Comment (Include rationale for comment)	Suggested change
***There are several important steps missing for companies to Get Started (**bolded**).** ***The concept of Scope is important--identify what assets the Framework applies to, specifically reference the use of a risk management approach and development of a list of risks (risk register).** ***Developing a roadmap and investment strategy, obtaining executive-level buy-in and funding, and ensuring Continuous Improvement are also important steps to Get Started.**	Apply simple approach to Get Started. *Missing critical steps- Page 1 (bolded) Step 1: Identify - **Determine [scope] what critical infrastructure to protect**; **Step 2: Self-Assessment - Assess current cybersecurity posture (using Security Index or ES-C2M2)**; Step 3: Conduct a Risk Assessment - Use one of the mentioned risk management approaches (ISO 31000, NIST 800-39, etc.) or the simple risk management process Phil lists in the Risk Management process suggestion below to develop a Risk Register); Step 4: Create Targets - Identify and prioritize opportunities for improvement utilizing risk management approach above and associate risks with Target objectives next to each of the 5 Framework Functions; Step 5: Planning and Alignment - Assess progress toward the target state. **Develop roadmap and investment strategy and** foster communications among **[and buy in from]** internal and external stakeholders (senior executives and Board).; Step 6: Implement Action Plan.; Step 7: **Ensure Continuous Improvement**
*** The listed risk management approaches (NIST 800-39, ISO 31000, etc.) are not trivial and providing a simple risk management approach will help many "Get Started".** *** The 5 Step Risk Management Process is a very basic, but common approach to risk management that will help progress security decision making and help with prioritization.**	Provide simple risk management process to Get Started in the Framework document. Suggested entry-- 5 Step Risk Management Process: Step 1 - Identify risks Step 2 - Prioritize list of risk findings (Risk Register) and determine if you need to Remove, Reduce, Transfer, or Accept the risk Step 3 - Establish security roadmap towards addressing identified risks Step 4 - Obtain executive level approval and funding for roadmap Step 5 - Continuously assess program using Security Index

***Aligned with most consultant/audit security program assessments and uses CMM** ***Use constructive, non-regulatory language like Security Index where we can set our own Goals or Targets** ***ES-C2M2 uses similar approach (embedded to assess each MIL)--Not implemented, Partially implemented, Largely implemented, Fully implemented, and Achieved--found in the ES-C2M2_Self-Evaluation_Toolkit_2of2.zip in the ES-C2M2 Report Builder spreadsheet** ***Tiers and Profiles is a confusing and** NEW **construct. We can move to this in CSF version 2.0, but let's not start here. No one raised their hands in the Raleigh workshop when we polled the group "Do you know how to use Tiers and Profiles?"** ***Suggest that NIST use a Survey Monkey to continue to broadly poll this question.** ***Security [Capability Maturity Model] Index is a simple construct and broadly used already without people knowing they're using it, they just are.**	***Offer options for a simple Self-Assessment (e.g. Security (CMM) Index and ES-C2M2).** ***Use** CMM/CMMI **as a simple self-assessment methodology for the CSF 5 Functions and** associated charts/graphs **SCMMI Index 1 - Initial / Ad-hoc - Not Implemented** **SCMMI Index 2 - Repeatable / Managed (Risk Informed) - Partially Implemented** **SCMMI Index 3 - Defined - Largely Implemented** **SCMMI Index 4 - Quantitatively Managed - Fully Implemented** **SCMMI Index 5 - Optimizing - Achieved** *** Set Goals or Targets associated with Security Index**
***Cross mapping allows each of the prominent, core security standards identified in the Information References to stand on its own merits and allows companies that have adopted at least one of the security standards apply the specific security standard.** ***H2Cross mapping allows each standard to clearly show what a company is doing to adopt/implement the Cybersecurity Framework with respect to the other security standards.**	Cross map prominent security standards in the Informative References. 1: Use the Alternative View version of Appendix A. The consolidated view (or mash up view) in the Preliminary Framework Cybersecurity.pdf is confusing. 2: Also provide a spreadsheet version of **Appendix A with the Alternative View** similar to what you released prior to Raleigh for the consolidate/mash-up view of Appendix A / Framework Core.XLSX http://www.nist.gov/itl/upload/preliminary_cybersecurity_framework-framework_core.xlsx
***Without a thorough cross mapping, NIST will have put into question the thoroughness of the existing security standard if a standard in the Informative References cannot fulfill a specific Subcategory element (row).** ***NIST will also have effectively created a new security standard without thoroughly performing the cross mappings.** ***Missing several controls that have been known to fail such as ISO\IEC 27001:2005 A.10.9.1, A.10.9.2, A.10.9.3, and A.8.2.2 that have been identified by HISPI as controls that have consistently failed in 2012 that led to compromised protected data.**	1: Must ensure NIST, COBIT, CSC, and ISO cross mappings are thorough/complete mappings (there are too may "NA" entries). 2: Ensure ISO\IEC 27001:2005 A.10.9.1, A.10.9.2, A.10.9.3, and A.8.2.2 are listed in the controls listings.
***The CSA CCM is open source material, where other cross mappings cost money, and the CSA is willing to work with NIST and US government to keep this cross mapping up to date.** ***The CSA CCM have been updated frequently (every 6 to 18 months). The CCM applies to single and to multi-tenant entities and is based on ISO and HITRUST.** ***CSA CCM already covers cloud which will become critical infrastructure.**	Use existing cross mappings such as the CSA CCM

***Phil and CSA is reconfiguring the CSA CCM to resemble the Framework by default. Release date is TBD but will be available by the end of the year.**	
Examples--SANS Quick Wins, Australian Signals Directorate Sweet Spot, and HISPI Top 20 ISO\IEC 27001:2005 Annex A Mitigating Controls** ***Use breach analysis reports—Ponemon, VZ, Mandiant, SANS, HISPI, Trustwave, and Microsoft** ***Approach identifies priorities** ***Cost benefit obtained through adoption of a small subset of controls known to fail** ***Can be different by Sector and Sub-sector, but believe that there are some universal truths on controls failures when it comes to technology controls** **- The Cybersecurity Framework released to date is missing controls that already have been known to fail according to the HISPI 20 ISO 27001 top failures-A.10.9.1, A.10.9.3, A.10.9.3, and A.8.2.2 should be controls listed in the Informative References but are not. These controls have failed the most in 2012 and have led to protected personal data breaches that were reported.** ******* **1. Patch Applications/Systems (cited by VZDBIR, SANS, AUS, HISPI, Microsoft, TW)** **2. OWASP 10 – SQL Injection/XSS (cited by OWASP, VZDBIR, HISPI, Microsoft, TW)** **3. Look at your logs and detect signs of compromise/attacks (cited by VZDBIR, Mandiant, HISPI, TW)** **4. Limit admin/privilege access (cited by all)** **5. Continuously scan for and remediate critical security vulnerabilities (cited by VZDBIR, SANS, AUS, HISPI, and Mandiant)**	Implement the Quick Wins approach. Identify what controls failed the most from breach data and analysis reports. Start Here (CSF Quick Wins): 1. Patch Applications/Systems 2. OWASP 10 – SQL Injection/XSS 3. Look at your logs and detect signs of compromise/attacks 4. Limit admin/privilege access 5. Continuously scan for and remediate critical security vulnerabilities