Australian Government

Department of Home Affairs

MICHAEL PEZZULLO

SECRETARY

DEPARTMENT OF HOME AFFAIRS

Opening Statement

Legal and Constitutional Affairs Legislation Committee

Senate Estimates

THURSDAY, 31 MARCH 2022

In the interests of time I will be brief.

In relation to the war between Russia and Ukraine, which was started when Putin launched an unprovoked, premeditated and barbarous attack on Ukraine, the Department is actively engaged in a number of areas of activity.

Since 23 February 2022, 5,598 visas have been granted to Ukrainians who are understood to be in Ukraine, 1,407 of whom have since arrived in Australia. All Ukrainian temporary visa holders in Australia and those who arrive in coming months will be able to apply for a temporary humanitarian visa. This visa is valid for three years and will allow visa holders to work, study and access Medicare. They will also have the opportunity to apply for other longer term visas should they wish to do so, though it is expected that those who have been displaced will eventually wish to return home.

# # #

Following the attack by Russia on Ukraine, cyber threats have increased globally, and the risk of cyber attacks on Australian networks, either directly or inadvertently, has increased. While the Australian Cyber Security Centre (ACSC) has no specific intelligence relating to an imminent or specifically foreseeable cyber attack on Australia, this could change quickly. In this context, I should like to draw to the attention of the Committee the statement which was released on 21 March 2022 by President Biden, who said that there was evolving intelligence that Russia may be exploring options for potential cyberattacks.

It is a challenge to calculate the extent to which the Russian state would consider destructive cyber attacks to be an acceptable and strategically valuable option in the current situation, and whether its appetite for conducting destructive cyber attacks on the United States or its allies and partners is likely to increase, noting longstanding propensities on the part of Russia to engage in aggressive cyber espionage and non-destructive intrusion.

In this environment, it would be prudent for Australian companies (especially the providers of essential services and critical infrastructure) and public agencies (at all levels of government) to get their 'shields up'. We all have to take active steps to enhance our cyber security posture and increase monitoring for threats. These actions will help to reduce the incidence and impacts of any cyber attacks. More information can be found on the ACSC and CISC websites.

The *Security of Critical Infrastructure Act 2018*, as amended on 3 December 2021, sets out a number of relevant measures, which the Minister and the Department are applying – or will apply – as appropriate across the following sectors: communications; data storage or processing; financial services and markets; water and sewerage; energy; health care and medical; higher education and research; food and grocery; transport; space technology; and the defence industry. Of note, the Act now provides for 'Government Assistance Measures' to be applied as a last resort, if an entity is unwilling or unable to conduct their own incident response, and when there is no other regulatory mechanism in place to resolve the incident.

The *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* (SLACIP Bill), which passed the Senate last night and the House of Representatives this morning, sets out a number of additional measures including: the obligation to adopt and maintain a Risk Management Program; the ability to declare Systems of National Significance (a smaller subset of critical infrastructure assets that are most crucial to the nation); and enhanced cyber security obligations that may apply to these systems. Again, the Minister and the Department will apply – as appropriate – relevant measures in the current environment.

Any overview of these new authorities would be incomplete without mention being made of the Australian Signals Directorate's (ASD) growing arsenal of defensive and offensive cyber tools and weapons. ASD's operational capabilities are a crucial complement to the authorities which are vested in Home Affairs. Through the earlier Cyber Enhanced Situational Awareness and Response programme and the new capability known as REDSPICE, ASD will play a critical role in shielding significant national systems, including those in private hands, using the aforementioned authorities. Just as significantly, its growing offensive capabilities will allow Australia to strike back at adversaries (lawfully and responsibily), the knowledge of which would complicate their calculations, and worsen their odds, should they ever contemplate cyber attacks on Australian networks.

The Department values its partnership with ASD, which will only intensify with the passage of the Bills mentioned earlier.

The Department is also engaged in other areas of activity in relation to the Russo-Ukrainian war some of which, in the interests of brevity, I will simply list: sanctions support; counter disinformation; counter foreign interference; social cohesion outreach; foreign fighter movements; ideologically motivated violent extremism; and supply chain risk assessment.