Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Mauricio Tavares (Privacy Test Driver)		20	765	If I had access to a system without being detected, after identifying any monitoring system, I would do my best said system would not report me.	Add “Care should be taken to ensure monitoring system is not being (accidentally/intentionally) misconfigured to submit inaccurate information.”
2	Mauricio Tavares (Privacy Test Driver)		16	635	How are the requirements achieved? The assumption here is a government agency will specify which requirements they are interested on. Literacy training may mean different things to different people. Case in point is if a business looks to hire an 3rd party to conduct such training, different 3rd parties may offer, say, for spear phishing a video or an interactive exercise. At the end of that, said party issues a certificate of completion. Is that enough? If there is an incident here, will agency then declare it was due to this requirement not successfully fulfilled?	
3	Mauricio Tavares (Privacy Test Driver)		25	905	Like any software, password managers are/should be kept current. That is still the case if using a third party, which we hope will have some document keeping track of updates and the reason for them.	Inspect password managers to ensure their latest software updates and patches are installed even if hosted by third party.

4	Mauricio Tavares (Privacy Test Driver)		33	1162	Who can access what and for how long. A lot of people forgets about the last part.	If possible, define duration of access
5	Mauricio Tavares (Privacy Test Driver)		34	1194	Probably should also mention said records are stored somewhere secure.	d. Ensure access to these records is logged and limited to authorized personnel
6	Mauricio Tavares (Privacy Test Driver)		50	1700	Note that virtualization techniques, once identified by an APT, makes the system running the virtualization a target.	
7	Mauricio Tavares (Privacy Test Driver)		51	1741	I've seen printers in a separate subnet, which had full access to the desktop subnet. What could possibly go wrong?	Ensure proper access control between different subnets is in place
8	Mauricio Tavares (Privacy Test Driver)		53	1802	some ports are non-persistent, only needing to be open to execute a specific (not) scheduled task	
9	Mauricio Tavares (Privacy Test Driver)		54	1030	I would like to add a new item. Virtualization is nice, but putting the minimum amount of services (I am a big believer of "you just had one job") makes it hard for someone to take a service and then hop to the other service it talks to. Reason is that we can then only have the port required for them to talk open, as opposite to having this other service there waiting for attacker to see what it does and use root to have fun.	Minimize the number of applications running on a system. Having a system performing multiple functions -- database, web server, mail server -- increases the attach surface of an APT. By having each function isolated, the impact of a compromise is minimized.
10						
11						