



National Cyber  
Security Centre

a part of GCHQ

---

# Early access to OBR Economic and Fiscal Outlook: NCSC analysis and technical recommendations



## Executive summary

In November 2025, the Economic and Fiscal Outlook (EFO) from the Office for Budget Responsibility (OBR) became available online ahead of its expected official release on the day of the Budget 2025.

Following the OBR's December 2025<sup>1</sup> report led by Baroness Sarah Hogg and Dame Susan Rice into how early access to the EFO occurred, the National Cyber Security Centre (NCSC) – a part of GCHQ – was tasked to conduct a further investigation, as per a key recommendation from that report.

The terms of reference of the immediate investigation for the December 2025 report focussed on how the early access to the market sensitive EFO happened. This investigation sought to further understand the scale of the access. The scoping questions for this investigation are set out in page 4 of this report. The report from December 2025 was reviewed as part of this investigation.

The findings and recommendations in this report are based on the NCSC's best understanding following discussions with the OBR, HM Treasury, Professor Ciaran Martin (as expert advisor from the December 2025 report), detailed log analysis, and a review of options to prevent this occurring again. As part of this investigation, the NCSC did not conduct any further technical analysis such as forensic analysis of servers used to host the EFO.

---

<sup>1</sup> [Report of investigation into the November 2025 Economic and fiscal outlook publication error](#)

## Findings and recommendations

- › The NCSC agrees with the December 2025 report that there appears to be nothing to evidence that the premature access to the report was the result of hostile cyber activity, connivance, or someone pressing the publication button too early.
- › The NCSC agrees with the December 2025 report that this incident occurred because of a misconfiguration of the way in which WordPress was implemented.
- › Due to additional logging data for the cached content delivery service that was not available to the OBR in the time frame of the rapid investigation for the December 2025 report, the scale of the access to the November 2025 EFO is much greater than originally thought. The original report identified 43 downloads whereas the additional logs identify at least 24,701 downloads. This includes new logging data that showed repeated unsuccessful attempts to access the EFO from one IP address on the 25<sup>th</sup> November 2025 until it successfully accessed the report on 26<sup>th</sup> November at 11:35.
- › The NCSC agrees with the December 2025 report on what occurred in advance of the March 2025 EFO publication. Misconfiguration of WordPress enabled early access to that report. New logging data showed that there were 16 successful accesses of the EFO report rather than one in the December 2025 report. All these accesses came from the same service provider. While there was previously a suggestion that the early access in March was from within a public sector organisation, given the logs available to the NCSC, there is nothing in there that provides strong evidence that this was the case.
- › Due to the unavailability of log data greater than 12 months prior, it was not possible to investigate EFO publications before March 2025. We therefore cannot rule out the possibility that there was early access of EFO publications from before March 2025.
- › From a technical perspective, to prevent this incident being repeated, the NCSC recommends that future market sensitive publications such as the EFOs should be published on GOV.UK.
- › The NCSC recommends that all government departments and arm's length bodies (ALBs) conduct a review to ascertain whether any information should be regarded as market sensitive and if so, ensure publication on GOV.UK.

## Contents

Executive summary.....	1
Findings and recommendations.....	2
Introduction .....	4
Caching Infrastructure .....	6
User Agents .....	7
Timeline of November 2025 event.....	8
March 2025.....	13
EFO publications in the period preceding March 2025.....	13
Causes of the event.....	14
Options for future publications.....	16
Option 1 - Use existing OBR website technology.....	17
Option 2 - Use external third party to host report .....	19
Option 3 - Replace the OBR website.....	20
Option 4 - Utilise GOV.UK.....	21
Recommendation for future EFO publications.....	22

# Introduction

The NCSC was tasked by Laura Gardiner, Chief of Staff at the OBR to perform an investigation of potential early access to the OBR's Economic and Fiscal Outlook (EFO) publications. This investigation was in response to a key recommendation from the December 2025<sup>2</sup> report led by Baroness Sarah Hogg and Dame Susan Rice that further analysis to their report should be performed.

The investigation performed by the NCSC forms part of a wider Budget Information Security review commissioned by James Bowler, Permanent Secretary to His Majesty's Treasury (HMT).

## **The scoping questions provided by OBR for this investigation were:**

- › Review the findings and diagnosis of the original review
- › A further probe into any early access to the March 2025 EFO publication
- › A probe into EFO publications in the period preceding March 2025
- › A fuller picture of what happened around the November 2025 Budget

The NCSC was also asked to consider options on how to prevent this for future market sensitive EFO publications.

The NCSC's role in this investigation, and approach to answering the scoping questions provided by the OBR, was limited to the provision of cyber security advice and investigation of technical logging data provided to it by the OBR. This activity was carried out under the NCSC's statutory remit to provide advice and assistance on the protection of information pursuant to section 3(1)(b)(ii) of the Intelligence Services Act 1994 (ISA). The NCSC is part of the Government Communications Headquarters (GCHQ), and the statutory functions of GCHQ are set out in section 3 of ISA.

Given this, in accepting the investigation, the NCSC agreed with the OBR that analysis would focus on the data available and no further data would be actively acquired e.g. no forensic examinations of the servers used to host the EFO.

To assist with this investigation the NCSC met on several occasions with OBR, HMT, and Professor Ciaran Martin<sup>3</sup>, who was one of the expert advisors for the December 2025 report. In these meetings the NCSC were made aware by Ciaran and HMT that more log files existed than were originally available for the December 2025 report. These additional log files were not available at the time because the OBR did not own the logs and had to request them through their third party hosting provider. The NCSC requested the OBR to supply the original log files as well as the additional log files that were previously

---

<sup>2</sup> [Report of investigation into the November 2025 Economic and fiscal outlook publication error](#)

<sup>3</sup> Professor Ciaran Martin was the NCSC's Chief Executive Officer from 2016 - 2020

unavailable to the OBR. The analysis for this report has been performed only on the log files provided.

**The log files supplied were:**

- › File transfer logs (SFTP) from the 26th to 27th November 2025
- › Account activity logs for the WP Engine service from the 15th October to 27th November
- › Web server logs for the file OBR\_Economic\_and\_fiscal\_outlook\_March\_2025.pdf for the 26th March 2025. This log file was previously unavailable to the OBR.
- › Web server logs for the file OBR\_Economic\_and\_fiscal\_outlook\_November\_2025.pdf for the 25th and 26th November 2025. This log file was previously unavailable to the OBR.
- › Audit file showing which themes and plugins were installed on the WP Engine server hosting the OBR site on the 26th March 2025
- › Audit file showing which themes and plugins were installed on the WP Engine server hosting the OBR site on the 26th November 2025
- › A log file of OBR website article publishing activity from the 8th June 2010 through to 27th November 2025
- › A log file of article editing logs for the OBR website for the 27th November 2025

All dates and times in this report are presented as UTC.

## Caching Infrastructure

The OBR website is hosted by a US company called WP Engine and uses the WordPress software platform. To support large numbers of users visiting WP Engine-hosted websites, the content delivery service Cloudflare is used to cache copies of webpages from their websites. This means that when a user requests a webpage, a copy is supplied from the Cloudflare cache, rather than from the original WP Engine website.

Cloudflare runs a large, distributed network around the globe of these caching servers which ensures that large numbers of users can access websites concurrently. Caching also speeds up access to websites, since the user's device only needs to communicate with the geographically closest Cloudflare server.

It is the NCSC's understanding that OBR have a contractual relationship with WP Engine and not with Cloudflare, and that Cloudflare are contracted by WP Engine.

When a request is made for a webpage that the caching server does not have, it sends a request to the origin website for that webpage and, if the request is successful, the caching server stores a copy of the webpage for a period of time. Cloudflare operate many caching servers. The exact functionality of the different servers is unknown, but it is standard practice that cached webpages may persist in a caching server for some time after the first request. The caching servers will periodically check that the webpage is still accessible from the original server, but this is not done on every request (this could cause the origin server to be overloaded and would delay requests from being serviced until the origin server could respond). As well as caching webpages, Cloudflare also provides the functionality for caching files hosted on those websites, like the files which were hosted on the OBR website.

In cases like this, where a file is purposely taken offline, a direct customer of Cloudflare would need to log into their Cloudflare administration dashboard and perform a purge of the specific page from the Cloudflare cache in order to ensure that all the systems in the global cache would immediately stop serving the stored copy and check for a new copy from the origin website. There is evidence of the OBR attempting to clear local caches for the OBR site at 12:02 and 12:08 on the 26<sup>th</sup> November using the WP Engine dashboard, to purge the file. As described above, this would not have been successful on clearing the global cached file on the content delivery service.

## User Agents

When a web browser (such as Google Chrome, Microsoft Edge or Apple Safari) requests a webpage from a web server, data is sent to the web server with information about the request. One of the pieces of data sent is a “User Agent”. This is a string of text which is used to identify the piece of software being used to request the page to allow the server to modify the response based on what the software can display. User Agent references can be useful in fault finding.

As an example, a common User Agent string is “Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36 Edg/143.0.0.0”. This User Agent includes details such as the operating system and version of the software being used. This User Agent also highlights that the browser is most likely Microsoft Edge, version 143.

It is worth noting that User Agent strings are not validated by the web server, and it is possible to configure web browsers; or other software accessing webpages, to send anything as the User Agent, so they are indicative of the browser used but there is no guarantee that those details are trustworthy.

An unusual User Agent seen across multiple webpage requests could indicate that the same device, configured in the same way, was used for all the requests.

## Timeline of November 2025 event

The log data available to the NCSC has been used to review the timeline of events on Wednesday 26<sup>th</sup> November in section 1.13 of the December 2025 report (as set out in the left column). Our review is based on the log analysis only, and as such any other part of the timeline where we have not been able to confirm, does not suggest that it is untrue. The NCSC findings from the log analysis to the timelines for the 26<sup>th</sup> November as set out in that report are as follows:

Event and timestamp	NCSC notes
<p><b>05:10</b> – The website host emailed OBR staff to confirm that server modification to accommodate higher website traffic at the time of EFO publication was complete.</p>	<p>As this information is not contained in the logs, the NCSC cannot confirm this from the log data available to us.</p>
<p><b>05:16</b> – Website activity logs show the earliest request on the server for the URL <a href="https://obr.uk/docs/dlm_uploads/OBR_Economic_and_fiscal_outlook_November_2025.pdf">https://obr.uk/docs/dlm_uploads/OBR Economic and fiscal outlook November 2025.pdf</a>. This request was unsuccessful, as the document had not been uploaded yet. Between this time and 11:30, a total of 44 unsuccessful requests to this URL were made from seven unique IP addresses.</p>	<p>Analysis of the full log data, not available to the original report, shows that download attempts for the file started at 15:22:06 on the 25<sup>th</sup> November. Prior to the file being uploaded there were 534 requests from ten unique IP addresses. Analysis of User Agent data in the logs shows six different browsers were used in attempts to access the file before it went live. In total there were eleven unique combinations of User Agent and IP addresses seen (one IP address showing two different User Agents). 520 of the 534 requests used the same User Agent (a relatively unusual one) and came from four of the IP addresses (according to the logs available, all four of these IP addresses are from the same Internet Service Provider). This User Agent requested the page between once a minute and once every 90 seconds from 16:24:10 25<sup>th</sup> November until the file was uploaded on the 26<sup>th</sup> November. The activity was paused for 5 hours 19 minutes from 23:57 on the 25<sup>th</sup> and for 3 hours 45 minutes from 05:25 on the 26<sup>th</sup>. Given this evidence, it is highly likely that the 520 requests were performed by an automation of some kind.</p>
<p><b>09:00 onwards</b> – The web developer set up webpages (no PDFs, Excel spreadsheets, or other documents were uploaded during this stage) in draft form in the content management system,</p>	<p>As this information is not contained in the logs, the NCSC cannot confirm this from the log data available to us.</p>

<p>creating IDs for all the downloads to be used across the website.</p>	
<p><b>11:02</b> – PDF documents were emailed to the web developer, including the EFO document.</p>	<p>As this information is not contained in the logs, the NCSC cannot confirm this from the log data available to us.</p>
<p><b>11:03–11:53</b> – The other supporting documents and files were sent to the web developer. 25 files were to be published in total.</p>	<p>As this information is not contained in the logs, the NCSC cannot confirm this from the log data available to us.</p>
<p><b>11:30–11:35</b> – The web developer began uploading documents to the draft area of the OBR website (which was understood by all involved to be not publicly accessible), including the EFO PDF.</p>	<p>As this information is not contained in the logs, the NCSC cannot confirm this from the log data available to us.</p>
<p><b>11:35</b> – The first successful request to the internet address (URL) <a href="https://obr.uk/docs/dlm_uploads/OBR_Economic_and_fiscal_outlook_November_2025.pdf">https://obr.uk/docs/dlm_uploads/OBR_Economic_and_fiscal_outlook_November_2025.pdf</a> was made. The IP address of this first successful request had made 32 previous unsuccessful attempts at this URL over the course of the morning. There was a total of 43 requests to this URL that were successful between this time and 12:07, from 32 unique IP addresses.</p>	<p>The first full download of the file occurred at 11:35:17 from one of the IP addresses which was used by the User Agent that had performed 520 of the 534 unsuccessful requests prior to the file being uploaded. Between this time and 12:07:15 when the file was renamed, there were 20,547 successful full downloads (Status code 200) and 2,125 successful partial downloads (Status code 206) of the file. 10,762 unique IP addresses fully downloaded the file.</p>
<p><b>11:41</b> – The first evidence online of the EFO being publicly available, via a Reuters news alert entitled: <i>'UK OBR ECONOMIC AND FISCAL OUTLOOK: BUDGET TAX RISES RAISE 26.1 BLN STG BY 2029–30'</i>.</p>	<p>The NCSC cannot confirm this from the log data available to us, however open-source research can show this is when it first appeared. For reference at this stage the log analysis tells us there was 13 successful downloads of the file, (two of which are previews, from Teams &amp; WhatsApp)</p>
<p><b>11:43</b> – An OBR staff member was first made aware by a (non-Reuters) journalist that Reuters was flashing extensive forecast details.</p>	<p>As this information is not contained in the logs, the NCSC cannot confirm this from the log data available to us.</p>

<p><b>Around 11:50 onwards</b> – Images of and facts from the EFO began appearing widely online from many people (suggesting the PDF had been widely downloaded, and/or shared by other means after download).</p>	<p>The log data suggests that the page was widely shared in a variety of ways. Many applications generate thumbnails of shared webpages. This process causes the application to retrieve the webpage and often uses a user agent, which can enable you to identify the application. Given this, analysing the User Agent strings in the logs, the following applications can be identified as retrieving the EFO PDF. The numbers indicate the number of times this User Agent was seen prior to the end of the Chancellor’s speech at 13:38:</p> <p><b>Social media:</b>  Mastodon: 138  BlueSky: 57  Facebook: 39  X: 28</p> <p><b>Messaging applications:</b>  WhatsApp: 298  Snapchat: 52  Microsoft Teams: 35  Discord: 17  Slack: 5  Telegram: 3  iMessage: 137</p>
<p><b>11:52</b> – Senior OBR and Treasury officials telephoned each other to discuss the breach. These Treasury officials made OBR staff aware of the URL leading to the PDF of the EFO that was accessible.</p>	<p>As this information is not contained in the logs, the NCSC cannot confirm this from the log data available to us.</p>
<p><b>11:53</b> – OBR staff and the web developer attempted to pull the PDF from the website, and also to pull the entire website (e.g., via password protection), but struggled to do so initially due to the website being overloaded with traffic.</p>	<p>Logs show that the password protection was enabled on the site at 12:00:54 and disabled at 12:14:36. Enabling password protection does not seem to have blocked users from accessing the file, possibly due to the caching service in place.</p>
<p><b>11:58</b> – An email was received to the OBR press inbox from a Reuters journalist confirming that Reuters had published details of the EFO and asking for comment.</p>	<p>As this information is not contained in the logs, the NCSC cannot confirm this from the log data available to us.</p>

<p><b>12:07</b> – The EFO PDF was renamed by the web developer.</p>	<p>The NCSC can confirm that the EFO PDF file was renamed at 12:07. Requests for the file from the origin website were unsuccessful after 12:07:15. Requests continued to be successful from the caching service at a diminishing rate – 1,869 requests for the file were successful (Status code 200 – indicating the entire file was requested and successfully returned) between this point and the EFO PDF being restored at 16:28:30. Due to the way that the caching service worked, a number of requests were being successfully serviced through until 16:16:20 (just 128 of the 1,869 successful requests were after 13:00). There were no successful requests after 16:16:20 before 16:28:30 when the EFO PDF was restored.</p> <p>Logs indicate that in addition (at 12:02:44 and 12:08:33) requests were made to clear the Content Delivery Network cache of the OBR site. This does not appear to have been immediately successful but from 12:08 onwards the numbers of successful requests drop substantially with fewer than 10 successful requests per minute against several hundred denied requests. Total requests peak at 12:24 with 7173 request that minute, of which four are successful. 161,999 requests were made for the EFO PDF file which were unsuccessful in the period between 12:07:15 and 16:28:30.</p>
<p><b>12:07</b> – The EFO PDF appeared on the Internet Archive. This means it was, at that precise time, visible entirely generally on the open internet via search engines. It is assumed that this happened very briefly in the rush to remove it.</p>	<p>As this information is not contained in the logs, the NCSC cannot confirm this from the log data available to us.</p>
<p><b>12:08</b> – The EFO PDF was removed from the website’s content management system, taking it offline.</p>	<p>As this information is not contained in the logs, the NCSC cannot confirm this from the log data available to us.</p>
<p><b>12:08</b> – The OBR Chair and staff drafted a statement setting out briefly what had happened and confirming that the OBR’s website was the source of the error.</p>	<p>As this information is not contained in the logs, the NCSC cannot confirm this from the log data available to us.</p>

<p><b>12:15</b> – This statement was posted on the front page of the OBR’s website, and on X (formerly Twitter).</p>	<p>As this information is not contained in the logs, the NCSC cannot confirm this from the log data available to us.</p>
<p><b>12:34</b> – The Chancellor’s Budget statement began, opening with a reference from the Chancellor to the early release of the OBR EFO.</p>	<p>As this information is not contained in the logs, the NCSC cannot confirm this from the log data available to us. However, open-source research confirms this.</p>
<p><b>13:38</b> – The Chancellor’s statement ended and the EFO and supporting documents were immediately pushed live.</p>	<p>As this information is not contained in the logs, the NCSC cannot confirm this from the log data available to us. However open-source research confirms this.</p> <p>For reference, by this time, there had been 22,347 successful full downloads of the EFO PDF. Of those, 984 are likely to be automated services requesting the file (such as preview generator for social media services or services taking a copy for search engine purposes or for archival purposes). The remainder are likely to be requests by real users. It is not possible to determine exactly how many individuals accessed the EFO PDF prior to the Chancellor’s statement ending but an approximate lower bound would be 14,110. This is based on unique User Agent and IP Address combinations. Users could however have accessed the PDF from multiple devices (hence with different User Agents) from the same IP address which would cause an overestimate of the count. Multiple users could also have accessed the PDF from the same IP address with identical software on different devices (such as in an office where all computers have the same version of a web browser installed) which would cause an underestimate of the count. Direct sharing of the PDF (e.g. as an email attachment) would not be captured in these numbers.</p>
<p><b>16:29</b> – The online version of the EFO PDF was updated with a correction slip at the front, after approval of these corrections by the House of Commons Journal Office.</p>	<p>According to the logs available to the NCSC, the EFO PDF became available again to visitors of the website at 16:28:30</p>

## March 2025

Paragraph 3.4 of the December 2025 report states “Indeed, a brief examination of online traffic prior to the March 2025 EFO indicates one successful attempt to secure pre-publication access to that EFO five minutes into the Chancellor’s Spring Statement speech on 26 March. There is no indication of any activity following this access, and at the time of going to press Professor Martin concludes the most likely explanation is benign. However, it illustrates that the problem exposed last week was not a new one. We could not, in the time available, carry out deeper forensic examination of other recent EFO events and we recommend that such an exercise is, with expert support, now urgently carried out.”

**NCSC Note:** From the original and additional logs available to NCSC, it is possible to identify 16 requests for the March EFO PDF prior to the end of the Chancellor’s Spring Statement. These requests occurred between 12:38:10 and 12:49:13. All the requests came from IP addresses belonging to the same service provider. Three different User Agents were identified. One of the User Agents relates to the generation of a thumbnail of the website generated by WhatsApp. This User Agent generated three requests. It is reasonable to infer that the URL was sent in three separate WhatsApp messages in the time frame prior to the embargo expiring. It is not possible from the log data available to NCSC to suggest that the early access in March 2025 came from an IP Address of a public sector organisation.

## EFO publications in the period preceding March 2025

Given the lack of availability of any relevant logs for EFO publications preceding March 2025, it is not possible to investigate these events. This means we cannot rule out there could have been early access to EFO publications before March 2025.

## Causes of the event

The NCSC agrees with the December 2025 report that there appears to be nothing to evidence that the premature access to the report was the result of:

- › Hostile cyber activity by foreign actors or cyber criminals
- › Connivance by anyone working for the OBR
- › Pressing the publication button too early on a locally managed website

The NCSC agrees that the cause appears to have been pre-existing configuration errors.

From the logs available to the NCSC, it has been possible to identify that the OBR website was running on the WordPress platform hosted by WP Engine, a US company, and that the platform had the Download Monitor (PRO) plugin installed.

Investigating the documentation for WP Engine, this does not seem to be a default feature of the WP Engine service and must have been explicitly installed at some point (research using the Internet Archive suggests that it was in place from at the latest January 2023 based on the links shown in the archive conforming to the format of the plugin).

Online research identifies Download Monitor as an extension to the WordPress platform from WPChill, a Romanian developer. Download Monitor can be used to add restrictions to downloads, such as time windows during which downloads can occur. In the default setup, Download Monitor does not expose the actual file of a download, and all requests are proxied through the application, enabling it to enforce the restrictions placed on the download.

One side effect of this is that users cannot view PDF files served by Download Monitor in their browser but are forced to download them and open a local copy. To support users' preferences to view PDFs more easily, Download Monitor supports an option called "Redirect to file". The documentation for this option mentions that "Enabling Redirect to file on PDF files will in most cases allow the user to view the PDF in the browser". However, the same documentation also warns "Enabling Redirect to file will expose the actual file URL, allowing users to bypass Download Monitor and share the direct file URL."

The fact that users could access the direct file URL is one of the underlying reasons why it was possible for users to download the EFO PDF prior to the embargo.

From the logs, this is how the Download Monitor installation for OBR's website was configured. Making this change necessitated reconfiguring the underlying security model of the website (making the download monitor uploads folder world readable) leading to the true location of the EFO files being available to anyone on the internet.

The change may have been made to enable users to view PDF documents more easily in their browser or to support the caching system used by the site to support times of heavy usage.

There are no logs available to the NCSC which would identify when this configuration change was made. However, as the December 2025 report stated that the procedures followed for the November 2025 EFO were the same as those for previous publications, it is likely that this configuration change has been enabled for quite some time.

## Options for future publications

Paragraphs 3.8 and 3.9 of the December report set out the need for a full review of OBR publishing operations and that “the process for publishing the EFOs (normally two times a year) should immediately be removed from the locally managed website and conducted in an environment more appropriate to the nature of the task”.

The NCSC has considered what options exist for future OBR website publications, including market sensitive EFO reports. The main consideration was in relation to cyber security and technical configuration. Other non-technical considerations (e.g. accessibility, independence of the OBR publication etc) which the OBR will need to additionally consider were not part of this work.

There are four options that were considered:

- › Use existing OBR website technology
- › Use external 3<sup>rd</sup> party to host report
- › Replace the OBR website
- › Utilise GOV.UK

All options require thorough testing and through-life support. Acknowledging that the OBR does not have a dedicated IT function, the NCSC recommends a solution which is secure by default and has a low ongoing maintenance requirement for the OBR.

## Option 1 – Use existing OBR website technology

As noted already, the current OBR website is a WordPress site that uses various plugins. This option focuses on uplifts to the existing platform, and is therefore the quickest and cheapest option, however it also provides the least robust end state with limited real-time visibility of events. It is likely to have a high ongoing support burden, due to having to continually re-evaluate the security posture of the system.

By sticking with the existing technology, there are three further options:

- › 1a – Disable the ‘Redirect to File’ feature
- › 1b – Use an alternative WordPress plugin
- › 1c – Create a publishing pipeline

### 1a – Disable the ‘Redirect to File’ feature

As noted earlier, the existing OBR website uses the “Download Monitor WordPress plugin with the “Redirect to File” option enabled. This means the file opens in the browser, rather than prompting the user to download it.

The steps required for this option are:

- › Disabling the “Redirect to File” feature, ensuring the configuration reverts to original install, alongside using the time-controlled publishing feature built into Download Monitor would appear to provide the desired functionality.
- › Testing would be required to confirm that this protects against direct URL access prior to publishing. This could be combined with a more complete penetration test, from a recognised company.

**Pros:** This is the lowest impact modification which appears to solve the problem. No new tools for admins to learn.

**Cons:** This option is considered high risk, as it relies on the security of the WordPress plugin, and any bugs within it may result in inadvertent information disclosure. Ongoing testing would be required prior to each publication, to ensure changes (patches, updates) to the software have not changed the relied-upon functionality. Additionally, it has no technical control against an administrator accidentally setting an incorrect publish date. This change requires the report to be downloaded which degrades usability of the site.

### 1b – Use an alternative WordPress plugin

A brief search of available WordPress plugins shows there are those available which would appear to provide the desired functionality (timed release of a PDF). One of these alternatives could be used to schedule publication.

It is worth noting that for the purpose of this report the NCSC has not performed any investigation as to the functionality or security properties of these plugins.

The steps required for this option are:

- › Identify an available plugin that contains the desired functionality. As the OBR uses a managed WordPress site, consideration should be given as to whether the plugin is supported on the platform.
- › Perform testing to ensure it operates as intended.
- › Ongoing support and maintenance of the functionality should also be considered.

**Pros:** Likely low impact and low cost.

**Cons:** This option is considered high-risk, as it relies on the security of the WordPress plugin, and any bugs within it may result in inadvertent information disclosure. Ongoing testing would be required prior to each publication, to ensure changes (patches, updates) to the software have not changed the relied-upon functionality.

### **1c - Create a publishing pipeline**

An automated publishing pipeline could be created, which would automatically publish the report to the website at the appropriate time.

This would operate on an internal (not publicly accessible) system, where the report would be uploaded and held, and at the appropriate time would upload the report to the public website using the REST API provided by the hosting software currently in use.

It is not clear whether a software product already exists which provides this functionality, or whether something bespoke would have to be developed. Development is anticipated to be a relatively small project.

The steps required for this option are:

- › Identify an appropriate software development team, which would be required to create, deploy and test this pipeline. This is likely to require external contractor effort.
- › Ongoing support and maintenance of the functionality should also be considered.
- › This option gives no consideration to whether the internal network would require any additional testing, such as penetration testing, as this is assumed to be covered by existing arrangements.

**Pros:** Improved security due to report remaining on internal network (presumably where it is written) until publication time.

**Cons:** New capability, which would require development, hosting, maintenance and funding. Ongoing requirement for support and testing. Would require functional testing before each event to ensure proper operation. Additional training required for administrators.

## Option 2 – Use external third party to host report

The OBR's process today is to host the EFO report within the same hosting environment as the main website. Therefore, the security controls of the OBR hosting platform apply to the report. An alternative to this is to host the file elsewhere, such as on a service offered by a cloud provider. This is a common pattern (although primarily used for scale/bandwidth reasons).

Examples of suitable products include Amazon Web Services' "S3" service, and Microsoft Azure Storage. Both have appropriate access controls, which are widely used across Government and the private sector for publishing information. By moving the hosting of the report to a third party site, this would mean well-understood security controls are used for the report. A similar user experience is likely to be able to be achieved as the existing site.

However, the admin interfaces of these third party products are likely to be more complex than the current provider, and therefore misconfiguration is possible.

The steps required for this option are:

- › Identify a suitable third party provider to host the report
- › Utilise the existing OBR website, and its publishing mechanism, to publish a webpage containing a link to the EFO report
- › Test third party controls with a time-sensitive release. Note that the access control of the third party site must be changed at publication time, otherwise the problem has simply been moved.

**Pros:** Relies on industry-standard access control. May improve scaling (timeline mentioned additional work done by existing hosting provider to increase capacity).

**Cons:** Additional complexity of new interface for administrators, increasing risk of inadvertent disclosure through misconfiguration. Additional cost/contracting of second provider. Reduced resilience by relying on two providers to host the site/report.

## Option 3 – Replace the OBR website

Develop a replacement to the OBR site on a new platform, designed to meet the needs of the organisation. This platform would follow Government’s Secure by Design and GovAssure processes.

As technology is not a core function and the publication process is event-based for the OBR, maintaining internal expertise and focus to run an effective Secure by Design process and achieving GovAssure outcomes will likely be challenging without support from another government department or commercial provider.

The December 2025 report suggests there is an existing independent.gov.uk platform that should be considered as it meets the needs of other similarly independent units and organisations. Following consultation with the Government Digital Service (GDS), we have learnt that independent.gov.uk is not a single platform with its own publishing capability; rather, it is a shared domain name, with multiple independently operated websites. As such, the NCSC does not believe this would provide a viable alternative to the existing site.

Depending on the likelihood that similar organisations (including sites under independent.gov.uk) are carrying similar risks, it may be worth exploring whether the creation of a new common hosting platform for use by ALBs, designed to meet the desired security outcomes, would be achievable for the level of spend available. A suitable organisation to manage this platform would need to be identified.

The steps required for this option are:

- › Investigate any “lessons learned” from the development of sites such as GOV.UK.
- › Engage suppliers capable of developing, hosting, and maintaining a new website.

Perform suitable testing (including penetration testing) of the new hosting solution.

**Pros:** The design of the new hosting can consider all requirements. May have wider impact, if other independent bodies could also benefit.

**Cons:** This is likely to be a significant undertaking, requiring a large ongoing investment. Extremely unlikely to complete in time for the next EFO Report.

## Option 4 – Utilise GOV.UK

The GOV.UK platform is designed and regularly used to publish complex embargoed sensitive document sets. This platform is likely the one most aligned to the relevant requirements without creating a bespoke site and is utilised by other ALBs.

The GDS operate the hosting of GOV.UK. There is a suite of publishing tools through which Government departments can administer their own section of the site, with features like scheduled publication built in. GOV.UK is designed to be secure and resilient, and should not increase the support, maintenance or testing burden of OBR.

This option proposes replacing the OBR website with hosting on GOV.UK. This would provide the necessary controls around secure publishing of the EFO report and maintain all the OBR content in one location. However, given the possible complexity of migrating the existing site, this option could be used in conjunction with Option 2, with GOV.UK acting as the “third party” (as an alternative to utilising a commercial third party).

The steps required for this option are:

- › Work with the GDS to obtain space on GOV.UK.
- › Migrate report (and possibly whole OBR site) across to GOV.UK.

**Pros:** Stable mature platform, built to meet similar use-cases. Part of a managed central service. Cost reduction to OBR if whole site is migrated from current hosting.

**Cons:** Migration of whole site would require significant effort to align to the data model and layout of GOV.UK. Partial migration (of only report) may degrade user experience.

## Recommendation for future EFO publications

After a review of the available options, the NCSC recommends proceeding with Option 4 – utilise GOV.UK for future market sensitive publications such as the EFOs. This platform is designed to handle this exact use case, and the security of it is well understood.

Options 1a and 1b are considered by the NCSC to be too high risk. These rely on the security of the (unverified) WordPress plugins, and simple software misconfiguration may continue to cause inadvertent disclosure. Options 1c, 2, and 3 would vastly increase the support burden, and likely require a larger IT team than OBR currently has resourced to manage the systems, and wider cyber risk.

It is acknowledged there is a large one-time effort required to transition the OBR's website to GOV.UK. If the complete transition is not possible due to resourcing or complexity, the combination of Option 2 and Option 4 (external hosting of the report on GOV.UK) should also be considered. This would provide the necessary security to the EFO report, whilst minimising the impact on the OBR's team of editors and site administrators.

Any of the options should be supplemented with a level of functional testing, to verify the correct operation of the selected solution. Additionally, it is recommended that supplementary monitoring is added during an event, to detect if the report file is inadvertently accessible and allow early remedial action to be taken.

The NCSC also recommends that all government departments and ALBs conduct a review to see if they hold and publish any market sensitive information outside of GOV.UK. If they do, then the NCSC recommends that Option 4 be applied as a priority to prevent this occurring elsewhere.

© Crown copyright 2026. Photographs and infographics may include material under licence from third parties and are not available for re-use. Text content is licensed for re-use under the Open Government Licence v3.0.

(<https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>)