From: Scruggs, Charles
Sent: Wednesday, January 3, 2018 11:28 AM
To: cyberframework <cyberframework@nist.gov>
Subject: SSA Comments on Draft Two of NIST Cybersecurity Framework v1.1

To Whom It May Concern,

Please see the attached comments from the Social Security Administration (SSA) on Draft *Two* of the NIST Cybersecurity Framework, Version 1.1. The attachments offers two separate tabs, one for Editorial Comments and one for Technical Comments. Please contact the undersigned if you have any questions.

Charlie

Charles H. Scruggs
Social Security Administration
Office of Information Security (OIS)
Division of Compliance and Assessments (DCA)
Risk Management Branch (RMB)

[*Attachment copied below*]

#	Org.	Com-mentor	Type	Pg. #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	SSA	OIS	E	18	663-664	3.3	Subcategories codes are not explained.	Mention the table (2) where the subcategory codes are used.
2	SSA	OIS	E	26		Appendix A, Table 2	ID.GV-1 NIST controls states 'controls from all families', but the privacy group is not aligned like the security controls.	Change the sentence to indicate just the 'security' control families.
3	SSA	OIS	E	27		Appendix A, Table 2	ID.GV-3 NIST controls states 'controls from all families (except PM-1)', but the privacy group is not aligned like the security controls.	Change it to indicate just the 'security' control families.
4	SSA	OIS	E	28		Appendix A, Table 2	Under the 'Category' column there is a	Remove the horizontal line.

							horizontal line above ID.RA-6 that does belong.	
5	SSA	OIS	E	25		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SC-24 to ID.AM-2.
6	SSA	OIS	E	26		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST controls PL-3 and SA-6 to ID.GV-1.
7	SSA	OIS	E	26		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control PL-9 to ID.GV-2.
8	SSA	OIS	E	27		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SC-24 to ID.AM-2.
9	SSA	OIS	E	27		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control PL-6 and RA-6 to ID.GV-4.
10	SSA	OIS	E	27		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SC-4 and SI-6 to ID.RA-1.
11	SSA	OIS	E	28		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control PL-5 to ID.RA-3.
12	SSA	OIS	E	28		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control CA-6 to ID.RA-4 and ID.RA-5.
13	SSA	OIS	E	28		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SC-34 to ID.RA-5.
14	SSA	OIS	E	28		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control PM-4 to ID.RA-6 and ID.RM-1.
15	SSA	OIS	E	30		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control PE-7 to PR.AC-2.

16	SSA	OIS	E	31		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SC-3 to PR.AC-4.
17	SSA	OIS	E	32		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control AT-4 and PL-4 to PR.AT-1.
18	SSA	OIS	E	33		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control AC-22 and SC-30 to PR.DS-1.
19	SSA	OIS	E	33		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SC-9 to PR.DS-2.
20	SSA	OIS	E	33		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SI-15 to PR.DS-5.
21	SSA	OIS	E	34		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SI-6 and SI-11 to PR-DS-6.
22	SSA	OIS	E	35		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SA-7 to PR.IP-3.
23	SSA	OIS	E	35		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SI-12 to PR.IP-6.
24	SSA	OIS	E	36		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control PL-6 to PR.IP-7.
25	SSA	OIS	E	37		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SI-9 to PR.IP-12.
26	SSA	OIS	E	37		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control MA-4 to PR.MA-2.
27	SSA	OIS	E	38		Appendix A, Table 2	Some NIST security controls	Consider adding NIST control SC-10 to PR.PT-4.

							were not included.	
28	SSA	OIS	E	38		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SC-2 and SI-17 to PR.PT-5.
29	SSA	OIS	E	39		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SC-10 to DE.CM-1.
30	SSA	OIS	E	41		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SI-15 to DE.DP-1.
31	SSA	OIS	E	41		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SA-19, SC-14, SI-10, and SI-14 to DE.DP-2.
32	SSA	OIS	E	41		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SI-13 to DE.DP-3.
33	SSA	OIS	E	41		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SA-22 to DE.DP-4.
34	SSA	OIS	E	41		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control SC-34 to DE.DP-5.
35	SSA	OIS	E	44		Appendix A, Table 2	Some NIST security controls were not included.	Consider adding NIST control CA-5 to RS.MI-3.
36	SSA	OIS	E	45		Appendix A, Table 2	For RC.CO-1 there is no 'Informative References' for NIST.	Enter NIST privacy controls IP-1, IP-2, IP-3, and IP-4.
37	SSA	OIS	E	45		Appendix A, Table 2	For RC.CO-2 there is no 'Informative References' for NIST.	Consider using CA-2, PM-1, and/or SE-1 for NIST controls.
38	SSA	OIS	E	25-45		Appendix A, Table 2	Privacy control family is not included in table 2.	Consider adding the following NIST privacy controls to the Identify function: AP-2, AR-

								2, AR-3, AR-4, DM-1, IP-1, SE-1, and UL-2.
39	SSA	OIS	E	25-45		Appendix A, Table 2	Privacy control family is not included in table 2.	Consider adding the following NIST privacy controls to the Protect function: AP-1, AP-2, AR-1, AR-3, AR-5, AR-6, AR-7, DI-1, DI-2, DM-1, DM-2, DM-3, IP-2, TR-1, TR-2, TR-3, and UL-1.
40	SSA	OIS	E	25-45		Appendix A, Table 2	Privacy control family is not included in table 2.	Consider adding the following NIST privacy controls to the Detect function: AR-2 and AR-4.
41	SSA	OIS	E	25-45		Appendix A, Table 2	Privacy control family is not included in table 2.	Consider adding the following NIST privacy controls to the Respond function: AR-8, DM-2, IP-3, IP-4, and SE-2.
42	SSA	OIS	E	46	3	Appendix B, Table 3	Definition of 'cybersecurity' doesn't match the information in the framework.	Add the terms 'identify' and 'recover' to the definition.
43	SSA	OIS	E	47	3	Appendix B, Table 3	The definition of 'Risk Management' is weak.	Use one of the definitions in NISTIR 7298 Rev. 2 page 164 (http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf).
44	SSA	OIS	E	49	Various	Appendix C: Acronyms	Some acronyms are missing.	Add the following acronyms: ANSI, CIS, CSC