#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
	FireEye, Inc		T	22, 23, 24, 25		Appendix A	While the Framework clearly states that it is not exhaustive, the current list of Informative References will not incentivize critical infrastructure companies to adopt measures that will defend against advanced cyber threats. As the recently publicized Beebus attack against drone manufactures demonstrates, our critical infrastructure is under attack from advanced cyber threat actors. These adversaries use sophisticated tactics such as exploiting previously unknown vulnerabilities (zero-day attacks) or using never seen before malware to steal US intellectual property and potentially disrupt or deny use of critical infrastructures. As currently constructed, the Framework will not mitigate risk from these kinds of attacks. By incorporating emerging best practices that use behavioral or virtualization techniques into the Framework, companies adopting the Framework will be in a better position to identify and block sophisticated threats. One example of a best practice that incorporates these approaches into an organization's defensive posture is the recently released NIST *Special Publication 800.53 Rev4, Security and Privacy Controls for Federal Information Systems and Organizations, Security Control 44* (SC-44, found in Appendix F-SC, page F-214). In spite of SC-44's widespread adoption across the Fortune 500, the Framework does not point to SC-44 as an informative reference. This oversight will leave critical infrastructure at risk to exploitation by advanced cyber threats, even after they spend resources adopting and implementing the Framework.	Incorporate SC-44 as an informative reference to the following subcategories: -DE.AE-2 Detected Events are analyzed to understand attack targets and methods (pg. 22); -DE.CM-4. Malicious Code is detected (pg. 22); -DE.CM-5 Unauthorized mobile code is detected (pg. 23); -RS.AN-1 Notifications from the detection system are investigated (pg. 24); -RS.AN-2 Understand the impact of the incident (pg. 24); -RS.AN-3 Forensics are performed (pg. 24); -RS.MI-1 Incidents are contained (pg. 25); & -RS.MI-2 Incidents are eradicated (pg. 25)
	FireEye, Inc		E	3	182	1.2	This sentence clarifies that the implementation of the Framework should be risk based and flexible.	Change the sentence beginning on line 182 to read "Because of these differences, the Framework is adaptive to provide a flexible and risk-based implementation."
	FireEye, Inc		G	6, 7	252, 259, 265, 273	2.1	In describing the Protect Function, the text uses the word "safeguard" where each of the additional Functions uses the word "activities" (arguably a broader term) in the same context. This implies that organizations should only implement "safeguards" under Protect and "activities" elsewhere. FireEye recommends that organizations need to implement safeguards AND activities so it is clear that safeguards and activities can coexist in each Function.	Change the description of each Function so that it reads "Develop and implement the appropriate safeguards and activities". Define Activity and Safeguard in the glossary (line 686).
	FireEye, Inc		E	9, 10		2.4	Clarity	Change the phrase Integrated Program to Integrated Risk Management Program

	FireEye, Inc		T	36, 39	509 and C.9	Appendix C	According to a December 2013 Ponemon Institute report on *The State of Advanced Persistent Threats,* organizations on average have experienced approximately 9 separate APT-related incidents in the past 12 months. In addition, the report states that 68% of respondents to a recent Ponemon survey indicate that zero-day attacks are their organization's greatest threat. These same respondents also overwhelmingly report that advanced cyber threats have successfully evaded their traditional IDS and AV solutions. These figures are consistent with FireEye research, which has identified numerous, discreet APT attack campaigns (e.g., Beebus, Gh0stRat, SpyNet) successfully targeting critical infrastructure sectors such as Energy, Telecom and the Defense Industrial Base. In light of the significant risk to US economic and national security and the increasing prevelance of advanced attacks, future iterations of the Framework must specifically identify the challenges associated with advanced cyber threats and offer risk management guidance.	Include "Mitigating Risk From Advanced Cyber Threats" as an area for improvement. Add the following as a new section C.9: Advanced cyber threats using sophisticated tactics are successfully targeting critical infrastructure companies with increased frequency. Traditional security defenses and best practices, however, do little to identify, prevent or mitigate risk from zero-day attacks and never-seen-before or polymorphic malware, leaving critical infrastructure companies vulnerable. To mitigate risk from these kinds of attacks, organizations require more information about the challenges associated with advanced cyber threats and guidance on how to defend against them.