NIST version reviewed: (Draft 2) Framework V1.1 (PDF) with markup

#	Document	Page #	Line #	Section Abreviation	Comment - Jan 19 2018
1	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup	3	184		CPS (cyber physical systems) needs definition / examples
2	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup		409		Tier does not equal maturity but implies decision making. Have heard a lot of companies derive this to be liability if not shoot for a mature tier. Can the guidance explain that Tier levels are in themselves risk based decisiosn and should be mad ebased on current impact and likelihood information available and reviewed at some interval.
3	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup		465		Policy - may need to say as Policy, Standard, and/or Procedure - some controls are process and don't go in policy by most company definitions.
4	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup		472		Measuring assets implies inventory accuracy but not pushed enough as critical to know what you got to make sure assessing the risk and covering your complete exposure.
5	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup		500		operational budget needs cyber maintenance on all asssets from a web page to any device to secure coding. Many hit major delays as lack budget for EOL and other maintance actives. Business needs to see cyber security as a sustain operations just like changing the oil in your car.
6	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup		674		Supply Chain - what about culture challenge, Availabilty, Integrity and confidentially normally opposite order of enterprise network as priorities; production lifecycle is ~10 years to life of plant and not 3-4 years like enterprise laptops/servers…
7	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup		680		Externap party SCRM
8	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup		715		OT - spell out and define
9	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup		846		measurement is a journey and changes should be constant - but sustain trending is important.
10	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup	35		ID.SC-4	3rd party monitoring greater than supply chain - include dependent infrastructure
11	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup			PR.AC-7	challenge is not always technically feasible with today's vendors
12	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup	49		RS-AN-5	push monitor vulnerabilites and exceptions to controls/firewalls
13	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup	7	184		Acronyms previously spelled out. Review throughout document
14	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup	8	217		Example would assist in definition of "mechanism for organization"
15	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup	34		ID.SC-1	ID.SC-1 may fall better into ID.GV category since required to ID.GV-3 "Legal and regulatory requirements regarding cybersecurity …:
16	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup	34		ID.SC-1	NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations MISSING REFERENCE. Is CSC 4: Vulnerability Assessment and Remediation the best reference to support this requirement?
17	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup	35		ID.SC-4	routine cadence defined? Clarify how often shoud this be expected to occur
18	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup	35		ID.SC-5	frequency? is this requiring an initial plan and test with no recurrence of validation of effectiveness
19	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup	37		PR.AR-7	commensurate with the risk of the transaction - Difficult to understand what this means
20	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup	39		PR.DS-8	Frequency or integrity checking needs to be defined
21	Framework for Improving Critical Infrastructure Cybersecurity v1.1 Draft 2 with Markup	49		RS.AN-5	Reference/Example what external sources would be recommended/required