#	Organization	Commenter	Type	Page #	Line #	Section	HIMSS Comments	Suggested change
		HIMSS		i	11 to 12	Note to Reviewers	HIMSS notes that privacy and security should be integrated into the business objectives of an organization in order to strengthen cybersecurity and support business objectives. Doing so helps to preserve an organization's goodwill, and meets expectations of customers/clients/patients. Security should be a shared responsibility with more people in the workforce having access to the data.	
		HIMSS		i	15 to 16	Note to Reviewers	HIMSS recommends that guidance and resources be flexible and workable. The guidance should recommend measures which are not onerous or too costly to implement. Onerous measures may result in users circumventing (or working around) the measures which are advocated through the guidance and resources. In addition, the guidance and resources listed should also promote innovation to encourage innovators to advance the state of the art and make the technology (e.g., access controls, incident detection, etc.) easier to use, more effective, and less costly.	

		HIMSS		i	29	Note to Reviewers	We note that the guidance does not list implementation measures, but should do so. In addition, it does not specify what a target profile for an organization could be. It is important to at least provide examples of what a maturity model or standard would be and to provide tools to assist an organization in measuring its progress against said model or standard. Otherwise, there may be conflicting and divergent understandings of what good (or best) privacy and security practices would be or could be.	Add in implementation measures and add more specificity regarding the target profile and what it could be (or should be).
		HIMSS		2	100-101	1	Business or cybersecurity risk management process: We note that the cost to implement is not mentioned. We suggest a discussion on a cost-benefit analysis, such as the benefits which would outweigh the costs.	Add in discussion about the cost-benefit analysis.
		HIMSS		3	164	1.2	Processes (in addition to systems) require attention (presumably, "systems" refers to computer technology). "Processes" means workflow, namely, the actions of people (e.g., non-automated steps in access management). We note that organizations can prioritize systems and processes that require attention.	
		HIMSS		5	206	2.1	Framework Core: we note that it seems unclear how the Framework Core will be measured and addressed. There are no implementation measures or a way to objectively measure how an organization is doing against a certain standard or model.	Add in implementation measures and tools for measurement.

		HIMSS		6	243-251	2.1	Framework Core: HIMSS notes that in terms of the "Identify" function of the framework core, it is important to include personnel and their know-how, in addition to understanding what technology resources an organization has. You need people to maintain and manage the technology resources. Not all organizations, however, have the personnel and know-how in-house and therefore they must outsource. Also, sometimes key employees (with such know-how) leave and there is a need for the organization to reconfigure in terms of role management.	Add discussion about personnel and their know-how, in addition to an understanding of what technology resources an organization has.
		HIMSS		6	246	2.1	Risk Assessment: HIMSS notes that examples could be tied to meaningful use and risk assessment.	
		HIMSS		6	252	2.1	Protect: HIMSS observes that encryption is not mentioned as a safeguard.	Add encryption as a safeguard.
		HIMSS		7	265	2.1	Respond: HIMSS observes that entities may respond differently as a function of their size, scale and financial position. Larger organizations may be able to have much more sophisticated response than, for example, a solo practitioner in the healthcare industry.	
		HIMSS		7	265-272	2.1	Framework Core: HIMSS notes that it is important to have a written incident response plan. The incident response plan should include people, processes, and technology and address what constitutes an incident and address all phases of incident response (including detection, handling, eradication, and notification and communications about the incident).	Add in a discussion about having a written incident response plan. NIST Special Publication No. 800-61 Rev. 2 could be listed as a helpful resource.

		HIMSS		7	273-280	2.1	Framework Core: HIMSS notes that recovery should not only address short-term recovery (e.g., incident eradication, business continuity, restoring to normal operations, etc.) after an incident, but also recovery in the long term (i.e., organizational resilience) to improve the security posture of the organization and strengthen its cyber-infrastructure. In addition, the recovery step should loop back to the identify function of the Framework Core and generally it should be emphasized that the five Framework Core functions are part of a cycle for which there is a constant feedback loop (including in view of any lessons learned in terms of people, processes, and/or technology after an incident).	Add to discussion more specificity regarding recovery in the short-term and long-term (namely, organizational resilience).
		HIMSS		7	282-291	2.1	Framework Core: HIMSS observes that the "target profile" is not defined. Although the Framework is intended to be flexible, some organizations may not know which model, standard, or other guidance should be followed as a best practice (or a good practice). In addition, even if a "target profile" were selected by an organization, the organization may not have the tools for objective measurement to help gauge its progress. Finally, the target profile may change over time as an organization's security posture improves and therefore the "target profile" may be fluid and dynamic in nature.	Add in implementation measures and add more specificity regarding the target profile and what it could be (or should be).
		HIMSS		8	308	2.3	Figure 3: HIMSS notes there is no mention of finance and cost.	Add in mention of finance and cost.

		HIMSS		9 to 10	332-346	2.4	Framework Core: Tier 1: We observe that a reactive, ad-hoc approach to risk management may result in a weak security posture and a repeating occurrence of incidents (which may rise to the level of breaches). It may also lead to underreporting or inaccurate and delayed reports of incidents or breaches with a	
		HIMSS		10	347-357	2.4	Framework Core: Tier 2: We note that with a lack of organizational-wide policy, there may be underreporting or inaccurate and delayed reports of incidents or breaches.	Add into discussion that an organizational-wide policy is a best practice.
		HIMSS		10	372-376	2.4	Framework Core: Tier 4: HIMSS notes that both business continuity and organizational resilience (to help strengthen an organization's cyber-infrastructure) are important action items in terms of "lessons learned" after an incident.	Add in discussion about business continuity and organizational resilience.
		HIMSS		11	386-389	2.4	Information Sharing: Tier 4: We note that both business continuity and organizational resilience (to help strengthen an organization's cyber-infrastructure) are important action items in terms of "lessons learned" after an incident.	Add in discussion about business continuity and organizational resilience.
		HIMSS		11	409-411	3.2	Establishing or Improving a Cybersecurity Program: We recommend that all six steps should be part of a continuous feedback loop. In addition, risk should not be just based upon simply regulatory requirements or legal liability, especially in the face of the growing problem of cybercrime. Risk, however, should be managed based upon organizational needs and customer/client/patient needs.	Add to the set of six steps an explanation which states that all six steps should be part of a continuous feedback loop. Lessons learned should serve as a tool to refine or otherwise revise the process as a whole.

		HIMSS		12	432-436	3.2	Establishing or Improving a Cybersecurity Program: We note that the action plan should include incident handling, response, recovery, and organizational resilience (to strengthen an organization's cyber-infrastructure).	Include the following elements in the action plan: incident handling, response, recovery, and organizational resilience.
		HIMSS		13-26	All	Table 1	Framework Core: For the standards, guidelines, and practices which are listed in the table, we note that it may be good to list which critical infrastructure sectors and industries within will benefit from those which are listed.	List which critical infrastructure sectors and industries within will benefit from those which are listed for the standards, guidelines, and practices.
		HIMSS		16	N/A	Appendix A	Risk Management Strategy: The risk management strategy may depend upon costs and level of risk (e.g., low or high). HIMSS observes that the solution may be different depending upon what these are.	
		HIMSS		16-21	N/A	Appendix A	Protect: We recommend that identity proofing, authentication, and authorization should be included in this discussion.	Add identity proofing, authentication, and authorization to the discussion.
		HIMSS		18	N/A	Appendix A	Data Security: We recommend that encryp	Add encryption to the discussion.
		HIMSS		19	N/A	Appendix A	Information Protection Processes and Procedures: We recommend that data quality and data integrity need to be included in the discussion. If the data is tainted, the data will not convey accurate information. Data quality is one of the most important aspects of business analytics and "big data."	Add data quality and data integrity to the discussion.
		HIMSS		22	N/A	Appendix A	Detection for malicious code: We note that it is important to detect malicious code based upon not only traditional signature detection, but with the use of other means such as heuristic detection, in view of the ever increasing number of malicious code that exists in the wild each day. Signatures are not always known and malicious code may exist in the wild even for years before said code is identified.	Add additional information regarding detecting of malicious code and include mention of traditional and non-traditional means of detection (e.g., heuristic detection).

		HIMSS		22	N/A	Appendix A	Detection: We note that it is important to adequately define what an anomaly or an event is. In the age of advanced persistent threat, a cybersecurity event may be one which may be unsuccessful or successful. It is therefore important to obtain an accurate baseline of what normal activity and operations look like for an organization. Static tools (e.g., traditional antivirus software and intrusion detection systems), in the face of advanced persistent threat and other sophisticated attacks, may not be enough to detect such occurrences. Intelligence-driven network security tools may be used to detect anomalies, events, and hopefully to head off threats before they become problematic (i.e., a successful attempt which infiltrates into a system, potentially exfiltrates data, and potentially causing harm, damage, or other adverse event). Also, in the age of insider threat, it is important to detect what is happening inside your organization (i.e., vis-a-vis trusted insiders) as well as outside. (To this end, the CERT guide for Mitigating Insider Threat may be considered as an appropriate reference.)	Add in more specificity regarding what an anomaly or an event is.
		HIMSS		24	N/A	Appendix A	Response: We observe that response may not be the same for all organizations.	

		HIMSS		26	N/A	Appendix A	Informative References: We note that the list of informative resources should be expanded to include ISACs, CERTs, public private partnerships, and other helpful resources such as NIST Special Publication No. 800-39 on Managing Information Security Risk (which may help organizations understanding the process for framing, assessing, responding, monitoring risk) and 800-55 on performance management for information security (which may help organizations with implementation measures, effectiveness/efficiency measures, and impact measures). In addition, relevant portions of these guidance documents should be incorporated into the Framework. Another informative reference which may be helpful to list is the CERT resource on mitigating insider threats.	Add a listing of ISACs, CERTs, public private partnerships, NIST special publications, and other resources that will be helpful. If the NIST Framework is flexible and scalable across critical infrastructure sectors, it should have a wide variety of useful and helpful references to assist various organizations.
		HIMSS		27	484	Appendix A	ID Identify. Business Environment: HIMSS recommends that there should be a discussion about costs.	Add in discussion about cost.
		HIMSS		28	491	Table 3	Methodology Column: Identify contractual, regulatory and legal, including Constitutional, requirements: We note that there needs to be a discussion about current regulations and legal requirements.	Add in discussion of current regulations and legal requirements.
		HIMSS		28	491	Table 3	Governance: Methodology column - PII: We note that this discussion also needs to mention policies on identity proofing, authentication, authorization, and patient consent.	Add discussion regarding policies on identity proofing, authentication, authorization, and patient consent.
		HIMSS		36	501	Appendix C	Authentication, identity proofing, authorization, transmission standards, and encryption need to be included in the discussion as well as addressing issues concerning preserving data quality and data integrity.	Add in discussion of authentication, identity proofing, authorization, transmission standards, and encryption and preserving data quality and data integrity.

		HIMSS		36	517	Appendix C	Authentication: HIMSS notes that the level of authentication should be commensurate with the level of risk.	Add in that the level of authentication should be commensurate with the level of risk.
		HIMSS		38	613	Appendix C	Privacy Standards: The notion of trust needs to be included in the discussion, including whether the communication is inside or outside the organization. Data use sharing agreements may be included in the discussion as well, in addition to the notion of consent.	Add in trust to the discussion.
		HIMSS		42-43	All	Appendix E	Glossary: If the NIST Cybersecurity Framework is to be a tool for communication using a common language, HIMSS notes that more terms need to be defined. In addition, it would be helpful to have more specificity in terms of the definitions. For example, depending upon how the term "cybersecurity event" is defined by an organization, an incident may or may not be flagged. An example of this is that an unsuccessful incident might be not defined as a cybersecurity event if the organization only defines these events as ones which are successful (but this may very well ignore the problem of advanced persistent threat). Another example of this is that if a cybersecurity event is defined by an organization in terms of an external event, then an event which occurs inside an organization (such as by a trusted insider -- i.e., insider threat) may not be flagged as a cybersecurity event. "Critical infrastructure" needs to be defined with more specificity so that an organization will understand whether it is part of the critical infrastructure or not.	Define with further specificity what a cybersecurity event is and critical infrastructure.