From: Richard Mensah (CENSUS/OIS CTR) <richard.mensah@census.gov>
Sent: Thursday, October 24, 2019 3:09 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Tameika L Turner (CENSUS/OIS FED) <Tameika.L.Turner@census.gov>; Ronald Ringgold (CENSUS/OIS FED) <ronald.ringgold@census.gov>; Ayokunmi Emmanuel Akingbade (CENSUS/OIS CTR) <Ayokunmi.Emmanuel.Akingbade@census.gov>; Megan Marie Murphy (CENSUS/OIS CTR) <megan.m.murphy@census.gov>; John Thompson Wood (CENSUS/OIS CTR) <john.t.wood@census.gov>
Subject: NIST Privacy Framework: Preliminary Draft Comments

Hello,

The U.S. Census Bureau Office of Information Security (OIS) has performed an analysis of the Privacy Framework (Preliminary Draft) and have identified questions and points of clarification, which are outlined in the attached excel.

Please confirm receipt of submission. Thank you.

V/R
Richard Mensah
Manager (Contractor)
Office of Information Security (OIS), US Census Bureau
Phone: 301-763-5547
Email: richard.mensah@census.gov

Please note, this email is being sent on behave of the U.S. Census Bureau OIS.

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/ Editorial/ Technical)
1	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	4	140-141	1	Can you elaborate on how the NIST Privacy Framework correlates with standard strategic practices like Privacy by Design?	Add elements of the Privacy by Design standard within framework.	General
2	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	11, 38 40	405-409, 858-943	2.3, App. E	Can you clarify how the Privacy Framework's Tiers are not maturity levels, when they are described in almost identical language to the maturity levels in the Cybersecurity Framework (CSF)?	Add an explanation describing how the Framework's Tiers are not maturity levels.	General
3	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	22	684	ID.DE-P3	Should agreements other than contracts be included, e.g., Memoranda of Understanding/Agreement (MOU/MOA), Service Level Agreement (SLA), Interconnection Security Agreement (ISA), Interface Control Document (ICD)?	Add language surrounding the use of various contracts like (MOAs/MOUs, SLAs, etc.)	General
4	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	33-37	704-857	App. D	Can organizations use the accounting concept of materiality, combined with fines from applicable laws, to measure risk impact?	Explain whether organizations can incorporate accountability concepts of materiality, combined with fines, to measure risk impact.	General

5	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	37	918-922	App. E	One of the elements of Privacy by Design is the incorporation of emerging technologies. Can you elaborate on the types of activities needed to keep up with emerging technologies?	Provide examples on the types of outcome-based activities needed to assist organizations in the incorporation of emerging technologies.	General
6	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	17	596	3.6	It is recommended that NIST create a separate Appendix for privacy and supply chain risk management. As a key concept in NIST SP 800-37 Rev 2, it would help readers understand how to tactically integrate privacy into supply chain risk management.	Create a separate Appendix for privacy and supply chain risk management. As a key concept in NIST SP 800-37 Rev 2, it would help readers understand how to tactically integrate privacy into supply chain risk management.	General
7	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	4	128	1	It is recommended that NIST incorporate specific guidance tailored towards smaller organizations.	Incorporate specific guidance tailored towards smaller organizations	General
8	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	27	684	PR.DP-P7	It is recommended to add supplemental information to address the timely response to privacy risks, which impacts both new and mature organizations.	Add supplemental information to address the timely response to privacy risks, which impacts both new and mature organizations	General
9	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	29	686	Appendix B: Glossary	It would be recommended that the framework is accompanied by a privacy dictionary that could be used internationally.	Create a privacy dictionary that could be used internationally.	Technical

10	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	41	945	Appendix F: Roadmap	It would be recommended to create an assessment tool within the Framework to determine whether the organization's incorporation of the Framework is implemented successfully.	Create a tool to measure successful incorporation of the Framework.	Technical
11	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	23	684	GV.AT-P1	One major concern within most organization is resources. Would it be possible to incorporate methods in which organizations can develop or retain more skilled privacy professionals?	Discuss means to develop/retain skilled privacy professionals.	Technical
12	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	5	154-172	1.1	Figure 1: The figure with three gears may be meant to show interactions, but in real life three gears all mesh together cannot move. It is recommended that another graphic be used, e.g., puzzle pieces, to make the point more effectively.	Change the Graphic in Figure 1.	General

13	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	6-19	203-214 Fig. 8	1.2.1 App. A	Figure 2: The Venn diagram implies that privacy breaches can only occur from cybersecurity risks. Privacy breaches can occur from non-cyber process failures. It is recommended this figure be modified to show “potential problems individuals could experience arising from system, product, or service operations with data, whether in digital or non-digital form,” as described in lines 215-216. Figure 8 in Appendix A partially address this concern.	Modify Figure 2 to show how “potential problems individuals could experience arising from system, product, or service operations with data, whether in digital or non-digital form."	General
14	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	33-37	704-857	App. D	Appendix D: It is recommended that the sub-sections be numbered, e.g., D.1. Organizing Preparatory Resources, D.1.3. Key stakeholders. This will help readers easily reference the sub-sections in this appendix.	Number the sub-sections in Appendix D.	General
15	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	23-24	684	GV.MT-P	It is recommended that a subcategory be added for monitoring sources external to the organization for reports of data breaches, and for indications of organization’s private data appearing in unapproved external sources.	Add a subcategory for monitoring sources external to the organization for breach reports.	General

16	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	23-24	684	GV.MT-P	It is recommended that a subcategory be added for monitoring the security and privacy status of all external and third-party data stores the organization uses for private data, e.g., cloud providers. Several recent data breaches have been caused by improperly secured cloud storage.	Add a subcategory for monitoring the security and privacy status of third-party data providers.	General

17	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	23-24	684	GV.MT-P	It is recommended that CSF category ID.RA be included in the Privacy Framework, particularly CSF subcategories ID.RA-2 "Cyber threat intelligence is received from information sharing forums and sources", ID.RA-3 "Threats, both internal and external, are identified and documented", and ID.RA-6 "Risk responses are identified and prioritized". It is further recommended that resources such as the National Vulnerability Database (NVD), Common Vulnerability and Exposures (CVE), Common Weakness Enumeration (CWE), Open Web Application Security Project (OWASP), Wikipedia's list of data breaches https://en.wikipedia.org/wiki/List_of_data_breaches , etc., be mentioned specifically in the list of resources.	Incorporate the CSF category ID.RA be included in the Privacy Framework, particularly CSF subcategories ID.RA-2, ID.RA-3, and ID.RA-6.	General

18	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	26	684	CM.AW-P	It is recommended a subcategory be added for notifying legal authorities of data breaches, within the time frames specified by applicable laws and regulations. Alternatively, subcategory CM.AW-P7 could be modified to include breach notification to legal authorities.	Add a subcategory for notifying legal authorities of data breaches, within the time frames specified by applicable laws and regulations. Or, modify CM.AW-P7 to include breach notification to legal authorities.	General
19	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	27	684	PR.DS-P	It is recommended that a subcategory be added for Data-in-use being protected. Alternatively, a Data-in-use protection subcategory be noted as an addition for the next revision of the Privacy Framework.	Add a subcategory for Data-in-use being protected.	General
20	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	27	684	PR.DS-P PR.DP-P5	It is recommended that a subcategory be added for the organization to monitor encryption standards, and update encryption tools (e.g., key size, algorithms) as necessary to maintain data privacy, confidentiality, and integrity. If this is to be part of subcategory PR.DP-P5, it is recommended the monitoring of encryption technology state-of-the-art be made explicit in the subcategory.	Add a subcategory for the organization to monitor encryption standards, and update encryption tools (e.g., key size, algorithms) as necessary to maintain data privacy, confidentiality, and integrity.	General

21	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	27	684	PR.DP-P3	It is recommended that subcategory PR.DP-P3 be modified to include that backups are kept only as long as required under backup, security, and privacy policies.	Modify subcategory PR.DP-P3 to include that backups are kept only as long as required under backup, security, and privacy policies	General
22	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	8	280	1.2.2	It is recommended that a cross-reference be developed to associate categories and subcategories with specific privacy legislation. This will allow readers to connect actions with applicable laws. Since the laws change frequently, it is further recommended that this cross-reference be published separately, to allow more frequent updates than the Privacy Framework itself.	Develop a cross-reference to associate categories and subcategories with specific privacy legislation.	General
23	U.S. Census Bureau	Tameika Turner (Tameika.L.Turner @census.gov)	37	849	Appendix D	It is recommended that once NIST SP 800-53 Revision 5 is published there is a corresponding mapping of the privacy and security controls to the Privacy Framework.	Create a corresponding mapping of the privacy and security controls to the Privacy Framework.	Technical