Australian Government
Australian Signals Directorate

ASD

REVIEW OF THE SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL

SUBMISSION TO THE PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY

12 February 2021

The Australian Signals Directorate (ASD) welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the proposed Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill).

Australian Signals Directorate

1. ASD is a statutory agency within the Defence portfolio. ASD's functions are outlined in the *Intelligence Services Act 2001* (ISA), with accountability under this Act to the Minister for Defence.

2. ASD's status as a statutory agency reflects its significant national responsibilities, including support for whole-of-government and whole-of-economy objectives. In particular, ASD provides nation-wide cyber security advice and services to governments, businesses, critical infrastructure entities, individuals and the community.

3. The Australian Cyber Security Centre (ACSC) within ASD is the Australian Government's lead on cyber security. The ACSC provides proactive advice and assistance across the whole of the economy, including critical infrastructure and systems of national significance (SoNS), federal, state and local governments, small and medium businesses, academia, the not-for-profit sector and the Australian community. It is the hub for private and public sector collaboration and information sharing to prevent and combat cyber security threats and minimise the harm to all Australians.

4. In the context of the increased volume and sophistication of cyber attacks, the reforms proposed in the Bill envisage ASD playing a greater role assisting to build cyber security resilience across critical government and critical infrastructure assets. The proposed Bill would also see ASD assist and support response and recovery efforts in the event of a serious cyber incident.

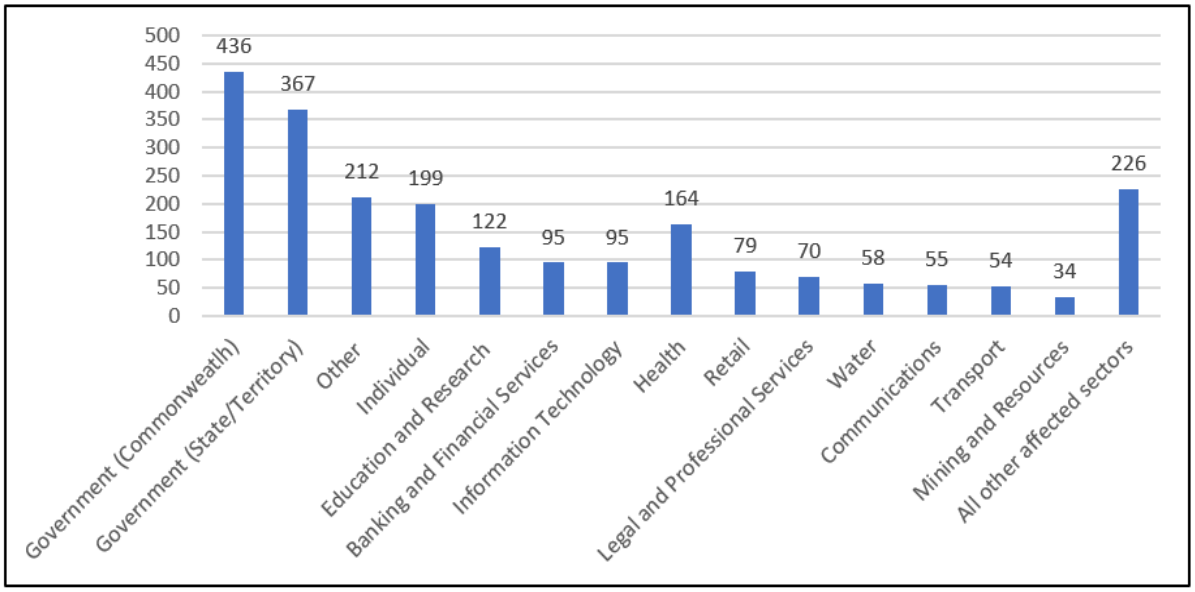
Threat Environment

5. ASD has observed malicious cyber activity against Australia's national and economic interests increasing in frequency, scale, and sophistication. In 2019–20, there were 2,266 cyber incidents reported to the ACSC.

6. While Australia has not suffered a catastrophic cyber attack on critical infrastructure, we are not immune. Australia is facing increasing cyber security threats to essential services, businesses and all levels of government.

7. In the past year we have seen cyber attacks on federal Parliamentary networks, transport and logistics, the health sector and universities (see figure 1). On 19 June 2020, the Prime Minister of Australia made a public statement regarding malicious cyber activity targeting Australian organisations across a range of sectors, including: governments, industry, political organisations, education, health, and other essential service providers and critical infrastructure operators. Internationally, we have seen cyber attacks on critical infrastructure including water services and airports.

Figure 1: Cyber security incidents, by affected sector (1 July 2019 to 30 June 2020)[1]



8. A cyber incident involving critical infrastructure information technology could have a serious impact on the safety, and social and economic wellbeing of many Australians. As our critical infrastructure is an interconnected system, compromise or disruption to one part of the system could flow across the entire sector.

9. Just over a third of all incidents reported to the ASD's ACSC over the last 12 months have been from Australia's critical infrastructure sectors. This is expected to be just a fraction of the number of cyber security incidents affecting critical infrastructure given the voluntary nature of reporting.

10. Malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale, and sophistication. Phishing and spearphishing remain the most common methods used by cyber adversaries to gain access to networks, or to distribute malicious content. Over the past 12 months, the ACSC has observed real-world impacts of ransomware incidents, which have typically originated from a user executing a file received as part of a spearphishing campaign.

11. While our cyber adversaries are becoming more adept, the likelihood and severity of cyber attacks is also increasing due to our growing dependence on new information technology platforms and interconnected devices and systems. The 5G mobile network will underpin Australia's transition to a more digital economy, and Internet of Things (IoT) devices will enable greater information flows and efficiencies than ever before.

12. ASD's knowledge of domestic cyber security threats and vulnerabilities relies on the Australian community and industry to voluntarily report incidents. This voluntary reporting and sharing of information assists ASD to identify threats and subsequently publish advice to mitigate the threat.

13. More incident reports to ASD through the provisions proposed in the Bill will assist in building improved national situational awareness and allow ASD to identify trends, and provide targeted advice to others in order to assist entities to better prepare and protect their networks and Australia's critical infrastructure.

[1] *ACSC Annual Cyber Threat Report July 2019 to June 2020*

Security Legislation Amendment (Critical Infrastructure) Bill 2020 – ASD Roles and Functions

14. Under the proposed Bill, ASD activities to support the resilience of critical infrastructure would include the following:

- receiving mandatory cyber security incident reporting
- participating in cyber security exercises and undertaking vulnerability assessments
- receiving relevant system information, including telemetry and system logs
- providing assistance under Government Assistance provisions to respond to a serious cyber security incident.

15. ASD's role under the Bill is consistent with, and complements, existing functions set out in the ISA. Where relevant to ASD's existing functions, such as the provision of advice and assistance, ASD will support relevant agencies such as the Department of Home Affairs in the implementation of activities in the proposed Bill.

Mandatory Cyber Security Incident Reporting – Cyber Security Incident Reporting (Part 2B)

16. The proposed Bill includes a mandatory reporting obligation for critical infrastructure assets to ASD under Part 2B. This will complement ASD's long-standing voluntary cyber incident reporting scheme operated in accordance with section 7(1)(ca) of the ISA.

17. Once a responsible entity becomes aware of a cyber-security incident, it must be reported within:

- 12 hours if the incident is having a significant impact on the availability of the asset, or
- 72 hours if the incident is having an impact on the availability, integrity or reliability of the asset or on the confidentiality of information about, or held by, the asset.

18. Timeliness of reporting is critical in understanding any trends, and in facilitating early advice and assistance, which may assist entities to take action before their networks are subjected to further or more extensive compromise. ASD will triage reports received according to the ACSC's existing Cyber Incident Matrix, which categorises incidents based on severity of impact and extent of compromise. ASD always uses anonymised or de-identified information in public advisory information to protect the identity of organisations that provide reporting.

19. The format and details of mandatory reporting will be prescribed in Rules, which will be developed by the Department of Home Affairs in consultation with industry. ASD will participate in this consultation process.

20. The type of reporting that assists ASD triage and respond to incidents includes information such as:

- the nature of the cyber incident and timing
- how the organisation became aware of the incident
- what remediation actions have been undertaken
- whether a data breach has occurred or is suspected, and if there is a risk of sensitive information being exposed
- the ability to share a copy of malware/malicious email (where relevant).

21. ASD uses information reported to develop advice and products that assist government, businesses and individuals protect themselves. This can include Alerts (see example at Attachment A – Solarwinds Orion Alert), Advisories or even diagnostic tools that organisations can deploy to identify if they have been compromised. ASD always use anonymised or de-identified information in public advisory information, protecting the identity of organisations that provide reporting.

22. ASD does not have a regulatory or enforcement function in relation to the requirement to report incidents under the Bill. The primary purpose of ASD receiving information under Part 2B will be to improve national situational awareness, allowing the production of anonymised mitigation advice to assist individual sectors or organisations more broadly to take steps to protect themselves.

Case study

ASD's experience is that organisations can be hesitant to report incidents or to work with ASD to resolve issues. This has a detrimental impact in being able to warn or advise people of risks in the Australian cyber threat environment, and to minimise impact on the victim by timely remediation of incidents. As an example, in 2019 a health care provider was the subject of a ransomware attack.

Over the course of ten days ACSC attempted to engage and assist the health care provider to identify malware on their network and ensure it was secure. After ten days the provider advised that their network had been disabled and they had lost access to all records. Over the following month the provider was forced to restore information from backup and during this time experienced impacts to patient care and business operations. Had the organisation engaged with ACSC earlier, it is possible the malware could have been removed from their system before it had the opportunity to encrypt their data.

Any delay in reporting incidents impacts ASD's ability to identify trends that could assist other organisations taking steps to protect themselves. Early reporting and advice can make it more likely that the impact of the malicious actor can be halted or minimised.

Under mandatory reporting of critical cyber incidents, entities considered to be critical infrastructure would have an obligation to report to ASD. This would provide awareness of incidents nationally, and ASD would be able to assess the need to issue targeted advice to the health sector or other businesses more broadly to assist in preventing the threat.

Enhanced Cyber Security Obligations (Part 2C)

23. Part 2C of the proposed Bill sets out a range of Enhanced Cyber Security Obligations which apply to designated SoNS. ASD officers may be called upon by Home Affairs as Designated Officers, to observe cyber security exercises and undertake vulnerability assessments conducted under Divisions 3 and 4 of Part 2C of the Bill.

24. ASD's role under the Bill complements existing ASD functions under the ISA, including to provide advice to entities on cyber security, and to cooperate with and assist specified agencies in connection with their functions.

25. Undertaking vulnerability assessments and exercising cyber security arrangements assists organisations to better prepare for cyber incidents, and take steps to address vulnerabilities or weaknesses in systems and processes. Involving ACSC in these activities prior to critical cyber incidents occurring can assist build awareness and familiarity of networks and processes, increasing the timeliness of future assistance by streamlining the need to spend time acquiring this knowledge during a crisis.

26. ASD already undertakes exercises with a range of partners, including critical infrastructure providers. These exercises can range from tabletop scenarios with senior decision-makers and exercising contact lists during a crisis, through to rehearsing key elements of business continuity planning, such as moving business functions to a backup site or restoring operation of a key asset. Cyber security exercises under the proposed Bill would help familiarise ASD incident responders with designated SoNS networks, systems, processes, and personnel, streamlining any future ASD assistance should a critical cyber security incident occur.

27. ASD also undertakes vulnerability assessments on a voluntary basis with critical infrastructure and government organisations. These assessments can range from paper-based assessments which validate the safe and secure design of a system or network, through to active testing against live environments to ensure that cyber security controls are effective and working as intended. Through vulnerability assessments, ASD can apply unique knowledge of threat tradecraft and targeting methodology to identify vulnerabilities, and assist entities mitigate them. Under the Bill, where requested by the Secretary of the Department of Home Affairs, ASD may undertake a vulnerability assessment as a Designated Officer.

Case study

ASD's experience is that not all providers are aware or understand their networks. Requiring exercises and vulnerability assessments would ensure that essential services are better prepared in the event of an incident. As an example, in late 2019 an energy provider became aware that they had a potentially compromised device on their network.

Although the provider was aware that they were potentially compromised, the provider had very limited knowledge of their own network, which complicated the response and timeliness of the response. The victim struggled to identify which of their outsourced providers owned the vulnerable device attached to their network. It took the entity two months to identify the owner to access relevant data from the device, which subsequently was not available.

During this delay, it is possible that the malicious actor had expanded their access or removed evidence of their activities. It remains unknown what the actor had access to or was able to do on the network. In this circumstance, ASD cannot rule out that a sophisticated or state-sponsored actor pre-positioned in the network with the future intent to deny or disrupt critical services.

If the entity undertook regular vulnerability assessments, it is likely they would have detected the public vulnerability on the device. In addition, had they undertaken regular cyber security exercises, they would have better understood their networks and had key contacts identified for their critical managed service providers, which would have ensured a more timely response.

Receive Relevant System Information – Enhanced Cyber Security Obligations for Systems of National Significance (Part 2C)

28. Under Part 2C, Division 5 of the Bill, ASD may receive system information (such as telemetry) directly from SoNS on either a periodic basis, or when certain conditions are met such as an alert from an intrusion detection system.

29. The Bill complements existing functions of ASD under section 7(1)(ca) of the ISA, where ASD enters into voluntary arrangements to ingest and analyse system data, and provide technical assistance and cyber security advice to entities.

30. Where system information is required it is likely that this data will vary depending on the critical infrastructure sector, and the current threat environment. Data which may be requested is likely to include data generated for the purposes of security and/or diagnostic monitoring. This could be data such as network logs, system telemetry and event logs, alerts, netflow and other aggregate or metadata that provide visibility of malicious activity occurring within the normal functioning of a computer network. System information does not include personal information within the meaning of the *Privacy Act 1998*.

31. This is the type of data and information ASD requests from entities when assisting to resolve a cyber incident.

32. ASD does not have a regulatory or enforcement function related to the direction to provide system information. Information reported to ASD under Part 2C, Division 5 will be used for providing improved understanding of the national cyber threat landscape, and issuing mitigation advice to businesses to assist them to protect themselves.

33. Where a SoNS is unable to supply the required data, ASD will provide advice and assistance to entities on implementing a capable monitoring system, or, when the Secretary of the Department of Home Affairs requires the installation of systems information software, may assist the entity to install the specified software.

34. System information and telemetry from SoNS will assist ASD in building a national cyber threat picture, and to develop timely and actionable cyber security advice to mitigate cyber threats at scale across Australian critical infrastructure, government, large corporations and small and medium businesses.

35. Detecting malicious cyber activity on an individual SoNS will allow ASD to distribute anonymised indicators of compromise and other threat intelligence. This may be achieved through the ACSC Partnership Program, cyber.gov.au, or via automated cyber threat intelligence sharing. This will empower other SoNS to defend their networks from emerging threats at speed and scale through distribution in a machine readable format.

Case study

The ACSC often becomes aware of vulnerabilities once they are publicly announced and has limited data available to understand the full impact and threat to critical Australian networks. Recent compromises highlight the value of real-time system information, such as telemetry, to pre-emptively identify malicious traffic and data exfiltration. As an example, in 2020, a compromise in software that is globally deployed became public.

Following the public announcement, it was not possible to establish quickly whether SoNS were affected, and if they had been compromised. As a result, ACSC spent significant time directly contacting entities to understand if compromised versions of the software were present on their networks and whether they had been exploited for malicious purposes.

The ACSC did not have relevant network telemetry from networks underpinning SoNS that would have allowed the ACSC to automatically alert individual organisations to vulnerabilities or malicious activity occurring on their networks, or understand how vulnerable Australian networks are to a particular adversary or threat.

The Bill seeks to rectify these information gaps by requiring certain network owners to provide to the ACSC, on request by the Secretary of the Department of Home Affairs, relevant network data or telemetry that identifies potential vulnerabilities that might be exploited by an adversary to gain access to their networks and steal information. Understanding of a network's vulnerabilities and subsequent threat exposure in advance (or close to real time) will allow the ACSC to provide tailored and timely advice to protect networks and assist preventing cyber security incidents.

Government Assistance – Intervention Request (35AX)

36. In the rare circumstance of a serious cyber security incident impacting the availability of key critical infrastructure assets, Part 3A, Division 5 of the Bill provides a mechanism for Government to directly assist an asset owner or operator in rapidly responding to, and remediating a cyber-security incident.

37. ASD may be requested by the Secretary of the Department of Home Affairs to assist in responding to a serious cyber security incident. The Minister for Home Affairs must consult with the asset owner or operator before authorising the Secretary to request ASD assistance, and the measures authorised must be proportionate and technically feasible.

38. The Bill includes significant oversight of the new arrangements. Under the proposed Bill, a request for ASD assistance from the Secretary of Home Affairs must be authorised by the Minister for Home Affairs, with the agreement of the Minister for Defence, and the Prime Minister; and the Minister for Home Affairs must be satisfied that:

- a cyber security incident has occurred, is occurring or is imminent
- the incident is having a relevant adverse impact on the functioning of a critical infrastructure asset
- the incident is posing a material risk to the social or economic stability of Australia, its people, national defence or national security
- the relevant entity or entities are unwilling or unable to take all reasonable steps to respond to the incident
- no other options for a practical and effective response exist.

39. In addition, other oversight arrangements are incorporated in the Bill that build on the existing oversight of ASD by the Inspector-General of Intelligence and Security (IGIS). This includes IGIS oversight of any actions undertaken by ASD under the Bill, the IGIS must be notified of a Ministerial Authorisation, and a requirement that ASD provide a report on any action undertaken to the Minister for Home Affairs and the Minister for Defence.

40. Interventions under this provision are limited. In responding to a critical cyber incident, ASD's incident response teams will only be able to undertake actions specified in the Ministerial Authorisation. This may include:

- Accessing, modifying or altering the functioning of computers – in order to understand complex systems, implement mitigations, restore from backups and install incident response tools
- Connecting or disconnecting computers or computer devices – in order to isolate a compromise and connect incident response tools to the network
- Accessing, restoring, copying, altering or deleting software – in order to investigate malicious activity, frustrate malicious actors and uninstall malware.

41. These types of activities are consistent with the actions that ASD undertakes when voluntarily assisting organisations that may be subject to a serious cyber security incident.

Case study

The threshold for government intervention outlined in the Bill is significant. In practice, the types of activities that ASD would perform would be consistent with the voluntary assistance provided to organisations.

As an example, ASD cyber security specialists have worked cooperatively with critical infrastructure operators in response to cyber incidents to remotely access their computers and networks to investigate and remediate a compromise and assist restoration of normal operations.

a. Remediating a compromise could include things such as installing specialised anti-malware or analytic tools and sensors, turning off parts of the networks to contain the spread of malware, deleting malicious software, and patching systems to prevent subsequent compromise.

b. Restoration of normal operations could include things such as restoring systems from backups, modifying configurations, and calling upon specialist industry expertise.

ASD will always seek to undertake this activity in close cooperation with the critical infrastructure owner.

Criminal Code Amendments

42. To effectively perform its functions and defend and respond to serious cyber incidents, including those that harm Australia's critical infrastructure, ASD may engage in computer-related acts offshore, such as affecting an adversary's computer or device. The increasing prevalence of internet-based communications that enable adversaries to actively obscure the geographic location of their devices, or that otherwise make it impossible for ASD to determine the physical location of a device, mean that there will be instances where acts reasonably intended to occur offshore are later identified to have inadvertently occurred on a device within Australia. Currently, ASD cannot mitigate this risk. Accordingly, ASD's ability to respond to malicious cyber activities may be restricted.

43. Schedule 2 of the proposed Bill seeks to overcome this operational gap by amending the limitation of liability for staff members or agents of ASD as currently outlined in section 476.5 of the *Criminal Code Act 1995* (Criminal Code). The new section 476.6 of the Criminal Code will replace ASD's existing limitations on liability by extending the immunity to circumstances where it is reasonable to believe that the actions would only occur offshore, even though the computer-related act, event, circumstance or result in fact takes place inside Australia. The amendments provide that a staff member or agent of ASD is not subject to any civil or criminal liability in circumstances where they engage in conduct:

- on the reasonable belief that it is likely to cause a computer-related act, event, circumstance or result to take place outside Australia (whether or not it in fact takes place outside Australia)
- in the proper performance of a function of ASD, as outlined in section 7 of the ISA.

44. The amendments will not provide ASD staff members with protection for activities where the intended computer-related act, event, circumstance or result would take place onshore, or where the activities would fall outside the proper performance of ASD's functions under the ISA.

45. The amendments are necessary to protect ASD staff members and agents from liability if they inadvertently affect a computer or device located inside Australia. The amendments will ensure ASD can continue to perform its functions to protect Australia's national security, foreign relations and national economic well-being in the increasingly complex online environment and from cyber activities intended to do Australia harm.

ATTACHMENT A: Potential SolarWinds Orion compromise

Home / About the ACSC / View all content / View all alerts / Potential SolarWinds Orion compromise

FireEye identifies global campaign leveraging malicious updates to SolarWinds software.

Alert status: HIGH

Background

On 14 December 2020, the ACSC issued an initial alert regarding potential compromise of the SolarWinds Orion software. This alert was informed by an announcement from cyber security company FireEye, who were monitoring a global intrusion campaign linked to compromise of the SolarWinds Orion software supply chain.

Update

As of 25 January 2021, the ACSC has received a number of reports from Australian organisations notifying that they were operating vulnerable versions of SolarWinds Orion. To date, no follow-on compromise of an Australian organisation through SolarWinds Orion has been identified.

The compromise of the supply chain meant that that organisations that were running SolarWinds Orion may have inadvertently installed malicious additions through normal update processes. The malicious software (malware) associated with the supply chain compromise is being referred to as SUNBURST.

Following the identification of SUNBURST, additional malware associated with the SolarWinds Orion supply chain compromise has been identified. These are commonly being referred to as TEARDROP and RAINDROP and have been identified during investigations of follow-on compromises of affected organisations.

During investigations of the supply chain compromise, additional malware targeting SolarWinds Orion was identified. This second set of malicious software is being referred to as SUPERNOVA. The SUPERNOVA malware is not believed to be related to the supply chain compromise, instead targeting an unrelated vulnerability in SolarWinds Orion.

Mitigation

SolarWinds have identified the vulnerabilities exploited by the compromise and issued patches for affected SolarWinds Orion versions.

Accordingly, ACSC's recommendation for mitigating potentially vulnerable versions of SolarWinds Orion is to apply the latest patches from SolarWinds as soon as possible. This recommendation applies to mitigate against both the SUNBURST and SUPERNOVA malware.

If immediate patching is not possible, the ACSC recommends vulnerable SolarWinds Orion instances be isolated from the internet and internal network connections minimised.

Additional information and supporting tools

The US Cyber security and Infrastructure Security Agency (CISA) has published a number of alerts regarding detection and mitigation of potential compromises of SolarWinds Orion, including CISA and third-party tools that may aid in the detection of follow-on compromise through SolarWinds.

Additionally, the ACSC encourages all organisations to continually assess and apply the Essential Eight strategies to protect their systems.

Assistance

The ACSC is monitoring the situation and is able to provide assistance and advice as required. Organisations that have been impacted or require assistance can contact the ACSC via 1300 CYBER1.

Content written for

- Individuals & families
- Small & medium businesses
- Large organisations & infrastructure
- Government

View all content

First published: 14 Dec 2020
Last updated: 25 Jan 2021