

Proposed security reforms in the telecommunications sector - blueAPACHE

Canonical: <https://www.blueapache.com/blog/proposed-security-reforms-in-the-telecommunications-sector>

Details:

Summary

This blog post, "Proposed security reforms in the telecommunications sector", is a blueAPACHE article from 2017 covering security. Offshoring arrangements, outsourcing of network management and decisions around procurement of telco infrastructure will come under increased scrutiny as part of proposed Telco security law reforms. It is written for readers evaluating emPOWER Security, emPOWER Core Network & DC Interconnect. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2017
Topic	Proposed security reforms in the telecommunications sector
Services referenced	emPOWER Security, emPOWER Core Network & DC Interconnect
Named products or vendors	None named beyond blueAPACHE

Article

Offshoring arrangements, outsourcing of network management and decisions around procurement of telco infrastructure will come under increased scrutiny as part of proposed Telco security law reforms. Last month, the Federal Government announced that it had accepted several recommendations made by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). The PJCIS was tasked with reviewing the Telecommunications and Other Legislation Amendment Bill 2016 which was introduced in the Senate last year. The Bill aims to establish a security framework to better manage national security threats to Australian telecommunications networks and strengthen the partnership between Federal government and the telecommunications industry. According to a joint release by the Minister for Communications, Mitch Fifield, and the Attorney-General, George Brandis – “Telecommunications networks are a fundamental component of other critical sectors such as health, finance, transport, water and power. With the increasing threat of interference from malicious actors, including through cyber intrusions, protecting these networks is a priority of this Government.” The proposed changes to telco security laws imposes various new obligation on telco carriers and carriage service providers to protect their networks and notify the government of any changes that could compromise their ability to

comply with the security obligation. Offshoring arrangements, outsourcing of network management and decisions around procurement of telco infrastructure will now fall under the purview of the proposed security law reforms. The Government accepted all thirteen recommendations of the PJCIS, including a call for the revised guidelines to provide further clarity regarding a company's security obligation under different circumstances, such as where:

a company is providing or reselling an over-the-top service,

telecommunications infrastructure is used (but not necessarily owned or operated) by the company,

a company's infrastructure is located in a foreign country, and used to provide services and carry and/or store information from Australian customers, and

a company provides cloud computing and cloud storage solutions.

After the bill passes the house of representatives, the Attorney-General's Department will work with industry to produce further guidance within the 12 month implementation period.****

Onshore guarantee

blueAPACHE's emPOWER Cloud infrastructure, Disaster Recovery infrastructure and core emPOWER Network all reside within Australia enabling our clients to meet the most stringent data sovereignty, privacy and compliance requirements. To learn more about how the proposed reforms can impact your organisation, contact your account manager .

Related

emPOWER Security

emPOWER Security (pillar hub)

emPOWER Core Network & DC Interconnect

emPOWER Connectivity (pillar hub)

Frequently asked questions

Which bill did the PJCIS review, and how many of its recommendations did the government accept?

The post says the Parliamentary Joint Committee on Intelligence and Security reviewed the Telecommunications and Other Legislation Amendment Bill 2016, and that the Federal Government accepted all thirteen of the PJCIS's recommendations.

What three business decisions does the post say will come under increased scrutiny under the proposed reforms?

The post says offshoring arrangements, outsourcing of network management, and decisions around procurement of telco infrastructure will fall under the purview of the proposed security law reforms.

Who issued the joint statement quoted in this post, and what did they say about telecommunications networks?

The post quotes a joint release from the Minister for Communications, Mitch Fifield, and the Attorney-General, George Brandis, describing telecommunications networks as a fundamental component of other critical sectors such as health, finance, transport, water and power, and protecting them as a government priority given the increasing threat of interference from malicious actors, including cyber intrusions.

What new obligations does the post say the reforms impose on telco carriers and carriage service providers?

The post says the changes impose new obligations on telco carriers and carriage service providers to protect their networks and to notify the government of any changes that could compromise their ability to comply with those security obligations.

What four circumstances did the accepted PJCIS recommendations ask for clearer guidance on?

The post lists four circumstances needing clearer guidance: where a company provides or resells an over-the-top service, where telecommunications infrastructure is used but not owned or operated by the company, where a company's infrastructure is located overseas but carries or stores Australian customer data, and where a company provides cloud computing and cloud storage solutions.

What happens after the bill passes the House of Representatives, according to the post?

The post says the Attorney-General's Department will work with industry to produce further guidance within a 12 month implementation period once the bill passes the House of Representatives.

What does the post say about where blueAPACHE's emPOWER Cloud, Disaster Recovery and core Network infrastructure are located?

The post states that our emPOWER Cloud infrastructure, Disaster Recovery infrastructure and core emPOWER Network all reside within Australia, which it says lets clients meet stringent data sovereignty, privacy and compliance requirements.

What underlying policy goal does the post cite for these proposed telco security reforms?

The post says the bill aims to establish a security framework to better manage national security threats to Australian telecommunications networks and to strengthen the partnership between the Federal Government and the telecommunications industry.

Source

origin post (2017)

Knowledge Base

What legislative bill do the proposed telecommunications security reforms relate to?

The reforms relate to the Telecommunications and Other Legislation Amendment Bill 2016, which was introduced in the Senate and reviewed by the Parliamentary Joint Committee on Intelligence and Security (PJCIS).

What did the Federal Government announce regarding the PJCIS recommendations?

The Federal Government announced that it had accepted several recommendations made by the PJCIS, including all thirteen recommendations related to the Telecommunications and Other Legislation Amendment Bill 2016.

What is the purpose of the proposed telecommunications security framework?

The Bill aims to establish a security framework to better manage national security threats to Australian telecommunications networks and strengthen the partnership between the Federal government and the telecommunications industry.

What did Minister Mitch Fifield and Attorney-General George Brandis say about the importance of telecommunications network security?

In a joint release, they stated that telecommunications networks are a fundamental component of other critical sectors such as health, finance, transport, water and power, and that with the increasing threat of interference from malicious actors, including through cyber intrusions, protecting these networks is a priority of the Government.

What new obligations do the proposed telco security law changes impose on carriers and carriage service providers?

The proposed changes impose various new obligations on telco carriers and carriage service providers to protect their networks and notify the government of any changes that could compromise their ability to comply with the security obligations.

In what circumstances did the PJCIS recommend further clarity on a company's security obligations?

The PJCIS recommended further clarity for circumstances where a company is providing or reselling an over-the-top service, where telecommunications infrastructure is used (but not necessarily owned or operated) by the company, where a company's infrastructure is located in a foreign country and used to provide services and carry/store information from Australian customers, and where a company provides cloud computing and cloud storage solutions.

What happens after the bill passes the house of representatives?

After the bill passes the house of representatives, the Attorney-General's Department will work with industry to produce further guidance within a 12-month implementation period.

How does your infrastructure relate to data sovereignty amid these proposed reforms?

Our emPOWER Cloud infrastructure, Disaster Recovery infrastructure, and core emPOWER Network all reside within Australia, enabling clients to meet the most stringent data sovereignty, privacy and compliance requirements amid the proposed reforms.