From: Nachtsheim, David CTR (FTA) <david.nachtsheim.ctr@dot.gov>
Sent: Wednesday, October 23, 2019 6:58 PM
To: privacyframework <privacyframework@nist.gov>
Subject: nist privacy framework: preliminary draft comments

Best Regards,

David Nachtsheim, Security+, Consultant

Information Assurance Specialist

Office of the Chief Information Officer

FTA | Department of Transportation

david.nachtsheim.ctr@dot.gov

Halvik Corp. | Indev LLC | dnachtsheim@indev.com

nachtsheim.d@hotmail.com

northstarmgtsvcs@gmail.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	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	1	15	Note to Reviewers	Consider alignment to/coordination with Federal Trade Commission (FTC) standards and practices relating to civil and criminal identity fraud and theft.		general
2	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	1	17	Notes to Reviewers	Organizations must be aware of the downstream use of information that is tangential or unrelated to the mission, including genealogy and historical research		general
3	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	1	17	Notes to Reviewers	It is possible that a small business may have a business process for intentional disclosure of privacy information. One common practice is the posting of notices to employees providing the identity and other privacy information of an individual who has passed bad checks or engaged in theft from the business. These sometimes include photos. The method of notification may also make the information available to customers and passersby.		general
4	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	1	16	Note to Reviewers	There is not enough discussion of physical records management – envision a day in the life of a paper-only entity, such as a church or club, and a small business or organization that hires record		general

						management services or uses online services, or is using a simple spreadsheet on a PC – develope a PF lite, the basics of privacy protection that SMBs can use		
5	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	10	347	Core	I agree with inclusion of Govern – P which should include assignment of governance and control roles, continuous monitoring, assessment and authorization of privacy risk policies, resources, and methods, and should include participation by information owners/LOB managers who are often not included in comparable cybersecurity activities		general
6	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	10	356	Profiles	Control should include management of privacy resources and processes, testing and assessment of effectiveness, detection and identification of weaknesses and plans to address weakness, similar to cybersecurity security assessment and authorization (SA&A) and Plan of Action and Milestones (POA&M)		general
7	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	11	385	Profiles	This presents potential overlap/alignment with general Enterprise Architecture principles and the potential to model/evaluate/describe privacy risk and privacy management reference model in conjunction with the EA business, data, service, and technology reference models, and in target architecture evolution planning		general

8	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	11	385	Profiles	This presents the potential overlap/alignment with OMB Capital Planning and Investment Control (CPIC) guidelines and non-governmental general investment planning principles, and the potential to model/evaluate/describe the value and cost of privacy risk governance, control, communication, detection, and mitigation in investment criteria and budget planning.		general
9	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	15	527	Applying the SDLC	The plan phase must include defining known interconnections with other data repositories and systems		general
10	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	16	570	Using the data processing ecosystem	Congress and State/Local legislatures should evaluate, adopt and apply privacy risk management principles and standards in all new legislation. Similarly, agencies should adress privacy risk managment goals and guidelines in all rulemaking.		general
11	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	16	583	Using the Data Processing Ecosystem	commercial products will benefit from the use of an accepted standard nomenclature and metrics, especially if certified by a testing or standards organization, similar to UL, ISO, IEC and others		general

12	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	1	16	Notes to Reviewers	Small/medium businesses/organizations are likely to be unsophisticated about privacy protection and need a set of minimum standards that can be used to select services and resources. A Buyers guide tool by NIST would provide a resource for vendors/makers to apply common terminology and performance metrics to describe their products. Perhaps NIST could encourage FTC to take the lead, or sponsor/participate in a consortium do this.		general
13	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	17	607	Informing Buying Decisions	Investors in publicly-traded or privately-managed businesses should be able to assess the management of privacy risk by the investment target, or prospective business partner, using commonly-applied criteria, in order to determine value and risk.		general
14	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	20	Table 2	CM.AW-P4	This recognizesf Privacy Act requirements for accounting of disclosures when requested by a record subject, and redress and correction of records		general
15	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	23	Table 2	GV.RM-P	Risk Management Strategy should have an annual performance plan for maintaining current profile with level of effort estimatess and performance metrics. Performance plan should		general

						include planned actions to develop increments of the target profile.		
16	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	24	Table 2	CT-PO-P1	Policies should encompass the lifecycle of consent during the full lifecuycle of the information, including consent focus/purpose, probable sharing with third parties under current agreements and mandates, and future sharing with new partners, and consent or denial of consent to share and consented usage.		general
17	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	24	Table 2	CT-PO-P2	Enabling data review should include ability to share metadata about the provenance and reliability of shared information, include date stamp, authenticity seal/hash, consented usage, consent inheritance, and consent validation, updating and revalidating consent due to changes in laws/rules		general
18	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	24		GV.MT-P3	policy should include a regular assessment schedule		general
19	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	24		GV.MT-P3	should include compliance testing and resulting lessons learned and training modification		general

20	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	24		GV.MT-P5	should include correction plans similar to cybersecurity Plan of Action and Milestones (POA&M)		general
21	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	24		GV.MT-P6	include lessons learned from assessments and tests		general
22	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	26	Table 2	CM.AW-P6	metadata about the provenance and reliability of information, include date stamp, authenticity seal/hash, consented usage, consent inheritance, and consent validation, updating and revalidating consent due to changes in laws/rules, blockchain tracing		general
23	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	26	Table 2	CM.AW-P7	organizations should include the timetable for breach disclosure in their policy, providing time for investigation, confirmation, notification to law enforement, and notice to public, individuals and organizations		general
24	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	27	Table 2	PR.DP-P6	This is difficult to understand. How is effectiveness shared? Do you mean effective protection technologies are share across the enterprise?		Editorial

25	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	27	Table 2	PR.DP-P9	include asset and service acquisition here or in a separate subcategory		general
26	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	27	Table 2	PR.DS-P7	COOP environment should also be separated		general
27	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	27	Table 2	PR.DS-P8	integrity checking mechanisms are also tested and verified		general
28	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	28	Table 2	PR.PT-P1	Address disposal of information, avoid printouts in trash		general
29	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	27	Table 2	PR.DS-P5	Recognize the data protection requirements relating to the physical layout and visual/audio barriers of facilities where privacy information is collected, displayed to information owners		general
30	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	24	Table 2	CT.PO-P1	may need to have or develop a process to reverify or update information if laws or regulations impose new privacy requirements		general

31	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	26	Table 2	CM.AW-P6	Some organizations may need identity fraud countermeasures and verfication/validation processes		general
32	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	29	687	Glossary	Should be a definition for data entity	Data Entity: An object in a data model or data repository that is a container for data and relationships to other objects.	technical
33	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	29	687	Glossary	Should be a definition for privacy data entity	Data Entity: An object in a data model or data repository that is a container for data that has a privacy attribute.	technical
34	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	29	687	Glossary	Should be a definition for consent	Consent: The explicit grant of permission to record and use	technical

							information for a stated purpose, given by the owner of the information.	
35	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	29	687	Glossary	Should be a definition for consent lifecycle	Consent Lifecycle: The series of defined changes that a grant of consent undergoes from the beginning of the consent until the consent expires or is withdrawn.	technical
36	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	33	718	Privacy Risk Mgt Practices	The organization can also adjust the priority of current resources to reallocate work or funds.		general
37	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	34	746	Appendix D	In the context of the framework, accentuate privacy	Individuals . . . , or service will be interested in not	editorial

							experiencing problems or adverse **privacy** consequences.	
38	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	34	747	Appendix D	suggest focus on stakeholder expectations	Understanding the stakeholders' goals and the types of outcomes they expect will facilitate . . .	editorial
39	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	34	761	Appendix D	include EA models	. . . forms such as enterprise architecture reference models, system design architedtures . . .	editorial
40	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	34	768	Appendix D	recognize that mapping should include extracts of data in cubes/datamarts/ lakes etc. for search optimization, data sharing, and analysis and that extracts may be intermingled with information from external sources. The process of extraction or intermingling is likely to change the privacy attributes of data.		general

41	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	34	780	Determining Privacy Capabilities	I believe the privacy objectives should form the basis of a system privacy plan, very much like a cybersecurity system security plan		general
42	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	33	730	Privacy Risk Mgt Practices	The organization should also reassess the level of effort and adjust resource allocations.		general
43	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	26	Table 2	CM.AW-P6	Recognize the potential for collection in the wild from video surveillance, scanners, facial recognition, license plate readers, IoT, kissing cams – address the responsibility of equipment maker/vendors, data aggregators, and consumer/user of equipment		general
44	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	26	Table 2	CM.AW-P4	recognize the privacy lifecycle of registration documents - identity, birth, voting, military discharge etc. - and verification systems - eVerify, gun background check		general
45	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	36	820	Conducting Privacy Risk Assessments	problematic data action can be related to user actions rather that system data processes, such as working at Starbucks or use of unauthorized thumb drive/unsecure wifi/phishing		general

46	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	36	831	Conducting Privacy Risk Assessments	impact will vary based on type of breach, for example release of information is different from loss of information is different from change of information		general
47	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	41	946	Roadmap	The NIST website should host a series of best practice guides and templates		general
48	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	37	855	Monitoring Changing Privacy risks	may need to reverify or update information if laws or regulations impose new privacy requirements		general
49	Northstar Management Services LLC	David Nachtsheim; northstarmgtsvcs@gmail.com	38	865	Implementation tiers definitions	There should be some direction at each tier relating to testing of risk management processes and resources		general