17 May 2023

Cyber Security NSW
Submission by email: policy@cyber.nsw.gov.au

Vulnerability Disclosure Consultation Paper

About us

The **UNSW Institute for Cyber Security** ('IFCYBER') has the mission to apply multi-disciplinary and cross-faculty research and teaching partnerships to address sovereign interests and Cyber Security socio-technical problems. IFCYBER is a large conglomerate of 140 experts in cyber security across each of our faculties. Unique to UNSW is our understanding that cyber security is multidisciplinary. We are interested in the human, organisational, social, economic, legal, and technical aspects of cyber security. Our aim is to consider 'real-world problems' and deliver 'real-world impact' – in Australia and globally.

The **UNSW Allens Hub for Technology, Law and Innovation** ('UNSW Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law and Justice, the Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the UNSW Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

QUT's School of Computer Science undertakes research at the frontiers of computer science knowledge, and we are committed to sharing our innovations with the world. The school includes over 30 on-going academics, as well as fixed-term staff, and over 100 higher degree research students. These staff and students lead and conduct research that has a real-world impact, through a focus on innovations that are smart, safe, and satisfying. We have expertise in machine learning, artificial intelligence, human-computer interaction, data and text mining, information security, cloud computing, and augmented and virtual reality. Our academics are involved in large research initiatives such as the ARC Centre of Excellence for the Digital Child, the Cyber Security Cooperative Research Centre, the QUT Centre for Data Science, and the Australian Acoustic Observatory.

About this Submission

We are grateful for the opportunity to make a submission on the Vulnerability Disclosure Consultation Paper. Our submission reflects our views as researchers; they are not an institutional position. This submission can be made public.

Question 8: Application of the Framework in the current legislative and policy landscape

The documents state that agencies should state that they will not “take legal action” against anyone in the public for security research activities that represent a good faith effort to follow the VDP. However, such statements may not be sufficiently protective. Computer offences in the *Crimes Act 1900* (NSW) do not involve an agency/entity bringing an action, but rather a prosecution. In that sense, it is not up to the agency whether an action will be brought (although the agency could simply not make a report, in which case information may never come to light).

The best way to protect good faith participants in a VDP from criminal consequences is to add a defence to relevant sections of the *Crimes Act* or to explicitly provide that good faith participation in a vulnerability disclosure program is taken to be authorised.

However, it may also be sufficient for the agency to (1) ensure that the description of what is authorised is sufficiently clear, (2) ensure that the description of what is not authorised is also sufficiently clear, and (3) explicitly state that any ambiguity in that description should be interpreted in favour of authorising activities that constitute good faith participation in the program. This avoids an individual committing a crime and facing prosecution merely because they misinterpreted what was permitted.

Good faith must of course also be defined. The definition could reference matters such as prompt reporting, not disclosing or threatening to disclose personal information, a reasonable belief that the actions were within the terms of the program, and lack of an intent or threat to cause harm to persons, property, or systems.

Question 10: How should NSW Government agencies handle reports that involved testing and disclosure but are not in the scope of good faith research?

This question highlights an exploitable gap in the proposed framework around *who* in the agency has the power to approve security researchers and clear reports for action. Confusion or doubt around delegation, processes and systems will create an opening for motivated actors not acting in good faith to exploit the vulnerability testing and reporting scheme.

In the draft Vulnerability Disclosure Framework there is no indication of how a vulnerability report will be checked, reviewed, assessed, audited, or remediated. The framework contains a reporting obligation on agencies to measure the impact of the scheme. The policy template mentions a restriction on public disclosure by a security researcher “until the reported issues have been validated and remediated.” (See page 4).

The framework contains an expectation of compliance with two international standards: ISO/IEC 29147:2018 and ISO/IEC 30111:2019. We note that ISO/IEC 29147:2018 contains guidelines on receiving reports about potential vulnerabilities, and that ISO/IEC 30111:2019 concerns vulnerability handling processes, including how to process and remediate vulnerabilities. Clarity around who will assess whether the guidelines in the mentioned standards have been implemented by an Agency and are consistent with the framework is desirable.

We comment on the following specific issues:

- *Issue: Difficulty in determining how to report: Even if a reporter sends a report to the correct entity, it may not end up with the correct team and may fail to get actioned.*

This issue may not be solved in current proposal since the medium of vulnerability reporting is still the same entity. A technical medium, such as a vulnerability submission system, which can report to both NSW Cyber and the entity at the same time, should be a solution to ensure Cyber Security NSW can monitor this process.

- *Issue: Lack of clear communication when reporting: Lack of response from agencies means many reporters have low confidence that the vulnerability is being remediated.*

The current framework lacks clarity from a technical perspective. Some potential solutions include:

- time limits should be accurately associated to the risk level of vulnerabilities.
- standards/toolkits for vulnerability risk evaluation should be recommended.
- technical standard for vulnerability reporting must contain principles that are comprehensive since cyber security incident responders need a validation and post-fix testing process.

Question 16: How much time is reasonable to acknowledge reports (e.g. 5 days)? What other guidance should be given to agencies about providing acknowledgement to reporters?

Reporting and fixing timing windows should be accurately associated to the risk level (technical) and potential impact (disclosure & exploit) of vulnerabilities.

Question 17: How much time is reasonable for Cyber Security NSW to provide agencies with vulnerability disclosure reports?

The reasonableness of the timeframe will be determined by the time it will take for Cyber Security NSW to verify the report and the security researcher. Another consideration to factor into the timeframe for providing reports will be the number and frequency of reports submitted to Cyber Security NSW. As the consultation paper notes, automation of acknowledgements may provide a partial solution for acknowledgements only. However, the more time consuming and detailed oriented work will need a longer response time, especially as that process may not be able to be automated, or only partially automated.

Some technical points

Consider capitalising ‘Internet’ in documentation to make it clear when referring to the worldwide set of interconnected networks.

ISO standards are internationally recognised but are not ‘industry’ standards (p3 Tab B) unless adopted by industry. The standards cited are correctly named ISO/IEC 29147:2018 and ISO/IEC 30111:2019.

In the list on Tab B p 3, alongside software as a service, could also reference infrastructure as a service and platform as a service, as these are also important examples.

In Tab B (2.3), it may be useful to give a brief description of what security.txt is, using the description from Tab D “a web resource to provide easier identification of security contact points and the location of policy information.”

In the list on Tab C p 3 of non-allowable types of testing, could usefully add:

- (distributed) denial of service (DDoS/DoS)
- physical attacks
- attempts to modify or destroy data

It could also be worth listing legal provisions that remain in effect (ie breach of those provisions is outside the scope of what is allowed) and those that are not breached by those acting in good faith under the policy (because their actions are authorised).

Overall comments

The new vulnerability framework will increase the workload of Cyber NSW significantly. This new function will need to be adequately resourced, and in some instances, automated where desirable for efficient use of resources.

Contributors (in alphabetical order):

Lyria Bennett Moses

Ruitao Feng

Sanjay Jha

Vicky Liu

Susanne Lloyd-Jones.