Date of Release: 12 Nov 2015 Copy No. 1

Department of Energy & Climate Change

Response to Tender for Cyber Security: Product Assurance Scooping Work

TENDER 1077/10/2015

Issue 1

Contents

1 INTRODUCTION

This document forms Thales's response to the tender 'Cyber Security: Product Assurance Scoping Work' (Tender Reference Number: 1077/10/2015). Pricing information is contained in the accompanying Annex A.

Thales understands the Department of Energy and Climate Change (DECC), wishes to appoint a supplier to investigate the current approaches which assure the cyber security of Industrial Control Systems (ICS) and other Operational Technology (OT), and the extent to which these systems are assured across the energy sector internationally.

This work package is to help DECC better understand:

- How OT/ICS[1] products are certified and tested,
- The extent to which OT/ICS products have been developed in accordance with security guidance, and
- The extent to which OT/ICS products have been tested and validated to ensure they perform their advertised security.

Thales confirms it will undertake a review of:

- OT/ICS products which are used in or relevant to the energy sector, including their function and any advertised security characteristics,
- Existing security standards and certifications for OT/ICS products. This shall specify:
    - Background details of the organisation either publishing the standards or granting certification,
    - The criteria used to certify products, and
    - Identify relevant energy sector products which have achieved certification or been developed in accordance to security standards.
- Previous security testing conducted on OT/ICS systems detailing what was tested and how, and
- Organisations (including academia) who are developing security standards, certification schemes, testing beds and testing criteria to assure the cyber security of OT/ICS products.

And provide recommendations on:

- Security characteristics that should be tested on OT/ICS products relevant or used by the energy sector (including how these can be tested),
- Suitable test laboratories/ranges that could undertake testing of OT/ICS products, and
- A list of OT/ICS products tested and certified, including where they are used and any specific products for the energy sector.

[1] The term ICS is used throughout this document to include both ICS and OT products and systems except where specific singular references to either ICS or OT are used.

2 OUR UNDERSTANDING

2.1 Industrial Control Systems

Redacted

2.1.1 Key components of an ICS

Redacted

2.1.2 ICS security standards

Redacted

2.2 Scope

Redacted

3 METHODOLOGY & DELIVERY

3.1 Our approach

The ICS and OT product assurance research will be broken into three activities:

- Work Item 1 - a background and literature review;
- Work Item 2 - analysis of assurance methodologies, standards and organisations; and
- Work Item 3 - product assessment.

The Gantt chart at Figure 4: Proposed Project Schedule Work Items (below) presents the proposed time-spans and effort involved for each of the work item in relation to the progress report requirements and final report delivery.

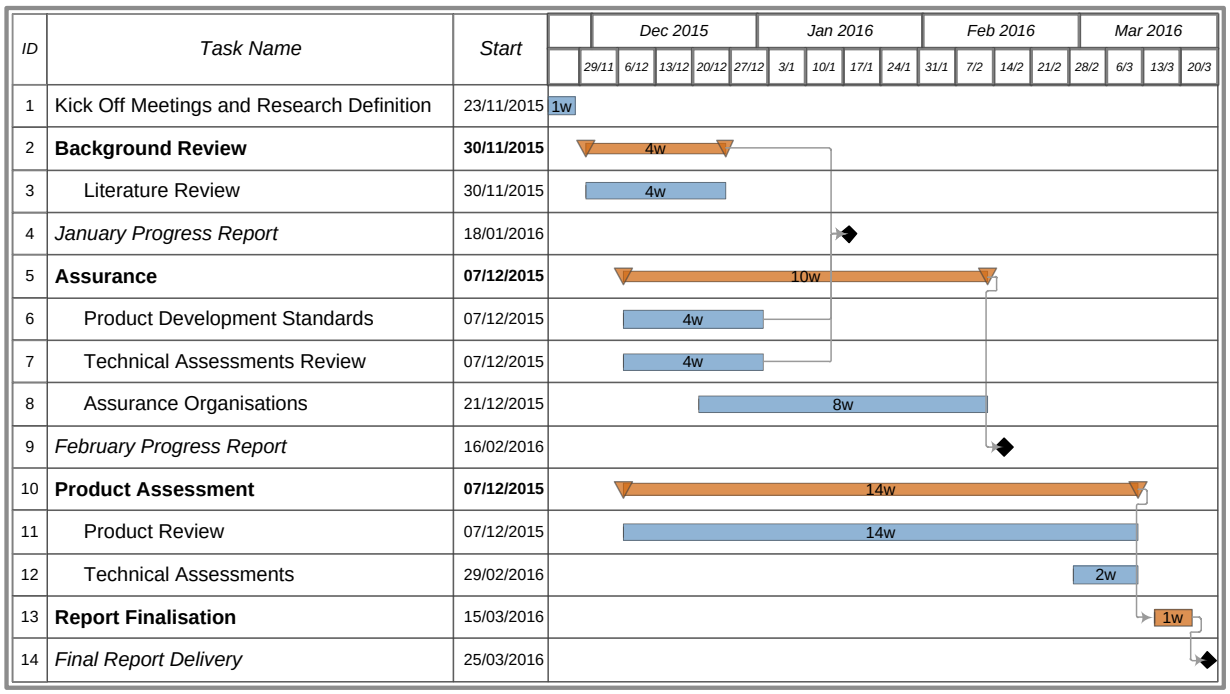

Figure 4: Proposed Project Schedule Work Items

3.2 Kick off meetings and research definition

The first component of the research is to meet with DECC; introduce team members and conduct a review of the relevant terminology in order to produce a comparative analysis of the issues being researched and confirm the scope. This would be prior to meetings with other key stakeholders. This would allow for the definition of a research scope and to be able to confirm the qualitative and quantitative processes that would be used for analysis.

3.3 Literature review (Work item 1)

The literature review will be conducted using appropriate open and closed source indexes and will cover published academic, government, industry papers and legislation, books and un-published sources.

The review will be split into the following sections and be accompanied by a complete bibliography in the report's appendices.

- ICS technologies,
- CNI[2] security,
- Risk assessment methodologies,

[2] Critical National Infrastructure

- Vulnerability research, and
- Media reports.

3.3.1 ICS technologies and environments

The first section will provide an overview of the different types of ICS technologies that are available in a solution agnostic manner. Future technologies will be considered after a review of historic and current systems. The review will range from monolithic mainframe systems through distributed and networked, to the potential for heterogeneous, agent-based (AI) systems that operate in environments of varying levels of trust.

3.3.2 CNI security

This component of the literature review will examine aspects of cyber security as related to CNI, including threat modelling, attack surfaces, solution implementations and published historical attacks. This will include UK domestic and relevant overseas material.

3.3.3 Risk assessment methodologies

Risk methodologies will be reviewed from a generalised position initially then focussed on CNI environments and ICS technologies. This will include IAS 1&2 (CESG), IRAM2 (ISF) and guidance from SANS Critical 20.

3.3.4 Platform vulnerability research

A review of publicly known vulnerabilities in ICS solutions will be undertaken and the results of the review will contain a breakdown of vulnerabilities by standard CWE (Common Weakness Enumeration) and Common Vulnerability and Exposures (CVE) dimensions and will make comparisons across technology types and manufacturers. This will be developed from direct knowledge Thales has gained from work with the UK energy sector and public sources such as the US Department of Homeland Security's ICS-CERT Alerts and Advisory notices. From this analysis Thales will be able to identify those manufacturers and platforms that show the highest levels of vulnerability by the type of deployment for further investigation.

3.3.5 Supplier / Operator information

Following from the platform vulnerability research Thales will identify the key suppliers and through questionnaire, and where time permits, understand their mitigations, development and assurance strategies.

3.3.6 Media research

A time-limited review of media (journalistic) articles will also be conducted.

3.4 Assurance, standards and organisations (Work item 2)

Redacted

3.4.1 Standards and certification

A core element of the research, this section will present the international standards and best practice that are relevant to ICS solutions, the areas in which they are used and the bodies and organisations that conduct certification. Attention will be paid to the different assessments that are conducted throughout a product's lifecycle, from design through production and implementation, though life monitoring to decommissioning.

As well as assessing technical products and solutions this section will examine the certifications that are available for professionals involved in the design, implementation and support of implementations.

The organisations that perform assurance will be examined in two primary categories – product development and technical assessment. Product development standards relate to the efforts performed to produce a product that conforms to quality-based standards, whilst technical

assessments are conducted to determine the actual capabilities (and vulnerabilities) of a production item.

3.4.2 Product development standards

Redacted

3.4.3 Solution architecture standards

In parallel to the product standards an assessment of any standards that are defined to assess the implementation of an ICS solution will be performed.

3.4.4 Technical assessment review

A detailed review into the tools, techniques and skills required to conduct cyber assessments of ICS products and their software. This will include details on activities such as software assessment, network stack testing, protocol fuzzing, firmware analysis and reverse engineering, and hardware attacks.

3.4.5 Assurance organisations

The requirements that must be fulfilled in order to provide assurance would be identified, incorporating all aspects of the product lifecycle.

Organisations that conduct product development standards and technical assessments will be researched and compared, and mapped to the standards identified in the previous section. Relevant organisations would be contacted for information on their ability or desire to provide ICS assurance services.

This will include organisations with the capability to test, assure and certify components and systems as well as those capable of auditing and certifying the operation of the components and systems.

3.4.6 Professional certification and training

The team will investigate the relevant training programmes, skill levels and certifications that are available in the industry.

3.5 Product assessment (Work item 3)

3.5.1 Product review

Redacted

3.5.2 Future technologies

Redacted

3.5.3 Technical assessments

Redacted

4 RISKS, ASSUMPTIONS, DEPENDENCIES AND CONSTRAINTS

4.1 Risks

Redacted

4.2 Assumptions

Redacted

4.3 Dependencies

Redacted

4.4 Constraints

Redacted

5 PROCESS TO CHANGE PROJECT SCOPE

In the event that DECC notify Thales in writing requesting a variation to the scope of the services being covered by the project, the Thales Lead Consultant will arrange for a meeting with DECC to clarify the requested changes to the scope. The Thales Technical Lead will respond to DECC in writing detailing the number of days additional effort required to address the change in scope.

6 INTELLECTUAL PROPERTY PLAN

Redacted

7 OUR TEAM AND EXPERIENCE

7.1 Thales experience

Redacted

7.2 Governance

Redacted

7.3 Our Team

Redacted

7.4 Thales customers

Redacted

ANNEX AND DISCLOSURE DOCUMENTS

PRICING REDACTED

Declaration 1: Statement of non-collusion

To: The Department of Energy and Climate Change

1. We recognise that the essence of competitive tendering is that the Department will receive a bona fide competitive tender from all persons tendering. We therefore certify that this is a bona fide tender and that we have not fixed or adjusted the amount of the tender or our rates and prices included therein by or in accordance with any agreement or arrangement with any other person.

2. We also certify that we have not done and undertake not to do at any time before the hour and date specified for the return of this tender any of the following acts:

(a) communicate to any person other than the Department the amount or approximate amount of our proposed tender, except where the disclosure, in confidence, of the approximate amount is necessary to obtain any insurance premium quotation required for the preparation of the tender;

(b) enter into any agreement or arrangement with any other person that he shall refrain for submitting a tender or as to the amount included in the tender;

(c) offer or pay or give or agree to pay or give any sum of money, inducement or valuable consideration directly or indirectly to any person doing or having done or causing or having caused to be done, in relation to any other actual or proposed tender for the contract any act, omission or thing of the kind described above.

3. In this certificate, the word “person” shall include any person, body or association, corporate or unincorporated; and “any agreement or arrangement” includes any such information, formal or informal, whether legally binding or not.

……
Signature (duly authorised on behalf of the tenderer)

……LYNN BULL…….
Print name

……THALES UK LIMITED……..…….
On behalf of (organisation name)

……12 November 2015……..…….
Date

Declaration 2: Form of tender

To: The Department of Energy and Climate Change

1. Having considered the invitation to tender and all accompanying documents (including without limitation, the terms and conditions of contract and the Specification) we confirm that we are fully satisfied as to our experience and ability to deliver the goods/services in all respects in accordance with the requirements of this invitation to tender.

2. We hereby tender and undertake to provide and complete all the services required to be performed in accordance with the terms and conditions of contract and the Specification for the amount set out in the Pricing Schedule.

3. We agree that any insertion by us of any conditions qualifying this tender or any unauthorised alteration to any of the terms and conditions of contract made by us may result in the rejection of this tender.

4. We agree that this tender shall remain open to be accepted by the Department for 8 weeks from the date below.

5. We understand that if we are a subsidiary (within the meaning of section 1159 of (and schedule 6 to) the Companies Act 2006) if requested by the Department we may be required to secure a Deed of Guarantee in favour of the Department from our holding company or ultimate holding company, as determined by the Department in their discretion.

6. We understand that the Department is not bound to accept the lowest or any tender it may receive.

7. We certify that this is a bona fide tender.

…….....
Signature (duly authorised on behalf of the tenderer)

……LYNN BULL……
Print name

……THALES UK LIMITED…….
On behalf of (organisation name)

……12 November 2015…….
Date

Declaration 3: Conflict of interest

I have nothing to declare with respect to any current or potential interest or conflict in relation to this research (or any potential providers who may be subcontracted to deliver this work, their advisers or other related parties). By conflict of interest, I mean, anything which could be reasonably perceived to affect the impartiality of this research, or to indicate a professional or personal interest in the outcomes from this research.

Signed ……  ……

Name ……LYNN BULL……..

Position ……Senior Contracts Manager

OR

I wish to declare the following with respect to personal or professional interests related to relevant organisations*;

- X
- X

Where a potential conflict of interest has been declared for an individual or organisation within a consortia, please clearly outline the role which this individual or organisation will play in the proposed project and how any conflict of interest has or will be mitigated.

- X
- X

Signed ……

Name ……

Position ……

Please complete this form and return this with your ITT documentation - Nil returns **are** required.

***** These may include (but are not restricted to);

- A professional or personal interest in the outcome of this research
- For evaluation projects, a close working, governance, or commercial involvement in the project under evaluation
- Current or past employment with relevant organisations
- Payment (cash or other) received or likely to be received from relevant organisations for goods or services provided (Including consulting or advisory fees)

- Gifts or entertainment received from relevant organisations
- Shareholdings (excluding those within unit trusts, pension funds etc) in relevant organisations
- Close personal relationship or friendships with individuals employed by or otherwise closely associated with relevant organisations

All of the above apply both to the individual signing this form and their close family / friends / partners etc.

If your situation changes during the project in terms of interests or conflicts, you must notify DECC straight away.

A DECLARATION OF INTEREST WILL NOT NECESSARILY MEAN THE INDIVIDUAL OR ORGANISATION CANNOT WORK ON THE PROJECT; BUT IT IS VITAL THAT ANY INTEREST OR CONFLICT IS DECLARED SO IT CAN BE CONSIDERED OPENLY.

Declaration 4: Questions for tenderers

In some circumstances the Department is required by law to exclude you from participating further in a procurement. If you cannot answer 'no' to every question in this section it is very unlikely that your application will be accepted, and you should contact us for advice before completing this form.

Please state 'Yes' or 'No' to each question.

Has your organisation or any directors or partner or any other person who has powers of representation, decision or control been convicted of any of the following offences?	**Answer**
(a) conspiracy within the meaning of section 1 or 1A of the Criminal Law Act 1977 or article 9 or 9A of the Criminal Attempts and Conspiracy (Northern Ireland) Order 1983 where that conspiracy relates to participation in a criminal organisation as defined in Article 2 of Council Framework Decision 2008/841/JHA;	NO
(b) corruption within the meaning of section 1(2) of the Public Bodies Corrupt Practices Act 1889 or section 1 of the Prevention of Corruption Act 1906; where the offence relates to active corruption;	NO
(c) the offence of bribery, where the offence relates to active corruption;	NO
(d) bribery within the meaning of section 1 or 6 of the Bribery Act 2010;	NO
(e) fraud, where the offence relates to fraud affecting the European Communities' financial interests as defined by Article 1 of the Convention on the protection of the financial interests of the European Communities, within the meaning of:	NO
(i) the offence of cheating the Revenue;	NO
(ii) the offence of conspiracy to defraud;	NO
(iii) fraud or theft within the meaning of the Theft Act 1968, the Theft Act (Northern Ireland) 1969, the Theft Act 1978 or the Theft (Northern Ireland) Order 1978;	NO
(iv) fraudulent trading within the meaning of section 458 of the Companies Act 1985, article 451 of the Companies (Northern Ireland) Order 1986 or section 993 of the Companies Act 2006;	NO
(v) fraudulent evasion within the meaning of section 170 of the Customs and Excise Management Act 1979 or section 72 of the Value Added Tax Act 1994;	NO
(vi) an offence in connection with taxation in the European Union within the meaning of section 71 of the Criminal Justice Act 1993;	NO

Has your organisation or any directors or partner or any other person who has powers of representation, decision or control been convicted of any of the following offences?	**Answer**
(vii) destroying, defacing or concealing of documents or procuring the execution of a valuable security within the meaning of section 20 of the Theft Act 1968 or section 19 of the Theft Act (Northern Ireland) 1969;	NO
(viii) fraud within the meaning of section 2, 3 or 4 of the Fraud Act 2006; or	NO
(ix) making, adapting, supplying or offering to supply articles for use in frauds within the meaning of section 7 of the Fraud Act 2006;	NO
(f) money laundering within the meaning of section 340(11) of the Proceeds of Crime Act 2002;	NO
(g) an offence in connection with the proceeds of criminal conduct within the meaning of section 93A, 93B or 93C of the Criminal Justice Act 1988 or article 45, 46 or 47 of the Proceeds of Crime (Northern Ireland) Order 1996; or	NO
(h) an offence in connection with the proceeds of drug trafficking within the meaning of section 49, 50 or 51 of the Drug Trafficking Act 1994; or	NO
(i) any other offence within the meaning of Article 45(1) of Directive 2004/18/EC as defined by the national law of any relevant State.	NO