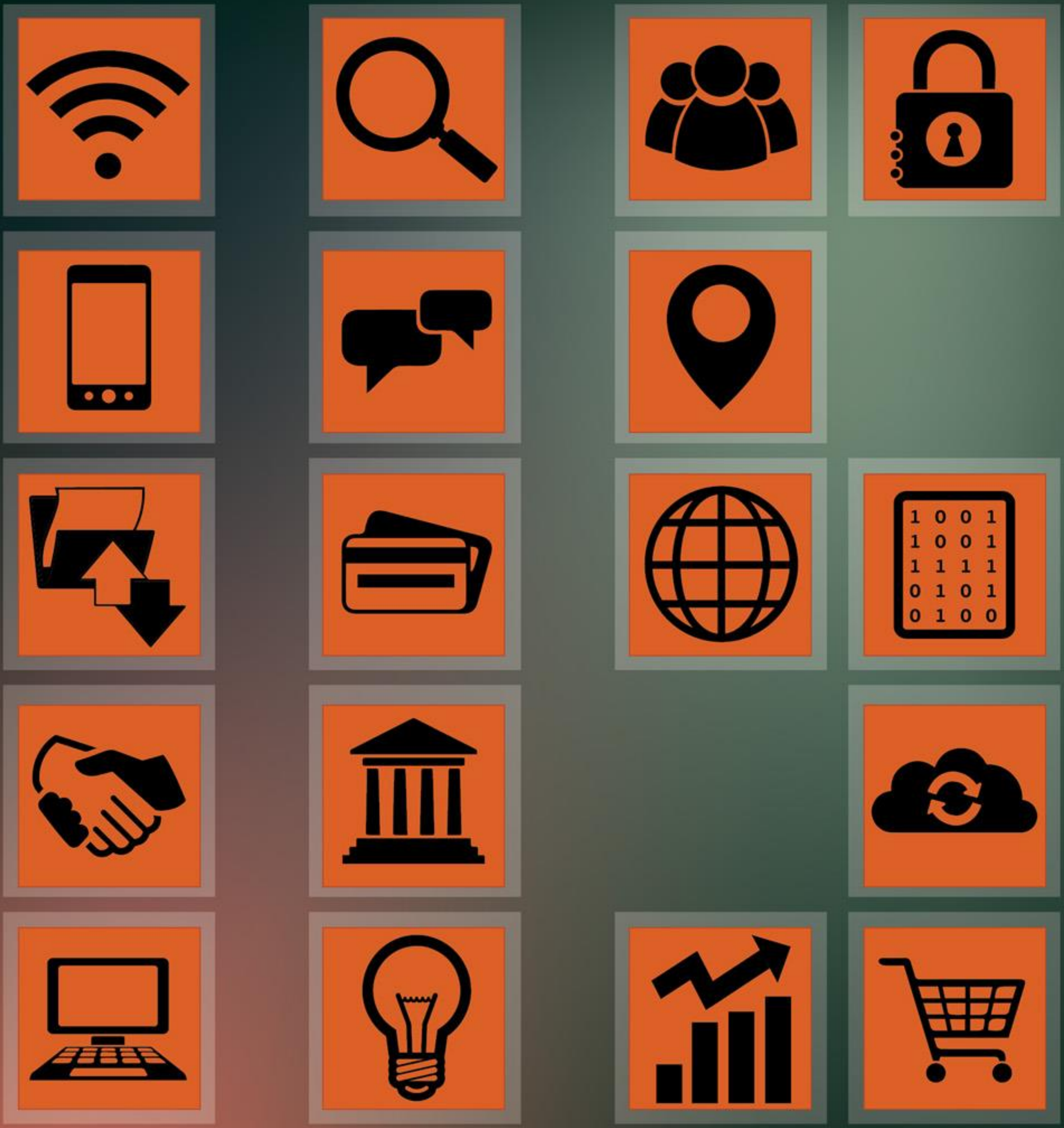

Privacy Impact Assessment – Safety by Design Assessment tool – Condensed report

For: **Office of the eSafety Commissioner**

Date: **10 May 2021**

INFORMATION
INTEGRITY
SOLUTIONS

managing the **privacy** of **individuals** is **complex** and we can help you get it **right**

Table of contents

Glossary

Abbreviation or term	Expansion or definition
APPs	Australian Privacy Principles (13 rules contained in the Privacy Act)
CCPA	California Consumer Privacy Act
eSafety	Office of the eSafety Commissioner
FTC	Federal Trade Commission (US regulator with responsibility for federal privacy enforcement)
GDPR	The EU's General Data Protection Regulation
IIS	Information Integrity Solutions (report author)
LGPD	Brazil's General Data Protection Law
Long-term data store	Database in the back-end of the tool that stores data collected by the tool's front-end. Contains information about the user interactions with the tool including progress through modules and responses to questions.
OAIC	Office of the Australian Information Commissioner
PbD	Privacy by Design
Personal data	'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.' (GDPR definition)
Personal information	'information or an opinion about an identified individual, or an individual who is reasonably identifiable' (Privacy Act definition)
PIA	Privacy Impact Assessment
Privacy Act	Australian *Privacy Act 1988* (Cth)
Return token	A random alpha-numeric code issued to a user when they launch the tool. The user can use the token to resume their progress through the tool. The token expires at a predetermined time after the user's last interaction with the tool.
SbD	Safety by Design
Session cookie	A temporary file stored on a user's browser. The SbD tool places a session cookie on the user's browser to allow it to record (and therefore 'remember') the user's progress through the tool. Session cookies erase when the user

Abbreviation or term	Expansion or definition
	closes their browser. The session cookies used by the tool contain minimal information.
Session ID	The alpha-numeric code assigned to a user of the SbD tool. User interactions with the tool and responses to questions are recorded in association with the session ID. In this way, the tool recognises such interactions as belonging to the same user. The session ID and return token are the same code.
Temporary data store	Database in the tool’s front-end. Contains information about the user interactions with the tool including progress through modules and responses to questions.

1. Executive summary

The Office of the eSafety Commissioner (eSafety) engaged Information Integrity Solutions Pty Ltd (IIS) to conduct a Privacy Impact Assessment (PIA) on its Safety by Design (SbD) Self-Assessment Tool. The tool is being developed to allow companies to assess their own e-safety practices and will provide resources and guidance to help them improve and embed SbD.

This PIA report:

- Maps information flows in the SbD tool
- Identifies privacy impacts for users of the tool
- Assesses the tool's data handling practices and systems for compliance with privacy regulations, good practice considerations and relevant guidelines
- Makes recommendations to address identified issues and risks.

1.1 IIS's overall opinion

IIS finds the privacy impact of the tool to be low. While there are some considerations for eSafety in terms of managing possible coverage by the GDPR, IIS finds that the tool would largely operate outside the coverage of most privacy regulations. This is because the tool has been designed to avoid collection of identifying data.

As a matter of good practice, IIS also considered the tool through the foundational privacy principles of transparency, data minimisation, purpose limitation, security, data retention and disposal, and individual rights. We find that the tool has been thoughtfully designed and is well-placed (with minor improvements in some areas) to meet the spirit of these principles. The most important consideration going forward is ensuring that relevant policies and procedures are documented and implemented, and that there are processes for oversight, assurance and governance of change.

IIS has made six recommendations for strengthening eSafety's approach:

- *Recommendation 1* – Manage GDPR coverage
- *Recommendation 2* – Manage identifiability risks
- *Recommendation 3* – Enhance transparency about the tool's data handling
- *Recommendation 4* – Be transparent with use of cookies
- *Recommendation 5* – Formalise decision about which data variables are transferred to the long-term data store
- *Recommendation 6* – Formally document governance processes

2. PIA scope and methodology

2.1 Scope

eSafety asked IIS to conduct a PIA on its proposed SbD self-assessment tool. This report aims to:

- Map personal information flows in the SbD tool
- Identify privacy impacts for users of the tool
- Assess the self-assessment tool's system and process design for compliance with privacy legislation and community expectations
- Make recommendations to address identified issues and risk.

In providing this report, IIS makes the following qualifications:

- The PIA considers possible security or technical issues for the solution, but it does not undertake detailed investigations or reviews of technical or security features
- The PIA is based on information gathered from eSafety as IIS did not conduct bespoke community or stakeholder consultations for this assessment
- IIS does not provide legal advice; rather it provides strategic privacy and security advice.

2.2 Methodology

In undertaking the PIA, IIS has taken the following steps:

- Planned activities for the PIA in consultation with eSafety
- Gathered information including reviewing documentation and meeting with eSafety staff
- Analysed privacy risk, taking into account:
    - The *Privacy Act 1988* (Privacy Act) and the requirements of the Australian Privacy Principles (APPs)
    - International privacy standards and regulations including the European Union (EU) General Data Protection Regulation (GDPR) and relevant privacy laws in the United States of America (USA), Canada, and New Zealand
    - Privacy by design and trust by design principles
    - Relevant privacy guidelines and frameworks
    - Privacy best practice stemming from IIS's knowledge and experience
- Prepared a draft PIA report and circulated the report to the eSafety for feedback
- Finalised the PIA report and prepared this condensed report for publication.

3. Project description

3.1 Background

eSafety launched the SbD program in 2019. Working with industry, eSafety established a set of SbD principles that encourage organisations to put user safety at the centre of the design, development, and release of online products and services. According to eSafety, the SbD principles have been well received by industry and stakeholders; 'however, the principles as currently presented are in a static document and are challenging for industry to apply practically to their circumstances.'[1]

Therefore, the next phase of the program involves the development of an interactive SbD Self-Assessment Tool ('the tool') that is the subject of this PIA. The tool will allow companies to assess their own practices and will provide resources and guidance to help them improve and embed SbD. eSafety has the tool under development and a prototype is being tested whilst content (modules and end reports) is developed and finalised.

3.2 Overview of the SbD Self-Assessment Tool

The tool will be broadly tailored to user type. User types will be determined along two main axis – (i) company size: start-up, mid-tier and top-tier; and (ii) the most relevant track for the person filling out the assessment: 'CEO/Director/Founder' or 'Product/Policy/Project Owner or Manager'. Questions in the modules will be multiple choice and answers will be weighted to allow the tool to score the company's performance. At the end of each module the user will receive an end report, providing a top-line assessment of their current position as well as guidance and resources to support continued improvement.

3.3 Nature of information and information flows

3.3.1 Nature of the information involved

There are two broad categories of information that is collected by the SbD tool:

1) Information about the user and their company
The tool asks the user to select the most relevant track or position type within the company, offering two options: (i) CEO/Director/Founder and (ii) Product/Policy/Project Owner or Manager.
The tool gathers the following information about the company in the 'About us' section: ● Size (0-250 employees, 250-1500 employees and more than 1500) ● Sector (social networking, video streaming, video gaming, entertainment, retail and so on)

[1] Office of the eSafety Commissioner, *Safety by design assessment tool: business requirements document – draft*, 28 September 2020, p 6.

- Communications tools offered by the company (voice call, video call, text chat, direct messaging and so on)
- Types of interactive tools offered (content generation, photo sharing, file sharing, and so on)
- Mode of registration to the company's service
- Known age of users.

eSafety's firewall also passively gathers a piece of information about the country of origin of the user derived from their device's IP address. The IP address is not stored within the tool and is not recorded long term within the database.

2) User responses to questions about e-safety (multiple-choice):

The main portion of the tool comprises questions that ask users about their companies' e-safety practice as structured by the modules. For example:

- Do your corporate values or mission statement refer directly to user safety? (Module 1)
- Do you have documented safety by design processes in place? (Module 2)
- Do you use any of the following tools to detect, moderate and report illegal or harmful content or behaviour? (Module 3)
- Have you translated the acceptable use policy into plain language and short form notices for users? (Module 4)
- Do you make information related to safety policies and standards publicly available? (Module 5)

3.3.2 Information flows

IIS has outlined the proposed information flows below:

Action	Description	Information involved
Launch of SbD tool	The user goes to the self-assessment tool via their web browser and begins a session. There is no registration or log-on process for users. The design intention has been to avoid potential collection of user personal information via a registration mechanism. Instead, the tool functions using cookies (see below). (eSafety's firewall records the user's IP address, but the tool does not. Instead, the tool records the country of origin that is derived from the IP address.)	IP address
Collection (of session ID to temporary data store)	The tool generates a code (a return token or 'session ID') for the user, which they are prompted to record for future reference. For as long as the return token is valid, the user is able to enter the code to return to their progress on the tool if they have exited the current session (e.g., due to time-out, browser crash, or needing to go away to find information to answer a question in the tool).	Session ID

Action	Description	Information involved
Collection (of user responses and progress through tool)	The tool generates (and places on the user's browser cache) an HTTP session cookie to track progress on the tool and user responses. The user goes through the tool's modules and answers questions. The questions and answers are recorded against their session ID and stored in the temporary data store in the application's front-end layer hosted on the Microsoft Azure data store within the application's service layer.	Session ID User responses and progress through the tool
User rights (deletion)	At any point the user may choose to 'restart' – this will wipe the data related to the relevant module (questions and answers), the session ID and cookie will remain.	Session ID
Use (of responses to generate end report)	Once the user reaches the end of a module, they can download an end report in PDF format that summarises the user's results and provides feedback. The report is generated automatically based on pre-defined weightings and scoring rules for the answers.	End-report (generated from pre-defined scoring of user responses)
Retention (of data about user interaction with the tool)	Data is encrypted on ingestion and transferred from the temporary store to the long-term data store twice a day; this information is retained to support the Reporting Specifications.	User responses and progress through tool
Use /disclosure (of data about how the tool is used)	Non-identifiable information transferred to the long-term data store is used by eSafety to assess and report on user engagement with, and responses to, the tool. Limited non-identifying information may be published (e.g., numbers of users that completed all modules). eSafety may also use the aggregated data of responses to questions to determine where to target guidance or other supporting material. No data will be used for enforcement activities. No companies will be identifiable in the data.	User responses and progress through tool
Disposal (of data in temporary data store)	The session ID expires after seven days where there has been no further activity in the tool by the user and the user has not completed their self-assessment. If the user completes all modules in the self-assessment, the session ID expires 72 hours after completion. When the session ID expires all data associated with it is automatically deleted from the temporary data store.	Session ID User responses and progress through tool
Disposal (of data in long-term data store)	The length of retention of this information is still under consideration.	User responses and progress through tool

4. Analysis of privacy issues

If eSafety manages identification risks for tool data, then the Privacy Act and GDPR will not apply. However, both incorporate standards that reflect good practice for information handling and have therefore been used as a frame for assessing the tool. In this section, we address coverage of the Privacy Act and GDPR and then assess the tool against core privacy principles, making recommendations where appropriate to strengthen privacy.

Issue	Findings	Recommendation
Coverage of the Privacy Act Whether the (Australian) Privacy Act applies to information processed by the tool.	eSafety is covered by the Privacy Act so it must comply with the Australian Privacy Principles (APPs) when handling personal information. Therefore, an important question is whether the tool processes 'personal information'. IIS reviewed the data that the tool will process and found that it is unlikely to meet the Privacy Act definition of personal information, as long as any identifiability risks are managed.	See **Recommendation 2**.
Coverage of the GDPR Whether the GDPR (the EU privacy law) applies to information processed by the tool.	As with the Privacy Act (above) the question about whether the GDPR applies rests on whether the tool collects and handles 'personal data'. The GDPR definition of personal data is broader than the Privacy Act definition of personal information. IIS identified three 'identifiability' risks for tool data. By identifiability risks, we mean risks that tool data is identifiable and therefore meets the personal data definition. Those three risks were: ● Whether the combination of data would allow the identity of a user of the tool to be inferred ● Whether the tool enabled identification of the user through use of an online identifier (like a cookie) ● Whether the data collected by the tool was *about* an individual. IIS found that there was a low likelihood of eSafety being able to identify the user from a combination of data collected by the tool. However, the tool does use session cookies. Under the GDPR this potentially renders data associated with the cookie 'personal' but only if it is *about* an individual. IIS found that tool data was largely about the users' companies rather than the	**Recommendation 1 – Manage GDPR coverage** Manage GDPR coverage. This could include steps such as: ● Removing the question that elicit information 'related to' the user's role and determining streams with another method (e.g., asking the user to select a stream) ● Seeking legal advice about the application of the GPDR to eSafety and the tool ● Launching the tool in selected jurisdictions before wider roll-out to the EU, to enable beta testing for compliance risks associated with data handling.

Issue	Findings	Recommendation
	user themselves, however eSafety could take further steps to reduce the risk of tool data meeting the definition of 'personal data'.	
Anonymity Ensuring users and their companies are and remain anonymous when using the tool.	eSafety made it clear that maintaining the anonymity of users of the tool and their companies is of paramount importance. eSafety intends users to feel free to give honest responses to module questions to enable the tool to give accurate scoring and feedback. eSafety also wishes to ensure that companies have confidence that SbD tool data cannot and will not be used for enforcement related purposes. Being able to assure users of their anonymity puts eSafety in the best possible position to assure companies that tool data cannot be used in connection with eSafety's enforcement activities. IIS has assessed identifiability risks to be low. However, identifiability is an ongoing risk to be managed and eSafety should ensure internal processing does not inadvertently render the data identifiable (e.g., due to accumulation or combination of the data). We suggested that eSafety take a structured approach to managing such risks. This could include applying a framework like the Five Safes. eSafety should also be mindful of this risk for any future iterations of the tool or changes in how it uses tool data.	**Recommendation 2 – Manage identifiability risks** a) Implement practices, procedures and systems to manage identifiability risk. For example, consider applying the Five Safes Framework to eSafety's management and use of tool data. b) Assess and manage identifiability risks for future iterations of the tool or changes to data handling and reporting.
Transparency Ensuring users understand how the tool processes data to equip them to make informed decisions about how they use the tool.	The Privacy Act requires entities to ensure the way they collect and handle personal information is transparent to individuals. In particular, APP 1 requires entities to make available a clearly expressed and up to date privacy policy which explains their general practices with regard to personal information handling. APP 5 requires entities to make individuals aware of certain information when collecting personal information (this is sometimes referred to as a 'privacy notice' or 'collection notice'). These principles align with the GDPR's right to be informed. As the tool in its intended operation does not collect or handle personal information, eSafety is not obliged to comply with APPs 1 and 5 (nor other similar overseas privacy regulations or standards). Nevertheless, IIS considers that it would be good practice for eSafety to make clear that it is	**Recommendation 3 – Enhance transparency about the tool's data handling** a) Offer users supporting information about how the tool handles data. Such information should be clearly expressed and could explain: ● That eSafety does not collect user personal information and cannot identify their company ● How the tool uses cookies ● How data is collected, used and stored

Issue	Findings	Recommendation
	not collecting or handling personal information and to give basic information about how the tool functions.[2]	● Any secondary uses of the data (e.g., for reporting, evaluation or product improvement). The information should be presented in a combination of both just-in-time notice and website copy. b) Establish internal protocols that ensure that changes to how the tool operates are reflected in public-facing explanatory information.
Data minimisation Whether the tool is configured in a way that minimises the amount of information it processes (therefore minimising the potential privacy impact).	Data minimisation refers to the idea that organisations should only collect the personal information necessary to achieve their objectives. Collecting less personal information means creating less risks that could impact on individuals' privacy. IIS finds that the SbD tool has successfully embedded 'data minimisation' as a design principle. The tool seeks to avoid collecting personal information or identifying the user's company. Use of the session ID and return token enables users to stop and continue with the tool while remaining anonymous, rather than having to submit an email address, for example, or create log-on credentials. To further guard against the possibility that personal or otherwise disclosive information is submitted by users, the tool contains no free text fields.	N/A
Session ID and cookie Ensuring cookies comply with EU requirements.	The session ID associated with the cookie on the user's device and the return token allows the tool to record the users' responses to questions. This is important functionality as it allows the tool to: ● Remember where the user is up to in their self-assessment, including which question in which module	**Recommendation 4 – Be transparent with use of cookies** a) Include some form of notice that the tool requires a 'strictly necessary' cookie to operate and that no other cookies are deployed to the user's device.

[2] We note that the tool already contains clear statements at relevant points during the tool's self-assessment process to explain how information is processed. For example, the return token page explains how long the token will work for and when it will expire.

Issue	Findings	Recommendation
	● Calculate and score the company’s performance and generate an end report at the completion of each module ● Enable the user to return to the tool at a later point without the tool ‘forgetting’ what responses they have submitted and which modules they have completed. In practice, this means that each time a user answers a question in the tool, the tool records the response with the user’s session ID, care of the session cookie. This information is stored in the temporary data store. Cookies that the SbD tool places on people’s devices and the data those cookies transmit to the temporary data store would not meet the Privacy Act definition of personal information. Therefore, the APPs do not apply. The EU regulates use of cookies via its Directive on privacy and electronic communications.[3] The Directive requires organisations that wish to use cookies on their websites to get consent from users first. However, organisations do not need user consent if the cookie is ‘strictly necessary’ for provision of a service over the Internet requested by the user. In IIS’s view, the tool’s use of cookies can be considered ‘strictly necessary’ to the operation of the tool, which is deployed at the request of the user and for their benefit as they navigate and complete the tool. The UK Information Commissioner’s Office does suggest that even where consent is not necessary, it is still good practice to provide users with information about cookies.[4]	b) Include information about use of cookies in public-facing supporting information (see **Recommendation 3**). c) Maintain a watching brief on developments involving the new ePrivacy Regulation, including relevant regulator decisions on the topic, as this will inform eSafety’s privacy risk profile going forward.
Long-term data store Ensuring data held in the long-term data store is used	The data held in the temporary data store drives the operation of the SbD tool. When the session ID and return token expire, the data in the temporary data store is deleted. However, twice a day data in the temporary data store is transmitted to the long-term data store. The long-	**Recommendation 5 – Formalise decision about which data variables are transferred to the long-term data store**

[3] The GDPR also regulates cookies to the extent that they collect and share personal data, which is not applicable to the cookie used by the tool.

[4] UK ICO, *Guide to Privacy of electronic communications regulations*.

Issue	Findings	Recommendation
appropriately and protected from unintended secondary uses.	term store is intended to collect and store data for reporting and evaluation purposes. IIS understands that currently all data is transferred by default, although eSafety is considering whether all or only a subset of the data is transferred across as part of BAU. As long as such data does not meet the definition of personal information, privacy risks will be minimised (and the APPs will not apply). That said, applying the principle of data minimisation will further reduce risk, including risks of misuse and function creep.	a) Apply a data minimisation approach to transfer of data to the long-term data store. Ensure that only data that is reasonably necessary for reporting and evaluation is transferred. b) If eSafety determines that all response data is reasonably necessary, consider revisiting this decision after a period of operation of the tool (e.g., 12 months) to check that such arrangements continue to be appropriate and to ascertain whether there are any opportunities to reduce the categories of data that are transferred and stored by eSafety.
User feedback surveys Ensuring user feedback surveys comply with privacy regulations.	eSafety raised with IIS the possibility that it would conduct user surveys to elicit feedback on the SbD tool. Such surveys would operate separately to the tool – that is, they would not form part of the tool's functionality and there would be no connection between survey responses and user interaction with the tool. Privacy considerations for user feedback surveys include: ● *Maintaining separation with the SbD tool* – to ensure SbD tool data is not inadvertently identified through linkage with identified survey data. ● *Anonymity and pseudonymity* – giving survey respondents the options not to identify themselves – if respondents are able to identify themselves then the Privacy Act and GDPR will apply. ● *Transparency* – offering survey respondents information about how eSafety will use (and/or disclose) survey data; if data is identified, ensuring that such information meets the requirements of APP 5. ● *Use limitation* – ensuring survey data is only used for the purpose it was collected (for example, product improvement); using de-identified information if possible.	N/A

Issue	Findings	Recommendation
	- *Data disposal* – disposing of survey data once it is no longer needed for the purpose it was collected.	
Purpose limitation Ensuring tool data is only used for the purpose it was collected and not additional unintended purposes.	The SbD tool collects data for the primary purpose of enabling the tool to function and score company performance. Scoring performance based on weighting of questions and the compiling of end reports is an automated process. There will be no regular staff member access to the temporary data store, other than for troubleshooting purposes, and the temporary data store has no human interface which further limits who may access data stored there. A secondary use of the data will be for reporting and evaluation. This occurs after the data is transferred from the temporary data store to the long-term data store. As long as de-identification is maintained (see **Recommendation 2**), then such data will not be personal information or personal data and therefore the Privacy Act and GDPR will not apply. This means that use of such data for reporting or evaluation will be allowable from a privacy compliance standpoint. However, data management considerations remain; strong governance, oversight and assurance will be critical to ensuring data is handled appropriately and protected from misuse or identification (see **Recommendation 6**).	See **Recommendations 2** and **6**.
Security Ensuring data is protected appropriately in flight and at rest.	While security risks may be low (from a privacy perspective) given the way the tool has been configured to avoid collecting personal information, some broader security considerations remain to ensure data is protected against identifiability and to ensure ongoing protection of company identities and confidential business information. eSafety is in the process of completing security risk assessments for the tool, including a Threat Risk Assessment and penetration testing. eSafety has also implemented a number of privacy and security risk management controls including: - Risk management framework to assess and manage risk	See **Recommendations 2** and **6**.

Issue	Findings	Recommendation
	● Data minimisation (with efforts made to avoid collection of information identifying individual users or their organisations) to reduce risk ● Minimal human interaction with, or access to, the front-end (with data processing fully automated) ● Selected ICT security controls such as: ● Data encryption at rest and in flight ● Firewalls to protect internal systems ● Access controls in place for the front and back-end ● Data breach response plan in place. IIS notes that the system will be subject to eSafety's existing information security arrangements. An important focus for eSafety (as raised elsewhere in the report) will be managing identifiability risks. If it is deemed that the data is personal information, relevant measures under the Commonwealth Protective Security Policy Framework (PSPF) would need to be followed. The information security requirements in the PSPF apply to all information assets owned by the Australian Government, or those entrusted to the Australian Government by third parties. Therefore, managing identifiability risk and implementing strong data governance arrangements (see **Recommendations 2** and **6**) will be critical.	
Data retention and disposal Ensuring tool data is not retained indefinitely and measures are in place to manage disposal.	Data retention is a relevant consideration for the tool response data that will persist in the long-term data store. However, given that the data is already intended to be (and to remain) non-personal information, there is less of a pressing need for the data to be disposed of, compared to if it were personal information. IIS does not have a specific recommendation here, except to reiterate that eSafety's collection and handling of tool response data should be guided by clearly defined project objectives. eSafety can retain the data as long as it	N/A

Issue	Findings	Recommendation
	is connected to a legitimate purpose (such as reporting and evaluation) and it is consistent with any existing internal requirements on data retention. It may be beneficial to formally document the basis on which eSafety will retain data in the long-term data store.	
Individual rights Ensuring individuals are empowered to manage their data.	Most privacy laws contain rights for individuals to ask to access personal information held about them and correct it if it is wrong (e.g., APPs 12 and 13 of the Privacy Act). The GDPR is notable for providing additional individual rights in certain circumstances, including rights to request that their personal data be deleted, to object to or restrict data processing, and to receive their personal data in a structured and machine-readable format. Access and correction rights are not applicable to the tool because it will not retain data that can be linked to an identifiable individual. Nevertheless, the tool is implemented in a user-friendly way that respects individual rights: ● Participation is voluntary ● Users can navigate the tool and its modules as they choose ● Users can change their responses, or restart and delete their responses, at any time. IIS commends eSafety for these arrangements. Data portability (as per the GDPR right to receive personal data in structured and machine-readable format) may be a best practice option to explore in future iterations of the tool but is not necessary for compliance at this point.	N/A
Governance Ensuring appropriate governance measures are in place to give confidence that privacy protections are operating effectively.	In addition to the foundational privacy considerations covered above, IIS considers that another important element for eSafety going forward is the governance of the tool. This includes governance of BAU: ● How will the tool be properly managed and overseen, and by whom? ● How is the tool performing based on the commitments eSafety has made?	**Recommendation 6 – Formally document governance processes** a) Document and implement policies and procedures to appropriately manage data collected by the tool. Such policies and procedures could cover matters including:

Issue	Findings	Recommendation
	It also includes governance of change: ● What is the decision-making process for making changes to the tool that could have an impact on data handling? ● Who gets to decide, who needs to be consulted and/or informed? Changes could include: modifying or adding questions, expanding the reporting specifications, new internal uses for the tool response data, changes to data retention, and who can access the long-term data store.	● Permitted uses of tool data (and a prohibition on use of data for enforcement activities) ● Staff access restrictions – including to both the temporary and long-term data stores ● Practices, procedures and systems for managing identifiability risks (see **Recommendation 2**) ● Data retention and disposal. Assign responsibilities and ensure that all relevant staff are aware of their roles. b) Document processes that: ● Establish oversight and assurance measures to ensure eSafety complies with its policies and procedures ● Set out the decision-making criteria, process and roles/responsibilities when considering changes to the tool and its data handling practices.

5. PIA recommendations with eSafety response

Recommendation	eSafety response
***Recommendation 1* – Manage GDPR coverage** Manage GDPR coverage. This could include steps such as: ● Removing the question that elicit information 'related to' the user's role and determining streams with another method (e.g., asking the user to select a stream) ● Seeking legal advice about the application of the GPDR to eSafety and the tool ● Launching the tool in selected jurisdictions before wider roll-out to the EU, to enable beta testing for compliance risks associated with data handling.	**Agree in part – Point 1 has been implemented**
***Recommendation 2* – Manage identifiability risks** a) Implement practices, procedures and systems to manage identifiability risk. For example, consider applying the Five Safes Framework to eSafety's management and use of tool data. b) Assess and manage identification risks for future iterations of the tool or changes to data handling and reporting.	**Agree**
***Recommendation 3* – Enhance transparency about the tool's data handling** a) Offer users supporting information about how the tool handles data. Such information should be clearly expressed and could explain: ● That eSafety does not collect user personal information and cannot identify their company ● How the tool uses cookies ● How data is collected, used and stored ● Any secondary uses of the data (e.g., for reporting, evaluation or product improvement). The information should be presented in a combination of both just-in-time notice and website copy. b) Establish internal protocols that ensure that changes to how the tool operates are reflected in public-facing explanatory information.	**Agree – recommendations implemented**
***Recommendation 4* – Be transparent with use of cookies** a) Include some form of notice that the tool requires a 'strictly necessary' cookie to operate and that no other cookies are deployed to the user's device. b) Include information about use of cookies in public-facing supporting information (see **Recommendation 3**). c) Maintain a watching brief on developments involving the new ePrivacy Regulation, including relevant regulator decisions on the topic, as this will inform eSafety's privacy risk profile going forward.	**Agree – recommendations implemented**

Recommendation	eSafety response
***Recommendation 5* – Formalise decision about which data variables are transferred to the long-term data store** a) Apply a data minimisation approach to transfer of data to the long-term data store. Ensure that only data that is reasonably necessary for reporting and evaluation is transferred. b) If eSafety determines that all response data is reasonably necessary, consider revisiting this decision after a period of operation of the tool (e.g., 12 months) to check that such arrangements continue to be appropriate and to ascertain whether there are any opportunities to reduce the categories of data that are transferred and stored by eSafety.	**Agree**
***Recommendation 6* – Formally document governance processes** Document and implement policies and procedures to appropriately manage data collected by the tool. Such policies and procedures could cover matters including: ● Permitted uses of tool data (and a prohibition on use of data for enforcement activities) ● Staff access restrictions – including to both the temporary and long-term data stores ● Practices, procedures and systems for managing identifiability risks (see **Recommendation 2**) ● Data retention and disposal. Assign responsibilities and ensure that all relevant staff are aware of their roles. Document processes that: ● Establish oversight and assurance measures to ensure eSafety complies with its policies and procedures ● Set out the decision-making criteria, process and roles/responsibilities when considering changes to the tool and its data handling practices.	**Agree – recommendations implemented**

INFORMATION INTEGRITY SOLUTIONS

Information Integrity Solutions Pty Ltd
PO Box 978, Strawberry Hills NSW 2012, Australia

P: +61 2 8303 2438
F: +61 2 9319 5754
E: inquiries@iispartners.com
www.iispartners.com

ABN 78 107 611 898
ACN107 611 898