Meeting with Joint Oireachtas Committee on Transport and Communications

Leinster House, 22 September 2021

Opening Statement by Minister of State Ossian Smyth, T.D.

Thank you Chairman

I am joined today by Richard Browne, Acting Director of the National Cyber Security Centre (NCSC), and Peter Hogan, Principal Officer in the Cyber Security and Internet Policy Division.

I am delighted to have this opportunity to present to the Committee on the Capacity Review of the NCSC which was completed last June. When we last met, Minister Ryan and I were awaiting the outcome of the review, which I am pleased to report was completed within the intended timeframe.

I know the Committee were keen to hear the recommendations of the Capacity Review and to ensure that the Government took appropriate steps to implement these as early as possible.

As the Members will be aware, in July Minister Ryan obtained Government agreement to a substantial expansion in the staffing of the NCSC from 25 to 45 staff over the next 18 months, and to at least 70 within 5 years. The associated budgetary increase for the NCSC for 2022 is estimated at €2.5 million.

The Government also agreed a significant package of other measures to further strengthen the capacity of the NCSC, including the development of legislation to establish the NCSC on a statutory basis with a set of formal powers and a legal mandate. These measures include:

- That the role of Director of the NCSC be re-advertised at a salary of €184,000 (Deputy Secretary scale) to reflect the scale and importance of the role and to attract experienced candidates
- The Director will have responsibility for building and leading the NCSC, further developing the operational capacity and expertise of the NCSC and supporting the development of the policy and legislative framework relating to cyber security in the State

- A single HQ for the NCSC which will provide the required security infrastructure and capacity. The NCSC will be accommodated within the Department's new Headquarters (HQ) in Beggars Bush
- Developing a 5 year technology strategy for the NCSC that scopes its internal requirements, and its relationship with academia and industry
- In addition to the recruitment of 20 additional fulltime roles, a cyber security graduate training programme will be initiated by the NCSC in 2021, with four computer science graduates recruited each year on contracts of three years duration.

I have already shared with the Committee Members a redacted version of the Executive Summary from the Capacity Review. In respect of the findings of the review and benchmarking exercise, there are some details which I cannot share due to national security considerations– both in Ireland and in those countries with whom comparison was made. I will endeavour to be as open and transparent with the Committee today and where necessary I will instruct my officials to follow up with written replies to the Members' questions.

The Capacity Review report recognised that the NCSC has grown considerably since its establishment in 2011. The consultants acknowledged that the NCSC team had developed significant expertise and capability in a relatively brief timeframe. The consultants found that staff at all levels of the NCSC are knowledgeable and highly motivated, with a clear understanding of the NCSC's role and purpose. The consultants also remarked positively on the progress of implementation of the National Cyber Security Strategy and the role the Interdepartmental Committee has played in driving this work.

The consultants were tasked with charting a five-year course for the continued development of the NCSC, taking account of the evolving threat landscape and the growing body of EU legislation on cyber security. The consultants proposed a new organisational structure for the NCSC and recommend that an incremental expansion be pursued over the coming 5 years. The Capacity Review recommends that as an initial step, headcount of the NCSC's operational team be increased from 25 to 41 FTE, with numbers continuing to grow to approx. 50 in Year 3 and approx. 70 in Year 5.

The Government in this regard has decided to go further in the initial expansion of staff.

The Capacity Review includes over 40 recommendations, categorised as high, medium and low priority, covering a range of issues from governance to technology to skills development. The Capacity Review recommendations will not be fully completed for some years, and there are many interdependencies within them. For instance, much of the recommended technology development requires a suitably-equipped HQ facility, and a clear legislative mandate is necessary for the NCSC's functions to expand further.

I would like to now provide the Committee with an update on the progress of implementing the measures agreed by Government in July.

Working with the Public Appointments Service, good progress is being made by the Department in progressing the delivering the increase in headcount recommended in the capacity review. I understand that in the coming weeks a number of open recruitment competitions will commence to recruit new staff with cyber security skills and experience to complement the existing team.

In addition, we are availing of the civil service mobility scheme to redeploy staff from across the civil and public service with an interest in the NCSC's work. We are taking a broad perspective on the skillsets necessary for the NCSC's range of functions including stakeholder engagement, project management and compliance. This process has already begun and we are currently seeking expressions of interest.

The competition for the NCSC Director, run by the Public Appointments Service, will be advertised this Friday. As was the case for the previous recruitment campaign, this will be an open process carried out in line with the established principles for senior recruitment to the civil and public service. I expect to see this competition concluded before year-end and the permanent director appointed as early as possible thereafter. The Public Appointments Service are using the services of an executive search company to assist in identifying suitable candidates.

In the interim, we took the decision to appoint Richard Browne as Acting Director to ensure the NCSC has a full leadership team in place during this important period of transition.

Mr Browne has previously served in this area since 2014 so he was able to hit the ground running when he returned in July. His focus is in implementing the measures agreed by Government in July and he and his team are already making good progress.

The development of the NCSC HQ will be managed as part of the redevelopment of the Department's offices at Beggars Bush, Dublin 4, expected to be completed in 2023. The Acting Director and Chief Technology Officer have worked closely with the Corporate Services area of the Department and the Office of Public Works over the past two months with a focus on the design and layout of the new HQ. This will be an important facility for the national response to a major cyber security incident and so we need to ensure it is fully equipped. There are also international standards for the security of accredited Computer Security Incident Response Teams (CSIRT) which will need to be factored into the design, construction and fit-out of the new facility.

While the new HQ is being developed, temporary accommodation will be required for the NCSC. The OPW has identified a suitable location for this temporary facility.

Under the supervision of the Acting Director, the NCSC admin and CTO teams are currently working on the design and procurement for the fit-out of this facility. Appropriate measures will be taken to ensure that this temporary facility can accommodate the NCSC as its staffing complement grows through 2022 and 2023. And we will ensure that it meets the exacting international security standards for the CSIRT.

The development of a technology strategy for the NCSC is closely linked to the new HQ project. The Acting Director and CTO have completed a review of the Capacity Review's recommendations in respect of technology to inform the development of the new strategy. The CTO has also identified a number of priority investments which are part of the Department's submission for the 2022 Estimates process.

Work has also commenced on the cyber security internship scheme which will complement the existing actions in the National Cyber Security Strategy on cyber careers and skills. This scheme will be a priority action following the imminent recruitment rounds I referred to earlier.

Finally, in respect of the proposed legislation for the NCSC, recognising the need to work in partnership with other Departments and agencies, at the recent meeting of the Interdepartmental Committee on the National Cyber Security Strategy a way forward was agreed by all members. To empower the NCSC to carry out its necessary functions, it is inevitable that the proposed legislation will provide for intelligence gathering, which will bring with it certain governance requirements as well as requirements on the legislative process. Officials in my Department are leading a consultation with relevant stakeholders which it is intended to complete before the end of this year. Thereafter, work will begin on drafting Heads of a Bill which I hope to see progress through the Oireachtas before the end of 2022.

I recently attended the Estonian Digital Summit, where there was much interest in the Government's response to the HSE cyber incident and the development of our NCSC. The conference theme was 'trusted connectivity', and I was pleased to have the opportunity to engage in constructive conversations with peer Ministers from a number of EU countries, as well as Singapore and the UK.

It was clear from the conference and discussions with other Ministers that the global landscape of cyber threats is at the top of the political agenda and that concerted international cooperation will be necessary to secure essential services in the face of these threats.

During my visit to Tallinn I also met with Ireland's secondee to the Cooperative Cyber Defence Centre of Excellence and paid a visit to the CCDCOE. I believe there are great resources in the CCDCOE that we can draw on to inform the further development of our own cyber capacity, both within the NCSC and across Government.

Thank you.

END