SAFE, SECURE AND PROSPEROUS:
A CYBER RESILIENCE STRATEGY
FOR SCOTLAND

PUBLIC SECTOR ACTION PLAN

THE CYBER SECURITY PROCUREMENT SUPPORT TOOL (CSPST) – GUIDANCE FOR SUPPLIERS

Version 1.1

This guidance has been produced for suppliers to the public sector by The Scottish Government Cyber Resilience Unit.

Please send all comments, questions or feedback to cyberresilience@gov.scot

Scottish Government
Riaghaltas na h-Alba
gov.scot

CONTENTS

INTRODUCTION

1. The cyber security of suppliers is increasingly important to the Scottish public sector. The number of cyber attacks targeting suppliers to the public sector has grown in recent years. Attacks can (intentionally or otherwise) disrupt and damage both suppliers' services and public services. Against this background, the Scottish public sector wants to ensure its suppliers have appropriate cyber security in place. That's because:

    - We have a duty to prevent our public services from being disrupted by cyber attacks on suppliers; and

    - We want to support our suppliers to improve their cyber security, because it's good for the sustainability and resilience of our digital economy and society.

2. To help improve supply chain cyber security, the Scottish public sector is being encouraged to adopt a more consistent approach. This will involve them implementing:

    - A **Guidance Note**, which has been produced for all public sector organisations, setting out best practice from the National Cyber Security Centre (the UK technical authority on cyber security).

    - The decision-making support tool called the **Cyber Security Procurement Support Tool (CSPST)**, which all suppliers bidding for public sector contracts may be asked to use.

3. This guidance is for suppliers to the public sector who wish, or who have been asked, to make use of the CSPST tool. It provides some basic information about how to use the tool, and what its benefits are expected to be.

Important

- **Completing a CSPST questionnaire can require time and effort, depending on (i) the risk profile of a contract and (ii) how well you understand your organisation's cyber resilience arrangements.**

- **It is vital that you leave sufficient time for your organisation to complete the CSPST questionnaire ahead of any procurement deadlines.**

4. The CSPST tool itself has been designed to be intuitive to use, and includes links to guidance and advice for suppliers. You can also access a presentation on CSPST here.

Future development of CSPST

5. A public sector working group will oversee developments and improvements to the CSPST tool.

6. The Scottish Government would welcome feedback from suppliers on the CSPST tool. Please send all feedback to cyberfeedback@gov.scot.

CYBER SECURITY PROCUREMENT SUPPORT TOOL (CSPST) DECISION MAKING SUPPORT TOOL – WHAT TO EXPECT

1. This section provides information on what to expect when a public sector buyer is using CSPST to assess the cyber security of bidding suppliers.

A. HOW DOES A PUBLIC SECTOR BUYER USE CSPST TO DETERMINE THE CYBER RISK PROFILE FOR A CONTRACT?

2. Before issuing a contract notice and invitation to tender, a public sector buyer will use the CSPST tool to complete a Risk Profile Assessment (RPA) for the contract. This will generate a cyber risk profile for the contract that, in turn, generates a risk-based question set for suppliers.

   The CSPST tool's risk-based question sets align with key authoritative pieces of guidance (from the UK National Cyber Security Centre) or the key requirements of widely-used cyber security certifications/accreditations.

   Each risk profile builds on the one preceding it – so if you meet the requirements of a lower risk profile, you will already at least be on the path to meeting the requirements of a higher one.

3. The basic (unadjusted) risk profiles are:

   - Very Low (aligned with NCSC advice on the most basic cyber security requirements for organisations, as set out in the Small Business Guide and Small Charity Guide).

   - Low (aligned with the additional requirements of the Cyber Essentials standard)

   - Moderate (aligned with the additional requirements of the 10 Steps to Cyber Security)

   - High (aligned with the additional requirements of the Network and Information Systems Cyber Assessment Framework, and the ISO27001 standard).

B. INFORMATION IN THE CONTRACT NOTICE AND INVITATION TO TENDER (RISK ASSESSMENT REFERENCE NUMBER)

4. The public sector buyer should have included information in the Contract Notice and Invitation to Tender about the minimum cyber security requirements for the contract, and how to access the CSPST tool to complete a Supplier Assurance Questionnaire. The key pieces of information you should look for are:

   - The link to the CSPST tool (which can be found here).
   - The unique Cyber Risk Assessment Reference Number for the contract (which you will need in order to access the Supplier Assurance Questionnaire for the contract)
   - The full list of questions and minimum answers that will be presented in the CSPST tool, which make up the minimum cyber security requirements for the contract (so that you can familiarise yourself with these before accessing CSPST).

5. If the public sector buyer is adopting a flexible approach to suppliers meeting minimum cyber security requirements, they should also have included a template for a **Cyber Implementation Plan (CIP)**. The CIP will allow you to set out credible plans to achieve any minimum cyber security requirements that you do not currently meet, if you are awarded the contract. A CIP template can be downloaded here.

C. HOW TO ACCESS CSPST AND COMPLETE AND SUBMIT A SUPPLIER ASSURANCE QUESTIONNAIRE (SAQ)

6. As part of preparing your bid for a public sector contract, you should register for and/or login to the CSPST tool. Note that, to ensure the security of your information, CSPST uses **two factor authentication**. You will therefore need to provide a mobile phone number to be able to access CSPST.

7. You should then select the **"Complete a Supplier Assurance Questionnaire"** option on your CSPST dashboard. When promoted, input the unique Cyber Risk Assessment Reference for the contract.

8. CSPST will then lead you through all of the questions in the Supplier Assurance Questionnaire (SAQ) that are relevant to the risk profile for the contract. You should **complete these questions**, taking care to provide frank and honest answers. The answers you provide will form part of the legally enforceable terms and conditions for the contract, and may be subject to audit.

   If you are relying on third parties to provide the network/IT that will be used to deliver the contract, you may need to seek information from them about whether they comply with the minimum requirements. Some companies publish information about their cyber security arrangements, and their compliance with key standards, on their websites.

   Note that, once completed for the first time, you can **re-use the answers** for future contracts with the same, or similar, risk profiles (see "Benefits of CSPST" below).

   In addition, the number of questions you have to answer will be **reduced** if you hold certain **certifications/accreditations** (Cyber Essentials, IASME Gold and/or ISO27001).

9. Just before you submit your final answers, you will have the opportunity to **download a draft SAQ report** that will help you understand whether you meet the minimum cyber security requirements for the contract. If you need to go back and change any of your answers (e.g. because you have made an error in your submission), you should do so at this point.

10. Once you are content with all of your answers, you should complete the submission of your SAQ in the CSPST tool. You will then be provided with a **final downloadable SAQ report**. You should **download this** and **submit it with all other tender documentation**.

11. If the SAQ report shows that you do not meet the minimum cyber security requirements for the contract, and the public sector buyer have said they will accept Cyber Implementation Plans (CIPs), you should also **complete a CIP** and **submit this alongside your final SAQ report**. The CSPST tool and the CIP template make clear that the CIP must set out **clear, credible information** on:

    - the supplier's proposed actions to achieve the requirements it currently does not meet – this may include proposed **alternative mitigations or controls** to manage relevant cyber risks; and/or

- the supplier's reasoning as to why compliance with specific minimum requirements is **not necessary for the contract**; and

- in line with any requirements specified by the contracting authority in CSPST and Instructions to Tenderers, the **date or contract phase** by which the supplier intends to achieve the requirements or have in place alternative mitigations or controls.

The commitments you make in a CIP will form part of the binding contractual terms and conditions.

D. WHAT HAPPENS NEXT?

12. The public sector buyer will then assess your SAQ report (and any completed CIP) alongside all other tender documentation. Contract award will be made based on all relevant criteria in the usual way, in line with procurement regulations.

E. BENEFITS OF CSPST

13. Completing an CSPST questionnaire for the first time can take time and effort. However, as the tool is expected to be used widely across the Scottish public sector, there are some significant potential benefits for your organisation in using it.

Benefits of CSPST

- **You can expect that the questions you are asked about cyber security by Scottish public sector organisations using CSPST will be more consistent. You shouldn't be faced with multiple different spreadsheets asking questions about cyber security based on different standards.**
- **Once entered into CSPST, your answers can be re-used for contracts with the same (or similar) risk profiles for any public authority using CSPST. This can help reduce significantly the amount of time spent answering questions on cyber resilience overall.**
- **CSPST can be useful as a cost-free way of assessing to what extent your organisation currently meets the requirements of cyber security certifications and authoritative National Cyber Security Centre guidance. This is because the risk profiles broadly align with these key pieces of guidance/certifications.**
- **By ensuring your cyber security arrangements align with the authoritative sources of guidance and certification used in the tool, you can gain greater confidence that you are managing the cyber risks to your business appropriately.**

F. FURTHER HELP AND GUIDANCE

14. The CSPST tool includes links to authoritative guidance. If you need further help or guidance on cyber security, please visit:

- the Scottish Government's Cyber Resilience Advice and Resources webpage

- the National Cyber Security Centre website, which includes a wealth of valuable resources such as the Small Business and Small Charity Guides to Cyber Security, the NCSC Board Toolkit, the Cyber Essentials scheme, 10 Steps to Cyber Security, the Network and Information Systems Cyber Assessment Framework, the NCSC Exercise in a Box, NCSC Response and Recovery Guide, the Cyber Security Information Sharing Partnership (CiSP) and the NCSC Top Tips for Staff.

15. The Scottish Government and its partners have made available some key sources of support that suppliers and private and third sector organisations in Scotland can access to help improve their cyber security and resilience arrangements.

- Digital Development Loans are unsecured 0% interest loans of between £5,000 to £50,000, which can be used to improve cyber security for SMEs.

- The Digital Boost Scheme, delivered by Business Gateway, offers an online digital health check that includes consideration of organisational cyber resilience, and access to tutorials and one-to-one advice from trained advisers.

- The Scottish Government is working with the Supplier Development Programme to provide advice and answer questions to public sector suppliers, including via a number of **events** and **webinars**.

- A training guide is available here that any organisation can use to help train their staff understand the basics of cyber security.

Scottish Government
Riaghaltas na h-Alba
gov.scot

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at

The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-83960-138-5 (web only)

Published by The Scottish Government, January 2020

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS756666 (01/20)