Grant Programme for Consumer IoT Assurance Schemes 2020/21: Application pack

Update 09/06/2020: Please note that the eligibility criteria has been amended to provide clarity for bidders. This grant is open for companies based in the UK who can deliver the intended grant objective in the United Kingdom and propose clear projects proposals that fit the criteria stated below. In case of a consortium of bidders the lead applicant must be based in the UK.

Content:

Applicants should read all sections carefully before applying for funding.

Section A: Objectives and context of the grant programme

A significant proportion of consumer Internet of Things (IoT) or 'smart' products currently on the market lack basic cyber security provisions. For example, 87% of IoT manufacturers reviewed in 2019 had no form of public vulnerability disclosure policy.[1] Universal default passwords, which often allow a device to be easily compromised, are still commonplace. Consumers are generally not aware of the lack of essential cyber security provisions in their IoT devices. Moreover, information about cyber security of IoT products is usually not provided to consumers at the point of sale, this is despite the fact that consumers rate cyber security as an important product feature.[2]

To address this issue, DCMS published the Code of Practice for Consumer IoT Security (CoP) in October 2018. Its 13 guidelines provide a baseline for consumer IoT products that manufacturers should embed to make them 'secure by design'. In April 2020, the European Standards Organisation ETSI published Final Draft of European Standard (EN) 303 645 on consumer IoT security,[3] and the CoP contributed to the development of this standard. DCMS is currently in the process of developing legislation to improve the security of consumer IoT devices. As announced in January new legislation will be based on certain provisions within EN 303 645 (which also align with the top 3 guidelines of the CoP).

[1] IoTSF, (2020). Consumer IoT: Understanding the Contemporary Use of Vulnerability Disclosure - 2020 Progress Report, https://www.iotsecurityfoundation.org/wp-content/uploads/2020/03/IoTSF-2020-Progress-Report-Consumer-IoT-and-Vulnerability-Disclosure.pdf

[2] Harris Interactive, Consumer IoT Security Labelling Survey Report, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798543/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report.pdf

[3] The EN is expected to be adopted in June/July 2020 following a vote by European National Standards Organisations.

This grant-making programme aims to catalyse industry take-up and implementation of cyber security good practice (as set out in the Code of Practice or the ETSI standard). We aim to do this through product assurance schemes which can play an important role in achieving good cyber security in 'smart' devices. Typically, such schemes provide consumers with an assurance label or kitemark that demonstrates that the product has undergone independent testing or a robust and accredited self-assessment process. In that way, assurance schemes can be vital in enabling consumers to make security-conscious purchasing decisions. In addition, feedback from the testing process which forms the basis of these assurance schemes can be communicated privately to manufacturers to help them improve their product.

However operating an assurance scheme for consumer IoT security can be challenging, mainly because:

- There is a broad variety of consumer IoT products, and what is considered appropriate security varies across products and their use cases. The CoP and ETSI standard necessarily contain outcome-focused provisions that provide flexibility for manufacturers to implement security solutions that are appropriate for their products.
- A software update can drastically change security risks associated with a product after it has undergone an assessment. Of course, security fixes are important in increasing security of devices and should not be discouraged.
- What is considered appropriate security may change over time as technologies and threats evolve.

<u>Objective of the grant programme</u>

The objective of this grant programme is to catalyse the development and uptake of industry-led assurance schemes for consumer Internet of Things (IoT) products. This can be achieved in a number of ways, including:

1. Increasing the number of consumer IoT products that undergo formal security assessment.
2. Ensuring that the assurance schemes available are of a high quality.
3. Ensuring that schemes are accessible and affordable to all manufacturers, including start-ups and SMEs. Self-assessment as well as external assurance should be an option for manufacturers.

An assurance scheme can achieve these objectives in a number of ways and we are open to different proposals. For example, we welcome schemes that cover the full spectrum of IoT and those that are sector-specific (e.g. just for children's toys, or just for smart TVs). Funding issued under this programme can be used to modify existing assurance schemes or to set up new ones. (Please see Section C of this pack for more detail on the selection criteria.)

Section B: Funding requirements and guidance

Demonstrative template of the Grant Offer Letter, Terms and Conditions and State Aid considerations (Declaration On De Minimis**)** is enclosed to this pack. Please note that these are sample terms and conditions and as such are subject to change before finalisation.

Grant programme management
The Secure by Design team within the Department of Digital, Culture, Media and Sport (DCMS) will run and manage the fund.

Maximum grant value
Applicants can bid for a grant worth of £170,000 at a maximum. (This is due to State Aid rules which set a maximum of €200,000 for government support.) There is £400,000 available as part of the grant programme in total. All funding must be spent by 31st March 2021.

State Aid considerations
Applicants will be required to state whether they have received any other aid funding in the past 3 fiscal years as part of the grant agreement if successful (see Annex 2 of this document for detail). As this grant funding constitutes State Aid, any amount you receive as part of this grant programme will count towards the State Aid limit. The total amount of aid funding received in this period must not exceed €200,000. If you are applying as part of a consortium, the total amount of funding you can apply for is still €200,000 per consortium, regardless of the number of companies that form the consortium.

Application criteria
Applicants must meet the essential criteria specified in Section C of this pack.

This fund is open to individual companies, or a consortium of organisations based in the UK, who can deliver the intended grant objectives in the United Kingdom and who propose clear projects proposals that fit the criteria stated below. In case of a consortium of bidders the lead applicant must be based in the UK.

Instructions for submitting bids
The grant will be open for applications from 29 May to 30 June 2020.

After reading the guidance to determine your eligibility and fit against the criteria, please write an application that reflects all of our criteria (sections 1 to 7, as outlined in Section C of this application pack) in the following format:

- MS Word or PDF file
- Font: Calibri, minimum font size 11
- Maximum page numbers for each criteria are given in Section C.

To submit your application, please send your word document to securebydesign@culture.gov.uk, adding “GRANT APPLICATION” to the subject line. Any applications received after the closing date will not be assessed. All available information

and guidance relating to this round of funding is contained within this document. The Secure by Design team can answer questions related to the grant application process. However, as the application process is competitive, we are unable to provide any support in completing the application.

Timeline:

- Applications will be assessed and due diligence will be performed by July 2020.
- All applicants will be informed whether or not they have been successful by the end of July 2020, grant award letters (grant agreement) will be signed following this.
- The first meeting with successful bidders will be held in August 2020 and subsequent meetings will be held on a regular basis. These will be agreed with grantees in advance.
- **All funding must be spent by 31st March 2021.**

Definition of IoT products:

We define consumer IoT products as network-connected (and network-connectable) devices and their associated digital services that are used by consumers, typically in the home or as electronic wearables. See ETSI EN 303 645 for more detail.

Evaluation and learning

Applicants are expected to produce a final report detailing what the funding has been used for, the work that has been done and impact delivered during the funding period (i.e. FY20/21) and share this with DCMS. See Section C for more detail.

Financial requirements

1. The DCMS financial year runs 1st April to 31st March. All funds awarded through this grant **must** be spent by 31st March 2021. If successful, your formal grant award letters (grant agreement) will set out the total amount of grant we will pay.
2. The grant award must not exceed 50% of your annual income/turnover or collective annual income/turnover if you are applying as a formal consortium.
3. All applicants will be expected to clearly set out a proposal for how much funding will be drawn down each month.You will need to support this with a detailed budget breakdown. Your drawdown requests and budget must fit the DCMS financial year.
4. Payments will be made monthly or quarterly (subject to agreement). You will need to provide a breakdown and evidence of actual, eligible expenditure in order to make a claim. We will only pay out the amount you can evidence as spent.
5. If you believe there is a clear and compelling reason to be paid at the point of need (e.g. to manage cash flow pressures), there is opportunity in the application form to set this out. Your request will be considered as part of the assessment process and subsequent due diligence but will not, in itself, disadvantage your application.
6. If your application and point of need request are approved you will be expected to provide evidence of the need (e.g. through cash forecasts) and subsequent monthly reconciliations for the duration of your project. The reconciliations (with supporting evidence) will be required before any further funding is released and will detail how funds received have been spent, identifying any underspend that may have arisen. You will also be required to complete a formal Financial Reconciliation Statement

(FRS) form at the end of the financial year. This will be provided by DCMS to evidence all appropriate spend against eligible grant activity.

7. You must be able to carry out performance and financial reporting in at least monthly intervals until the end of the funding period (i.e. 31 March 2021) and performance reporting in at least quarterly intervals until the end of the project period (i.e. 31 March 2022) and provide evidence of expenditure on the use of grant funds. Funds must be shown as restricted funds in your accounts and you must be able to identify separately the value and purpose of the grant in your audited accounts. You will be asked to describe the financial management systems and processes you will put in place to ensure you can achieve this in your application.

Usage of grant funding

Grant funding must not be spent on:

- Debts or loans
- Projects outside our funding priorities
- Retrospective funding
- Business as usual activities
- Anything not covered by the objectives of this grant programme
- Payments reimbursed or to be reimbursed by other public or private sector grants

Applications from consortia

Applications from consortia should be submitted only once, by the lead partner organisation. Please note that DCMS is unable to award a grant to multiple organisations so the lead partner would be responsible for distributing funding through an invoicing arrangement and managing working relations with other partners. The lead partner is the responsible body based in the UK, who will share the grant award letters (grant agreement) and ensure that the terms and conditions of the grant offer are upheld by all parties involved.

Multiple applications

Applicants can make a maximum of two applications. Applications as part of a consortium bid, either as a lead or non-lead, will count as one of your allocated amount. You must submit a separate, stand-alone application for each project.

If you are submitting more than one application (including consortium bids), please specify which is your preferred one. In the event of a large volume of applications, we reserve the right to consider your specified preferred application.

Evaluation and monitoring

We are committed to ensuring that funded work is appropriately monitored and evaluated and that lessons learnt and examples of good practice are made widely available; data collection and monitoring should be built into every application.

Applicants will be expected to list anticipated outputs, outcomes and impacts, and to explain the data collection and monitoring systems that will be put in place to enable these to be evidenced, in order for projects to be properly evaluated by DCMS. Applicants are also

expected to produce a final report detailing what the funding has been used for, the work that has been done and impact delivered during the funding period (FY20/21) and share this with DCMS.

Grantees are expected to participate in any evaluation or research work commissioned by DCMS regarding the grant scheme. This could include DCMS commissioning an external research provider to conduct an impact evaluation of the grant scheme, with grantees required to supply the research provider with relevant data and to actively participate in the research. Grantees are also required to submit regular monitoring information to DCMS and/or DCMS' appointed research provider.

What to expect from DCMS if you are successful?

- We will carry out a detailed due diligence check, which may involve requests for further information and initiate the financing process.
- Successful applicants will be asked to reconfirm the amount of funding requested.
- We will send a grant award letter (grant agreement) with specific terms and conditions.
- The monitoring process will be agreed before funding is awarded.
- We will work with successful applicants to send out a press release (or any other relevant comms).

What checks are you expected to undergo?

Your organisation will also need to pass our due diligence checks which ensure:

- You are registered with the Charity Commission and / or Companies House website and have filed all required returns.
- If you have been funded by another part of Government, we seek feedback from that department.
- You are not already receiving funding for this project from Government, meaning your project is funded twice.
- That there is no indication of fraud, DCMS do not tolerate fraud, bribery or corruption. Applications will be checked against various databases to assess accuracy of the information provided. Post event evaluation and assurance will also be carried out and any instances of fraud or misappropriation of funds uncovered will result in a request for clawback of funding, and/or may lead to civil or criminal proceedings to recover monies.
- We expect applicants to provide clarity on additional questions raised through an internal due diligence processes.
- Whether your organisation is already receiving, has received or will receive funding that will exceed the overall State Aid funding limit past €200,000 over 3 years. You will be asked to complete a self-declaration (see Annex 2 for details).

Section C: Assessment criteria and scoring

Key terms and timelines

Grant programme	DCMS initiative to support industry-led consumer IoT security assurance schemes by issuing multiple grants.
Funding period	Period in which DCMS can issue grant funding. This begins upon signing of the grant award letters (grant agreement) and ends on **31 March 2021**. The grantee is required to provide monthly updates on performance and finances throughout this period. (Whilst unlikely, DCMS reserves the right to extend that period.)
Project	Project proposed by a bidder (or consortium of bidders) for which funding is sought. This can involve setting up a new or improving an existing assurance scheme.
Project period	The project runs from the signing of the grant award letters (grant agreement) until **31 March 2022**. The bidder is required to provide regular performance updates, at least quarterly, to DCMS throughout the project period. (The project period is a year longer than the funding period because we expect that for many proposed projects that most of the impact will be realised after March 2021.) It is important to note that funding will only be provided until 31 March 2021 and grantees **must** spend any funding by then.
Impact	Benefits, and disbenefits, expected to be realised by the project throughout the project period, which lasts until 31 March 2022.
Output	Output and activities delivered within the funding period (until **31 March 2021**).

DCMS will select bids in the following process:

- Step 1: Bids will be scored against the criteria set out below (criteria 1-7).
- Step 2: We will consider the full set of bids that we have received and, if necessary, make choices that avoid market fragmentation. To enable this we will group bids we deem to be similar in the same category (e.g. covering the same specific consumer IoT category, such as children's toys or smart TVs, or resulting in competing consumer-facing labels etc.). This means that only one bid from each category may be chosen and that the successful bids may not necessarily have the highest overall scores.

1. **Essential Criteria**

Each of the following criteria must be met by applicants to qualify for funding. Please confirm this in your application, providing evidence where necessary.

1. The assurance scheme is for consumer IoT products or one category of consumer IoT (e.g. just for children's toys, or just for smart TVs).
2. The entity bidding must be based in the UK. In case of a consortium of bidders, the lead applicant must be based in the UK.
3. The entity bidding (or all entities that are part of a joint bid) can deliver the intended grant objectives in the UK.
4. The majority of products assessed by the assurance scheme are intended for the UK market. This is to ensure that the majority of impact will be delivered in the UK.
5. The assurance scheme is based on the UK Code of Practice for Consumer IoT Security and/or Final Draft EN 303 645 v2.1.0, or a subset thereof (e.g. the Top 3 guidelines of the Code of Practice). Assurance schemes can also require additional measures than those set out in the above documents. (This requirement is to help counteract market fragmentation.)
6. Grant funding will only be used for activities that would otherwise not be carried out. (Funding can be used to improve/expand schemes that are already in development or operating, but it must not be used to support "business as usual" or for activities that would be funded via other means).
7. The bidder commits to providing DCMS with regular financial and performance updates as set out in Section B. The format of this reporting will be agreed by both parties in advance.
8. Bidding organisations must have at least some experience in designing and/or operating a consumer product assurance scheme or a cyber security assurance scheme. This includes either experience with product assurance and/or self-assessment. Please provide brief evidence.

2. Impact expected to be achieved with grant funding

- Applicants should include a detailed description of the overall **impact** the project will deliver (referring to the objectives of the grant programme where appropriate) and how this will be achieved. Particular emphasis should be placed on the **output** that is expected to be delivered within the **funding period (until 31 April 2021)**.

Achieving the desired impact may be done in multiple ways, including, but not limited to:

- Increasing the number of consumer IoT products that are expected to undergo assurance (please break up estimates per quarter). If your assurance scheme is already operating, please state the number of products that have undergone assurance in FY19/20 and the number of *additional* products that will undergo assurance as a result of this funding.
- Increasing the quality of assurance outcome (e.g. through better assessment or better tailoring to specific consumer IoT category).
- Ensuring adequate accessibility (including affordability) and facilitating greater take-up.

3. Assurance scheme design

- Explain in detail how the scheme will be developed or expanded and how the

scheme's design/delivery will help achieve the expected **impact.** Please include, as required:

1. The assurance output (e.g. the type of products your assurance scheme will be testing).
2. The assurance outcome (e.g. manufacturer receiving detailed feedback that helps them improve their products or establishment of a consumer-facing label that will help inform consumers' purchasing decisions).
3. Description of how you plan to provide the service to manufacturers and the assurance method (e.g. self-assessment, one-off 3rd party evaluation, continuous 3rd party evaluation).
4. The use of assurance levels (specified in terms of functional, process or testing requirements) for different risk profiles, if appropriate.
5. Quality control measures for the scheme (e.g. regular spot-testing of products that have undergone assurance, monitoring and responding to abuse of assurance logos or markings).
6. Articulation of risks and appropriate mitigations to set up/expand a successful consumer IoT security assurance scheme.
7. Explanation of how your scheme will relate to other national and international schemes and how mutual recognition will be handled.

4. Organisation's capacity and capability to deliver the proposal

1. Experience of internal and external staff that will deliver the **project** and the size of the team that will be delivering the project (Evidence will be requested later that these *are* the staff that will work on this project).
2. Access to resources needed to deliver the **project impact** (e.g. established relationship with testing houses, access to labs/other facilities if needed).
3. Evidence of delivering similar projects in the past and their outcomes delivered against initial targets or evaluation criteria.
4. Provide examples of how you are planning to encourage uptake of your scheme and your expectation as to the size of the uptake by the end of funding period and beyond.
5. The capacity to evaluate outputs and outcomes on a regular basis according to the project plan and provide regular reporting to DCMS throughout the **project duration.**

5. Project sustainability following the end of the funding period (31 March 2021 - March 2022)

Evidence of the ability to achieve the **project impact**, as well as any other long-term impact, once the **funding period** has ended (31 March 2021 - March 2022). That can include:

1. Financial and other resources that will be available after March 2021 until March 2022.
2. Long-term business plan for assurance schemes, which should include detailed plans for delivering **impact** after the **funding period** (applicants can refer to the objectives of the grant where appropriate).
3. Articulation of risks and appropriate mitigations to set up/expand a successful consumer IoT security assurance scheme.

6. Monthly project and financial plan

Applications should include:

1. Detailed monthly project plan including milestones. This must cover the **output** that is expected to be delivered within the **funding period**, and any

activities that are necessary beyond **March 2021** to achieve the expected overall project **impact**.

2. Detailed monthly financial plan over the funding period, setting out what the grant funding would be used for. Please align this with the DCMS financial year.
3. Identify your key performance indicators (KPIs) to achieve the **impact**.
4. Please describe the financial management systems and processes you will put in place.

7. Amount of funding

In this section, applicants should state:

1. Amount of grant funding requested. It should be noted that applicants are not allowed to bid for more than £170,000 due to State Aid considerations.
2. If you intend to submit a point of need request, please state so in this section.
3. Any cash match-funding offered by the bidder.
4. Please provide information on the steps you will take to achieve cost-effectiveness and efficiency throughout the project.

Criteria scoring overview

Criteria	Criteria weighting	Maximum number of pages
1. Essential criteria	Pass/Fail	1
2. Impact expected to be achieved with grant funding	20%	4
3. Assurance scheme design	20%	4
4. Organisation's existing capacity and capability to deliver the proposal	20%	2
5. Project sustainability following the end of the funding period (31 March 2021 - March 2022)	10%	2
6. Monthly project and investment plan	10%	2
7. Amount of funding	20%	1

Each question response will be evaluated and marked on a scale of 0-4 where:

0 – Serious concerns: e.g. application does not meet requirements, and/or raises serious concerns
1 – Minor concerns: e.g. application meets some requirements but with gaps and/or some minor concerns
2 – Adequate confidence: e.g. application meets most/all requirements, but lacks sufficient detail or evidence in some areas
3 – Good confidence: e.g. application meets all requirements and provides a detailed response but lacks evidence in minor areas
4 – Excellent confidence: e.g. application meets all requirements, provides a detailed response and evidence which demonstrates a particularly strong understanding of the requirements.

Your score will be determined by the marks awarded for each criteria (out of 4), in accordance with the applicable weighting.

For example, if the weighting for a question is 20%, a mark of 4 for that question would lead to a score of 20%. A mark of 3 would lead to a score of 15%, a mark of 2 would lead to a score of 10%, a mark of 1 would lead to a score of 5%, and mark of 0 would lead to a score of 0%.

The Department reserves the right to reject any bidder who scores ‘0’ in any of the questions, and/or achieves an overall score of less than 50%.