Cabinet Office
70 Whitehall London SW1A 2AS

Dame Meg Hillier
Chair, Public Accounts Committee
House of Commons
SW1A 0AA

14 December 2022

Dear Chair,

I am writing to you in relation to recommendation 2 of the Thirtieth Report of the 2021-22 Session of the Public Accounts Committee, on 'Challenges in implementing digital change'.

The recommendation asked for the Central Digital and Data Office (CDDO) in Cabinet Office to "*work with departments and map legacy systems across government to document what is there, why it exists, how critical it is and to use this to produce a pipeline of legacy systems prioritised with milestones for action.*" The report recommended that we share this pipeline with the Committee.

Since the Committee published its report and recommendations, CDDO has established a programme of work focused on mapping legacy systems in order to prioritise remediation activity. The programme has engaged strategically and built relationships with Department for Work and Pensions (DWP), HM Revenue & Customs (HMRC), Home Office, Ministry of Justice (incl HM Courts & Tribunals Service), Department for Environment Food & Rural Affairs, and Department for Education, understanding the exposure to legacy risk, their asset estates, and the frameworks and data gathering mechanisms they have in place. Our assessment of HMG departments is that these organisations comprise the bulk of the legacy estate.

In order to map and assess the criticality of legacy related risk across multiple government departments we have devised a single common framework, which has been developed with departments utilising existing legacy frameworks and industry models.

To assess legacy IT, assets have been judged by departmental experts using two components of risk: 1) the impact of legacy system failure; including impact on national security, financial impact, impact on public services and reputational damage and; 2) the likelihood of failure, which may result from issues including ageing unsupported software, an associated diminishing skilled workforce capable of maintaining it, and security vulnerabilities etc.

Departments we have engaged with are aware of their legacy estate and are actively managing it. There are several examples of best practice where systems with a high potential impact from system failure are being managed effectively to ensure a very low likelihood of failure, resulting in a low overall risk criticality. Departments are also looking at the legacy problem more broadly;

investing in the underlying infrastructure (cloud, networks and security etc), devices and applications.

From this initial data collection, information on over 100 of the most critical and vulnerable assets across six departments have been obtained.

A list of the top 20 most critical and vulnerable legacy assets and their responsible departments is included in the annex.

Key themes identified in the analysis performed with the current draft information include:

Causes of critical legacy systems

The priority factors contributing to the vulnerability of legacy assets are:

1. Software currency - the assets contain software which has already gone out of support or it is highly likely they will become out of support in the next 3 years.
2. Security - the assets either have known security vulnerabilities or a very high likelihood that they exist.
3. Fitness for purpose - the assets either are currently not meeting business needs or have a high likelihood they will not in the next 3 years.
4. Expertise - the availability of skills capable of maintaining and supporting legacy assets is likely to diminish over the next 3 years.

Legacy funding plans

All of the current top 20 highest-risk assets have established and funded risk mitigation plans to reduce their legacy risk over the next three years: there are 11 cases which have funded plans due to be completed by end FY 23/24 with a further 7 expected to be mitigated the following year. All funded plans are expected to complete by the end of FY 25/26.

CDDO will continue to engage with departments, iterating and building upon the current set of departmental data and monitoring the presence of remediation plans. It has also established a funded plan to investigate options to improve the currency of the data collected through software automation. This program looks to work with an industry partner to prototype the software infrastructure to automatically elicit this data directly from departments that can support this capability. CDDO will use this data to populate a risk framework dashboard and keep track of HMG legacy more accurately and updated more frequently than can be done at present.

I trust that this provides a satisfactory overview of our work to address legacy IT issues.

Yours sincerely,

Alex Chisholm
Permanent Secretary for the Cabinet Office

Annex A - List of top 20 legacy assets in criticality order

Dept.	Asset Name	Whether the plan is funded	Planned risk mitigation period (financial year)
DWP		Yes	FY 23/24
HMCTS		Yes	FY 23/24
HMRC		Yes	FY 24/25
HMRC		Yes	FY 23/24
HO		Yes	FY 25/26
HO		Yes	FY 24/25
HO		Yes	FY 25/26
HMRC		Yes	FY 23/24
HMCTS		Yes	FY 23/24
HMCTS		Yes	FY 23/24
HMCTS		Yes	FY 23/24
HMCTS		Yes	FY 23/24
HMCTS		Yes	FY 24/25
HMRC		Yes	FY 23/24
HMCTS		Yes	FY 24/25
HMCTS		Yes	FY 23/24
HMCTS		Yes	FY 23/24
HO		Yes	FY 24/25
HO		Yes	FY 24/25
HMRC		Yes	FY 24/25