From: Masayuki Negishi <Masayuki.Negishi@maples.com>
Sent: Friday, October 18, 2019 9:14 AM
To: privacyframework <privacyframework@nist.gov>
Subject: NIST Privacy Framework: Preliminary Draft Comments

Dear Sir/Madam,

Thank you very much for your work on this new framework.

As a privacy professional working in a cross-functional team of risk and compliance professionals (including information security specialists), I very much welcome initiative such as this, which I believe can help in standardising industry best practices, and bringing about a closer alignment between security practices and privacy practices.

By creating a privacy-specific framework which is closely aligned with the now well-established NIST Cybersecurity Framework, you will be enabling organisations to adopt a holistic approach to information governance without having to consider fragmented set of standards, and it is encouraging to see that we finally have a credible alternative to the now somewhat outdated AICPA/CICA Privacy Maturity Model.

I believe that the preliminary draft is well written and I could not identify any major issue with its contents, but I have set out some suggestions for possible improvements in the attached feedback form.

Please kindly note that whilst I'm submitting my comments from work, I'm submitting my comments purely in my capacity as one privacy professional who takes a keen interest in your organisation's work and my comments do not reflect or purport to reflect the views of the Maples Group.

Thank you.

Yours faithfully,

Masayuki Negishi
CIPP/E, CIPP/US, CIPM

Masayuki Negishi
Group Data Protection Counsel

MAPLES GROUP
Direct +44 20 7466 1689 | **Mobile** +44 7766 424 067
Maples Fiduciary Services (UK) Limited, 11th Floor, 200 Aldersgate Street, London, EC1A 4HD, England

maples.com

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial /Technical)
1	N/A (individaul submission)	Masayuki Negishi / masayuki.negishi @maples.com	4	119 to 152	1.0	It might be worth adding a more explicit reference to privacy laws as a factor which organisations must take into account in addressing privacy laws. The main body of the document touches on regulation and compliance in various places but I think this is a point worth emphasising up front in the Introduction.	Consider adding something like this, say, at end of line 136 on p4: "The way in which privacy laws regulate the handling of *data* about *individuals* can vary significantly depending on context, industry sector, jurisdiction, and so on, adding to the complexity."	General/Editorial
2	N/A (individaul submission)	Masayuki Negishi / masayuki.negishi @maples.com	8	260 to 262	1.2.2	Privacy professionals (especially those who work in non-US jurisdictions) won't typically see privacy notice/consent as a means of sharing risk with individuals. If anything, their instinct might be to emphasise that consent cannot be used to excuse an organisation's non-compliance.	Consider explaining how a risk sharing happens through notice/consent, e.g. by adding a footnote at end of line 262.	General/Editorial

3	N/A (individaul submission)	Masayuki Negishi / masayuki.negishi @maples.com	10	351	2.1	"Identifying legal/regulatory requirements" is currently included in Govern-P, but shouldn't that form part of Identify-P? Such requirements give rise to specific risks (risk of non-compliance), and aren't activities in Govern-P meant to address what we discover through Identify-P?	Consider moving "Identifying legal/regulatory requirements" to Identify-P, somewhere in Line# 341-346.	General/Editorial
4	N/A (individaul submission)	Masayuki Negishi / masayuki.negishi @maples.com	10	358 to 360	2.1	It might be worth emphasising that Control-P is about controlling the risks identified through Identify-P.	Consider changing the first sentence as follows: "The Control-P Function considers data management from both the standpoint of the organization and the individual, and addresses the controls required to manage the privacy risk identified through Identify-P."	General/Editorial

5	N/A (individaul submission)	Masayuki Negishi / masayuki.negishi @maples.com	12	419 to 423	3.0	It might be worth noting that the Privacy Framework can also be used to support things like privacy impact assessment and privacy by design (e.g. GDPR Art 25 and 35).	Consider adding something like this at the end of Line# 423: "Naturally, the Privacy Framework can serve as a foundation to support activities and initiatives such as privacy impact assessment and privacy by design."	General/Editorial
6	N/A (individaul submission)	Masayuki Negishi / masayuki.negishi @maples.com	14	476 to 544	3.3	By choosing the right set of activities and repeating them, the Privacy Framework can be aligned with the Plan-Do-Check-Act (PDCA) cycle which is central to management systems like ISO27001. Might be worth mentioning this.	Consider touching on the potential synergy between the Privacy Framework and the PDCA cycle somewhere in 3.3, or somewhere else in 3.X.	General/Editorial
7	N/A (individaul submission)	Masayuki Negishi / masayuki.negishi @maples.com	22	Sub-category ID.RA-P1		See comment #3 above regarding Identify-P. Shouldn't identifying legal/regulatory requirement (i.e. compliance risk) be part of Risk Assessment ID.RA-P?	Consider adding "identifying legal/regulatory requirements" as example of contextual factors listed in ID.RA-P1.	General/Editorial

8	N/A (individaul submission)	Masayuki Negishi / masayuki.negishi @maples.com	23	Sub-category GV.PP-P5		See comment #3 and #7. Shouldn't identifying legal/regulatory requirement (i.e. compliance risk) be part of Risk Assessment ID.RA-P? If so, it might be worth clarifying that GV.PP-P5 does not include the "identify" aspect.	Consider tweaking GV.PP-P5 as follows: "Legal, regulatory, and contractual requirements regarding privacy (as identified through ID.RA-P) are understood and managed."	General/Editorial
9	N/A (individaul submission)	Masayuki Negishi / masayuki.negishi @maples.com	23	Category GV.AT-P		Is it worth emphasising that the privacy-related training etc. should encompass the privacy-related requirements the organization is required to address?	Consider tweaking sub-categories GV.PAT-PX by expanding each of them as follows "… their roles and responsibilities, and the privacy-related requirements relevant to them."	General/Editorial