Australian Government
Department of Home Affairs

Department of Home Affairs submission to the Inquiry into the Optus Network Outage

Senate Standing Committee on Environment and Communications

17 November 2023

OFFICIAL

Table of Contents

OFFICIAL

1. Introduction

The Department of Home Affairs (the Department) is the lead agency for cyber security and critical infrastructure policy, the Department's regulatory functions for critical infrastructure (including aviation, maritime and telecommunications security), identity security and protection and background checking under the AusCheck scheme. This includes responsibility for the *Security of Critical Infrastructure Act 2018* (SOCI Act) and Part 14 of the *Telecommunications Act 1997* (Tel Act).

The National Cyber Security Coordinator, together with the National Office of Cyber Security, leads the coordination of consequence management for national cyber incidents, whole of government cyber incident preparedness efforts and the strengthening of Commonwealth cyber security capability. The National Emergency Management Agency (NEMA) supports whole-of-government and whole-of-nation coordination through the National Coordination Mechanism (NCM) and the National Situation Room.

As a result, the Department played a role in supporting the Government's response to the incident.

2. Home Affairs' role in the response

The Department made first contact with Optus at around 7:00am on 8 November 2023. Senior officials at the Deputy Secretary level of Home Affairs reached out to Optus via Signal message to offer the Department's assistance in responding to the incident. Throughout the morning, the Department monitored the situation, liaising with Optus and other Government agencies as the situation unfolded.

Optus advised that it did not believe the outage to be the result of a cyberattack, instead attributing the outage to unspecified technical issues. This understanding shaped the Department's response, with the Cyber and Infrastructure Security Group leading due to its responsibility for critical infrastructure security. The National Cyber Security Coordinator remaining engaged to ensure coverage in case the information about a cyberattack changed. This understanding also shaped what response actions were available to the Department under relevant legislative frameworks. It should be noted, however, that at the time of the outage, neither Optus nor the Department were able to categorically rule out a cyberattack or other malicious action being the cause of the incident. At the time of writing this submission, the Department has not received any further information that would rule out any malicious action as the cause.

Shortly after 9:30am an Acting First Assistant Secretary from the Department invited Optus via email to provide a situational update to Australian, state and territory government stakeholders through the NCM to be co-chaired by senior officials from the Department, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) and NEMA. An initial NCM was scheduled to be held at 2:00pm. The Department received further updates from Optus throughout the day, including advice that services were starting to be restored from 1:00pm. At the 2:00pm NCM meeting, Optus briefed Commonwealth, State and Territory officials on what it knew about the incident. This included some technical detail of the fault that was causing the outage, although a number of details remained unclear.

Together with other agencies, the Department co-chaired a further NCM meeting at 4:00pm which brought together Commonwealth officials and each of the major telecommunications carriers. At the second meeting Optus provided an update for the benefit of other carriers, and the co-chairs invited each of the carriers to discuss any second and third order consequences or impacts of the outage, including to emergency call service availability. At this meeting Optus advised that 98% of its customers had been re-connected to their network.

Following Optus' resolution of the incident, the Department is identifying lessons – this is being undertaken in cooperation with the review announced by the Minister for Communications, the Hon Michelle Rowland MP. As the regulator for telecommunications security, the Department will also consider whether this incident highlights any potential failures by Optus to comply with its legislative obligations. The Department of Home Affairs also hosts the national coordination function for the protection of critical infrastructure and will work to learn from and share lessons from this incident.

3. Impact of the incident

As this incident highlights, Australia's critical infrastructure sectors are deeply interconnected. Significant disruption in one sector may have severe, cascading and compounding impacts and consequences on the delivery or support of other critical infrastructure services. The Optus outage has highlighted the consequences which can occur as a result of this interdependency, with the event impacting the availability of other critical infrastructure services, including hospital services, financial services and public transport. It also demonstrated the flow-on impact to businesses, which also act as key third-party service providers to other sectors (as well as individuals) across the economy. This adds to the significant impact of the outage on the day-to-day operation of tens of thousands of businesses and millions of individual Australians.

The Department is committed to working with critical infrastructure providers to ensure the ongoing availability of critical infrastructure despite a wide range of potential hazards. Secure and resilient critical infrastructure is vital to the functioning of Australian society. Any disruption or degradation of critical infrastructure can have severe consequences for the availability of essential services, and the safety, well-being and prosperity of Australians. Accordingly the Department is continuing to work closely with critical infrastructure operators to strengthen their security and resilience.

The Department, at the direction of Government, is also working to further strengthen our legislative frameworks – including specifically for the telecommunications sector – to ensure that we have all the tools necessary to keep Australia's critical infrastructure secure.

4. Direct impacts to the Department's ICT networks

The Department's Global Service Centre (GSC) experienced a full outage from early Wednesday morning. Alternative contact points and services, including those delivered via the Department's websites, remained online. GSC client telephone services were gradually restored from approximately 1:00pm, with some clients experiencing longer than usual wait times during the afternoon. All services have returned to normal. Some Australian Border Force operations were partially impacted, however Business Continuity Plans (BCP) were successfully enacted. BCPs were implemented at the Australian Government's National Situation Room and National Security Hotline housed within NEMA.

5. Our legislative frameworks

The Department works closely with critical infrastructure operators to ensure they protect and manage risks to their assets.

Optus is not required to comply with critical infrastructure risk management program rules under the SOCI Act because telecommunications security obligations are administered under the Tel Act. The Government is working closely with industry to consider the options for developing a dedicated risk management program and broader obligations for the telecommunications sector.

Telecommunications Act 1997

The Department is responsible for administering security obligations under Part 14 of the Tel Act which contains a regulatory framework intended to manage the national security risks of sabotage, espionage and foreign interference to Australia's telecommunications networks and facilities.

The core security obligation in Part 14, in Section 313(1A) of the Tel Act, requires licenced carriers to 'do their best' to protect their networks and facilities from unauthorised access and interference. There is no evidence to suggest the Optus outage of 8 November involved unauthorised access or interference. While the accompanying Administrative Guidelines suggest that telecommunications entities should consider all hazards as part of their core security obligation, this is not an explicit legislative requirement.

There are a number of powers available to the Department and the Minister for Home Affairs that may be used in response to an incident of this nature. Under Section 315C of the Tel Act, the Secretary can obtain documents from a carrier to assess their compliance with their security obligation. Section 315B of the Tel Act includes the power of the Minister for Home Affairs to direct a carrier to do or not do a specified thing or act, although this requires that the Minister first be given an adverse security assessment by the Director-General of Security. Section 313(3) of the Tel Act requires carriers to provide government officers and authorities such help as is reasonably necessary to safeguard national security (amongst other reasons). However, these powers are principally focussed on acts of unauthorised access or interference to a provider's networks or facilities, and are not specifically contemplated in the case of a technical failure.

Security of Critical Infrastructure Act 2018

Optus, like other telecommunications carriers, is considered a responsible entity for a critical telecommunications asset under the SOCI Act. However, the telecommunications sector is not subject to certain requirements already implemented in other sectors – notably the obligation to establish, maintain and comply with a Risk Management Program (RMP) under section 30AH of the SOCI Act. The Department, alongside DITRDCA, has been working with the telecommunications sector to co-design a harmonised security regulatory framework for the telecommunications sector. This includes the development of a bespoke telecommunications RMP.

The RMP obligation, once turned on for the telecommunications sector would uplift core security practices, and ensure responsible entities adopt a holistic and proactive approach towards identifying, preventing and mitigating risks from all hazards. An RMP obligation requires responsible entities to:

- Take an all hazards approach when identifying hazards that may affect the availability, integrity, reliability and confidentiality of their critical infrastructure asset.
- Consider risks to their critical infrastructure asset and establish appropriate strategies to minimise or eliminate the risk from occurring, so far as is reasonably practicable. This includes both proactive risk management as well as establishing and maintaining processes to detect and respond to threats, such as deep network issues, as they are being realised to prevent the risk from eventuating.
- Have robust procedures in place to mitigate the impacts of a hazard, and recover from that impact as quickly as possible. This includes thinking holistically about the cascading impacts to other critical infrastructure sectors, having appropriate communications plans in place, and implementing redundancies.
- Continuously update their RMP, including post incidents to ensure the currency of content and internal assessment processes to ensure the adequacy of their program.

By placing the onus of adequate risk management on the entity's Board, the RMP obligation enhances engagement and review of internal auditing risk mitigation processes. Anecdotal evidence from industry suggests the Board exposure resulting from the SOCI legislative framework, including the RMP obligation, helps to elevate risk management to the Board level.

The SOCI Act also holds a series of intervention powers that may be used to address a cyber incident. The Government Assistance framework under the SOCI Act provides the Minister for Home Affairs with the ability to authorise the Secretary of the Department of Home Affairs to do any or all of the following things in response to a cyber security incident:

- Gather information to determine if another power in the SOCI Act should be exercised.
- Direct an entity to do, or refrain from doing, a specified act or thing.
- Request an authorised agency (i.e. the Australian Signals Directorate) to provide support (with agreement from the Prime Minister and Minister for Defence).

The powers cannot be used unless a cyber security incident on a critical infrastructure asset can reasonably be considered capable of causing significant damage or harm to Australian interests. Government assistance measures have not been used to date, which is reflective of the fact that Government will not use these measures lightly. Part 3A powers apply exclusively to cyber security incidents impacting critical infrastructure entities, including telecommunications assets. If the 8 November outage had been a cyber incident caused by a malicious actor, the powers may have been available. This would not have been the case if the incident had been caused by a non-cyber related incident such as a severe weather event, or a negligent or malicious insider.

Longer term consequences of significant incidents impacting critical infrastructure can often lead to reputational damage and loss of confidence in a system, market, entity or nation—and as a result cause damage to Australia's national interests. As the Optus outage has demonstrated, risk is more complex than ever and consequence management cannot be limited to a single vector. The loss of services, regardless of the cause, resulted in significant impacts on a business and personal level, and caused huge consumer distress. The Government is considering possible avenues to ensure legislative levers are sufficient to manage these consequences.

6. Regulatory implications

While the Department has not commenced a formal investigation into Optus' compliance with its obligations under Part 14 of the Tel Act at this time, a future investigation cannot be ruled out.

The Secretary of the Department may also consider undertaking an assessment of critical infrastructure assets operated by Optus, under section 57 of the SOCI Act, to determine if there is a risk to national security relating to the assets.

7. How would we have managed a cyber attack?

If the cause of this disruption had been related to a cyber attack, the primary response pathway for the Department would have been led by the National Cyber Security Coordinator, through the National Office of Cyber Security. The Coordinator would have led engagement with senior industry and government officials to support a response and consequence management, including public communications on the status and any response activity underway. Core engagement and coordination activity would have been undertaken through the Cyber Security Response Coordination Unit (CSRCU), within the National Office of Cyber Security.

The CSRCU works collaboratively with key government stakeholders to support industry and other government partners impacted by a cyber incident. In managing the flow-on consequences of an incident, in such a scenario the CSRCU would have worked alongside teams leading technical responses (such as the Australian Signals Directorate's Australian Cyber Security Centre), law enforcement operations (the Australian Federal Police), emergency management activities (led by NEMA) and government service delivery areas. The CSRCU would have also engaged relevant Australian Government and state or territory departments and agencies leading or delivering response activities within their jurisdictions, particularly if impacts to core services (energy, food and logistics, transport) had been significant and/or prolonged through the NCM with support from NEMA.

The response by the Coordinator and the CSRCU would have been based on the lessons identified from the recent telecommunications sector wide consequence management exercise, held on 8 September.

Given the significant role that regulatory and other agencies would have played in any cyber-related response, the convening role of the NCM would still have been leveraged. Depending on the duration of the incident, the NCM would have been managed and maintained as a key response mechanism to support the response to ongoing disruption or other impacts to service delivery. The NCM would have supported second and third order consequence management through targeted NCMs to provide shared situational awareness, rapid problem definition and de-confliction across lines of effort to stabilise the situation.

The National Cyber Security Coordinator, the National Office of Cyber Security, and the CSRCU are non-regulatory in nature. Any consideration of regulatory measures would have been separate to the consequence management function the Department would have undertaken should the Optus outage have been related to a cyberattack.