12 February 2019

Parliamentary Joint Committee on Intelligence and Security
By online submission

REVIEW OF THE TELECOMMUNICATIONS AND OTHER LEGISLATION AMENDMENT (ASSISTANCE AND ACCESS) ACT 2018 – BSA COMMENTS

BSA | The Software Alliance (**BSA**) thanks the Parliamentary Joint Committee on Intelligence and Security (**Committee**) for the opportunities to comment on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (**Bill**) (as it was then known), including at a public hearing held by the Committee on 19 October 2018, and through written submissions made to the Committee on 12 October 2018 and 31 October 2018.[1]

BSA and our members[2] reaffirm our significant interest in the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (**Act**) as introduced and passed by the Australian Parliament on 6 December 2018. We would like to offer the following comments and recommendations for the Committee's consideration in its review of the Act.

A. GENERAL COMMENTS

We continue to acknowledge and support the Australian Government's desire to have more powerful tools to aid in the fight against criminal and terrorist activities, while urging the adoption of further safeguards to ensure that the authorities under the Act are not exercised to the undue detriment of privacy, security, and trust in the digital economy.

We commend the Committee on the positive recommendations made in its Advisory Report of 5 December 2018 (**Advisory Report**) to improve the drafting of the Bill. These include the following recommendations:

- Recommendation 9 – for the Bill to be amended to clarify the meaning of 'systemic weakness' and to clarify that technical capability notices cannot be used to create a systemic weakness (**Recommendation 9**); and
- Recommendation 11 – for the Bill to be amended to allow a designated communications provider (**DCP**) to seek a binding assessment on whether a technical capability notice (**TCN**) fulfils certain pre-conditions for issuance (**Recommendation 11**).

[1] Copies of our 12 October 2018 and 31 October 2018 written submissions are available at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Submissions.

[2] BSA's members include: Adobe, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Baseplan Software, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

We note that the Act includes most of the Committee's recommendations. However, further improvements can be made to the Act, including to give better and fuller effect to the Committee's recommendations.

In particular, the Act can be amended to improve, among other things:

- oversight of the issuance and variation of technical assistance notices (**TANs**) and TCNs; and
- the definition of 'systemic weakness'.

Our specific comments and recommendations in this regard are in section B below.

We also offer additional comments and recommendations, in relation to other concerns we have with the Act, in section C below.

B. SPECIFIC COMMENTS AND RECOMMENDATIONS TO IMPLEMENT COMMITTEE RECOMMENDATIONS

1. Improve oversight of issuance and variation of TANs and TCNs

There continues to be insufficient independent oversight of the issuance of mandatory TANs and TCNs under the Act. We support further enhancements to the Act, including to fully implement the Committee's Recommendations.

1.1 Address deficiencies in implementing Committee recommendations

We note that the Act now contains a more defined process for an affected DCP to seek an assessment[3] of whether a TCN fulfils certain pre-conditions before being issued or varied (including compliance with the prohibition[4] against requiring a DCP to implement or build a systemic weakness or systemic vulnerability) (**TCN Assessment Process**). This is ostensibly in furtherance of the Committee's Recommendation 11.

While we appreciate this improvement in the Act (as compared with the Bill), the Act does not fully implement the Committee's Recommendation 11. For example, under the current TCN Assessment Process in the Act:

- the assessors are appointed by the Attorney-General (**AG**) only[5] (which could create concerns over their independence), instead of being appointed jointly by the AG and the DCP as contemplated under Recommendation 11;
- the assessors need only consider[6] whether the relevant pre-conditions have been met for issuance of a TCN, instead of needing to agree that these conditions have been met as contemplated by Recommendation 11; and
- the assessment does not appear to be binding on the AG[7] as contemplated by Recommendation 11.

[3] See Schedule 1, item 7, sections 317WA and 317YA of the Act.

[4] See Schedule 1, item 7, section 317ZG of the Act.

[5] See Schedule 1, item 7, sections 317WA(2) and 317YA(2) of the Act.

[6] See Schedule 1, item 7, section 317WA(7) of the Act.

[7] Under Schedule 1, item 7, sections 317WA(11) and the 317YA(10) of the Act, the AG only needs to "have regard to" the relevant assessment report.

Additionally, the TCN Assessment Process in respect of the variation of TCNs[8] omits certain matters from the list of matters to be assessed (as compared to the TCN Assessment Process in respect of the issuance TCNs), such as:

- whether the requirements imposed by the TCN as proposed to be varied are reasonable and proportionate;[9]
- whether compliance with the TCN as proposed to be varied is practicable;[10]
- whether compliance with the TCN as proposed to be varied is technically feasible;[11] and
- whether the TCN as proposed to be varied is the least intrusive measure that would be effective in achieving the legitimate objective of the TCN as proposed to be varied.[12]

This results in a potential loophole whereby DCPs could be made to do acts or things, under a varied TCN, that would otherwise have been prohibited under the initial TCN.

We note that the amendments in sheet no. 8625 tabled by the Opposition in Parliament[13] (**8625 Amendments**) would give better effect to Recommendation 11, as they provide for the assessments to be binding on the AG and for the assessors to have to agree on the matters to be assessed. Additionally, the 8625 Amendments, which would require the same list of matters to be considered in respect of both the issuance and the variation of TCNs, would resolve the potential loophole mentioned above. However, further amendments will still need to be made to ensure that the assessors are jointly appointed by the AG and the DCP (and not by the AG only) to give full effect to Recommendation 11.

In respect of TCNs, we also note that the timeframes for DCPs to be consulted before the issuance or variation of TCNs (including for the TCN Assessment Process to run its course) can be truncated in the event of 'urgency'.[14] There is, however, no definition or guidelines as to what constitutes 'urgency'.

In respect of TANs, we further note that, while DCPs must be consulted before the issuance of TANs, the consultation can also be dispensed with in cases of 'urgency'.[15] Additionally, there is no requirement to consult DCPs for variations of TANs, and the overall TAN regime does not include a similar assessment process as the TCN Assessment Process.

Due process would be enhanced by having greater transparency on what constitutes 'urgency' in respect of the issuance and variation of TANs and TCNs, requiring consultations with the DCP for both the issuance and variation of TANs, and including in the TAN regime a similar assessment process as the TCN Assessment Process.

We recommend that:

- with respect to the TCN Assessment Process, the 8625 Amendments should be adopted, with further amendments to require the joint appointment of the assessors by the AG and the DCP;
- the Act should include a definition and/or provisions providing greater clarity on what constitutes 'urgency';
- the TAN regime should require DCPs to be consulted before TANs are issued or varied; and

[8] See Schedule 1, item 7, section 317YA of the Act.

[9] As compared with Schedule 1, item 7, section 317WA(7)(a)(ii) of the Act.

[10] As compared with Schedule 1, item 7, section 317WA(7)(a)(iii) of the Act.

[11] As compared with Schedule 1, item 7, section 317WA(7)(a)(iv) of the Act.

[12] As compared with Schedule 1, item 7, section 317WA(7)(a)(v) of the Act.

[13] Available at: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195.

[14] See Schedule 1, item 7, sections 317W(3) and 317Y(3) of the Act.

[15] See Schedule 1, item 7, section 317PA(2) of the Act.

- the TAN regime should include a similar assessment process as the TCN Assessment Process.

1.2 Provide for greater judicial oversight

In our submission of 12 October 2018 to the Committee (**12 October Submission**), we had recommended that the assistance and access regime should be underpinned by judicial authorization and incorporate a robust judicial oversight and challenge mechanism.

Subject to our comments in section B1.1 above, Recommendation 11, if fully implemented in the Act, would provide a firm opportunity for an affected DCP to request and make representations in an assessment of whether a TCN should be issued (or varied), and would require one of the assessors to be a person who has served as a judge for a period of 5 years (but who no longer holds commission as a judge). Recommendation 8 of the Committee's Advisory Report (which the Act has implemented)[16] would also require TCNs to be approved by the Minister of Communications prior to their issuance.

While these additional safeguards are positive improvements upon the Bill for due process and oversight, the determination of whether a TCN (or TAN) should be issued (or varied) should ultimately involve an independent, objective judicial authority. This is especially important considering the intrusive nature of TANs and TCNs and their potential to compromise the security and privacy of organizations and individuals. Relating to this, we support the amendments in sheet no. 8627 tabled by the Opposition in Parliament[17] (**8627 Amendments**), which would provide for greater judicial involvement and oversight in the issuance and variation of TANs and TCNs.

To enhance due process and transparency under the Act, we reiterate that the assistance and access regime should include a procedure to allow an affected DCP to challenge a decision to issue or vary a TAN or TCN on its merits. This would also include the ability to request a review of the decision based on any new evidence that arises after the decision is made. At the minimum, the Act should not exclude the new Part 15 of the *Telecommunications Act 1997* (i.e., the provisions governing the issuance of technical assistance requests (**TARs**), TANs, and TCNs) from the scope of the *Administrative Decisions (Judicial Review) Act*, so as to afford affected DCPs full and proper recourse to judicial review in respect of decisions under the new Part 15 of the *Telecommunications Act 1997*.

We recommend that:

- the decision to issue or vary a TAN or TCN should be made or approved by an independent judicial authority and, in relation to this, the 8627 Amendments should be adopted at the minimum; and
- the Act should incorporate a procedure to allow an affected DCP to challenge a decision to issue or vary a TAN or TCN on its merits and, in relation to this, the Act should be amended to remove the exclusion of the new Part 15 of the *Telecommunications Act 1997* from the scope of the Administrative Decisions (Judicial Review) Act at the minimum.

1.3 Additional improvements to oversight mechanisms

Under the Act, there is no need for law enforcement agencies to show that they have gone through an escalation of process before turning to issuing a TAN or TCN. It would be useful to clarify the processes that agencies will have to go through to prove that they have exhausted all options before escalating their request to require a TAN or TCN to be issued to a DCP. This would prevent

[16] See Schedule 1, item 7, section 317TAAA(1)(b) and the related section 317XA(1)(a)(ii) of the Act.

[17] Available at: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195.

agencies from using the Act as an 'easy way out' to get access to encrypted communications, especially in situations where less intrusive means of accessing such information are available.

Additionally, there is currently no single agency overseeing the issuance of TANs and TCNs (and TARs) under the Act. This may result in a DCP receiving multiple requests for similar information and assistance from different agencies, which would unnecessarily burden the DCP and result in inefficiency in the provision to and receipt by law enforcement agencies of information and assistance.

We recommend that:

- there should be a transparent escalation process adopted under the Act for law enforcement agencies to go through prior to issuing TANs or TCNs; and
- there should be a central agency under the Act to coordinate the issuance of TANs and TCNs (and TARs).

2. **Improve definition of 'systemic weakness'**

Pursuant to Recommendation 9, we note that the Act now includes in section 317B[18] the following definitions for 'systemic weakness' and the related 'systemic vulnerability':

> "***systemic vulnerability*** means a vulnerability that affects a whole class of technology, but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified."
>
> "***systemic weakness*** means a weakness that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified."

However, the above Act definitions are broad and ambiguous. For example, it is unclear:

- what constitutes 'a whole class of technology'; and
- when a target technology would not be 'connected with a particular person' (and hence fall within the definitions of 'systemic weakness' and 'systemic vulnerability' and be covered by the general prohibition against requiring DCPs to implement or build systemic weaknesses and systemic vulnerabilities), especially when considering that the definition of 'target technologies' in the Act is extremely broad and includes services, software, or equipment that are used or 'likely to be used', 'whether directly or indirectly', by the target individual.

The breadth and ambiguity of the current definitions will result in great difficulty in proving when a systemic weakness or systemic vulnerability is created. Put another way, these definitions significantly reduce the effectiveness of the general prohibition in section 317ZG[19] against requiring DCPs to implement or build systemic weaknesses or systemic vulnerabilities.

In our 31 October 2018 submission to the Committee, we had proposed amending section 317ZG (of the Bill) to include definitions for 'systemic weakness' and 'systemic vulnerability', and to ensure that the acts and things that a DCP can be required to do under the assistance and access regime should not include implementing or building any weakness or vulnerability in any system, product, service, or component.

[18] Schedule 1, item 7, section 317B of the Act.

[19] Schedule 1, item 7, section 317ZG of the Act.

We have updated our proposed amendments (to account for the existing language of section 317ZG in the Act) and offer these for the Committee's re-consideration:

(Red double-underlined text = text to be added; red struck-through text = text to be deleted)

"**317ZG Designated communications provider must not be requested or required to implement or build a systemic weakness or systemic vulnerability etc.**

(1) A technical assistance request, technical assistance notice or technical capability notice must not have the effect of:
   (a) requiring a designated communications provider to implement or build a systemic weakness~~,~~ or a systemic vulnerability~~, into a form of electronic protection~~; or
   (b) preventing a designated communications provider from rectifying a systemic weakness~~,~~ or a systemic vulnerability~~, in a form of electronic protection~~.

(2) The reference in paragraph (1)(a) to implement or build a systemic weakness~~,~~ or a systemic vulnerability~~, into a form of electronic protection~~ includes a reference to implement or build a new decryption capability ~~in relation to a form of electronic protection~~.

(3) The reference in paragraph (1)(a) to implement or build a systemic weakness~~,~~ or a systemic vulnerability~~, into a form of electronic protection~~ includes a reference to one or more actions that would render a ~~systemic~~ method~~s~~ of authentication or encryption less effective.

(4) Subsections (2) and (3) are enacted for the avoidance of doubt.

~~(4A) In a case where a weakness is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic weakness into a form of electronic protection includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person.~~

~~(4B) In a case where a vulnerability is selectively introduced to one or more target technologies that are connected with a particular person, the reference in paragraph (1)(a) to implement or build a systemic vulnerability into a form of electronic protection includes a reference to any act or thing that will, or is likely to, jeopardise the security of any information held by any other person.~~

~~(4C) For the purposes of subsections (4A) and (4B), an act or thing will, or is likely to, jeopardise the security of information if the act or thing creates a material risk that otherwise secure information can be accessed by an unauthorised third party.~~

(5) A technical assistance request, technical assistance notice or technical capability notice has no effect to the extent (if any) to which it would have an effect covered by paragraph (1)(a) or (b).

(6) In this [section][Part]:

system includes product, service, and component.

systemic weakness means a weakness in a system that extends, or carries the risk of being extended, beyond a targeted system in a manner that affects:
   (a) other systems;
   (b) the integrity of activities or processes, including patch management or configuration, that are integral to the functionality or security of other systems; or
   (c) other users of the targeted system or other systems.

systemic vulnerability means a systemic weakness that can be exploited to negatively impact a system or a user of the system."

We would again welcome the opportunity to continue refining the language above in discussion and collaboration with the Committee and other relevant Government and Opposition stakeholders.

We also note that the amendments in sheets nos. 8626 and 8629 tabled by the Opposition in Parliament[20] (**8626/8629 Amendments**) offer an alternative to the current drafting of section 317ZG. While the 8626/8629 Amendments do not include any definition for 'systemic weakness' or 'systemic vulnerability', the amendments nonetheless do address to a certain degree our concerns.[21] We would accordingly be prepared to support the adoption of the 8626/8629 Amendments at the minimum.

We recommend that:

- our proposed amendments above to section 317ZG should be adopted (with further refinements as may be appropriate in consultation with the Committee and other relevant Government and Opposition stakeholders); and
- as an alternative to our proposed amendments, the 8626/8629 Amendments should be adopted.

C. ADDITIONAL COMMENTS AND RECOMMENDATIONS

In addition to the specific comments and recommendations in section B above to implement the Committee's Recommendations, we offer the following comments and suggested amendments to the Act for the Committee's consideration.

1. Clarify that the Act does not introduce new interception authorities

New section 317ZGA[22] provides that a TCN has no effect to the extent that it requires the DCP to ensure that a telecommunications service or telecommunications system has: (i) a capability to enable a communication passing over the system to be intercepted; (ii) a capability to transmit lawfully intercepted information to applicable delivery points; or (iii) a delivery capability. This appears to ensure that interception capabilities are to be dealt with under the *Telecommunications (Interception and Access) Act 1979* (**TIA Act**).[23]

To further clarify that the Act does not grant any new interception authority, whether under TCNs or TANs, **we recommend that**:

- section 317ZGA should be expanded to cover TANs (*mutatis mutandis*); and/or
- a new provision should be inserted (possibly in the current section 317ZH[24]) to the effect that "a technical assistance notice or technical capability notice has no effect to the extent (if any) to which it would require a designated communications provider to build or implement a capability to intercept communications, unless the designated communications provider is a carriage service provider or carrier for the purposes of the Telecommunications (Interception and Access) Act 1979."

---

[20] Available at: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195.

[21] The 8626/8629 Amendments import the key factor, from our proposed amendments, for determining when there is a systemic weakness (or systemic vulnerability) – i.e., the risk that the weakness affects other users/information. However, the 8626/8629 Amendments have added a 'materiality' requirement, which we would prefer to have excluded, as it raises the threshold for determining what is a systemic weakness or systemic vulnerability.

[22] Schedule 1, item 7, section 317ZGA of the Act.

[23] See also paragraph 307 on page 45 of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 – Supplementary Explanatory Memorandum – Amendments to be Moved on Behalf of the Government*, available at: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195.

[24] Schedule 1, item 7, section 317ZH of the Act.

2. **Limit the Act's scope in terms of extraterritorial effect and organizations subject to the Act**

One of the recommendations in our 12 October Submission was to limit the application of the Bill, in terms of both extraterritorial effect and the types of organizations that were subject to the Bill. In this regard, we note that the Act continues to apply not only to organizations directly providing communications services in Australia, but also to organizations operating outside of Australia and anywhere in the supply chain, including organizations that might have no control over the final product or service and virtually no link to Australia.

Furthermore, TARs, TANs, and TCNs can be issued to a DCP for the purposes of enforcing the criminal laws of a foreign country.[25] This means that the Act could potentially be leveraged by other countries to bypass their own law enforcement processes.

We recommend that:

- it should be an explicit requirement that a TAN or TCN should be issued to the organization that is the most appropriate to provide the required assistance;
- the extraterritorial application of the Act should be limited by:
  - expressly carving out organizations that are not actively targeting the Australian market for their business activities;
  - expressly carving out organizations that do not exercise control over the final product or service (to address supply chain implications);
  - extending the defense in section 317ZB(5)[26] to:
    - non-compliance with a TAN or TCN in respect of activities within Australia where compliance will result in a breach of another jurisdiction's laws;
    - non-compliance with a provision contemplated under Schedules 2 through 5 of the Bill, in respect of activities in foreign jurisdictions as well as within Australia; and
    - criminal penalties that the Provider may be exposed to in Australia due to non-compliance with any provision of the Bill where compliance will result in a breach of another jurisdiction's laws;
  - confining the applicability of the Act to only crimes punishable under the Australian legal system; and
  - inserting a new provision (possibly in section 317ZH, or an expanded section 317ZGA in line with our recommendation in section C.1 above) to the effect that "a technical assistance notice or technical capability notice has no effect to the extent (if any) to which it would require a designated communications provider to do an act or thing in violation of a foreign country's law."

3. **Limit TARs, TANs, and TCNS to serious offences with a higher penalty threshold and to narrowly-defined national security circumstances**

In our 12 October Submission, we had recommended limiting the list of purposes for which TARs, TANs, and TCNs could be issued to preventing or detecting serious crime and protecting against an identified threat to national security under a narrowly defined set of circumstances. We commend, in this regard, the Act's inclusion of a 'serious Australian offence' qualifier in respect of the purposes for which TARs, TANs, and TCNs may be issued.[27]

[25] See Schedule 1, item 7, sections 317G(2), 317L(2), and 317T(2) of the Act.

[26] Schedule 1, item 7, section 317ZB(5) of the Act, which provides a DCP a defence against civil penalties for non-compliance with a TAN or TCN, where compliance with the TAN or TCN in a foreign jurisdiction will result in the Provider breaching the laws of that jurisdiction.

[27] See Schedule 1, item 7, sections 317G(2), 317L(2), and 317T(2) of the Act.

However, we note that 'serious Australian offence' is defined in Section 317B as "an offence against a law of the Commonwealth, a State or a Territory that is punishable by a maximum term of imprisonment of 3 years or more or for life." While this is consistent with the Committee's Recommendation 2 in its Advisory Report,[28] the 3-year imprisonment threshold covers many other types of offences that are not as serious as terrorism or child abuse, which the Act was intended to capture.[29] Additionally, this threshold is not aligned with the TIA Act, which defines 'serious offence' as, among others, "an offence punishable by imprisonment for life or for a period, or maximum period, of **at least 7 years**" (emphasis added). The definitions should be aligned for clarity and to avoid confusion in the Australian law enforcement regime. We further note that there remains no definition or criteria in the Act for what is considered 'national security'.

We recommend that:

- the definition of 'serious Australian offence' under the Act should be aligned with the definition of 'serious offence' under the TIA Act; and
- with respect to national security, the use of TARs, TANs, and TCNs should be limited to protecting against an identified threat to national security under a narrowly defined set of circumstances (such as preventing an imminent national security threat to Australia and its citizens).

4. **Ensure the protection of technical information including source code**

Another concern raised in our 12 October Submission was on the disclosure of technical information such as source code, which constitutes one of the most valuable assets of BSA's members.

We recommend that:

- the Act should include additional protections in respect of the use and protection of technical information, such as a purpose limitation, obligations to have in place appropriate security measures, and limitations on retention periods;
- technical information that DCPs may be compelled to disclose should be limited to information that is public or commonly shared under commercial non-disclosure agreements; and
- DCPs should not be required to reveal their sensitive intellectual property, including source code and, in relation to this, a new provision should be inserted (possibly in section 317ZH or an expanded section 317ZGA in line with our recommendation in section C.1 above) to the effect that "a technical assistance notice or technical capability notice has no effect to the extent (if any) to which it would require a designated communications provider to disclose or provide any source code that it has not already made available publicly or previously disclosed or provided to a government entity."

5. **Improve handling of vulnerability information**

In our 12 October 2018 Submission, we also commented on the risks associated with vulnerabilities that have not yet been patched and that could be exploited by bad actors, including nation state bad actors, who learn of those vulnerabilities. Given the broad new information gathering powers granted to law enforcement under the Act (including remote access searches and seizure of evidence on computers) it is very likely that law enforcement and intelligence officials will handle vulnerability information, including information on vulnerabilities of which the DCPs themselves are unaware.

[28] The Committee's Recommendation 2 is for the industry assistance measures under the Bill, so far as they relate to criminal law enforcement, to apply to offences with a penalty of a maximum period of 3 years' imprisonment or more.

[29] See paragraph 4 on page 2 of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 – Explanatory Memorandum*, available at: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6195.

We recommend that:

- DCPs should not be compelled to reveal details of vulnerabilities that have not yet been patched; and
- a transparent policy for handling and disclosing vulnerabilities the Government discovers and that are unknown to DCPs should be included in the Act.

6. **De-criminalize unauthorized disclosures of information by employees of DCPs**

The provisions in section 317ZF[30] against unauthorized disclosures of information appear not to require any *mens rea* and could result in employees of DCPs, who are seeking to comply with a TAR, TAN, or TCN, but who make innocent and/or inadvertent disclosures, being exposed to imprisonment for up to 5 years. For example, if an engineer, who is an employee of a DCP, were to be required to build a tool pursuant to a TCN and: (i) the engineer asks another colleague a technical question relating to the TCN; or (ii) if the TCN were so burdensome and consequential to the DCP's business that the engineer and/or the DCP's lawyers must consult the business head or the CEO of the DCP, they could face imprisonment of up to five years (as these scenarios might not be covered under the exceptions in section 317ZF).

To ensure that DCPs are not unduly hindered in their ability to address TARs, TANs, or TCNs, **we recommend that** unauthorized employee disclosures of information should be de-criminalized by, for example, deleting section 317ZF(1)(b)(ii).

7. **Provide a longer time period for DCPs to comply with TANs and TCNs**

DCPs are, by default, given 90 days to comply with TANs and 180 days to comply with TCNs.[31] These are short periods of time considering the need for the DCP to develop an approach to comply with the relevant requirement(s). The Act should not set an arbitrary number that does not reflect the realities on the ground such as the need to shift resources and meet internal processes to comply with the request.

We recommend that the window of compliance should be determined in consultation with the DCP, based on the degree of compliance needed (e.g., amount of information sought, types of information sought, etc.).

D. CONCLUSION

As we noted in our earlier submissions to the Committee, the issues concerning the assistance and access regime are complex and sensitive. Accordingly, in addition to the comments and proposals above, BSA would again like to commend, for the Committee's consideration, the other recommendations in our 12 October 2018 Submission which have not been specifically reiterated above, but which remain unaddressed in the Act.

BSA and our members remain at the disposal of the Committee and the Australian Government and Opposition stakeholders to help develop and deliver other enduring solutions to address the challenges of accessing evidence in the digital age.

BSA | THE SOFTWARE ALLIANCE

[30] Schedule 1, item 7, section 317ZF of the Act.

[31] See Schedule 1, item 7, sections 317MA(1)(b) and 317TA(1)(b) of the Act.