Customer but the Customer hereby grants the Supplier a royalty-free, non-exclusive

and non-transferable licence to use such materials as required until termination or expiry of the Agreement for the sole purpose of enabling the Supplier to perform its obligations under the Agreement.

9.2 All intellectual property rights in any materials created or developed by the Supplier pursuant to the Agreement or arising as a result of the provision of the Services shall vest in the Supplier. If, and to the extent, that any intellectual property rights in such materials vest in the Customer by operation of law, the Customer hereby assigns to the Supplier by way of a present assignment of future rights that shall take place immediately on the coming into existence of any such intellectual property rights all its intellectual property rights in such materials (with full title guarantee and free from all third party rights).

9.3 The Supplier hereby grants the Customer:

9.3.1 a perpetual, royalty-free, irrevocable, non-exclusive licence (with a right to sub-license) to use all intellectual property rights in the materials created or developed pursuant to the Agreement and any intellectual property rights arising as a result of the provision of the Services; and

9.3.2 a perpetual, royalty-free, irrevocable and non-exclusive licence (with a right to sub-license) to use:

(a) any intellectual property rights vested in or licensed to the Supplier on the date of the Agreement; and

(b) any intellectual property rights created during the Term but which are neither created or developed pursuant to the Agreement nor arise as a result of the provision of the Services,

including any modifications to or derivative versions of any such intellectual property rights, which the Customer reasonably requires in order to exercise its rights and take the benefit of the Agreement including the Services provided.

9.4 The Supplier shall indemnify, and keep indemnified, the Customer in full against all costs, expenses, damages and losses (whether direct or indirect), including any interest, penalties, and reasonable legal and other professional fees awarded against or incurred or paid by the Customer as a result of or in connection with any claim made against the Customer for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Services, to the extent that the claim is attributable to the acts or omission of the Supplier or any Staff.

10 Governance and Records

10.1 The Supplier shall:

10.1.1 attend progress meetings with the Customer at the frequency and times specified by the Customer and shall ensure that its representatives are suitably qualified to attend such meetings; and

10.1.2 submit progress reports to the Customer at the times and in the format specified by the Customer.

10.2 The Supplier shall keep and maintain until 6 years after the end of the Agreement, or as long a period as may be agreed between the Parties, full and accurate records of the Agreement including the Services supplied under it and all payments made by the Customer. Such access is subject to an agreed time, scope, location and subject to any confidentiality obligations the Supplier is bound to adhere. The Supplier shall on

request afford the Customer or the Customer's representatives such access to those records as may be reasonably requested by the Customer in connection with the Agreement.

11 Confidentiality, Transparency and Publicity

11.1 Subject to clause 11.2, each Party shall:

11.1.1 treat all Confidential Information it receives as confidential, safeguard it accordingly and not disclose it to any other person without the prior written permission of the disclosing Party; and

11.1.2 not use or exploit the disclosing Party's Confidential Information in any way except for the purposes anticipated under the Agreement.

11.2 Notwithstanding clause 11.1, a Party may disclose Confidential Information which it receives from the other Party:

11.2.1 where disclosure is required by applicable law or by a court of competent jurisdiction;

11.2.2 to its auditors or for the purposes of regulatory requirements;

11.2.3 on a confidential basis, to its professional advisers;

11.2.4 to the Serious Fraud Office where the Party has reasonable grounds to believe that the other Party is involved in activity that may constitute a criminal offence under the Bribery Act 2010;

11.2.5 where the receiving Party is the Supplier, to the Staff on a need to know basis to enable performance of the Supplier's obligations under the Agreement provided that the Supplier shall procure that any Staff to whom it discloses Confidential Information pursuant to this clause 11.2.5 shall observe the Supplier's confidentiality obligations under the Agreement; and

11.2.6 where the receiving Party is the Customer:

(a) on a confidential basis to the employees, agents, consultants and contractors of the Customer;

(b) on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company to which the Customer transfers or proposes to transfer all or any part of its business;

(c) to the extent that the Customer (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions; or

(d) in accordance with clause 12.

and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Customer under this clause 11.

11.3 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of the Agreement is not Confidential Information and the Supplier hereby gives its consent for the Customer to publish this Agreement in its entirety to the general public (but

with any information that is exempt from disclosure in accordance with the FOIA redacted) including any changes to the Agreement agreed from time to time. The Customer may consult with the Supplier to inform its decision regarding any redactions but shall have the final decision in its absolute discretion whether any of the content of the Agreement is exempt from disclosure in accordance with the provisions of the FOIA.

- 11.4 The Supplier shall not, and shall take reasonable steps to ensure that the Staff shall not, make any press announcement or publicise the Agreement or any part of the Agreement in any way, except with the prior written consent of the Customer.

12 Freedom of Information

- 12.1 The Supplier acknowledges that the Customer is subject to the requirements of the FOIA and the Environmental Information Regulations 2004 and shall:

12.1.1 provide all necessary assistance and cooperation as reasonably requested by the Customer to enable the Customer to comply with its obligations under the FOIA and the Environmental Information Regulations 2004;

12.1.2 transfer to the Customer all Requests for Information relating to this Agreement that it receives as soon as practicable and in any event within 2 Working Days of receipt;

12.1.3 provide the Customer with a copy of all Information belonging to the Customer requested in the Request for Information which is in its possession or control in the form that the Customer requires within 5 Working Days (or such other period as the Customer may reasonably specify) of the Customer's request for such Information; and

12.1.4 not respond directly to a Request for Information unless authorised in writing to do so by the Customer.

- 12.2 The Supplier acknowledges that the Customer may be required under the FOIA and the Environmental Information Regulations 2004 to disclose Information concerning the Supplier or the Services (including commercially sensitive information) without consulting or obtaining consent from the Supplier. In these circumstances the Customer shall, in accordance with any relevant guidance issued under the FOIA, take reasonable steps, where appropriate, to give the Supplier advance notice, or failing that, to draw the disclosure to the Supplier's attention after any such disclosure.

- 12.3 Notwithstanding any other provision in the Agreement, the Customer shall be responsible for determining in its absolute discretion whether any Information relating to the Supplier or the Services is exempt from disclosure in accordance with the FOIA and/or the Environmental Information Regulations 2004.

13 Protection of Personal Data and Security of Data

- 13.1 For the purposes of this clause, "DP Legislation" means the General Data Protection Regulation (EU 2016/679), the Data Protection Act 2018 and legislation that amends, re-enacts or replaces it in England and Wales. The definitions and interpretations in the DP Legislation apply to this clause.

- 13.2 Supplier shall act as a Processor in respect of any personal data provided to the Supplier by the Customer, or on Customer's behalf, in connection with the Services ("Personal Data") and will process the Personal Data at all times in compliance with Supplier's obligations under DP Legislation and this Agreement. Customer must tell

Supplier in writing if Customer provides the Supplier with special category data. The Award Letter will set out any additional scope of the processing carried out by Supplier.

- 13.3 Customer warrants and represents that it has any necessary consent, provided any necessary notice and done all things required under the DP Legislation and applicable legislation or regulation in jurisdictions outside the UK (together with the DP Legislation, the "Privacy Laws") to disclose Personal Data to Supplier in connection with the Services.
- 13.4 Supplier shall:
 - 13.4.1 only process the Personal Data: (a) to the extent necessary to provide the Services to Customer (including for Supplier's reasonable business purposes such as facilitation and support of our business and quality control, updating and enhancing client records, analysis for management purposes and/or statutory returns); (b) in accordance with Customer's specific instructions (save to the extent Supplier reasonably considers such instructions infringe DP Legislation, in which case Supplier shall notify Customer); or (c) as required by any competent authority or applicable law;
 - 13.4.2 implement appropriate technical and organisational measures to maintain the security of the Personal Data and prevent unauthorised or unlawful access to, or processing of, or any accidental loss, destruction or damage to that Personal Data;
 - 13.4.3 keep, and procure that Staff keep, Personal Data confidential in accordance with any confidentiality obligations;
 - 13.4.4 notify Customer in writing without undue delay of discovery of, and provide reasonable cooperation in the event of, any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data in Supplier's possession or control;
 - 13.4.5 provide full cooperation and assistance to Customer in relation to any request by a data subject to have access to Personal Data held about them or in relation to a reasonable request, allegation or complaint by a competent authority or data subject and, unless prevented from doing so by applicable law, Supplier will notify Customer in writing without undue delay of receipt of any request and in any event within 5 days of receipt of any request; and
 - 13.4.6 delete or return all Personal Data to Customer upon request on termination or expiry of our engagement and destroy all copies of the Personal Data (save to the extent that retention of copies is required by applicable law or professional regulation).
- 13.5 Supplier shall maintain a record of its processing activities and provide such cooperation and information to Customer as is necessary for Customer to demonstrate compliance with Customer obligations under DP Legislation, including permitting Customer, or a third party acting on Customer's behalf, to audit Supplier's compliance with its relevant obligations under DP Legislation and this clause.
- 13.6 Supplier shall not use any subcontractor to process Personal Data as a sub-processor without Customer's prior written consent other than Staff and third parties who facilitate the administration of Supplier's business or support its infrastructure and shall ensure that where a sub-processor is duly engaged to carry out specific processing activities (a) such processing is subject to a written contract with that sub-

processor containing data protection obligations no less onerous than those set out in this clause; and (b) Supplier shall remain liable for the acts and omission of any such sub-processor with respect to the processing of Personal Data.

- 13.7 Supplier shall not process or transfer Personal Data to any jurisdiction outside the European Economic Area ("EEA") other than to a country deemed to provide an adequate level of protection for personal data by an applicable regulator or to the extent permissible by DP Legislation.
- 13.8 Supplier shall not be required to transfer personal data to any other third party as part of the Services. If Supplier has to enter into further agreements with Customer, Customer affiliates or Customer legal advisers, or take further steps to comply with relevant Privacy Laws in performing the Services, Customer will pay Supplier's reasonable costs in connection with compliance with applicable Privacy Laws and entering into such agreements, an estimate of which shall be provided in advance of Supplier incurring those costs.
- 13.9 Customer will reimburse Supplier for any loss, costs and expenses in connection with any claim that Supplier has breached Privacy Laws, from a data subject whose personal information is provided to Supplier by (or on behalf of) Customer or Customer's affiliates.

14 Liability

- 14.1 The Supplier shall not be responsible for any injury, loss, damage, cost or expense suffered by the Customer if and to the extent that it is caused by the negligence or wilful misconduct of the Customer or by breach by the Customer of its obligations under the Agreement.
- 14.2 Subject always to clauses 14.3 and 14.4:
 - 14.2.1 the aggregate liability of the Supplier in respect of all defaults, claims, losses or damages howsoever caused, whether arising from breach of the Agreement, the supply or failure to supply of the Services, misrepresentation (whether tortious or statutory), tort (including negligence), breach of statutory duty or otherwise shall in no event exceed a sum equal to 125% of the Charges paid or payable to the Supplier; and
 - 14.2.2 except in the case of claims arising under clauses 9.4 and 18.3, in no event shall the Supplier be liable to the Customer for any:
 - (a) loss of profits;
 - (b) loss of business;
 - (c) loss of revenue;
 - (d) loss of or damage to goodwill;
 - (e) loss of savings (whether anticipated or otherwise); and/or
 - (f) any indirect, special or consequential loss or damage.
- 14.3 Nothing in the Agreement shall be construed to limit or exclude either Party's liability for:
 - 14.3.1 death or personal injury caused by its negligence or that of its Staff;
 - 14.3.2 fraud or fraudulent misrepresentation by it or that of its Staff; or
 - 14.3.3 any other matter which, by law, may not be excluded or limited.

14.4 The Supplier's liability under the indemnity in clause 9.4 and 18.3 shall be unlimited.

15 Force Majeure

Neither Party shall have any liability under or be deemed to be in breach of the Agreement for any delays or failures in performance of the Agreement which result from circumstances beyond the reasonable control of the Party affected. Each Party shall promptly notify the other Party in writing when such circumstances cause a delay or failure in performance and when they cease to do so. If such circumstances continue for a continuous period of more than two months, either Party may terminate the Agreement by written notice to the other Party.

16 Termination

- 16.1 The Customer may terminate the Agreement at any time by notice in writing to the Supplier to take effect on any date falling at least 1 month (or, if the Agreement is less than 3 months in duration, at least 10 Working Days) later than the date of service of the relevant notice.
- 16.2 Without prejudice to any other right or remedy it might have, the Customer may terminate the Agreement by written notice to the Supplier with immediate effect if the Supplier:
- 16.2.1 (without prejudice to clause 16.2.5), is in material breach of any obligation under the Agreement which is not capable of remedy;
 - 16.2.2 repeatedly breaches any of the terms and conditions of the Agreement in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms and conditions of the Agreement;
 - 16.2.3 is in material breach of any obligation which is capable of remedy, and that breach is not remedied within 30 days of the Supplier receiving notice specifying the breach and requiring it to be remedied;
 - 16.2.4 undergoes a change of control within the meaning of section 416 of the Income and Corporation Taxes Act 1988;
 - 16.2.5 breaches any of the provisions of clauses 7.2, 11, 12, 13 and 17;
 - 16.2.6 becomes insolvent, or if an order is made or a resolution is passed for the winding up of the Supplier (other than voluntarily for the purpose of solvent amalgamation or reconstruction), or if an administrator or administrative receiver is appointed in respect of the whole or any part of the Supplier's assets or business, or if the Supplier makes any composition with its creditors or takes or suffers any similar or analogous action (to any of the actions detailed in this clause 16.2.6) in consequence of debt in any jurisdiction; or
 - 16.2.7 fails to comply with legal obligations in the fields of environmental, social or labour law.
- 16.3 The Supplier shall notify the Customer as soon as practicable of any change of control as referred to in clause 16.2.4 or any potential such change of control.
- 16.4 The Supplier may terminate the Agreement by written notice to the Customer if the Customer has not paid any undisputed amounts within 90 days of them falling due.
- 16.5 Termination or expiry of the Agreement shall be without prejudice to the rights of either Party accrued prior to termination or expiry and shall not affect the continuing rights of the Parties under this clause and clauses 2, 3.2, 6.1, 6.2, 6.6, 6.7, 7, 9, 10.2, 11, 12, 13, 14, 16.6, 17.4, 18.3, 19 and 20.7 or any other provision of the Agreement that either expressly or by implication has effect after termination.

16.6 Upon termination or expiry of the Agreement, the Supplier shall:

- 16.6.1 give all reasonable assistance to the Customer and any incoming supplier of the Services; and
- 16.6.2 return all requested documents, information and data to the Customer as soon as reasonably practicable.

16.7 Supplier is entitled to terminate this Agreement immediately by giving notice in writing to the Customer on 60 days' prior notice in writing or such shorter period required by any applicable law or any regulator if: (a) circumstances arise or have arisen which Supplier reasonably considers do or may impair its impartiality, objectivity or independence in respect of the provision of the Services; or (b) for legal, regulatory or other justified ethical reasons

17 Compliance

17.1 The Supplier shall promptly notify the Customer of any health and safety hazards which may arise in connection with the performance of its obligations under the Agreement. The Customer shall promptly notify the Supplier of any health and safety hazards which may exist or arise at the Customer's premises and which may affect the Supplier in the performance of its obligations under the Agreement.

17.2 The Supplier shall:

- 17.2.1 comply with all the Customer's health and safety measures while on the Customer's premises; and
- 17.2.2 notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Agreement on the Customer's premises where that incident causes any personal injury or damage to property which could give rise to personal injury.

17.3 The Supplier shall:

- 17.3.1 perform its obligations under the Agreement in accordance with all applicable equality Law and the Customer's equality and diversity policy as provided to the Supplier from time to time; and
- 17.3.2 take all reasonable steps to secure the observance of clause 17.3.1 by all Staff.

17.4 The Supplier shall supply the Services in accordance with the Customer's environmental policy as provided to the Supplier from time to time.

17.5 The Supplier shall comply with, and shall ensure that its Staff shall comply with, the provisions of:

- 17.5.1 the Official Secrets Acts 1911 to 1989; and
- 17.5.2 section 182 of the Finance Act 1989.

18 Prevention of Fraud and Corruption

18.1 The Supplier shall not offer, give, or agree to give anything, to any person an inducement or reward for doing, refraining from doing, or for having done or refrained from doing, any act in relation to the obtaining or execution of the Agreement or for

showing or refraining from showing favour or disfavour to any person in relation to the Agreement.

- 18.2 The Supplier shall take all reasonable steps, in accordance with good industry practice, to prevent fraud by the Staff and the Supplier (including its shareholders, members and directors) in connection with the Agreement and shall notify the Customer immediately if it has reason to suspect that any fraud has occurred or is occurring or is likely to occur.
- 18.3 If the Supplier or the Staff engages in conduct prohibited by clause 18.1 or commits fraud in relation to the Agreement or any other contract with the Crown (including the Customer) the Customer may:
- 18.3.1 terminate the Agreement and recover from the Supplier the amount of any loss suffered by the Customer resulting from the termination, including the cost reasonably incurred by the Customer of making other arrangements for the supply of the Services and any additional expenditure incurred by the Customer throughout the remainder of the Agreement; or
 - 18.3.2 recover in full from the Supplier any other loss sustained by the Customer in consequence of any breach of this clause. ;

19 Dispute Resolution

- 19.1 The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the Agreement and such efforts shall involve the escalation of the dispute to an appropriately senior representative of each Party.
- 19.2 If the dispute cannot be resolved by the Parties within one month of being escalated as referred to in clause 19.1, the dispute may by agreement between the Parties be referred to a neutral adviser or mediator (the “**Mediator**”) chosen by agreement between the Parties. All negotiations connected with the dispute shall be conducted in confidence and without prejudice to the rights of the Parties in any further proceedings.
- 19.3 If the Parties fail to appoint a Mediator within one month, or fail to enter into a written agreement resolving the dispute within one month of the Mediator being appointed, either Party may exercise any remedy it has under applicable law.

20 General

- 20.1 Each of the Parties represents and warrants to the other that it has full capacity and authority, and all necessary consents, licences and permissions to enter into and perform its obligations under the Agreement, and that the Agreement is executed by its duly authorised representative.
- 20.2 A person who is not a party to the Agreement shall have no right to enforce any of its provisions which, expressly or by implication, confer a benefit on him, without the prior written agreement of the Parties.
- 20.3 The Agreement cannot be varied except in writing signed by a duly authorised representative of both the Parties.
- 20.4 The Agreement contains the whole agreement between the Parties and supersedes and replaces any prior written or oral agreements, representations or understandings between them. The Parties confirm that they have not entered into the Agreement on the basis of any representation that is not expressly incorporated into the Agreement. Nothing in this clause shall exclude liability for fraud or fraudulent misrepresentation.

- 20.5 Any waiver or relaxation either partly, or wholly of any of the terms and conditions of the Agreement shall be valid only if it is communicated to the other Party in writing and expressly stated to be a waiver. A waiver of any right or remedy arising from a breach of contract shall not constitute a waiver of any right or remedy arising from any other breach of the Agreement.
- 20.6 The Agreement shall not constitute or imply any partnership, joint venture, agency, fiduciary relationship or other relationship between the Parties other than the contractual relationship expressly provided for in the Agreement. Neither Party shall have, nor represent that it has, any authority to make any commitments on the other Party's behalf.
- 20.7 Except as otherwise expressly provided by the Agreement, all remedies available to either Party for breach of the Agreement (whether under the Agreement, statute or common law) are cumulative and may be exercised concurrently or separately, and the exercise of one remedy shall not be deemed an election of such remedy to the exclusion of other remedies.
- 20.8 If any provision of the Agreement is prohibited by law or judged by a court to be unlawful, void or unenforceable, the provision shall, to the extent required, be severed from the Agreement and rendered ineffective as far as possible without modifying the remaining provisions of the Agreement, and shall not in any way affect any other circumstances of or the validity or enforcement of the Agreement.

21 Notices

- 21.1 Any notice to be given under the Agreement shall be in writing and may be served by personal delivery, first class recorded or, subject to clause 21.3, e-mail to the address of the relevant Party set out in the Award Letter, or such other address as that Party may from time to time notify to the other Party in accordance with this clause:
- 21.2 Notices served as above shall be deemed served on the Working Day of delivery provided delivery is before 5.00pm on a Working Day. Otherwise delivery shall be deemed to occur on the next Working Day. An email shall be deemed delivered when sent unless an error message is received.
- 21.3 Notices under clauses 15 (Force Majeure) and 16 (Termination) may be served by email only if the original notice is then sent to the recipient by personal delivery or recorded delivery in the manner set out in clause 21.1.

22 Governing Law and Jurisdiction

The validity, construction and performance of the Agreement, and all contractual and non-contractual matters arising out of it, shall be governed by English law and shall be subject to the exclusive jurisdiction of the English courts to which the Parties submit.

Annex 2 - Charges

Pricing (IR)

#	Item	Price	Comments or Clarification	Max Score
1.	Service set-up cost			-
2.	Annual Retainer, inclusive of 20 days			-
3.	Additional days rate card			-
4.	Other Additional costs		N/A	-
			Max score available	



DEFRA Cyber Incident Response Tender

Itt 8280

10 March 2021

Contents

ER1- Team Qualifications and Experience	24
ER2- Cyber Incident Response	24
ER3- Operating Hours	25
ER4- Deployment	26
ER5- Forensic Capability	28
ER6- SC Clearance	29
FR1- Threat Intelligence	30
FR2- Unused Support Days	33
FR3- Forensic Evidence	34
SR1- Malware Detected	36
SR2- Zero-day Threat	38
SR3- Foreign IP Address	41

ER1- Team Qualifications and Experience

Question

Members of the Supplier CIR Team must be suitably qualified, experienced and current in their specialist areas, including but not limited to incident response, threat analysis, malware analysis and forensic analysis. Please provide a number of anonymised CVs showing example experience and qualifications of the team leads only. The Authority understands you will have a mixture of experience in the team, but we would like to understand the experience, breadth and qualification level and types of a typical team lead. We are keen to understand that you have a good breadth of knowledge.

Answer

Please see separate attachment 'ER1- Team Qualifications and Experience'.

ER2- Cyber Incident Response

Question

The Supplier CIR Team must have current experience in responding to cyber security incidents for large organisations who have a mixture of cloud and legacy services provided by multiple suppliers. This does not necessarily mean government clients. Please provide details of your experience of responding to security incidents for large complex organisations and details of any experience in responding to security incidents for organisations that act as the service integrator.

Answer (468/500 words)

KPMG's Cyber Response team has a depth of recent experience in responding to significant and complex incidents for large organisations with multi-supplier and multi-technology estates. Please find below two examples of our recent response work for a large public sector body and for a service integrator and manager.

Complex Organisation with Multi-Supplier Infrastructure

KPMG is contractually retained as the primary national Cyber Incident Response provider for NHS Digital (NHSD). The Service Level Agreements for this contract include a 24/7 incident hotline, availability for a triage call within 1 hour of notification and deployment of resources to any nominated site in England within 4 hours.

In May 2020, KPMG was notified of an ongoing ransomware attack at a Birmingham location in which files had been encrypted on critical servers belonging to the trust's

heating, ventilation and air conditioning (HVAC) control system. The infrastructure used to control the HVAC systems was separated from the rest of the hospital's network and was maintained by a third-party supplier. KPMG (in compliance with the stated SLAs) was engaged to help contain the spread of the ransomware from these servers and to investigate the root cause of the attack. Our team collected forensic evidence from the impacted systems and deployed an Endpoint Detection and Response tool to assist with active monitoring and threat hunting on the network. This revealed that the root cause of the incident had been an unpatched server with an open RDP port vulnerable to security vulnerability 'BlueKeep (CVE-2019-0708)' which had allowed the attacker to execute code remotely and inject malware onto the system. Following remediation, KPMG provided recommendations to improve the trust's security posture and to mitigate the risk of similar incidents.

Service Integrator

KPMG responded to a catastrophic data corruption event at the software-as-a-service division of a global conglomerate. The impacted client acted as a 'Service Integrator' for a number of energy corporations globally. At the time KPMG were notified, most of their Windows Azure hybrid environment was not functioning and administrators were faced with errors when rebooting systems. The incident had soon spread to the department's production environment and live systems were ceasing to function.

KPMG were engaged to perform a detailed forensic investigation of the incident and were deployed in less than one hour to support the client. Over the period of the response, KPMG rapidly assessed the complex network architecture, identified critical data sets requiring preservation, and subsequently identified the origin of the intrusion. KPMG provided on-going support to the client to securely rebuild the infrastructure and provided protective monitoring for a six-week period until the client was able to establish their own in-house monitoring capability. KPMG worked alongside the NCSC to attribute the attack and it was determined (with medium to high confidence) to be deployment of trojan malware 'Shamoon' by threat group APT 33.

ER3- Operating Hours

Question

Supplier CIR Team must be able to provide support by telephone as well as by visiting client site. Please provide details of the operations support your CIR team can provide covering service hours as well as details of any limitations where support may not be available or the service level reduced, for example outside of office hours or bank holidays. We would like to understand your standard response times via calls as well as visiting DEFRA sites within the UK. Note – once on a given task the CIR Team will be expected to provide the appropriate level of support demanded by the severity of the incident.

Answer (389/500 words)

KPMG UK Cyber Response operates an on-call 24/7/365 duty team which enables incidents to be triaged and a call arranged within 1 hour of notification. Once DEFRA has triggered an incident alert, the on-duty case manager will contact you through your preferred channel (pre-agreed at the onboarding stage) to establish an incident triage call and to provide initial recommendations and containment actions. Once an incident is received, it is logged, and resources and tooling are allocated to the incident based on its severity and business impact. KPMG's incident management prioritisation process will incorporate and be directly aligned to DEFRA's departmental priorities. This will be captured and validated with you during our onboarding process.

KPMG's response can be scaled to meet Defra's needs in the event that the scope of our required support escalates rapidly. KPMG UK has access to KPMG's global response team to provide additional 'surge' capacity; we will agree the protocols and data handling arrangements for use of global resources during the onboarding process. Our global Cyber Incident Response capacity and capability can be deployed as a 'follow-the-sun' response model i.e. recovery, containment and investigation activities will be conducted around the clock as required by the incident. KPMG is highly experienced at dealing with incidents that occur out of office hours or during national holidays.

KPMG's cyber incident response hubs are based regionally across Bristol, London, Manchester, Leeds and Birmingham and enables rapid deployment of KPMG staff to Defra sites in the UK. KPMG also uses an optimised remote cyber response solution to deliver effective and efficient off-site incident-handling capabilities as required by DEFRA. For example, KPMG has developed a proprietary incident triage tool that can be used to collect forensic artefacts from compromised systems without on-site deployment being required. This means we can commence analysis of impacted systems for indicators of compromise immediately ahead of obtaining the full forensic images. The KPMG response team can deploy powerful endpoint detection and response (EDR) tools to maximise our visibility and monitoring across the entire network during an incident or in instances where we need enhanced containment measures. EDR tooling can also be used to block or quarantine malicious processes running on the endpoints as part of our containment strategy. These extensive remote and on-site capabilities enable KPMG to begin incident response procedures from the moment notification is received.

ER4- Deployment

Question

The Supplier must be able to deploy its CIR Team, in person, to respond to incidents at any location within the UK as specified by the Authority within 24hrs. Please provide details of your ability to provide this as well as any limitations.

Answer (434/500 words)

DEFRA has a large IT estate, spanning 370 sites across the UK and 12 major hubs that are likely to be focal points for timely incident response. The KPMG Cyber Response team is based at the following regions; Bristol, London, Manchester, Leeds and Birmingham. If onsite support is required across any of DEFRA's UK sites, KPMG will deploy trained responders in accordance with our agreed SLAs. In 2020 alone, KPMG responded in-person to more than 175 incidents across a range of incidents and sectors. KPMG's standard incident response service level agreements require no modification to meet your mandatory 24hr deployment requirement. Further evidence is provided below:

NHS Digital

KPMG's cyber incident response retainer with NHS Digital includes a service-level agreement of telephone-triage within **1 hour** and on-site support at any elected UK site within **4 hours** of notification. In 2020, KPMG responded to multiple incidents at 4 distinct UK locations and has maintained 100% compliance with the terms of our SLA.

Victrex plc

KPMG has a cyber incident response retainer with the British-based supplier of highperformance polymer solutions. The terms of this retainer dictate a service-level agreement of telephone-conference call within **6 hours** and on-site support at any elected UK site within **12 hours** of notification. In 2020, KPMG triaged and resolved a cloud-security incident within the stated SLAs.

NHS Blood and Transplant

KPMG has a cyber incident response retainer with NHS Blood and Transplant. NHSBT provide critical healthcare services in the UK and are responsible for national blood donation programs and maintenance of the organ donor list. The terms of our retainer dictate a service-level agreement of telephone-conference call within **4 hours** and on-site support at any elected UK site within **8 hours** of notification. KPMG are operating at full compliance with these SLAs.

UK multi-site case study

KPMG was notified of a Phobos ransomware infection reported at the UK headquarters of a large supplier of emergency services products. When KPMG were notified of the attack, the infection had spread to two other UK sites and was continuing to infect new systems (including backups). KPMG was tasked with containing the active threat and removing the malware and any persistence mechanisms from the network. Within a few hours, the KPMG team had deployed its proprietary artefact collector and was analysing evidence from a number of impacted systems. Simultaneously, our EDR tool was deployed across

the national network in collaboration with the organisation's security team to monitor for re-emerging threats. KPMG investigators performed root-cause analysis of the incident and produced a detailed timeline of events that included the initial compromise, privilege escalation and persistence activities.

ER5- Forensic Capability

Question

The Supplier CIR Team must protect the security of the Authority, and preserve evidence suitable to support criminal prosecution, when conducting any investigation. To support this please outline your forensic capability as well as the government security classification level you can hold.

Answer (495/500 words)

Government Security Accreditations

KPMG is a NCSC-certified Incident Response provider and routinely provides services to organisations of national significance. We have a dedicated and secure laboratory infrastructure (one of the largest UK NCSC accredited labs) in which we conduct forensic investigations using both industry-standard and proprietary software. Our forensics team adopts a three lines of defence model to provide a secure and safe environment for the data held using a variety of access controls, security devices, and monitoring tools. KPMG complies with several HMG frameworks including HMG Security Policy Framework.

KPMG holds the following certifications which are reviewed at least annually:

- ISO/IEC 27001:2013 in October 2019
- Cyber Essentials Plus: Certificate number 1231671484736600 dated 28th June 2019.
- List X status accredited by MOD DE&S PSyA (last review conducted March 2019).

KPMG Cyber Response Services systems and lab networks are certified under the following;

- Cyber Essentials Plus: Certificate No. 7051158210837777 (review conducted 08 May 2019).
- ISO EC 17025:2017 in June 2019.

Forensic Capabilities

Our forensic methodology and chain of custody procedures ensure that end-to-end work processes are repeatable, verifiable and auditable at every stage. Our processes will include a complete chain of custody and audit log procedures for each collection effort and ensures the provenance of the evidence is fully defensible. Commencing an investigation, our team will collect documents and media using the most suitable method. Should it be needed, our team will maintain detailed contemporaneous notes and can prepare a report, witness statement or affidavit to support the tasks performed. All work would be undertaken in accordance with the NPCC and the guidelines set out in the ACPO Good Practice Guide for Computer Based Electronic Evidence.

During the analysis stage, KPMG uses a range of industry-standard tools including, X-Ways, FTK Imager, Autopsy, EnCase, Relativity, Arsenal and more. Since forensic imaging can consume critical response time, KPMG has also developed its own incident triage tool that can be used to collect high-level forensic artefacts from compromised systems whilst we await transfer of the full disk images. With these specialised tools, KPMG's investigators are able to produce a detailed timeline of events and attacker activities to facilitate rootcause analysis of the incident.

Following the investigation, KPMG will create a summary incident report to summarise the analysis findings and recommendations. Should it be required, a full forensic report can be prepared. The findings and lessons-learned will be outlined for you to feed into your existing security improvement processes. We will provide cross-industry insight and advise you on remedial actions to minimise the impact of future incidents. Typical summary and detailed forensic reports outlining such findings are given in supporting documents 'Sample Memo Report' and 'Sample Detailed Forensic Report'. Where required, KPMG has specialised e-discovery software that will enable you to classify data impacted by the breach. We would also be able to assist with the creation of court trial bundles and have experience in the development of load files for specialist court presentation software such as Opus 2 Magnum.

ER6- SC Clearance

Question

All Supplier CIR Team members must hold a minimum level of HMG SC clearance - or be prepared to obtain it. The Authority will sponsor clearance for a small team of CIR specialists and is aware of staff turnover issues. Please confirm the number of SC cleared members of your current team together with details of how the security levels will be maintained during the term of the contract.

Answer (335/500 words)

KPMG has a central team that manages and maintain all clearances and hold an account with UKSV. This team monitors all staff clearances. This includes the aftercare management of clearance such as, annual Security Appraisals, Joiner, Movers and Leavers. New joiners must confirm they have read, understood and will comply with the Information Security Policies as part of their on-boarding process. They must also complete all mandatory information security eLearning within the first 60 days of joining. KPMG Human Resources is responsible for providing the new joiner with the minimum access required to perform their role whilst maintaining segregation of duties and on a risk-assessed basis will implement access requests. KPMG complies with several HMG Security frameworks, including HMG Security Policy Framework and Cyber Essentials.

It is acknowledged that in providing cyber incident response services to a government department such as DEFRA, the team may require access to classified information. At the time of writing, there are **39** individuals with HMG SC clearance or above within the cyber security team at KPMG UK. This confirms KPMG's ability to provide security cleared cyber professionals to handle DEFRA's assets and evidence in the event of a security incident.

KPMG's is a major provider of many kinds of cyber security services to the public sector. Our experience of delivering a number of testing and response engagements means we have experience of engaging effectively with NCSC, Threat Intelligence providers, Government Agencies and Regulators. The team regularly holds discussions with the NCSC (we are one of the largest UK NCSC accredited labs), NCA, Cabinet Office – Government Security Group, NCA and the City of London Police regarding cyber security threats. We are a trusted security advisor to HMG across a number of cyber disciplines via the NCSC Information Exchanges and other bodies. Our Team is a NCSC-Certified Incident Response (CIR) provider and regularly provides services to organisations and networks of national significance. Currently, we are the primary incident response provider for NHS Digital, NHS Blood and Transplant and Post Office UK.

FR1- Threat Intelligence

Question

The Supplier shall be able to leverage emerging threat intelligence (from their own research and other customers) and inform Defra of mitigation activity. As part of the set-up process the CIR partner will have a good understanding of the Authority, its IT estate, and cybersecurity capabilities. This will allow our CIR partner to identify threat intelligence that is relevant to the Authority and suggest mitigation activities when appropriate.

The CIR Partner will become the Authority's prime cyber threat intelligence partner so please provide details of your current threat intelligence capabilities and any example where this has helped mitigate threats against clients.

Please also describe what you need from the Authority and what your approach will be in order to provide this service. Please confirm what format this will be presented in.

Answer (741/750)

Threat intelligence looks beyond the network perimeter and is integral for an effective security strategy that protects an organisation, its customers and its assets. Combining our industry experience with our technical skills, KPMG works closely with clients to deliver a tailored threat intelligence service to help them better understand their attack surface and the adversaries they face.

Defining Intelligence Requirements

Together, KPMG and DEFRA would define the cyber intelligence requirement using good practice for intelligence development provided by the National Police Chief's Council (NPCC). KPMG will request information pertinent to DEFRA's assets (e.g. domain names, IP addresses, software versions and patch levels). The primary step of our offering would be to elicit your intelligence requirements by understanding your business, people, processes and technology. By considering DEFRA's operations and handling of previous incidents, the KPMG team can interpret gaps in their threat intelligence and plan for what will be required in the future. The more granular and specific the information gained, the more tailored and impactful intelligence requirements become.

Other key activities at this stage may include Threat Modelling and Crown Jewels Analysis. Threat modelling requires a deep search of internal activities, assets and capabilities to create a threat profile. This can be used to ascertain which adversaries may target the organisation and for what reason. Once a company's assets and capabilities are highlighted (on site server containing financial information or cloud stored intellectual property etc), Crown Jewels Analysis can define how the parts are prioritised and the level of security it requires.

Intelligence Collection

A combination of internal data sources (SIEM, network logs, incident management) with external feeds (paid/free, OSINT, ISAC groups, threat reports) will enable analysts to produce impactful reporting to fulfil DEFRA's intelligence requirement. Our service offering includes the collection of near real-time data using tools such as global intelligence leader 'Recorded Future' as well as other customised investigative methods including our own internal analysis team which provides contextualisation and threat and risk reporting.

KPMG understand that when it comes to information, more is not always better. We are therefore precise in the collection stage and would ensure that DEFRA are provided with the most impactful data to enable them to make informed decisions. When ingesting these feeds, KPMG would organise the information, categorise findings based on risk classes, and conduct human analysis and contextual enrichment using our cyber threat intelligence analysts.

Based on the scoped requirements, KPMG's threat intelligence service may also include the following:

- Use of next generation cyber security monitoring solutions such as Swoop in order to monitor the entirety of the network, enrich the performance of the Sentinel solution and provide threat hunting capabilities across legacy infrastructure.
- Tailored vulnerability management and exploit threat assessments performed on DEFRA's infrastructure.
- Bespoke information regarding situational awareness, management risk profiles, SIEM use case development and development of threat profiles and personas.
- KPMG could support with intelligence research into priority threat actors by liaising with law enforcement colleagues e.g. Cyber Griffin in the City of London Police (who provide the national cyber-crime leadership for policing).

Reporting

Generally, monthly reports are delivered, with periodic prioritized alerting of threats. However, this can be tailored to DEFRA's modular preferences and budget. (An example report 'Sample Intel Report' is given as a separate attachment). Our threat intelligence tools are optimised to integrate directly with MS Sentinel and adopt the industry leading threat intelligence services provided by KPMG's in-house Cyber Security Operations Centre (CSOC) that also use Sentinel as the primary SIEM solution.

Case Study: Threat Intelligence and Cyber Response

In a recent case, KPMG Cyber Response Services (CRS) team responded to a client who had experienced a leak of company data onto the web. It was soon understood that the source of the leak had been an internal file storage service which had been misconfigured and become accessible to the Internet. Working alongside KPMG CRS, the KPMG threat intelligence team was engaged to conduct intelligence searches to reveal whether any company intellectual property remained in the public domain following the incident. After conducting a combination of open source and dark web searches, the team discovered a large credential leak affecting 80+ employees which had occurred two months prior. The client had not previously been aware of this leak and KPMG subsequently guided them through appropriate response actions to mitigate the risks posed. As evidenced here, close collaboration between cyber response and threat intelligence would be key to mapping and defending DEFRA's unique threat landscape.

FR2- Unused Support Days

Question

The Supplier CIR Team is to provide an annual retainer price that is inclusive of 20 days of support. Unused CIR support days shall be available to support activities such as table-top exercises or small security reviews. Please provide information on the mechanism that will be in place to ensure value for money for any unused support days.

Answers (457/500 words)

KPMG has vast experience of improving incident preparedness services in government. We will develop a service catalogue for DEFRA, prioritising which services can improve maturity, service readiness and effectiveness. KPMG will track the hours used by DEFRA out of the proposed 20-day balance and provide monthly updates (in the form of our reporting dashboard) to assist DEFRA in managing the consumption of these hours. Any unused calloff days are mapped to other KPMG services according to the attachment 'CIR Retainer Days Support'.

Our range of services includes (but is not limited to) the following:

Maturity Assessments

KPMG can help DEFRA develop agile cyber risk management frameworks that enable your organisation to implement cost effective technologies safely and at scale. With a holistic view, we leverage comprehensive risk data that enables impactful decisions and helps to reach broader organisational goals.

Incident Response Readiness Review (Assessment and simulation)

KPMG's response readiness reviews help organisations to respond and recover from incidents by assessing how effectively they have planned for a breach by answering key questions about the organisation's preparedness for an incident. KPMG will leverage our 4Di service to conduct table-tops to deliver a powerful, immersive experience that will fully test multiple aspects of your cyber response capability. This has been used effectively across HMG (e.g. Dept for International Trade) and with KPMG clients globally.

Cloud Security Review

KPMG's cloud security reviews look at how securely an organisation's data is stored on the cloud. We assess cloud security configurations against control specifications, for instance those recommended by the National Cyber Security Centre (NCSC) and cloud vendors. A cloud security review will provide you with a clearer picture of how secure your data is on the cloud and whether data handling procedures using the cloud follow best practice.

Cyber Resilience

Cyber resilience refers to an organisation's ability to recover from a successful cyber-attack with as little business disruption, regulatory conflict, and reputational impact as possible. KPMG's resilience team has worked with some of the largest clients in the world, including major banks, energy companies, insurance companies, and multinational conglomerates. Thanks to this experience— such as developing crisis management programmes for global FTSE Top 50 clients – KPMG is well placed to identify gaps in cyber resilience planning and to evaluate and mitigate risk.

Penetration Testing

KPMG provides specialised penetration testing services to quantify the risks to an organisation's data from both external and internal threats. Our testing delivery team is CREST certified with penetration testing certifications such as CCSAS, CCSAM, CCT, and CRT, as well as defensive certifications such as CREST Certified Technical Security Architect and Network Intrusion Analyst. KPMG has a defined XBEST methodology which describes in detail how to conduct simulated attack testing and supplements the KPMG Security Testing methodology.

FR3- Forensic Evidence

Question

Outline how you will collect, store and handle forensic evidence and your procedure for returning evidence to the Authority or providing proof of destruction to maintain Chain of Custody.

Answer (499/500 words)

Collection

When responding to an incident, the KPMG forensic team will collect documents and media using the most suitable method for the given situation. We maintain detailed evidence chain of custody with contemporaneous notes and can prepare a report, witness statement or affidavit to support the tasks performed. When evidence is collected by members of the forensic technology team, the items are signed into our Evidence Management System used to track and maintain chain of custody. All data collected from or provided to clients is encrypted during transfer. All media would be secured in numbered sealed evidence bags to prove authenticity of media content upon receipt. We also use Property Receipts to record the collection and return of media.

Storage

KPMG has a dedicated and secure incident response laboratory infrastructure which is one of the largest UK NCSC accredited labs. Our forensic labs are situated within a secure office with locked down access by swipe card. All doors are controlled by the access points and have camera audit trails on the doors. The area also has an intruder alarm that is activated when the area is not occupied by cleared personnel. We ensure that all documents and media are kept securely and safely and that there is a clear, identifiable audit trail available on request.

Handling

All evidence handling is undertaken in accordance with the guidelines set out by the NPCC and in the ACPO Good Practice Guide for Computer Based Electronic Evidence:

- A defensible chain of custody – the KPMG team will ensure that the provenance, integrity and continuity of each document or item of media which we have received or obtained can be demonstrated.
- A verifiable and auditable approach – our methodology and chain of custody procedures ensure that our end-to-end work processes are repeatable and auditable at every stage.
- Where appropriate, all data is imaged in a forensically sound manner, maintaining and matching all data and metadata from the original media/records. An MD5, SHA1 and SHA256 hash of the computer image and the documents collected, verifies that the collected document exactly matches the original.
- The original evidence is stored in secured storage facilities and working copies are used for processing. The data is given an evidence number and this information is entered into our Evidence Management System.

Returning/Destroying Evidence

When a project has been completed, we take instructions from our client as to whether data should be returned, destroyed or retained. As soon as it becomes apparent that any items in our possession may be required in litigation or for police, regulatory, government authority, Insolvency Act or other lawful inquiries, the retention period of any records, not just KPMG working papers, is extended until the end of the inquiries, including the conclusion of any action and the time of appeal has passed. Temporary data held upon the KPMG network or secured cloud locations will be deleted periodically during the engagement and removed entirely at the end of the engagement. Evidence of these actions can be provided where required.

SR1- Malware Detected

Question

Symantec Endpoint Protection (SEP) alarmed that malware is present on a large number of DEFRA endpoints (outbreak alert). After a call with the SOC and an opportunity to review the SEP management console the CIR partner suggests the following actions. Please outline options that the SOC manager could brief to the Leadership team as an increasing number of laptops are now waiting to be rebuilt.

Answer (999/1000 words)

Once KPMG would be notified about the incident through the dedicated hotline, a team of first responders would be mobilised to the incident as well as an incident 'Case Manager' who will lead the triage call and ultimately the investigation. The triage call would ensure that the details and operational impacts of the incident are fully communicated to KPMG and that DEFRA's primary objectives and priorities are clearly understood so that they may direct the team's recommendations and first response. KPMG would review the SEP console for indicators (e.g. hashes, IPs, domains) that can help us determine the malware family and possibly attribute it to some of the trends that we have observed during the same time period.

From the SEP console, KPMG would look to clarify the following important questions:

- How many machines have been infected?
- Are those infected devices of a common operating system or network segment?
- At what rate is the infection spreading?
- Did SEP successfully block or quarantine the threat or did the SEP remediation fail?
- What are the signatures associated with this malware?

From the DEFRA team, KPMG would seek to understand:

- How are users and business operations affected so far? (e.g. account lockouts, data encryption, slowed systems)
- What actions have been taken so far?
- What is the extent of coverage of SEP across the DEFRA network?
- What are the high priority services and systems?

Having clarified this key background information, the case manager can proceed to advise on suitable containment strategies. Common to all containment options that could be taken by DEFRA would be the ongoing collection and analysis of forensic artefacts from

devices identified to have been infected. Since forensic imaging can consume critical response time, KPMG has developed a lightweight incident triage tool that can be used to collect high-level forensic artefacts. The tool will enable our team to begin analysing key impacted systems for indicators of compromise whilst KPMG assist DEFRA to execute their preferred containment strategy.

An effective response strategy is one that carefully manages the threats faced whilst preserving crucial organisational systems and services. For each of the following options, a 'risk vs reward' assessment would be conducted with information provided by KPMG to enable DEFRA leadership to decide on their strategy going forward.

Option 1: Elimination of attacker communication channels

The safest immediate approach to prevent the threat posed by the attacker whilst keeping the systems operational would be to discontinue the device's internet connection whilst keeping it live on the internal network. The benefit of this approach would be that it eliminates any malicious C&C channels on the system, preventing further attacker access or data exfiltration activities. It is recognised however that this may pose an operational cost to DEFRA which will depend on the device's specific business function.

An alternative strategy would be to block the specific IP addresses and domains suspected to be C2 channels of the malware. This would pose less interruption to business-as-usual operation, however there is a risk that some channels may be missed, or the attacker is able to pivot to another channel to maintain control. The choice taken here would be made on the basis of a carefully considered risk assessment that balances the continued operation of the infected devices with the threat posed by continued attacker communication.

Option 2: Identification of malware spreading mechanisms

KPMG could look to identify the mechanism through which the malware has spread throughout the network based on a sample that is extracted for analysis. The behaviour of the malware would be reviewed for indicators of common spreading techniques used such as SMB, WMI or WinRM. DEFRA would be immediately informed of any such mechanisms or corresponding indicators of compromise (e.g. files created, or domains contacted) identified. If required, KPMG could also perform memory forensics to investigate and identify malicious behaviours that do not leave detectable traces on the filesystem.

Identifying infection mechanisms is a key incident containment step and the findings would enable DEFRA to take the appropriate actions to detect and block further spreading of the malware. This option poses minimal disruption to DEFRA's operations and would therefore be recommended by KPMG to the leadership.

Option 3: Network and Endpoint Monitoring

Whilst these packages are being analysed, KPMG will be able to assist the DEFRA SOC with monitoring for threats. If KPMG's EDR tool (Cylance) is deployed across the network, its advanced machine learning capability can be leveraged to identify and block known and unknown malware, fileless attacks and payload execution in real-time. It is however recognised that deployment of a third-party endpoint agent may not be possible on DEFRA's environment. In this case KPMG could work with the technologies already in use by DEFRA to assist their internal security team. Our team has advanced threat hunting capabilities and will be able to support the DEFRA team in querying their Azure Sentinel SIEM for indicators of malicious activity on the network.

Such monitoring activities would be key to providing the DEFRA leadership with confidence to regular business operation. A benefit of KPMG assisting with this strategy would be the option to deploy the KPMG 'follow-the-sun' model for 24/7 monitoring if required. A risk associated with such an approach to security is the possibility that an attacker may lie dormant on a network and therefore remain undetected for long periods. Rebuilding the infected systems would eliminate the possibility of such a backdoor persisting, however, may result in the loss of data if backups are not recent. KPMG would recommend using monitoring procedures as part of a hybridised return to business to ensure the security of online systems awaiting a rebuild.

Conclusion

KPMG does not use a 'one-fits-all' approach to incident response and the steps taken to contain and investigate the incident will be highly dependent on direction provided by DEFRA and may change course as new findings come to light. The above services are however demonstrative of the depth of options that would be available to DEFRA in the event of the incident described.

SR2- Zero-day Threat

Question

The CIR partner informs DEFRA that a known zero-day threat now has an exploit. It informs DEFRA that part of its estate is vulnerable to this threat. What mitigating actions do you suggest we take? Please respond to this in three parts: 1) if the zero-day effects a windows OS, 2) google chrome or, 3) a CISCO appliance. What further information would you require from us and how would that inform your decision?

Answer (986/1000 words)

As DEFRA's main cyber incident response provider, KPMG would acquire an in-depth knowledge of the department's information technology. In the event that an exploit is crafted for a known zero-day threat affecting DEFRA, KPMG would issue an urgent update detailing the risks it poses.

The following are some of the key details which may be issued to DEFRA in the update:

- The vulnerability would be identified by its *Common Vulnerabilities and Exposures* (CVE) record.
- The CVSS score (*Common Vulnerabilities Scoring System*) of the vulnerability would be provided. This score would be contextualised for DEFRA by providing considered expertise on the metrics used to calculate it. For instance:
 - a) How complex is the exploit?
 - b) Which privileges are required? (Pre/post authentication)
 - c) Is the exploitable service publicly exposed?
 - d) Is user interaction required?
 - e) What is the impact of the exploit? For example: Privilege escalation may be considered lower impact than remote code execution (RCE).
- Key attack scenarios may be provided based on knowledge of DEFRA's priority infrastructure and services.
- If a vendor mitigation or workaround is available, KPMG would provide details for the implementation.

KPMG would assess the impact of the exploit on DEFRA's estate:

- How many vulnerable systems are there and where are they located on the network?
- What is the purpose and usage of the affected systems? For example, a vulnerability in payment processing software would be more critical than one in a meeting room booking system.
- How critical to your business is their continued operation?
- Who owns and maintains these systems? (KPMG is aware of the nature of DEFRA's multi-provider IT estate)

When considering mitigation strategies, DEFRA will consider the cost and disruption caused by implementing the strategy with the risks posed by the threat of exploitation. In general terms, three options are as follows:

- 1) Take the affected hardware or software out of use until a patch is available. This is the safest course of action but is likely to cause the most disruption to business.
- 2) Issue a quick-fix mitigation as advised by the vendor. This will enable the affected service to remain operational, however the fix itself may be disruptive.
- 3) Implement detection and response capabilities specific to the exploit. This will minimise the disruption caused to operations, however, is not guaranteed to prevent exploitation of the vulnerability so the risk remains elevated.

Windows OS

DEFRA operate a multi-technology environment and the Windows operating system is widely used in both user-device and server infrastructure. With thousands of endpoints running Windows software, a zero-day exploit of the operating system could pose a critical threat to the security of DEFRA's assets and information if left unmanaged.

In this scenario, the option to take the affected devices offline could be majorly disruptive to DEFRA's business and would likely only be considered if the vulnerable Windows service is externally exposed and poses an immediate threat. As an intermediate solution, any existing hardening mitigations should be implemented after considering compatibility issues they may cause. For vulnerable services or configurations on Windows systems, Active Directory Group Policy Objects (GPOs) may be used to centrally disable or limit features to reduce the chances of exploitation.

Where the impact of the mitigation is in fact greater than the probability-adjusted impact of the exploit, DEFRA would still be able to implement detection capabilities specific to the exploit. For instance, YARA rules may centrally be added to your Symantec Endpoint Protection console to identify and block execution associated with the exploit.

Google Chrome

Chrome is a popular Web Browsing software and is likely to be the application through which many of DEFRA's staff and suppliers access the internet. A vulnerability in Chrome browser could expose a sizeable attack surface to your organisation. In most cases, Google Chrome is an internet-accessing application, and it is possible that this exploit may be launched when a user visits a malicious or compromised website.

In this instance, if the exploit poses an elevated risk over other browsers, DEFRA should block the application across their estate until a patched version is released. This is likely to cause minimal disruption as there are a number of readily available substitution browsers to choose from. The cyber risk of its continued use in your estate would outweigh the benefit that its use provides to your organisation.

This control can be achieved by blocking the chrome user-agent on your perimeter firewall or by using GPO to block chrome execution on your endpoints.

Cisco appliance

DEFRA's network architecture is reliant on the functionality and security of Cisco networking appliances. Exploitation of a vulnerability in these devices could expose DEFRA to a range of threats including authentication bypass, remote code execution and more. The threat posed will be largely dependent on the size of the attack surface. Appliances such as VPN gateways and perimeter firewalls are internet-facing by design and therefore will pose an elevated risk in relation to internal network appliances such as switches in a LAN.

The option to take the impacted hardware offline could be majorly disruptive to DEFRA's business and would likely only be recommended if the exploit is internetfacing with no mitigations possible. Where a workaround is released, this should be implemented on all affected devices after consideration of any potential disruption caused by the changes.

If no such hardening options are available or the impact of the mitigation is greater than the probability-adjusted impact of the exploit, DEFRA would still have the option to implement detection capabilities specific to the exploit. For instance, Snort rules specific to a network vulnerability may be added to your IDS/IPS to detect and block attempts to exploit it.

Summary

The decision to fix or leave an issue is, at root, a business decision and every organisation has their own risk appetite. As CIR provider, KPMG will take every step to ensure that DEFRA is well informed and advised when making the important decisions presented in scenarios such as these.

SR3- Foreign IP Address

Question

One of the on-prem windows servers is beaconing out to IP in China. This is happening increasing often (10 times this week and once last month). Our current approach is for the hosting partner to run an AV check and if positive the server is rebuilt with no investigation. As this is becoming more frequent and suggesting persistence how do you suggest we approach this?

Answer (956/1000 words)

The reported beacon to a Chinese IP could be an indicator of compromise (IoC) and it is strongly advised to investigate its origin. Many variants of malware will connect to external IP addresses as a means of maintaining access to a network. Such 'Command and Control' (C&C) connections can provide a channel for inbound attacker-commands and outbound data exfiltration from the network. The example described however is **not a confirmed incident** and it is possible that the beaconing activity could be originating from legitimately installed software. KPMG's approach would be driven by identification of the root cause of the beacon to facilitate the appropriate actions to be taken.

DEFRA's current approach is to first run an AV scan on the server. Whilst this is a good first step to detect any well profiled malware, an AV scan will not always detect new or specialist malware. Furthermore, attackers use a multitude of techniques to avoid AV detection such as fileless malware and remote interaction via protocols such as FTP, SSH and RDP. In this scenario, the beacon to a Chinese IP could be an indicator of compromise and this warrants further investigation whether the AV scan is positive or not.

Rebuilding the machine without investigating the source of the connection would wipe critical evidence from the server and may prevent proper handling of the incident if the activity was in fact malicious. Additionally, rebuilding the server may not prevent an attacker on the network from pivoting to another system. This could explain why the incident is recurring on different machines on the network.

Once KPMG is notified of the incident, we will arrange a triage call with DEFRA to ensure that DEFRA's primary objectives are fully communicated. Key questions asked by KPMG during the triage call would include:

- What was the IP address?
- What are the source and destination port numbers?
- How and when was the beaconing activity detected? When did this activity start?
- Is the beaconing persistent after server is switched off?
- How many devices have beacons to the identified IP?
- What is the operating system of this device? How does this device connect to the rest of the network?
- What activity has DEFRA taken so far?
- Have any users reported unusual activity? If so what?
- Is there any sensitive or PII data stored on this server?
- Does this server host any priority/critical services?

Following this call, KPMG will take some of the following steps to support DEFRA in responding to this beaconing event.

Artefact collection and analysis of affected host

KPMG has developed an incident triage tool that can be used to remotely collect high-level forensic artefacts for analysis. A triage package from the affected server would be taken and the KPMG team would analyse the relevant artefacts such as the active connections and running processes to identify the origin of the beaconing. Once the process or service responsible for the beaconing activity is identified, a copy of the executable or dynamiclink library file would be requested for analysis.

If the originating process is unknown to DEFRA or behaving in an unexpected way, KPMG would perform some static and dynamic analysis on the sample to reveal its likely behaviours and purpose. If required, KPMG could also perform memory forensics to investigate and identify malware that does not leave detectable traces on the hard drive.

Network Traffic Analysis

It may also be possible to implement live network taps to collect network traffic data. This would provide an understanding of any malware communication mechanisms and visibility into which devices on the network may have been infected. As an important additional priority, the network traffic logs could later be used to review if any data exfiltration has occurred from the network. KPMG could perform a statistical analysis of the network traffic in order to detect anomalous behaviour, such as abnormally large volumes of outgoing traffic.

KPMG would also be able to review your firewall and network logs with a focus on traffic to and from the identified IP in China. This will allow us to identify if any other servers on the network are (or have been) in contact with this IP. Since it is common for threat actors to utilise more than one IP address, we would look to identify any other suspicious network traffic to other external IPs from these logs.

Intelligence

KPMG would perform open source intelligence (OSINT) on the Chinese IP as well the publicly facing IP of the beaconing server using public sources of intelligence such as VirusTotal and Shodan. KPMG may also be able to leverage licensed feeds using tools such as global intelligence leader 'Recorded Future' and other customized solutions and investigative methods. These intelligence sources may provide an indicator of the threat actor's initial vector of access as well as a view of the attacker's techniques, tactics and procedures.

Conclusion

DEFRA's current approach to this event would not address the root cause of the incident and may explain why the issue has persisted on several occasions. Rebuilding the machine without conducting analysis results in the loss of crucial evidence needed to determine whether the source of the activity is benign or malicious. Conversely, KPMG's approach would begin with the collection of key artefacts from the server to enable identification of the process or service responsible for the beaconing.

DEFRA may at this point confirm that the activity is legitimate, and no further response is required. If this is not the case however, KPMG would perform analysis on the executable to identify its intended purpose and behaviour. KPMG would perform network analysis and intelligence gathering to give the DEFRA team the best possible understanding of the incident's root cause and enable them to decide on a suitable remediation strategy going forward.