Freedom of Information Act 2000 (FOIA)

Decision notice

Date: **16 June 2020**

Public Authority: **Department for Work and Pensions (DWP)**
Address: **4th Floor**
Caxton House
Tothill Street
London
SW1H 9NA

Decision (including any steps ordered)

1. The complainant has requested information about the Universal Credit programme and its information technology systems.

2. The DWP relies on sections 22 (future publication) and 31(1) (a) (prevention of crime) to withhold the requested information.

3. The Commissioner's decision is that DWP incorrectly relied on section 22, but correctly relied on 31(1) (a), to withhold the requested information.

4. The Commissioner requires the public authority to take the following steps to ensure compliance with the legislation.

    - The requested information withheld by reference to section 22 is to be released to the complainant.

5. The public authority must take these steps within 35 calendar days of the date of this decision notice. Failure to comply may result in the Commissioner making written certification of this fact to the High Court pursuant to section 54 of the Act and may be dealt with as a contempt of court.

Background

6. On 8 March, 2012 the Welfare Reform Act 2012 received the Royal Assent and introduced the framework of Universal Credit.

7. The Universal Credit aimed to simplify the benefits system by moving from the then current benefit structure to a simple streamlined payment. People's benefits were to be withdrawn at one unified rate. The plan was to migrate recipients from their current benefits and tax credits systems onto the Universal Credit starting in 2013 and finishing in the next Parliament[1].

8. The Universal Credit Programme Board acts as the programme's main oversight and decision-making body. The main purpose of the UC Programme Board is to provide advice and support to the Universal Credit Director General, who is accountable for the delivery of Universal Credit.

Request and response

9. On 6 September 2018, the complainant wrote to DWP and requested information in the following terms:

    - RFI1: Since 01 January 2016 has the UC programme been subjected to any reviews by the Infrastructure and Projects Authority ("IPA") (e.g. PARs, Gateway Reviews, health checks etc)? If so please disclose any reports produced by the IPA as a result.

    - RFI2: Since 01 January 2016 has the UC full service IT system been the subject of any assessments, health checks or tests by any external organisations (excluding the IPA)? If so please disclose any reports produced by those organisations as a result.'

10. The DWP responded on 02 October 2018. It stated as follows:

    - The Department holds the information you are seeking. However, Section 22 of the Freedom of Information Act exempts this information from disclosure. This is because the information is intended for publication at a future date".

[1] https://www.gov.uk/government/news/universal-credit-introduced

11. Following an internal review the DWP wrote to the complainant on 09 November 2018. It maintained its reliance on section 22 to withhold the requested information.

12. On 20 June 2019, the DWP informed the complainant that it had changed its position on external reviews related to the UC IT system. It no longer intended to routinely publish those reviews. The section 22 exemption therefore was no longer applied to that part of the complainant's request. However, it told the complainant, it was now withholding this information on the basis of the provisions contained in sections 31(1) (a) which covers the prevention of crime. The utilisation of section 31(1)(a) is to prevent criminal attacks targeted at the IT system being facilitated by the information contained in the reports.

Scope of the case

13. The complainant contacted the Commissioner on 14 November 2018 to complain about the way his request for information had been handled.

14. The Commissioner considers she has to determine whether the DWP correctly relies on section 22 to withhold the requested information regarding UC programme reviews and section 31(1) (a) to withhold the requested information regarding UC IT system "health checks".

Reasons for decision

Request 1

"Since 01 January 2016 has the UC programme been subjected to any reviews by the Infrastructure and Projects Authority ("IPA") (e.g. PARs, Gateway Reviews, health checks etc)? If so please disclose any reports produced by the IPA as a result".

15. The DWP has informed the Commissioner that the following information is in scope of the complainant's first request for information.

12/09/2016 – 15/09/2016 The Infrastructure and Projects Authority (IPA) Health Check – this has already been published in the House of Commons library[2]

[2] http://data.parliament.uk/DepositedPapers/Files/DEP2019-1052/Infrastructure_and_Projects_Authority_Health_check.pdf

02/03/2017 – 03/03/2017 The Infrastructure and Projects Authority (IPA) Action against the Plan (AAP) – publication scheduled for 2020

04/09/2017 – 07/09/2017 The Infrastructure and Projects Authority (IPA) Health Check - publication scheduled for 2020

06/03/2018 – 09/03/2018 The Infrastructure and Projects Authority (IPA) Independent Review of UC Full Business Case - publication scheduled for 2021

16. Section 22(1) provides that –

'Information is exempt information if-

(a) the information is held by the public authority with a view to its publication, by the authority or any other person, at some future date (whether determined or not),

(b) the information was already held with a view to such publication at the time when the request for information was made, and

(c) it is reasonable in all the circumstances that the information should be withheld from disclosure until the date referred to in paragraph (a).'

17. This exemption is also subject to the public interest test. So, in addition to demonstrating that section 22 of the FOIA is engaged, the public authority must consider the public interest arguments for and against disclosure and demonstrate that the public interest in favour of disclosure is outweighed by the public interest in favour of maintaining the exemption.

18. The DWP confirmed that the Universal Credit Programme had a settled intention to publish Infrastructure and Projects Authority (IPA) Performance Assurance Reviews (PARs). This approach was agreed as part of the Universal Credit transparency approach since the early work to publish Universal Credit Programme Board papers in March 2018.

19. Neil Couling, the Universal Credit Senior Responsible Owner (SRO), wrote to the Information Commissioner in August 2018 and said:

"I have considered our broader position in terms of the release of UC Programme papers going forward and strongly believe that any record of

our discussions relating to the safe delivery of Universal Credit can only be helpful in building public confidence".

20. Under this strategy, the September 2018 PAR health check will be published (i.e. placed in the House of Commons library) in September 2021.

21. The Commissioner accepts that the DWP, as expressed by its chief executive Neil Couling, had an intention (expressed in 2018) to publish the UC programme reviews.

22. The Commissioner needs to be satisfied that in all the circumstances of the request it is reasonable to withhold the information until the date of publication. The Commissioner cannot say that the decision, in the particular circumstances, to publish the information at a later date by the DWP is not reasonable. The Commissioner therefore finds the exemption is engaged.

23. Though the exemption is engaged the Commissioner must consider the public interest arguments for and against disclosure and determine in this case whether the public interest in favour of disclosure is outweighed by the public interest in favour of maintaining the exemption.

24. The DWP identified that there are enduring public interest arguments that favour releasing information. In particular, in promoting government transparency and accountability. Additionally, openness will generally allow for more informed debate on Universal Credit issues and increase trust in the quality of public administration, particularly associated to large Government projects and programmes.

25. Regarding the public interest factors for maintaining the exemption it says it was worth noting that it is committed to publishing PAR reports 3 years after the date of the report. The effectiveness of IPA reviews is dependent on them receiving candid assessments of projects from civil servants. Though the IPA does not attribute views to individuals, interviewees may be less frank if there was an expectation of the report being published imminently.

26. Early publication of the reports will have a debilitating effect on the Programme's ability to move forward and the capacity of the SRO and the UC management team to focus on what is necessary to make progress. There is a wealth of detail in PAR reports with comments on structures, constructs and issues. Publishing that detail is bound to generate enquiries that will distract the UC management team.

27. It is a mistake to assume that simply because there is a press team that burden will fall on them. They are not project specialists capable of interpreting the archive. Follow-up enquiries, which it expects to be

voluminous will swamp UC managers both in terms of explanation and then in clearing lines for publication or answering Parliamentary questions and preparing for debates.

28. IPA reviews are an external assurance mechanism to provide the SRO with the assurance that the project is on track to deliver. The Universal Credit Programme has a publication strategy to routinely release the content of IPA review reports.

29. It is reasonable to permit government departments to release routine project review reports at regular intervals after the review date. This approach balances the need to prioritise resources to address key project priorities with the need to divulge the detail of project review findings to contribute to the improvement of wider project management approaches across government.

30. In the early days of the Universal Credit Programme, there was an argument that there was limited public information about the UC Programme. This is now no longer the case. There is now copious information on the performance of the Universal Credit Programme already in the public domain.

31. The Commissioner is troubled by the DWP submissions regarding the application of the public interest test. In that the submissions are made without evidence to support the assertions that civil servants will be less frank and such will be the reaction upon releasing the information that its UC managers will be swamped with enquires.

32. At the time of this decision the Infrastructure and Projects Authority (IPA) Health Check (2016) had already been published in the House of Commons library. It would be remiss of the Commissioner not to note that it appears to have attracted little attention from the media. The Commissioner not being able to discern any newspaper articles where the said report has been referenced.

33. In the absence of evidence, regarding the adverse effects of releasing the withheld information prior to its intended date of publication, the Commissioner is not persuaded that the public interests favours maintaining the exemption. The Commissioner, of course, takes cognisance (as did the DWP) of the enduring public interest factors that favour releasing the withheld information. Namely, it will promote government transparency and accountability. Additionally, as correctly identified by the DWP, releasing the information will generally allow for "more informed debate on Universal Credit issues and increase trust in the quality of public administration, particularly associated to large Government projects and programmes".

34. After considering the varying competing factors, the Commissioner's decision is that the public interest in favour of disclosure is clearly not

outweighed by the public interest in favour of maintaining the exemption. The information withheld by reference to section 22 should therefore be released to the complainant.

Request 2

•Since 01 January 2016 has the UC full service IT system been the subject of any assessments, health checks or tests by any external organisations (excluding the IPA)? If so please disclose any reports produced by those organisations as a result.'

35. Section S31(1)(a) states

(1) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be

likely to, prejudice—

(a) the prevention or detection of crime;

36. DWP position is that the release of the IT security and vulnerability reports requested would be likely to prejudice prevention of crime and, because of the nature of the information included in the types of reports requested, it would put DWP systems, a part of the Critical National Infrastructure, at increased risk of successful attack. Any resulting breach or compromise would seriously undermine public trust, put delivery of public services at risk and potentially entail substantial cost in corrective actions.

37. Security reports of the type being requested detail technology or process vulnerabilities or weaknesses that would enable an attacker of the type detailed below to exploit and compromise the service. Impacts are assessed that range from significant personal data losses, resulting in claimant distress through financial hardship and possible identity theft; to increased departmental web enabled fraud leading to increased monetary losses. Widespread and longer term compromises or denial of service could also result in a degradation in confidence in the welfare system and possible civil unrest.

38. Cyberspace lies at the heart of modern society; it impacts our personal lives, our businesses and our essential services. A secure online environment is essential to HM Government, which is providing an ever-increasing number of online services to UK citizens and businesses as part of a major digital services transformation programme.

39. The ability to conduct online transactions securely is central to the delivery of public and commercial services and communications. However, some individuals and groups use cyberspace for malicious

purposes. These 'hostile actors' exploit cyberspace to conduct espionage operations or launch damaging computer network attacks.

40. Since 2010, the Government has categorised major cyber-attacks on the UK and its interests as a top-tier threat to national security. This means that such an attack is highly likely and/or would also have a high impact. The impact of technology, and especially of cyber threats, was identified as one of the four "particular challenges … likely to drive UK security priorities for the coming decade" in the 2015 National Security Strategy and Strategic Defence and Security Review 2015 (2015 NSS & SDSR). Its importance was reaffirmed by the Government's National Security Capability Review in March 2018.

41. The past year has seen cyber-attacks on the health, telecommunications, energy and government sectors in the UK and although the UK has yet to suffer the most severe form of cyber-attack—which the Government defines as an attack leading to the sustained loss of essential services, severe economic or social consequences, or a loss of life, the head of the National Cyber Security Centre (NCSC), Ciaran Martin, has said this is a matter of 'when', not 'if'.

42. The May 2017 WannaCry attack, which affected NHS services for several days, should serve as a stark warning of the implications of such an attack for national security.

43. Given the Government's emphasis on cyber threats in the 2015 National Security Strategy & Strategic Defence and Security Review, as well as the string of high-profile cyber-attacks in 2016 and 2017, the joint committee overseeing protection of the UK's Critical National Infrastructure decided to launch an inquiry into the cyber security of critical national infrastructure (CNI) as the first inquiry of the 2017 Parliament.

44. The joint committee of the UK's Critical National Infrastructure issued a report in 12/11/18. This report included the following assessment of the likelihood of cyber-attacks.

45. In the two years since the Government's National Cyber Security Strategy 2016–2021 (the 2016 NCSS) was launched, more than 1,000 cyber-attacks have required the involvement of the NCSC—an average of ten a week. Although most of these will not have affected the UK's CNI, these figures do include the May 2017 WannaCry attack, which affected NHS services, as well as attacks on the UK and Scottish Parliaments in June and August 2017, and on the energy and telecommunications sectors. The past year has also seen the Government start to make joint or co-ordinated announcements with other countries that publicly attribute major attacks to other states. The

most noteworthy of these in relation to CNI was the Technical Alert released jointly with the United States in April 2018, which disclosed Russia's "sustained presence in UK and US internet infrastructure".

46. However, while states continue to be the dominant actors behind cyber threats to the UK, the DWP believes that their behaviour and apparent motivations are changing. The Cabinet Office notes that states are "starting to explore offensive cyber capabilities to damage, disrupt or destroy the systems or networks of their adversaries", whereas previous campaigns had tended to focus on espionage and IP theft.

47. Ciaran Martin singled out Russia as being particularly problematic in this regard, citing "a consistent rise in [its] appetite for attack on critical sectors" and its 'prepositioning' for future disruptive attacks. Referring to the joint Technical Alert released with the United States in April, he explained that Russia has established a foothold [in the UK's internet infrastructure], an intrusion that you can use for ongoing espionage purposes or can develop as the potential for a hostile, disruptive and destructive act in the future.

48. He added that Russia has also begun to diversify its targets, for example to include "softer power democratic institutions". North Korea has similarly changed its approach, moving from "political retaliation attacks"—by attacking Sony Pictures in 2014, for instance—to "the theft of money", through ransomware attacks such as WannaCry and reportedly stealing more than $81 million from the central bank of Bangladesh in February 2016 via the SWIFT payments system.

49. It is also clear that states are no longer the only actors with the ability and resources to attack CNI, which generally benefits from more advanced defences than other parts of the economy. Ciaran Martin averred that we have seen an evolution of cybercrime, where some of the most sophisticated attackers [such as organised crime groups] are now operating at almost nation-state level. A range of experts have provided additional evidence of these threats.

50. The cyber threat to the UK's CNI is growing. It is also evolving: hostile states are becoming more aggressive in their behaviour, with some states—especially Russia—starting to explore ways of disrupting CNI, in addition to conducting espionage and theft of intellectual property. Furthermore, while states still represent the most acute and direct cyber threat, non-state actors such as organised crime groups are developing increasingly sophisticated capabilities.

51. Fast-changing threats and the rapid emergence of new vulnerabilities make it impossible to secure CNI networks and systems completely. Continually updated plans for improving CNI defences and reducing the potential impact of attacks must therefore be the 'new normal' if the

Government and operators are to be agile in responding to this changing environment and in taking advantage of constant technological innovation. Building the resilience of CNI to cyber-attacks in this way will make it harder for an attacker to achieve their objective—whoever that attacker may be, whatever their motive and however they choose to attack.

52. This evidence illustrates that the threat of a cyber security attack on DWP systems, including the Universal Credit system, is a real and significant risk. Against this security assessment DWP officials need to ensure that systems are secure and vulnerabilities are identified.

53. The reports requested in this FOI request are part of DWP's efforts to support the National Security Strategy and are specifically designed to identify system vulnerabilities. Publication of these reports could reveal system vulnerabilities and expose DWP systems to cyber-attack and further technical scrutiny, which might create additional vulnerabilities.

54. As the joint committee of the UK Critical National Infrastructure reports, significant attacks have already been made against National Infrastructure and this confirms that the threat of a cyber-attack against DWP's Universal Credit system is more than a hypothetical possibility.

55. Release of the requested reports, will provide a potential attacker with key information on system weaknesses and increase their capability to compromise the service. This will likely increase the ability to commit fraud through identity theft. Additionally, compromising key security features will reduce the Department's capability to detect and defend against criminal activities.

56. The arguments above illustrate that DWP IT systems are an integral part of the UK's Critical National Infrastructure. As such, for example, their misuse could potentially lead to the failure to pay benefits to over 2 million people which could in turn lead to civil unrest or facilitate the risk of monetary fraud.

Commissioner's Analysis

57. In order for a prejudice-based exemption, such as s31(1)(a) to be engaged, the following criteria must be met:

• the actual harm which the public authority alleges would, or would be likely to, occur if the withheld information was disclosed has to relate to the applicable interests within the relevant exemption;

• the public authority must be able to demonstrate that some causal relationship exists between the potential disclosure of the information being withheld and the prejudice which the exemption is designed to

protect. Furthermore, the resultant prejudice which is alleged must be real, actual or of substance; and

• it is necessary to establish whether the level of likelihood of prejudice being relied upon by the public authority is met – i.e. disclosure 'would be likely' to result in prejudice or disclosure 'would' result in prejudice.

58. The relevant applicable interests cited in this exemption are the prevention or detection of crime.

59. With regard to the first criterion of the three limb prejudice test described above the Commissioner accepts that potential prejudice to law enforcement activity, which the DWP alleges would be a consequence of disclosing the requested information, relates to the interests which the exemption contained at section 31(1)(a) is designed to protect. In that releasing the withheld information could theoretically lead to, or bring about, prejudicing the prevention or detection of crime.

60. The Commissioner next considered whether the DWP had persuaded her that some causal relationship exists between the potential disclosure of the information being withheld and the prejudice which the exemption is designed to protect. And, if so, whether the resultant prejudice which is alleged is real, actual or of substance.

61. The DWP has persuaded the Commissioner that releasing the withheld information would be likely to prejudice the prevention or detection of crime. In that the Commissioner accepts that releasing the withheld information, which is deemed to be a worldwide dissemination, would be likely to aid those who would commit criminal acts against the DWP IT systems. In this context the Commissioner takes cognisance of the fact that those who would attempt to unlawfully access the DWP IT systems would include those ranging from the inept to the most accomplished and this includes state actors. Accordingly it would mean that a suite of information, with all its dangers (both known and unknown), is placed in the hands of the most adroitly skilled "hackers". This when combined with information already known or accessible to malicious actors, persuades the Commissioner that releasing the withheld information would be likely to prejudice the prevention or detection of crime and the harm that would be likely to be done could be extreme

62. The Commissioner for the reasons above finds the exemption engaged.

63. Section 31(1) is a qualified exemption and therefore subject to the public interest test set out in section 2(2)(b) of FOIA. The Commissioner has therefore considered whether in all the circumstances of the case the public interest in maintaining the exemption outweighs the public interest in disclosing the withheld information.

64. The DWP identified the following public interest arguments in favour of releasing the withheld information;

- Open government, freedom of information and data innovation are all dependent on a transparent approach to information management.

- Transparency is important to improved public services. Public reporting of data promotes higher quality and more efficient services, choice and accountability.

- Open data is seen as the key to opening up government and driving economic growth. It is in the process of creating and embedding a culture of transparency across DWP.

65. The DWP identified the following public interest arguments in favour of withholding the withheld information;

- The past year has seen cyber-attacks on the health, telecommunications, energy and government sectors in the UK and, the head of the National Cyber Security Centre (NCSC), Ciaran Martin, has said this is a matter of 'when', not 'if'. The May 2017 attack, which affected NHS services, should serve as a stark warning of the implications of such an attack for national security.

- In these circumstances, revealing vulnerabilities and increasing exposure to the present threat would increase the risks to this part of our critical national infrastructure and therefore to the delivery of critical public services: this would not be in the public interest.

- Whilst Universal Credit is not formally registered as a CNI asset, as detailed earlier, the service is growing month on month and is pivotal to delivering financial and welfare support under the Welfare Reform Act.

- Should a widespread compromise or outage of the service occur as a result of a cyber-attack, assisted by the release of the requested reports, the inability to support the welfare of UK society will likely result in a loss in confidence in the welfare system and may lead to civil unrest.

66. The Commissioner notes that she has been persuaded that releasing the withheld information would be likely to prejudice the prevention of crime namely criminal intrusion of the DWP IT systems. Disruption, caused by criminal acts in this context, could likely cause significant difficulties to those dependent on welfare or pension payments from the DWP. The DWP service users, by definition, can be the more vulnerable members of the public.

67. The Commissioner recognises the perennial public interest factors for releasing the withheld information. Openness and transparency as to the acts and omissions of public authorities. The Commissioner appreciates that the public will benefit from knowing how the DWP tests the security of its computer systems and data storage. However the Commissioner doubts the overall strength of public interest factors for releasing the withheld information specific to the circumstances of this matter.

68. On balance, the Commissioner is satisfied that the public interest arguments in favour of maintaining the exemption clearly outweigh the public interest arguments in favour of disclosing this information. In particular, the public interest is best served by not aiding those that would criminally interfere or otherwise intruded into the DWP's IT system. The disruption and harm that could be caused to very vulnerable people is such that the public interest is clearly to keep the likelihood of this occurring to a minimum.

69. The Commissioner stresses that her decision is predicated, as it has to be, on the circumstances prevailing at the time of the information request. The passage of time is likely to weaken the DWP's reliance (if it were to maintain such) on this exemption. What may be a justifiable security concern at the time of this information request may not be if the request was made at a later date.

Right of appeal

70. Either party has the right to appeal against this decision notice to the First-tier Tribunal (Information Rights). Information about the appeals process may be obtained from:

    First-tier Tribunal (Information Rights)
    GRC & GRP Tribunals,
    PO Box 9300,
    LEICESTER,
    LE1 8DJ

    Tel: 0300 123 4504
    Fax: 0870 739 5836
    Email: grc@justice.gov.uk
    Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

71. If you wish to appeal against a decision notice, you can obtain information on how to appeal along with the relevant forms from the Information Tribunal website.

72. Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this decision notice is sent.

Signed
Gerrard Tracey
Principal Adviser
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF