National Cyber Security Centre
a part of GCHQ

SECURE BY DEFAULT PARTNERSHIP PROGRAMME 2017

Request for Proposal (RFP)

Reference 15262

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk

PART A - Overview

1. Thank you for your interest in the Secure by Default Partnership Programme. The main objective of the programme is to develop several strong case studies of the application of new technologies in the public sector, showing just how good we can make the usability of device whilst making sure they're secure enough and meet all the policy requirements of your organisation.

2. The technologies we're trialling aren't brand new untested technologies. They already exist in commercial products today and are fully supported by their manufacturer. However, they're new to use in much of the public sector, and their uptake has been limited. We're trying to accelerate the uptake by showing how these technologies can improve the way your staff use IT – a good case study is a great way of showcasing the benefits of the technology.

3. We're looking to assist a number of proactive organisations to adopt new technologies, learn from their experiences, and share the results of their adoption with the wider public sector.

4. In return for adopting new technologies, sharing your experiences and providing a written case study report, you'll get access to:

    a. A nominated NCSC technical expert to answer questions about the technologies, give implementation advice, and provide on-site technical support;

    b. A further £25,000 to spend on equipment, infrastructure, software licenses, support costs etc (split into 2/3rds at the start of the programme, 1/3rd at the end of the programme);

    c. Advice and guidance on accreditation and PSN compliance from nominated individuals

5. We think this is a great opportunity to get new technologies into the hands of your users, and we're looking for Government departments, local authorities, healthcare trusts, law enforcement agencies, or any other public sector organisations who would make great case studies given the above support, regardless of size or function of the organisation. If you're in a sub-team of one of these organisations that would make a good case study, then that's fine too.

6. For this round of deployments, we're looking to partner with about 4 organisations.

PART B – Why are NCSC doing this?

7. We all know the strengths and weaknesses of passwords as authenticators, and whilst alternatives are available, the world is moving very slowly to those alternatives. This means that users are frequently left frustrated by corporate password policies which require them to remember multiple complex passwords and develop their own coping strategies which frequently result in a reduction in overall security.

8. We want to accelerate the move to new approaches to solve existing problems, and are targeting specific pain points that users currently have with IT. However, in attempting to encourage the adoption of new technologies, we're invariably asked the same three questions:

    a. Who else is doing this?

    b. Will this affect my accreditation?

    c. Can I connect this technology to PSN?

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk

9. The aim with these case studies is to show that this can be done successfully in the public sector, and that there are clear business benefits to be achieved. We understand that adopting a new technology can be seen as risky when there are existing technologies that meet similar requirements, so in order to mitigate those risks, we're going to assist where possible – both in providing technical expertise, but also in providing access to our policy experts, and providing upfront funding too. The hope is that by de-risking these new approaches, we can speed up adoption of these technologies across the public sector and wider – greatly increasing the usability of IT whilst not compromising its security.

PART C – What are NCSC looking for?

10. The initial engagement requires you to be part of the public sector, as described above, and provide a proposal to us on your proposed case study. As funding is limited, we will assess certain aspects of your organisation and your situation will be taken into account in our decision on who to partner with. The decision will be based on the following high-level criteria:

    a. How the technology will fundamentally change the way the organisation, or certain business process in the organisation operate;

    b. How quickly you'll be able to start working on integrating the technology. We're not looking for overnight deployments, but we'd expect to see some movement within a few months;

    c. How much control over your IT estate you have. If there are lots of external system integrators involved in running your network, it'll slow down the rollout process (and likely make it more expensive);

    d. Evidence of trialling new things, even if those trials haven't worked out for the best;

    e. How much authority the team has to make changes to how they use IT;

    f. Experience working with, or deploying existing NCSC architectures (e.g. EUD Security Guidance, or Walled Garden Architectural Pattern);

    g. Teams with existing network architectures that would work well with these new technologies;

    h. Willingness to discuss the benefits and challenges with deploying the technologies.

11. It's worth noting that these points don't need to apply to the entire organisation you work for – if you're in a sub-team which is a good candidate for these partnerships then we'd still like to hear from you.

12. If you think you're a good candidate for building a case study of these technologies, read on to find out more.

PART D – What we want from you

13. Whilst we're making good investment in terms of time and money, there will be some onus on you to support the implementation of these technologies. We know how the technologies work, and how to implement them, but you're the experts in your existing networks and business processes. Navigating all of these is crucial to successful implementation of the technologies, so you'll definitely to provide plenty of help.

14. In short, you'll be expected to:

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk

a. Produce a plan of key milestones you'll pass in implementing the technologies, together with expected dates for meeting them;

b. Produce a plan of how you'll use the time and money investments;
c. Work with our technical experts on planning and implementing the technologies;

d. Invest some of your own time and money into the activities;

e. Produce a formal written case study of your experiences which we can share online;

f. Present the case study in a short presentation at a future event TBD (possibly CyberUK in Practice 2018).

PART E – Technologies to be showcased

15. If this scheme proves to be successful, we will expand on it and support further technologies in future. However, to begin with, we're focussing on building and documenting a demonstration of the following:

16. Alternatives to Passwords

a. Last year we focussed on a number of Microsoft technologies. This year, we're taking a wider approach and looking at the broader problem of *reducing reliance on passwords*, and inviting participants to implement some novel ways to remove or replace passwords with more usable but equally (or more) secure alternatives within their own networks.
b. For example, participants could replace passwords with
    1. Hardware-backed alternatives;
    2. Single sign on to apps and websites;
    3. Biometrics; or
    4. Nothing
c. Native security controls are very much preferred, so avoid adding third-party products to achieve these outcomes;
d. Open standards are very much preferred.
e. Some good examples of this are:
    i. Windows Hello
    ii. Touch ID (iOS)
    iii. Android Fingerprint authentication
    iv. FIDO U2F or UAF
    v. Web app single sign on
    vi. Certificate, Kerberos or Windows Hello for Business authentication
    vii. Bitlocker network unlock
    viii. Risk management policies which balance Usability vs Security

17. Existing network topology requirements

a. A remote access VPN (Ideally IKEv2 or DirectAccess, or the option to switch to either of these)

b. An internal web service supporting Single Sign On (PKI, Kerberos, or SAML)

18. Ideally you'll have a network resembling the recommended network architecture for End User Devices as detailed in the EUD Security Guidance, but this isn't a strict requirement.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk

PART F – Timetable

19. The key indicative dates for the 2017 programme are currently anticipated to be as follows:

Event	Date
Public announcement of programme	2 May 2017
Deadline for applications	30 June 2017
Partners announced	17 June 2017
Agreements signed and funding transferred	August 2017
Case study completed	1 March 2017
Organisation presents case study at future event to be determined (possibly CyberUK in Practice 2018)	Spring 2018

20. Any dates provided above are for guidance only and NCSC reserves the right to reasonably amend the timetable as it sees fit. Amendments to the timetable will be notified to the Organisations as soon as practicable.

PART G – Request for RFP, Response Proforma and Submission Instructions

21. Submission for the Secure by Default Partnership must be made by the deadline given in the table at Part F. Any Response received after the deadline will unfortunately not be opened or considered. NCSC, however, in its own absolute discretion extend the Deadline and in such circumstances will notify all Organisations that apply/have shown an interest in applying of any change in good time before the Deadline.

22. Proposals must conform to the following submission instructions:

    a. Organisations must follow the instructions for preparation of their Response contained in this section Part G (Submission Instructions). Failure to do so may result in Responses not being considered.

    b. Organisations must submit the information as defined in the Response Proforma. Responses should be concise keeping to the work count for each question.

    c. Responses using the Response Proforma and additional documents as per the Statement of Work are to be submitted via e-mail as described on the form.

    d. Organisation must provide the Response Proforma in Word format (version irrelevant).

23. No additional documentation should be submitted with the initial Response, however where referenced in a response, NCSC may ask to see these documents at a later stage. Therefore Organisations must ensure they can be made available upon request by NCSC. Organisations may also be asked to clarify their Responses, or provide more detail about certain issues.

PART H – Contact with NCSC

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk

1. Requests for further information about and clarification of this Request must be submitted to NCSC's e-mail address as follows:

   a. Name: platform@ncsc.gov.uk
2. No approach of any other kind in connection with this Request should be made to any person within, or associated with NCSC unless otherwise advised by NCSC.

PART I – Commercial

1. Organisations will be assessed in line with Part C above. Funding is limited and therefore NCSC will be assessing Responses objectively against pre-determined criteria in line with the amount of funding available.

2. In the event the Authority declines your Application, please advised this does not preclude any future engagement and shall unfortunately be due to the limited funding and effort available for this initiative.

3. Agreements will be required to be signed for the purposes of this initiative. If your organisation is a Central Government department, the Authority will provide a Memorandum of Understand (MoU) for your review and signature. If a local authority, NCSC will provide a lightweight contract for your review and signature. Regardless of this, if you have not previously engaged with NCSC (or CESG/GCHQ) then you will be required to complete a form to set up your organisation on NCSC systems. This shall enable NCSC to pay you in relation to the agreed funding, in line with the Agreement.

4. With regards to Intellectual Property (IP) created during the course of the Agreement, NCSC has no requirement to own the rights to this IP, however will require a perpetual, irrevocable, royalty-free licence at no charge to NCSC.

5. Any Agreement shall set out the following as a minimum:

   I. Definitions and Interpretations

   II. Scope and Objectives

   III. Guiding Principles

   IV. Obligations of the Parties

   V. Staff

   VI. Costs

   VII. Governance and Dispute Resolution

   VIII. Confidentiality

   IX. Intellectual property

   X. Freedom of Information

   XI. Term, Variation and Exit

   XII. Outcomes

6. If you have any queries about the Agreement subsequently provided, please e-mail Commercial.IA@gchq.gsi.gov.uk.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk