Rt Hon. Oliver Dowden CBE MP
Deputy Prime Minister and
Chancellor of the Duchy of Lancaster
Cabinet Office 70 Whitehall London
SW1A 2AS

Rt Hon. Dame Margaret Beckett DBE MP
Chair, Joint Committee on the National Security Strategy
House of Commons
London
SW1A 0AA

10 July 2023

Dear Chair,

Thank you for your letter of 14 June.

Strengthening our national resilience is a priority for this Government. As you will be aware, we recently published the new Biological Security Strategy and will shortly publish an updated National Risk Register.

All of this work is underpinned by the Resilience Framework, which sets out our broader approach to national resilience. It is an ambitious, wide-reaching and long-term plan that is already working to strengthen our national resilience. The Resilience Framework fulfils the commitment the Government made in the Integrated Review and I can assure you that the amended title does not reflect a change to our ambition.

Whilst the Cabinet Office had previously consulted under a holding title of the 'National Resilience Strategy', the title of the final publication was changed so that it more clearly reflected the focus on the structures and capabilities that underpin our resilience to all risks. The Resilience Framework addresses the core areas raised by stakeholders and experts during this consultation, and has been well received by the partners with whom we are now implementing its commitments.

I have endeavoured to answer your specific questions in turn below.

By what date does the Government plan to have translated the objectives outlined in the Resilience Framework into clear plans with specific, measurable outcomes?

The Resilience Framework sets out the timetable for each of its specific commitments and we are proceeding with urgency to deliver the programme. As well as the publications I refer to above, my department is undertaking a review of the Lead Government Department model and the generic response capabilities that it allows us to deliver. We are expanding our risk assessment process to

consider chronic risks and strategic vulnerabilities, and revitalising the National Exercising Programme to test our response to key risks. In addition, my colleague the Secretary of State for Levelling Up, Housing and Communities is leading work to strengthen Local Resilience Forums. The Government will continue to engage with Parliament to provide accountability on the programme, including through the forthcoming annual statement to Parliament.

By what date does the Government plan to have completed its mapping of existing resilience capabilities? We would welcome an update on progress by the end of the year, in private if necessary, as well as the output of this analysis.

As you are aware, the Government's principal tool for identifying and assessing risks is the National Security Risk Assessment (NSRA). The NSRA is complemented by the National Resilience Planning Assumptions, which provide the Government and emergency responders with benchmarks for the common consequences of identified risks. The Government then identifies the capabilities that enable a successful response to these planning assumptions.

The Cabinet Office is currently leading a comprehensive assessment of these capabilities and expects to complete this programme in the autumn. We are also simultaneously working to strengthen our resilience to the cascading impacts of the biggest risks we face, which by their nature, would be likely to exceed the benchmarks set by the National Resilience Planning Assumptions. This work will support cross-government action to prevent and address these system-wide impacts. I would be happy to provide you with a private update on both these programmes later in the year.

Why has the Government not yet introduced a TLOD model of risk management, in line with this Committee's recommendation and private sector best practice?

The "three lines of defence" model is used by some corporations to aid in their risk management process. However, whilst we recognise many businesses manage complex risks to a complex set of interests, we think there are material differences to the task of Government, which is to prepare for and treat risks to the nation at large. This means we need to be prepared to deal with a constantly changing landscape of risks to societal, security, geopolitical and economic factors.

Rather than construct a final line of defence that is expected to assure the wide range of risks and associated mitigations that the UK faces at any one time, the Government applies the Lead Government Department model. This enables risks to be managed by the departments that hold the expertise and capability to do so most effectively, with their own Ministerial and Permanent Secretary accountability and associated governance.

As well as coordinating this overall process, the Cabinet Office provides support and challenge on departmental work on risks, in particular on cross-cutting or complex risks. This includes the work of the National Security Council (Resilience) subcommittee, which I chair. This committee brings together Ministers to discuss and agree risk analysis, our strategies to prevent or mitigate risks, and our plans to prepare for them. In addition, the Cabinet Office is designing a new programme for training and exercising, and, as referenced above, is undertaking specific work to strengthen cross-Government planning for the highest impact risks which are likely to exceed the assumptions set out in National Resilience Planning Assumptions.

Alongside our internal work on risk, the Government engages with external challenge from

Parliamentary Committees, think tanks, experts and academia. It invited increased expert challenge in the development of the most recent NSRA and we are committed to continuing to involve external experts in our work.

To reflect the priority and seniority that this topic requires, will the Government consider elevating the Resilience Director to Director General level?

Making tangible progress to strengthen our national resilience is dependent on our ability to drive through our programme with consistency and focus. It requires the collaboration and coordinated effort of a wide community of actors inside and outside of Government, which is driven effectively through the dedicated focus of the Resilience Director - the Head of Resilience - and her team in the Resilience Directorate. Where escalation or additional influence is needed to address barriers or issues, the Head of Resilience can and does draw on officials at Director General level who support this programme such as the Director General for EDS or the Deputy National Security Adviser. I work closely with the Head of Resilience and, as Deputy Prime Minister, chair NSC (Resilience) to coordinate this work at the most senior levels of Government.

Over which timescale, and in which areas, is the Government piloting the new Chief Resilience Officer leadership role, and how will it judge the success (or otherwise) of this initiative?

The Department for Levelling Up, Housing and Communities is leading the Strengthening Local Resilience Forums programme. It has asked for Expressions of Interest from LRFs to join the pilot programme and is now assessing those applications. Approximately eight LRFs will be selected as pilot areas, representing the breadth and variation of regions and places, and these will be announced later in 2023. The programme is intended to run for two years from early 2024 and will be evaluated by an independent contractor, which will be selected in the coming months.

Will the Government pursue central oversight and assessment of the consistency of LRF performance, in addition to local democratic accountability? If so, how?

As part of the Strengthening Local Resilience Forums programme that I set out above, the Government is actively considering options for assuring multi-agency activity at the Local Resilience Forum (LRF) level. This includes consideration of how effective differing levels of central oversight would be. We recognise the critically important role that LRFs play in national resilience and want to ensure that we are supporting them in the most effective way.

Has the Government considered introducing enforceable mandatory cyber security standards for regulated sectors, particularly for CNI operators?

The National Cyber Strategy 2022 committed us to work with operators to achieve resilience against common attack methods as quickly as possible and to put in place more advanced protections where appropriate. Operators regulated under the Network and Information Systems (NIS) Regulations 2018 must already meet at least the baseline standard set for each sector. Similar cyber security requirements are already in place under regulatory frameworks covering the finance, telecommunications, civil nuclear and chemicals sectors. We are working to develop additional specific and ambitious cyber resilience targets for all critical national infrastructure sectors to meet by 2025 and are examining plans to bring all private sector businesses working in critical national infrastructure within the scope of cyber resilience regulations.

The Government has committed to reviewing how it can better support the insurance industry in risk areas in which the market is currently failing to provide adequate cover. By what date does the Government plan to have completed this exercise? We would welcome an update by the end of the year.

Since the publication of the Resilience Framework, the Cabinet Office has been engaging widely with the insurance industry stakeholders to understand how we can collaborate on the Government's vision for a 'whole-of-society approach' - exploring how we can share data and expertise to inform risk assessment processes and a shared understanding of risk, as well as the modelling and quantification of the potential impacts of risk events to inform resilience policy.

The Government is developing an 'action plan' on insurance - setting out how we will work with the industry to support the expansion and good functioning of risk transfer markets in a way that drives broader risk-mitigating behaviour. My department is working to complete this exercise by the end of this year and I would be happy to provide an update to the Committee at that point.

There are currently no plans to introduce a public scheme for hostile state-backed cyber threats as it would not be an appropriate use of public funds. The Government's principal position is that it does not intervene to assume liability for risks where the market could feasibly perform this function, in order to protect the taxpayer. The UK cyber insurance market is relatively young; we are keen to foster further collaborative work between Government and industry to maximise insurance coverage and to strengthen the market overall, while increasing broader awareness of cyber risks and encouraging investment and best-practice to reduce exploitable vulnerabilities across our critical sectors - deterring future attacks. Our focus is supporting industry on deterrence.

What further plans does the Government have to communicate directly with the public on resilience and preparedness, before the next crisis occurs?

The Government provides tailored, actionable information to the public on specific risks, for example the 'WeatherReady', 'Run Hide Tell' and 'Cyber Aware' campaigns. As set out in the Resilience Framework, we are considering how to go further and exploring additional ways to make communications on risk personalised and more relevant, actionable and accessible. To ensure the approach is appropriately targeted and grounded in evidence and best practice, the Government will conduct an annual survey of public perceptions of risk, resilience and preparedness that uses a representative sample of the population. As noted in the Resilience Framework, the survey will help to ensure the Government's approach to risk communication is built on an understanding of how aware the public is of the risks we face and how prepared they are for emergencies.

The recently published 'Crisis Communications Operating Model' from the Government Communications Service sets out how the communication function will structure itself, and allocate roles and responsibilities to prepare, respond and recover from crisis situations. One purpose of the operating model is to ensure structures are in place to communicate clearly to businesses, local organisations, voluntary organisations, community groups, and the public, both in preparation for and during a potential emergency or crisis.

As you mention in your letter, the Government has now launched and successfully tested the Emergency Alerts service, which will help to save lives in emergency situations by issuing alerts

detailing the situation and the actions people need to take to stay safe. The system is now ready to use in emergency situations.

As well as communicating directly with the public, we also need to provide practitioners with the information and tools so they can communicate with and support the public. The 2023 National Risk Register (NRR) will be published shortly. This iteration of the NRR is aimed at expert practitioners, such as those in businesses and voluntary sector organisations who do not have access to the internal National Security Risk Assessment, ensuring they have a sufficient level of information to support their risk assessment work and contingency/business continuity planning.

Yours sincerely,

Rt Hon. Oliver Dowden CBE MP
Deputy Prime Minister