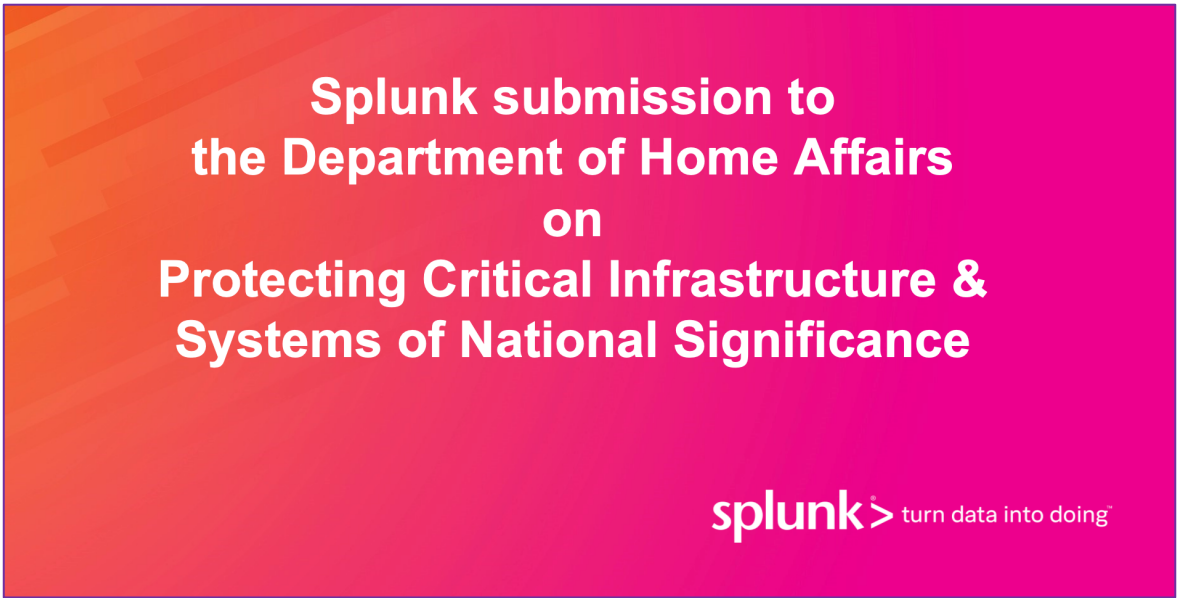
Splunk submission to the Department of Home Affairs on Protecting Critical Infrastructure & Systems of National Significance



Summary

Splunk is a global Data and Cloud company which provides analytical, security and performance capabilities to many of Australia's largest critical infrastructure providers.

Splunk supports the Government's refresh of its cyber security strategy and critical infrastructure protection framework. Based on our capabilities and experience, Splunk is pleased to offer our perspectives on protecting Australia's essential services by uplifting the security and resilience of its critical infrastructure.

In this submission, Splunk is offering eight recommendations for Government to consider:

1. Amend the definition of critical infrastructure.
2. Review international standards and regulation relevant to the Data and Cloud sector and consider these with stakeholders during 2021's co-design activities, leading to adoption of appropriate elements into best practice guidelines and regulatory obligations.
3. Work with each Regulator to assess the time and resources needed for them to become effective.
4. Provide a representative to each Regulator or a dedicated advice mechanism.
5. Establish a consultation mechanism(s) for the Data and Cloud Sector Regulator to engage key non-government stakeholders.
6. Add a requirement for insider threat software capability as an obligation for Systems of National Significance and Regulated Critical Infrastructure Entities, and in the best practice guidelines for other Entities.
7. Establish a pilot program for a critical infrastructure secure hub, offering cyber security focussed capabilities to smaller providers.
8. Wherever possible, automate information sharing and threat technical responses.

General

Why listen to Splunk?

Splunk is one of the world's leading companies in the Data and Cloud sector. Splunk focuses on the most secure and best use of data - from any source, in any structure, and over any timeframe - to produce better decisions and outcomes. While Splunk is known for its cyber security ecosystem, it also has leading solutions for Business Analytics, AppDev and ITOps. Splunk supports on-premise deployments, has significant organic Cloud capabilities, and is also deployable on sovereign and global hyperscale Cloud solutions.

Due to the ever-growing importance of Data in the digital lives of government, business and the community, Splunk has a unique cross-sector perspective into the performance and security issues facing critical infrastructure providers. Splunk's capabilities are used by a large number of Australia's biggest companies, including Telstra, multiple banks, NSW Rail, Woolworths and Coles, AGL, and by Government (including the Department of Defence). Based on our capabilities and experience, Splunk's submission reflects the value Government can gain from collaboration and security uplift "between and across critical infrastructure sectors".[1]

Splunk believes that we offer Government views relevant to Data in all of Australia's critical infrastructure sectors.

Structure

In this submission, Splunk is offering views on selected Questions in the *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper* ("the Consultation Paper"). These views, and related recommendations, are in seven sections:

- View - Q1 - Covered sectors.
- View - Q2 - Definition.
- Views - Q3 and Q5 - Critical entity identification and assessment.
- View - Q20 - Insider threat.
- View - Q15 - Avoiding regulatory duplication.
- Views - Q17 and Q18 - A regulator for the Data and Cloud Sector.
- Views - Q9, Q12, Q19, Q23, Q24, Q25, Q26, and Q27 – Matters related to cost, sharing and response.

[1] *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper*, Page 5.

View - Q1 - Covered sectors

Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?

Splunk supports the Government broadening the sectors and functions considered to be critical infrastructure. In particular, **Splunk strongly supports the inclusion of Data and the Cloud as a critical infrastructure 'sector'**. This is due to the ever-growing importance of Data in the digital lives of government, business and the community. This trend will continue as Australia moves towards a Data and Internet of Things (IoT) enabled society and economy.

In our paper *Splunk Predictions 2020*, we state that the world is on the cusp of a third consecutive decade of enormous transformation in which Data will shape our future. Related predictions include:

- 2020 will be the dawn of a connected decade, with Artificial Intelligence/Machine Learning (AI/ML), Natural Language Processing, augmented reality, IoT, and 5G all maturing and becoming both commonplace and transformative.
- In 2020, Cyber attacks will hit home (literally) through attacks on critical infrastructure and services.
- 2020 will be the year of dark data, the 55% of an organisation's total data that it either doesn't know exists or doesn't know how to find, analyse, and use.
- 2020 will see 5G's IoT push previewing the post-smartphone era, beginning to take hold in healthcare and the industrial space.
- Hackers will find new low-hanging fruit in the cloud, exploiting the emerging vectors brought to bear by cloud native technologies such as containers and Kubernetes, taking advantage of organisations' learning curves to launch new attacks at a scale and speed we have not seen in the on-premise world.
- Attackers will attack AI while it's still learning, to sabotage training data and then disrupt decision-making.

Data is the epitome of the binding interdependencies that exist and flow dynamically between and across critical infrastructure sectors.

More than this, Splunk suggests that Data and Cloud is part of a sub-set of sectors which are critical to the daily functioning of all critical infrastructure. Data and Cloud should be seen as a horizontal player, providing services across critical infrastructure and all other sectors in the Australian economy. Data and Cloud providers are not the data owners and are best seen as data services: securing data; ensuring data availability; providing tools to analyse, extract value from, and manage data; and providing compliance assistance, such as protecting privacy.

View - Q2 - Definition

Do you think the current definition of Critical Infrastructure is still fit for purpose?

> *Those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security.*[2]

A product of its times, the current definition of critical infrastructure in the Australian Government's *Critical Infrastructure Resilience Strategy* is no longer fit for purpose. Specifically, it is too narrow to meet the challenges outlined in the *Cyber Security Strategy 2020* and the Consultation Paper.

Recommendation 1. Splunk suggests that the Government consider amending the current definition as follows:

- **Recommendation 1-1:** Broaden the four elements covered in the definition to include Data. In a digital society and economy, Data is critical and has intrinsic value.[3] The current elements in the definition (physical facilities, supply chains, information technologies and communication networks) are not broad enough to cover the unique nature of Data as a critical infrastructure sector in itself, and as an enabler to all other sectors.
- **Recommendation 1-2:** Consider changing the impact timeline wording from "an extended period" to include more immediate periods. In a digital world, attacks on sectors such as energy, banking and finance, water or Data could have immediate and significant adverse impact on Australia. Alternatively, any timeline reference could be deleted, allowing the consequence of the unavailability ("… would significantly impact on …") to stand as sufficient, time-independent criteria.
- **Recommendation 1-3:** Include Australia's political wellbeing in the definition. With widely publicised hacking attacks against Australian government networks and systems, as well as global reporting of digitally conducted foreign interference in sovereign political processes, Government might consider adding Australia's political wellbeing into the definition alongside social and economic wellbeing.

In amplification of the current definition of critical infrastructure, the DHA-run Workshop on 24 August 2020 proposed the following definition of a critical infrastructure asset in the Data and Cloud sector: *Any asset or system involved in the storage, processing or hosting of information on a commercial basis.* Splunk assumes that this sub-definition is intended to be read in the context of its parent critical infrastructure definition, specifically the impact statement beginning "which if destroyed, degraded or rendered unavailable …".

Similar to the comments made previously in this Section, and Recommendation 1-1, this definition does not encompass Data outside of "information" being its object. Splunk

[2] Critical infrastructure definition in the *Critical Infrastructure Resilience Strategy Plan (2015)*.
[3] For further detail see our comments in the *View – Q1 – Covered sectors* section.

believes that Data has intrinsic value and certain Data sets will be critical to Australia's interests. It is a philosophical question whether Data might therefore be considered 'infrastructure' within the meaning of this Consultation Paper and the Government's intent.

Views - Q3 and Q5 - Critical entity identification and assessment

Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?

How should criticality be assessed to ensure the most important entities are covered by the framework?

Splunk supports the inclusion of an interdependency criteria in determining the relative importance of critical infrastructure entities to Australia.

The *Cyber Security Strategy 2020* notes that "highly sophisticated nation states and state-sponsored actors continue to target governments and critical infrastructure providers".[4] Such sophisticated actors can use systematic approaches in their tradecraft; such as planned cyber reconnaissance to identify direct or indirect attack vectors as part of a 'kill chain' to achieve a desired outcome.[5] Inherent in these approaches is the tactic of gaining access at a vulnerable point and then moving to connected systems where the target information is, or where the desired impact can be achieved.

As implied by the Consultation Paper's reference to "risk within and across sectors",[6] an interdependency of threats requires Government to have an interdependency of understanding of Australia's critical infrastructure entities and their functions. This understanding should include Data interdependencies.

[4] Page 13.
[5] See Lockheed Martin's cyber kill chain (https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf). Another military-grade example is Target Systems Analysis doctrine.
[6] Page 4.

View Q15 – Avoiding regulatory duplication

Would the proposed regulatory model avoid duplication with existing oversight requirements?

Splunk recognises the role of appropriate regulation and strongly supports the intent to avoid regulatory duplication.

Splunk notes that Data and the Cloud are global in nature, and providers potentially have to comply with national, regional and international regulatory frameworks. Examples include privacy, data security, sovereignty provisions, and foreign acquisition and takeover acts. The range and complexity of these requirements can lead to ambiguity, increased compliance costs and, potentially, to conflicting framework requirements.

An example of positive consideration of international frameworks can be found in the Therapeutic Goods Administration's (TGA) 2020 *Consultation Paper on the Scope of Regulated Software-based Products.* This Paper found that there is considerable alignment between other countries and organisations and their approaches to regulation of software-based products.[7] However, data related to medical devices was arguably missing from the TGA's thinking (at that time) when compared to at least one of the cited international benchmarks, the *European Union's Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR*.

There is considerable value in international benchmarking with like-minded regulatory frameworks. However, the inclusion of data, in the context of critical infrastructure, appears to be relatively less mature. Appropriate international standards for regulation of Data and the Cloud are likely to assist in the Government's consideration of its regulatory model and requirements. This is consistent with the drive for sector best practices and particularly relevant to the Australian Data and Cloud sector, as it lacks a natural regulator.

Consequently, Splunk suggests that:

- **Recommendation 2:** DHA review international standards and regulation relevant to the Data and Cloud sector and consider these with stakeholders during 2021's sector specific co-design activities. This should lead to the adoption of appropriate elements of International frameworks into the Data and Cloud sector's best practice guidelines and regulatory obligations.

[7] Page 10, paragraph 3.

Views Q17 and Q18 – A regulator for the Data and Cloud Sector

Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?

What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?

Splunk notes that there is no current Sector Regulator for Data and Cloud. In the DHA-run Workshop on 24 August 2020, it was suggested that DHA's Critical Infrastructure Centre might fulfil this role if a "natural" regulator could not be found.

Given the lack of maturity of the frameworks around Data and Cloud as a 'sector', we believe this suggestion has merit. As a Sector Regulator, the Critical Infrastructure Centre would bring a deep understanding of the government's intent for the regulatory role, a holistic view of how other sector regulators were functioning, and a channel into DHA to rapidly raise and address Data and Cloud issues.

Splunk notes that cyber security, Data, and related technologies are complex and constantly evolving. Not every Sector Regulator will have a sufficient, appropriately skilled workforce to design, implement and oversee new cyber security-related obligations for their sector's regulated Entities and Systems of National Significance. This resourcing issue will need to be addressed for regulation to be successful. Noting the Critical Infrastructure Centre already holds a number of regulatory roles, adequate resourcing levels will be key to this new tasking.

Each Sector Regulator is likely to need different types and levels of support and Splunk suggests that:

- **Recommendation 3:** Government work with each Regulator to assess the time and resources needed for them to be able to become effective.
- **Recommendation 4:** Government consider providing a representative to each Regulator or a dedicated advice mechanism.
- **Recommendation 5:** The Sector Regulator establish a consultation mechanism(s) to engage key non-government stakeholders.

Finally, Splunk considers that, in the long term, a specialist Data and Cloud Sector Regulator may need to be established. As Data and Cloud continue to grow, and the Sector's regulatory frameworks mature, this potential need should be periodically reviewed.

View - Q20 - Insider threat

In the AusCheck scheme potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?

Splunk recognises the importance of criminal and national security checks of staff in relevant security environments. Splunk conducts such checks itself and, to conduct its work with governments and defence forces, has a considerable number of employees with Five Eyes security clearances. While important, such checks offer a snapshot in time of an individual's potential security risk and may only be conducted once or with years in-between. It is also understood that national security assessments are resource and time intensive.

Splunk believes that a continuous assessment model which monitors and analyses appropriate data about employees' at-work behaviour is the most practical way to measure and flag insider threats. A continuous assessment model complements checks by providing longitudinal information on an individual's insider threat risk profile as their life circumstances change. Insider threat analysis software is widely available and provides an effective, affordable, scalable, time sensitive, and privacy appropriate way for critical infrastructure providers to manage such threats.

Splunk suggests that:

- **Recommendation 6:** The Government consider adding the requirement for insider threat software capability for Systems of National Significance and Regulated Critical Infrastructure entities, and into the to-be-issued best practice guidance for other Entities.

Views – Q9, Q12, Q19, Q23, Q24, Q25, Q26, and Q27 – Matters related to cost, sharing and response

The Consultation Paper raises multiple points on the relationship between critical infrastructure sectors and government, including the cost of compliance, the ability and willingness to share threat information, and supporting effective response to threats and breaches.

Cost and workforce

In regard to cost, Splunk's perspective is that there will be both capital and operational cost in meeting Government requirements. It is reasonable to assume that these costs will increase with additional obligations applicable to Regulated Entities and Systems of National Significance. It is also reasonable to assume that such costs will more easily absorbed by large critical infrastructure owners and operators, and by those who already have a mature cyber security posture within a holistic security framework. The cost impacts for smaller critical infrastructure providers, possibly regional or those in smaller states, may be harder for those businesses to absorb.

Splunk notes that, in addition to cost, smaller critical infrastructure providers may also face skills and experience gaps in their workforce.

In the Townhalls conducted after the Consultation Paper's release, officials stated that Government was not considering providing funding to industry to assist with additional costs.

Acknowledging this, Government may wish to consider other ways to assist smaller infrastructure providers address the cost and workforce implications of meeting regulatory obligations. For example, the Government might consider adapting an initiative proposed in the *Cyber Security Strategy 2020* for smaller government Departments faced with similar issues.[8] This is the concept of secure hubs. While there would be implementation issues, it is worth asking how else will these providers achieve the necessary cyber security standards? A genuinely collaborative possibility would be for Government to consider a pilot program for a critical infrastructure secure hub, possible consisting of a combination of Cloud and best-practice SIEM/SOC/SOAR capabilities. Such a pilot program could offer smaller critical infrastructure providers access to information, technical capabilities and skills that may not otherwise be available to them in the short to medium term.

Recommendation 7: Government consider establishing a pilot program for a critical infrastructure secure hub, offering cyber security focussed capabilities and skills to smaller critical infrastructure providers.

[8] Page 40 under the Harden Australian Government IT initiative, specifically to "strengthen defences of (government) networks by centralising their management and operation, including secure hubs. This centralisation seeks to reduce opportunities for malicious actors to target smaller companies with less secure IT".

Sharing and response

Splunk's perspective on information sharing and responses, such as playbooks, is that whatever measures the Government and critical infrastructure sectors take to improve cyber security, their effectiveness will be substantially increased where they are implemented automatically. That is, manually-based/unconnected threat intelligence sharing and response measures are unlikely to be successful as attackers move increasingly to take action and counter-action at machine speed, potentially aided by AI/ML.

Recommendation 8: Government consider supporting the automation of collaboration and technical responses wherever possible, for example by supporting approaches such as Security Orchestration Automation and Response.

Conclusion

Splunk appreciates the opportunity to provide input to Government on how to best protect Australia's essential services by uplifting the security and resilience of its critical infrastructure. As Data and Cloud are the digital home and lifeblood of modern societies, business and government, Splunk sees both as critical to the future of Australia's social, economic, political and security wellbeing.