#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	Smart Card Alliance	N.Pattinson	G				The document has a fundamental lack of appreciation for strong authentication and how this can be a valuable aspect of assurance in cybersecurity.	Incorporate Strong Authentication into the cybersecurity framework to strengthen the known and trusted devices and parties within the framework.
2	Smart Card Alliance	N.Pattinson	G	5	216	2.1	The five functions listed as Identity, Protect, Detect, Respond and Recover are inadequate and can be improved. Identification alone is insufficient to protect against vulnerabilities.	Recommend a sixth function be incorporated into the strategy. This function should be after Identity and before Protect. The new function should be Authenticate. This should apply to machines, devices and people who are within a cybersecurity framework scope. The Smart Card Alliance would be happy to work with NIST on defining this aspect of the Framework.
3	Smart Card Alliance	N.Pattinson	G	36	501	Apdix C	Authentication should not be left for furthur improvement; it should be baked in from the beginning of a framework definition.	See #1 in this response,
4	Smart Card Alliance	N.Pattinson	G	7		2.2	The Framework Profile should incorporate authentication within its scope and how to better improve the authentication of machines, devices and people participating the the cybersecurity profile(s).	Incorporate Strong Authentication into the cybersecurity Framework Profile scope.
5	Smart Card Alliance	N.Pattinson	G	9		2.4	The first tier, Tier 1, is labelled Partial. This is a weak label in regard to cybersecurity protection and in reality this Tier level is undesirable.	Recommend Tier 1 be renamed from Partial to Vulnerable.
6	Smart Card Alliance	N.Pattinson	G	12	422	3.2	A Target Profile is a critical step within an organization's assessment of Framework Elements.	Ensure an Identity Management concept is incorporated into the Target Profile, allowing to identify and authenticate machines, devices and people within the framework scope and to what level of authentication will be utilized to maintain integrity of access.

7	Smart Card Alliance	N.Pattinson	G	13		Apdix A	In light of previous comments regarding identity management and ability to authenticate, include in the Framework Core a section on Authentication. Reference to the U.S. Federal government's implementation of identification and authentication policies is recommended as wide adoption of these national standards by organizations is a beneficial direction for cybersecurity assurance. Reference to other commercial authentication standards is also important.	Authentication can incorporate levels of Assurance (OMB 04-04), Identity assurance (FIPS201) and Identity authentication (FIPS201). Related documents should include NIST SP 800-73, SP 800-76, SP 800-79, SP 800-116. Also OMB 11-11. Add other standards that are relevant to authentication as well (e.g., OATH OTP standard, assurance levels in Common Criteria). The Smart Card Alliance would be happy to work with NIST on identifying the appropriate standards.
8	Smart Card Alliance	N.Pattinson	G	36	508	Apdix C	Supply Chains Risk Management practices and certification are being developed within The Open Group.	Incorporate references to http://www.opengroup.org/getinvolved/forums/trusted within the scope of risk mitigation of supply chain in the Cybersecurity Framework.
9	Smart Card Alliance	N.Pattinson	G	36	518	Apdix C.1	The discussion in section C.1 appears to abdicate authentication from the Cybersecurity Framework and drop it into NSTIC and IDESG activities. Neither of these organizations is focused on comprehensive authentication to the extent that will benefit a Cybersecurity Framework. IDESG aims to provide an ecosystem where many approaches to identification and authentication can potentially interoperate. It is important to ensure any outcomes from NSTIC or IDESG do not deflect from the fundamental need for authentication with a cybersecurity framework from the outset.	Improve the language to lay out the need for authentication in a cybersecurity framework regardless of NSTIC and IDESG eventual outputs.

10	Smart Card Alliance	L.Suneborn	G	TBD			This document provides good guidance and topics to consider when a creating and designing a framework. However, there is no mention of process and procedure to guide relevant IT staff when an intrusion is detected in a deployed system.	Suggest adding a subsection (can fit in several location in this document) that provides guidance during an intrusion. Sequence of events may be: 1. Detect; 2. Assess & Identify; 3. Respond; 4. Recover. The Smart Card Alliance would be happy to work with NIST on defining this aspect of the Framework.