Sam Standring, User of meter now but considering a pump, P:714-889-9899, samstand2@gmail.com

Response Requested: Public

Comment #1:

Document: Protection Profile, Page: 2, Lines: 7 and 2

Comment:

I simply won't get a pump until security from hackers and accidents is perfect.

Perfect defined as not more than one person dies in a million.

All manufacturers safety security testing must be fully transparent to public.

This means not only the good results shown to public but all!

How does any involved organization expect to achieve the level security satisfactory to all of the organizations?

Please include all public and private organizations considered!

Proposed Change:

Make all data on failures and mortality public to all.

Must be found easily on simple Plain English Google search.

RESPONSE:

Thank you for your comments and proposed change.

The evaluation of a product under DTSec includes an analysis of detailed, proprietary design aspects that are confidential. Those involved in an evaluation (e.g. DTSec working evaluation project managers and accredited test lab members involved in the evaluation project) will typically be governed by a confidentiality agreement between the individual and the organization that owns the product. Therefore, DTSec is unable to make any guarantees about whether detailed evaluation results or evaluation failures will be made public, as such disclosure must be approved by the product vendor. This is quite common in the world of security evaluations. Furthermore, downstream health effects are not covered by the standard or its evaluation program, and therefore, mortality events are beyond the scope of DTSec and fall more within the realm of government regulatory bodies, such as FDA.

Changes to standard and/or protection profile made in response: NONE

Gustavo Avitabile, University Federico II of Naples, Italy, P:+393483424939,
gustavo.avitabile@unina.it

Response Requested: Public

Comment #1:

Document: Standard, Page: 11, Lines: 344-347

Comment: I think that vulnerability discovery is unavoidable in any complex system, and the policy should be to provide updates and a simple mechanism to install them. Therefore, the evaluation procedure should include the availability of an adequate update mechanism, and time taken from vulnerability identification to update installation.

Proposed Change: ... However,if certified products are subsequently reported to contain vulnerabilities that conflict with the applicable ST requirements, and such vulnerabilities are not shortly remediated, DWG reserves the right to remove those products from the evaluated products list. DWG reserves ...

RESPONSE:

Thank you for your comments and proposed change.

Philosophically, DTSec working group agrees with you that complex systems are highly likely to require patching in order to maintain the assurance levels initially attained through a DTSec evaluation. While we considered making an update mechanism an explicit requirement in the protection profile, we opted to leave it out in the current revision for the following reasons: First, an update mechanism may be impractical for less complex devices since the cost to manage field upgrades may exceed the cost of replacing the unit. Secondly, the standard is already explicit in its requirement that an evaluated product continue to maintain the same level of assurance post-approval. As you point out in your reference to the standard, the DWG reserves the right to remove products from the approved list if severe vulnerabilities remain unpatched. This threat implies the need for the developer of a complex device, which suffers from frequent vulnerability disclosures, to include an update mechanism in order to prevent the device from losing its approved status. Thirdly, any update installed to the device, regardless of mechanism (e.g. over-the-air or tethered) must be authentic, as covered by existing requirements. Furthermore, any new content brought into the TOE must follow the standard's requirement for assured maintenance, meaning it must meet the same requirements as the original product and is subject to re-evaluation. Therefore, trusted updates are already implicitly covered, and we do not currently see a need to add an explicit trusted update requirement at this time to the protection profile.

Changes to standard and/or protection profile made in response: NONE

Geoff Duke, EWICS TC7 and Johnson and Johnson Diabetes Care Companies, P:0044 1463 721730, gduke@its.jnj.com

Response Requested: Public

Comment #1:

Document: Protection Profile, Page: 3, Lines: Augmentation required to Line 40

Comment: List fails to link to guidance from IEC82304 (Healthcare Software) , ISO80002-1, ISO 80001, ISO 270001.

These would ba appropriately referenced in new sections of this document, should it be structured in a hierarchical and scalable manner. Currently it is not possible to direct sections to be appended because the document itself is not hierarchically structured. Architecture, Functional Models, Gray Box Analysis, Risk Management are not considered with any clarity. Cybersecurity is part of software risk management so needs to be represented as such.

Proposed Change: Restructure emphasizing factures that should be considered as part of the design and which should be analyzed using reliability-based tools such as Fault Trees, FMEA, Cause and Effect (Ishikawa), Funcational Analysis, Gray Box Analysis as part of the design phase thus iterating requirements. Not possible to suggest a single change as the issue is systemic.

RESPONSE:

Thank you for your comments and proposed change.

IEC82304 is not yet ratified and hence unsuitable for reference in the standard at this time. We agree that it would be suitable to reference once it has been ratified, as general-purpose computing platforms are in scope for future product evaluations. It should be noted that the initial set of expected products (e.g. meters, pumps) are not expected to fall under IEC82304. There are a great many standards that could, in theory, be referenced by DTSec. However, adherence to such standards is not strictly required by DTSec. Rather, it is expected that product developers who already follow accepted medical device and software standards will be able to reuse the artifacts generated as part of these processes by providing them to the DTSec security evaluators. If a developer does not follow these standards today, that developer is not strictly precluded from bringing a product forward for evaluation under DTSec. However, the developer will be required to provide whatever design, implementation, and testing artifacts are needed by the security evaluator to perform the security evaluation and meet the AVA_VAN.4 level of assurance against vulnerabilities. The ISO standards you referenced, while excellent sources of guidance for medical device developers, are therefore not necessary. In our opinion, the addition of more referenced standards within DTSec is unlikely to improve a developer's ability to pass a DTSec evaluation, nor significantly improve the standard itself.

We appreciate your comments regarding the hierarchical structure of the standard. The standard can benefit from more rigorous numerical structuring, as you suggest, and so we are adding proper hierarchical numeric labeling to all sections of the

standard. For the sake of brevity, we will not detail in this response summary all individual numerical label additions, as they are added to all of the section headers.

In your comments, you reference the lack of mention of security-relevant design, development, and testing techniques (Architecture, Functional Models, Gray Box Analysis). While these examples are certainly sensible examples for product developers to have in their arsenals, the DTSec standard is intentionally not prescriptive with respect to the specific techniques that a developer should use in its proprietary development processes. A product that has poor security architecture amidst high complexity is less likely to pass a DTSec evaluation because of a corresponding high likelihood of vulnerabilities. However, the craft of secure product design and implementation is beyond the scope of this standard. This standard, rather, is laser focused on the evaluation of a final product's security functionality, regardless of the developer's specific journey from concept to final product.

We agree with your comment that security (and security evaluation) is one part of an overall safety risk management program, since security threats add safety risk to devices. We will add some wording to clarify this.

Changes to standard and/or protection profile made in response:

- **Added hierarchical, numerical labels**
- **Addition of section 1.2, "Role of DTSec in Medical Device Safety Risk Assessment", to the standard. This section explains the importance of cybersecurity risk assessment in perspective of an overall safety risk assessment program and provides detailed examples of how the DTSec program helps fulfill the spirit of common regulatory guidance in cybersecurity risk assessment (uses FDA premarket guidance as the example).**

Geoff Duke, EWICS TC7 and Johnson and Johnson Diabetes Care Companies, P:0044 1463 721730, gduke@its.jnj.com

Response Requested: Public

Comment #1:

Document: Standard, Page: 4, Lines: 90 to 909 inclusive.

Comment: Para 1: Very loose language that does not add value as it is not qualified in the context of providing a yardstick for requirement, design or risk.

Para 2: This section does not add value as it is technology-related and impossible to meet given that there is no conviction to a particular standard or suit of standards, for which existing guidance and standards already exist in industry. Note that 'Availability' has a reliability discipline-related explicit definition.

Para 3: Highly subjective 'requirement' that could not be measured or assessed against predicate standards. There is an implicationj that there is widespread ad-ho, unreliable and low assurance elecronic products available but in what context is not stated. This reads as an emotive response to a subjective and uninformed assessment of the current situation.

Proposed Change: Generally: add IEC80002-1, ISO27001 IEC80001 and IEC82304 plus IEC62304:

Focus on Cybersecurity as part of Ris Assessment.

Secion 1 (1) Devices shall be designed to be secure from unauthorized or inadvertant access to data and device function. This shall be achieved through best practice design that utilizes reliability-based analytical methods as part of a Risk Management Programme intrinsic to an iterative design process.

Section 1 (2) Critical electronic components and finished products shall be independently verified wherever possible with their design documentation and risk assessment(s) relating to a recognised lifecycle model and standard (ie IEC62304, IEC82304, ISO800020-1, ISO80002 [include in reference section])

RESPONSE:

Thank you for your comments and proposed change.

We have responded to your comments regarding the referencing of other/different standards in the other feedback item.

We agree with your comment that security (and security evaluation) is one part of an overall safety risk management program, since security threats add safety risk to devices.

We agree that the life-cycle process (and existing standards that address them, such as IEC 62304) is critical in the overall cybersecurity mission. However, DTSec does not

aim to restate the use of existing standards such as it were. Rather, DTSec aims to fill the gap of existing standards: the lack of developer-independent evaluation of security.

Changes to standard and/or protection profile made in response:

- **Addition of section 1.2, "Role of DTSec in Medical Device Safety Risk Assessment", to the standard. This section explains the importance of cybersecurity risk assessment in perspective of an overall safety risk assessment program and provides detailed examples of how the DTSec program helps fulfill the spirit of common regulatory guidance in cybersecurity risk assessment (uses FDA premarket guidance as the example).**

Salvatore Turco, Department of Clinical and Experimental Medicine, University Federico II, Naples - Italy, P:+393356299190, salvatoreturco3@tin.it

Response Requested: Public

Comment #1:

Document: Protection Profile, Page: all, Lines: all

Comment: no comment

Proposed Change: no

RESPONSE:

Changes to standard and/or protection profile made in response: NONE

Malcolm Clarke, Brunel University, BSI, IEEE 11073, P:00447973255276,
malcolm.clarke@brunel.ac.uk

Response Requested: Public

Comment #1:

Document: Standard, Page: 1, Lines: 1

Comment: This standard, with few modifications, could apply to any medical device. We would therefore like to comment, and extend invitation, for DTS to liaise with IEEE 11073 to determine if these standards could better be published through the IEEE.

There are many advantages that would result. IEEE is an SDO (DTS is not), and so the publsihed standard would receive greater perceived value, be more widely adopted (it could go forward for joint ISO/IEEE publication) and existing conformance and testing procedures could be applied.

Proposed Change: We would like to extend invitation for DTS to liaise with IEEE 11073 to determine if these standards could better be published through the IEEE.

RESPONSE:

Thank you for your comments. DWG welcomes a discussion with IEEE.

Changes to standard and/or protection profile made in response: NONE

Bryan Mazlish, Founder, Chief Technology Officer at Bigfoot Biomedical, Inc., P:(408) 514-4474, bmazlish@bigfootbiomedical.com

Response Requested: Public

Comment #1:

Document: Protection Profile, Page: 11, Lines: 193-198

Comment: Bigfoot Biomedical, Inc. is dedicated to reducing the burden of life with Type 1 Diabetes by bringing to market solutions and systems that are both safe and effective. One potential way to improve therapy adherence is to permit the person with diabetes (PWD) to interface with their diabetes devices through the convenience of their personal smartphones. Although there are always security risks associated with any internet connected device that permits the user to download third-party software, there are a variety of techniques that can mitigate the risks associated with a system connected to a commercial-off-the-shelf (COTS) smartphone. Accordingly, it is premature for the Diabetes Technology Society to conclude that "it is unlikely that a smartphone . . . would be able to meet the assurance requirements of this [Protection Profile]." This proposed revision thus seeks to highlight the need for appropriate security features to authenticate and authorize commands sent from a smartphone, yet eliminate the language that could impede the development of connected systems that would materially improve the quality of life for a PWD.

Benefits of a Connected Smartphone

Allowing PWDs to view data or send commands to their diabetes devices using their personal COTS smartphones can improve their lives by allowing them to discretely self-monitor and/or make adjustments to their therapy. Many PWDs are reluctant to interact with their diabetes devices and/or dedicated remote control devices when in a public or social setting due to a desire to avoid unwanted attention. See e.g., http://www.medscape.org/viewarticle/708784 (describing social embarrassment being an obstacle to insulin treatment). Allowing a PWD to more inconspicuously interface with their medical devices using a personal COTS smartphone could potentially improve therapy adherence.

Additionally, in the event of a failure or loss of device, COTS smartphones will likely be more accessible and replaceable as compared to a dedicated, proprietary remote control device. If a PWD loses or damages a dedicated remote control device, such as a device that has "customized firmware the limits the smartphone to clinical operation alone," that person may not be able to quickly procure a replacement from the device manufacturer, while COTS smartphones are prevalent and thus quickly replaceable.

Connection to a personal COTS smartphone may also reduce the number of devices that a PWD carries around, thus reducing the burden of living with diabetes. The proliferation of mobile applications on COTS smartphones offers consumers the ability to conduct multiple tasks with a single computing device that fits within their pocket -- indeed, the COTS smartphone has already replaced more than 40 individual gadgets in our lives. See http://www.wired.com/2013/04/convergence/. Consumers no longer need to walk around with multiple devices in order to take pictures, navigate the physical world, listen to music, or perform sensitive financial transactions. The FDA has recognized how mobile medical

applications can "leverage the portability mobile platforms can offer" and discusses how mobile medical applications can be used to control medical devices. Mobile Medical Applications: Guidance for industry and Food and Drug Administration Staff, issued February 9, 2015, pp. 6 & 14 (available at http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf). The FDA also has a goal of "promot[ing] the development and availability of safe and effective interoperable medical devices" that "exchange and use information safely and effectively with other medical devices as well as other technology." Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff, document issued January 26, 2016, pp. 1-2 (available at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf). The FDA recognizes that consumers continue to demand that their COTS smartphones be able to perform or assist with all types of tasks, including allowing for interoperability with their medical devices, and PWDs should also be able to take full advantage of the smartphone revolution.

Leveraging the processing power and user interface of a COTS smartphone has the potential to improve the user experience and/or reduce the cost of a medical device. An interface using a familiar mobile platform may be more intuitive for new users to learn and use than a novel, proprietary interface on a dedicated device.

Because connected COTS smartphones have the potential to reduce the burden of diabetes and improve therapy adherence, the Protection Profile should avoid premature statements about whether a connected COTS smartphone could meet the Protection Profile's outlined mandatory security requirements.

Securing a Smartphone Connected System

Contrary to the draft Protection Profile's assertion on lines 193-198, a diabetes management system that includes a connected COTS smartphone can be designed such that it meets the mandatory requirements of the draft Protection Profile. While the draft Protection Profile appropriately highlights the need for each component of a diabetes management system to provide the utmost protection for the patient, the evaluation of each component should be considered within the context of how the component interacts within the overall system. Although a COTS smartphone provides a wide variety of cyberattack surfaces for both malicious and accidental manipulation, a COTS-smartphone-connected system can leverage features of other system components in the mitigation of those threats that cannot be adequately addressed on a COTS smartphone alone.

Instead of making conclusory statements about what types of devices would likely meet the standards of the Protection Profile, the Diabetes Technology Society has the opportunity to follow the example set by the FDA in recognizing the need for mobile medical applications, interoperable medical devices, and robust cybersecurity. The Diabetes Technology Society should focus on the need for diabetes device manufacturers to design systems to be secure by "identifying assets, threats, and vulnerabilities" and "suitable mitigation strategies" early "during the design and development of the medical device." Content of Premarket Submissions for Management of Cybersecurity in Medical Devices at p. 4. Moreover, evaluations of whether a device provides proper cybersecurity should consider "the likelihood the vulnerability will be exploited (either intentionally or unintentionally), . . . the

probable risk of patient harm due to a cybersecurity breach," and "the usability of the device in its intended environment of use." Id.

Although the inclusion of a COTS smartphone in any connected diabetes device system presents significant protection challenges, these challenges can be mitigated by controlling how a COTS smartphone interacts with the other system components. Security risks do not need to be addressed solely on the smartphone; these risks may be mitigated at any level of the overall system, from the hardware of a diabetes device, to the connection between a COTS smartphone and the hardware, to user protocols, to cloud services. By example, commands could be protected in transit from a cloud service to a device using a key which is never shared with the smartphone. By leveraging security features in the device hardware (e.g. a secured root of trust) and cloud, cryptographic keys can be stored in a manner that adequately mitigates a disclosure threat. A connected diabetes device component should be evaluated based on the level of protection provided by the overall system and not merely the platform on which that component resides.

Conclusion

Robust cybersecurity is a necessity for any connected diabetes device, and manufacturers of connected diabetes devices and systems must employ an early, holistic approach to system security. The goal of robust cybersecurity, however, does not justify premature conclusions about whether different types of components of potential diabetes management systems can adequately address the associated security risks. Because of ample benefits of allowing communications with a COTS smartphone, lines 193-198 of the draft Protection Profile should be revised to leave open the possibility that manufacturers of connected diabetes devices may implement security features that accomplish the goals of the Protection Profile.

Proposed Change: The two complete sentences on lines 193-198 of the draft Protection Profile should be changed to read as follows:

At time of this writing, a smartphone with arbitrary access to the internet and installed apps would require security features commensurate with the associated risks of the connected system to meet the assurance requirements of this PP due to frequent discovery of vulnerabilities and lack of compliance of smartphone software to IEC 62304 software life cycle processes. For example, an internet connected system that authenticates the validity of commands from a commercial-off-the-shelf smartphone may be evaluable under this PP/ST.

RESPONSE:

Thank you for your detailed comments.

Comment #1: We agree that the PP should not make assumptions or be overly prescriptive with respect to what may or may not be evaluable under this standard. Ultimately, the ST will define the specific product requirements based on risk assessment performed by the appropriate stakeholders, including the evaluator, the product developer, and the DWG. Please see Change #1 for new language.

Changes to standard and/or protection profile made in response:

1. **Protection Profile, Page 11, Lines 193-198: Replace the existing 6 lines with the following: "these safety-relevant portions of the smartphone (hardware, software) would be in scope for evaluation and need to be sufficiently protected from non-safety relevant portions of the smartphone. The precise specification of the scope, evaluation boundary, and security requirements would be codified in the ST."**

Zachary Rothstein, Advanced Medical Technology Association (AdvaMed), P:202-434-7224, zrothstein@advamed.org

Response Requested: Public

Comment #1:

Document: Standard, Page: N/A, Lines: N/A

Comment: February 11, 2016

David Klonoff, MD, FACP, FRCP

President

Diabetes Technology Society

Re: DTS Standard and Protection Profile for Connected Diabetes Device Security (DTSec)

Dear Dr. Klonoff:

The Advanced Medical Technology Association ("AdvaMed") appreciates the opportunity to provide comments in response to the Diabetes Technical Society ("DTS") Standard and Protection Profile for Connected Diabetes Device Security ("DTSec"). AdvaMed represents manufacturers of medical devices, diagnostic products, and health information systems that are transforming health care through earlier disease detection, less invasive procedures, and more effective treatment. Our members range from the smallest to the largest medical technology innovators and companies.

Our specific comments in response to both documents were transmitted in a separate file to Dr. David Klonoff because this web submission does not allow for the upload of a document. However, we generally believe that a separate, unique standard for connected diabetes devices is neither appropriate nor practical. Furthermore, we suggest that the DTS place more emphasis on the U.S. Food and Drug Administration's ("FDA") final guidance, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, and draft guidance, Postmarket Management of Cybersecurity in Medical Devices.

The FDA guidances mentioned above significantly rely on a risk-based approach for medical device cybersecurity. Moreover, they utilize widely accepted cybersecurity management concepts, such as essential clinical performance and controlled versus uncontrolled risk, and reference FDA-recognized standards such as IEC 60601-1:2005 and ISO 14971:2007. The DTSec documents, however, do not take a similar approach nor do they assess risks based on their impact to the device's essential clinical performance. Similarly, the DTSec documents are based almost exclusively on standards that are not recognized by FDA, such as ISO/IEC 15408-1, ISO/IEC 15408-2, and ISO/IEC 15408-3.

Because the DTSec documents do not apply a risk-based approach to medical device

cybersecurity management, all connected diabetes devices would be subject to the same security requirements. Such a result is not appropriate. For example, a blood glucose meter, which is generally considered a simple, lower risk device, should not be required to meet the same security requirements as a complex and higher-risk system, such as an artificial pancreas. Any process that evaluates risk should take into account the device's essential clinical performance by considering the exploitability of the vulnerability and the severity of the health impact to patients should the vulnerability be exploited. See, e.g., Postmarket Management of Cybersecurity in Medical Devices, p. 12 ("The presence of a vulnerability does not necessarily trigger patient safety concerns, rather it is the impact of the vulnerability on the essential clinical performance of the device that might trigger patient concerns.").

We are also concerned about the reliance on lab accreditation, which is outlined as part of the Assurance Program. Such a system could, in fact, undermine a device's cybersecurity rather than enhance it because in order to evaluate and test the device the lab would be required to receive from the manufacturer confidential design information. Disclosure of this information creates an opportunity for a breach to occur or to be exploited in the future.

Rather than rely on lab accreditation, we believe manufacturers should conduct their own testing and participate in an Information Sharing Analysis Organization ("ISAO"), as described in the FDA's draft guidance, Postmarket Management of Cybersecurity in Medical Devices. The DTSec fails to mention such collaborations and instead relies on the DTSec Working Group ("DWG") to provide assessments on new risks and vulnerabilities for connected diabetes devices. We question whether the DWG on its own has the expertise and capabilities required to carry out the necessary cybersecurity activities associated with this task, such as monitoring new IT threat sources and vulnerabilities. If the DWG lacks such resources, it is possible that the labs would not test for the most recent cybersecurity threats or new product-specific vulnerabilities.

* * *

AdvaMed appreciates your consideration of these comments. Please do not hesitate to contact me at 202-434-7224 or zrothstein@advamed.org if you have any questions.

Respectfully submitted,

/s/

Zachary A. Rothstein, J.D.

Associate Vice President

Technology and Regulatory Affairs

Proposed Change: N/A

Comments on DTS Standard for Connected Diabetes Device Security (DTSec)

Line Number	Type of comment (General/ Technical/Editorial)	Comment/Proposed Change	Rationale
General	General	AdvaMed represents manufacturers of medical devices, diagnostic products, and health information systems that are transforming health care through earlier disease detection, less invasive procedures, and more effective treatment. Our members range from the smallest to the largest medical technology innovators and companies.	N/A
General	General	We recommend that DTS rely on FDA's final guidance document titled, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," and draft guidance titled, "Postmarket Management of Cybersecurity in Medical Devices," for managing cybersecurity risks associated with medical devices. We do not believe a separate standard for connected diabetes devices is appropriate.	While we appreciate the importance that the DTS has placed on cybersecurity safety and the efforts that they have undertaken to focus on this critical issue, the FDA has issued premarket (finalized in October, 2014) and postmarket (draft released in January, 2016) guidance documents concerning the management of medical device cybersecurity. These documents rely heavily on a risk-based approach to cybersecurity management, use concepts such as essential clinical performance and controlled versus uncontrolled risk, and incorporate concepts from FDA-recognized standards such as IEC 60601-1:2005 and ISO 14971:2007. The proposed DTSec documents, however, do not reference a similar cybersecurity risk management approach, nor do they provide direction for assessing risks based on their influence on the essential clinical performance of a device. Moreover, the DTSec documents are based almost exclusively on standards, such as ISO/IEC 15408-1, ISO/IEC 15408-2, and ISO/IEC 15408-3, which are not recognized by FDA. Given these significant differences, we believe that manufacturers and interested stakeholders should follow the cybersecurity management processes outlined in the FDA guidance documents.
General	General	The "Protection Profile for Connected Diabetes Devices (CDD)"	While we appreciate that DTS drafted the Protection Profile

Line Number	Type of comment (General/ Technical/Editorial)	Comment/Proposed Change	Rationale
		indicates that simple devices, such as bG meters, must meet the same security requirements as complex systems, such as an artificial pancreas. We believe, instead, that the process should focus on assessing the risk to the device's essential clinical performance by considering the exploitability of the vulnerability and the severity of the health impact to patients if the vulnerability were exploited.	specifically for CDDs, simple devices, such as bG meters, do not require their own cybersecurity standard because they do not hold protected health information or personally identifiable information. Such simple devices undergo a self-security check during start-up, and cybersecurity management is controlled through good engineering practices (rather than lab accreditation), which can be subject to regulatory review. Because the DTSec and Protection Profile do not apply a risk-based approach to cybersecurity management, the Protection Profile document applies the same security requirements to all CDDs. This is unreasonable because a particular vulnerability is not necessarily the same across all device types and does not necessarily have the same influence on essential clinical performance. As FDA has stated, "[t]he presence of a vulnerability does not necessarily trigger patient safety concerns, rather it is the impact of the vulnerability on the essential clinical performance of the device that might trigger patient concerns." FDA Draft Guidance, Postmarket Management of Medical Device Cybersecurity, p. 12, lines 351-55. DTSec and the Protection Profile for CDD do not adhere to this approach.
General	General	N/A	Overall we believe the document requires more clarity and specificity to distinguish what is meant by "wired" and "wireless" technologies, and which types are in and out of scope.
35-38	General	Standards are typically developed by an ANSI certified organization so that its use, distribution and modification is governed by established rules.	Establish and communicate the rules for modification of the standard.
120	Technical	We believe multi-point wired LAN/WAN (*e.g.*, Ethernet) and wireless (*e.g.*, Wi-Fi and BTLE) networks should be in-scope, and point-to-point wired (*e.g.*, USB, RS232) and wireless (*e.g.*, NFC) networks should be out-of-scope.	We believe the document requires more clarity and specificity to distinguish what is meant by "wired" and "wireless" technologies, and which types are in and out of scope.

520

Line Number	Type of comment (General/ Technical/Editorial)	Comment/Proposed Change	Rationale
122	Technical	Diabetes devices connected in point-to-point networks (*e.g.*, wired USB, NFC wireless) should be out-of-scope for this standard.	We believe the document requires more clarity and specificity to distinguish what is meant by "wired" and "wireless" technologies, and which types are in and out of scope.
143-144	General	Remove: ". . . how can I be sure that a wireless diabetes device actually delivers the security claimed in the functional requirements?" We recommend removing the security assurance program from the standard.	We do not believe security requirements should be treated differently than other requirements. The sufficiency and completeness of a security requirement can be reviewed; however, verification and validation of a security requirement is not different than other applicable requirements.
148-150	General	Remove: "In addition to the program for creation and approval of security requirements, this standard also defines the assurance program for evaluating and certifying products against those requirements"	As stated above, we recommend removing the security assurance program from the standard.
152	Technical	Insert new paragraph: "This standard does not cover connected diabetes devices used for research purposes, nor those used as investigational devices. The standard is intended specifically for multi- point networked diabetes devices that are used as consumer products."	This language would provide additional clarity concerning the types of devices that are in-scope.
215-216	Technical	"Evaluations are performed against STs created by the product manufacturer based on an approved PP." Additional clarity is needed for the ST lifecycle.	N/A
218	General	We suggest clarifying who approves the ST specification that is defined by the manufacturer, including information about at what stage of the development this should occur.	N/A
235	Technical	Evaluation of the System Risk Analysis should be included in any security evaluation of a medical system. This provides a more thorough understanding of the system and the possible hazardous situations.	N/A
242	Editorial	"threats ~~threat~~"	N/A
246-248	General	Remove: "that are tightly coupled to device implementation."	Requirements that are tightly coupled to device implementation would require information about the device implementation, which we believe would be overly burdensome. Furthermore, imposition of design and implementation constraints over a manufacturer may

Line Number	Type of comment (General/ Technical/Editorial)	Comment/Proposed Change	Rationale
			raise copyright concerns.
252	General	Clarify: "(and associated audit)"	This phrase does not clearly define who performs the audit for compliance with IEC 62304.
257	General	The standard should clarify that it applies only to products placed into commerce after the effective date.	N/A
258	General	Clarify or remove: "consistent."	We believe the standard should not use subjective terminology. Instead, objective and measurable terms should be used.
259	Technical	We suggest removing the section that would allow vendors to obtain de-facto certification of a product for its life.	Passing the evaluation and certification of the standard should not remove the burden of having to successfully pass the evaluation for subsequent versions of the product. The initial evaluation and certification should not serve as a de-facto life-time certification. Rather, re-certification of subsequent versions should be based on the associated security risk assessment, as modifications could be significant or present an underlying security risk.
260	General	Clarify or remove: "similar products."	We believe the standard should not use subjective terminology. Instead, objective and measurable terms should be used.
267	General	Clarify or remove: "moderate to high potential attack."	We believe the standard should not use subjective terminology. Instead, objective and measurable terms should be used.
268-270	General	Clarify or remove: "and more"	We believe the standard should not use subjective terminology. Instead, objective and measurable terms should be used.
272-273	Technical	Delete: "or devices that are not exposed to such attack threats (e.g. non-networked devices used only within hospitals"	Assurance evaluations of non-networked devices are out-of-scope for the standard, so this language should be removed.
278-284	General	Delete: "While DWG is . . . and resource product evaluation."	It is unclear how the component ST produced by a component supplier (such as SSL protocol, BTLE, and cryptographic libraries) can consider the device in which the component is used. We recommend clarifying that this section does not imply that DTS approves the STs of security components such as SSL protocol,

Line Number	Type of comment (General/ Technical/Editorial)	Comment/Proposed Change	Rationale
			BTLE, and cryptographic libraries, and that diabetic device manufacturers are not required to limit their use to only the components approved by the DTSec.
290	General	Remove: Lab accreditation proposal, outlined as a part of the Assurance Program. A more viable proposal would be the manufacturer's participation in an Information Sharing Analysis Organization (ISAO), as described in the FDA's draft guidance concerning the postmarket management of medical device cybersecurity.	The lab accreditation proposal could undermine security rather than enhance it. In order to successfully carry out evaluation testing, accreditation labs must typically receive design secrets from the device manufacturer. Disclosure of design and vulnerability secrets to such laboratories creates a breach opportunity that should be avoided. The FDA's draft guidance concerning the postmarket management of medical device cybersecurity correctly places an emphasis on sharing and collaborating on cybersecurity-related issues. For this reason, the draft guidance recommends that manufacturers participate in an ISAO. It is expected that private and public stakeholders from the information technology community, healthcare delivery organizations, clinical user community, and medical device community will participate in ISAOs to assess cybersecurity risks and identify vulnerabilities. The DTSec fails to mention such collaborations; rather, these documents rely on the DTSec DWG to provide assessments on new risks and vulnerabilities for new requirement implementation by the testing labs. It is unclear whether the DWG has the expertise required to carry out the necessary cybersecurity activities, such as monitoring new IT threat sources and vulnerabilities. If not, it is possible that these labs would not test for the most recent cybersecurity threats or new product-specific vulnerabilities. As a result, we believe manufacturers should conduct their own testing and engage with ISAOs.
295-297	General	Remove or revise: "As such, DTSec governs the accreditation of independent testing labs that perform evaluations against this standard and the certification of lab results under this standard."	Describe how DTSec will be audited to ensure it is appropriately using the powers entrusted to them through this standard. Define the independent entity governing over DTSec.

527

Line Number	Type of comment (General/ Technical/Editorial)	Comment/Proposed Change	Rationale
298	General	Define the rules for the fees, cost and schedule for lab approval and device accreditation.	The lab accreditation schedule and fees may significantly impact manufacturers. Similarly, lab approval costs and schedules may impact labs.
306-307	General	Clarify or remove: "DWG reserves the right to accept or reject lab applications based on numerous factors, including but not limited to . . . ."	Clearly define the requirements and qualifications that labs must fulfill to be accredited.
320	General	Clarify or remove: "Since such competence may not be included within the scope of the lab's accreditation, the lab must demonstrate its suitability during the application process to DWG."	There should be a standard or minimum expected level of specified lab capability. As drafted, this phrase is too subjective, so we recommend defining the method of measurement for the competency of the lab.
330	General	Clarify or remove: "assurance bar."	We believe the standard should not use subjective terminology. Instead, objective and measurable terms should be used.
331	General	There is no timeframe specified for how long it should take for lab evaluation of a product, submission of the report to DWG, DWG acceptance, and DWG listing of the product. This overall process could take months from product submission to product listing, which could have a negative impact on the manufacturer's time to market. There should be objective metrics around the expected timeframes for the activities within this process in order to set lab, manufacturer, and DWG expectations for performance.	N/A
333	General	Clarify or remove: "successfully passes evaluation."	We believe the standard should not use subjective terminology. Instead, objective and measurable terms should be used.
337-338	General	Delete: "Product shall not be considered certified under DTSec until the evaluation report is formally accepted by DWG."	We do not believe DTSec should retain a formal review and acceptance of the lab report. If the lab is accredited, the lab should be capable of certifying the product.
344-347	General	Rather than using an "Evaluated Products List," manufacturers should maintain their cybersecurity risk management programs throughout the entire lifecycles of their devices and assume all testing responsibilities.	As stated in the FDA's draft guidance concerning the postmarket management of medical device cybersecurity, "[a]n effective cybersecurity risk management program should incorporate both

528

Line Number	Type of comment (General/ Technical/Editorial)	Comment/Proposed Change	Rationale
			premarket and postmarket lifecycle phases and address cybersecurity from medical device conception to obsolescence." DTSec does not take into account that cybersecurity threats are constantly evolving throughout the product's lifecycle. Prior to removing products from the "Evaluated Products List," DWG should conduct a risk analysis to understand whether or not the vulnerability triggers patient safety concerns and has an impact on the essential clinical performance of the device. Only after a thorough risk analysis is conducted should DWG consider removing the product from the "Evaluated Products List." Such an activity is most easily accomplished by the device manufacturer who is better suited to maintain the cybersecurity risk management process for a device over its lifecycle.
347-350	General	Delete: "DWG reserves the right to remove those products from the evaluated products list until the vulnerabilities are remediated. DWG reserves the right to remove products from the evaluated products list if they suffer from a large volume of recurring vulnerabilities, even if all reported vulnerabilities have been remediated"	We do not believe the security certification portion should be retained. Cybersecurity certification should not remain static because the evaluation is done at a single point in time. Theoretically, a new vulnerability could be found in the system the day after its evaluation.
348	General	Define: "large volume"	We believe the standard should not use subjective terminology. Instead, objective and measurable terms should be used.
360-361	General	Clarify or remove: "An ST shall be reviewed and approved by DWG before it may be used in any evaluation under DTSec."	ST is the input for security requirements, so it would be too late to review it before the evaluation. Instead, it should be reviewed before the device is designed. However, this would require a two-level review and approval process which would be unduly burdensome for the manufacturer. As a result, we believe timing and review schedules should minimize their impact on product development.
362	General	Update this section to include the ability for manufacturers to make "vulnerability" related changes in parallel with submissions or on an expedited path to enable manufacturers to update software to close	The ability to quickly update software is a security mitigation in and of itself. Submissions/acceptances inherently work against quick response.

Line Number	Type of comment (General/ Technical/Editorial)	Comment/Proposed Change	Rationale
		vulnerability concerns as quickly as possible.	In order to not limit the effectiveness of a manufacturer's "update ability," either allow for a manufacturer to make rapid changes to address vulnerabilities, or create an expedited approval route. The standard calls for manufacturers to submit full reports of changes as well as maintain a plan to quickly mitigate any discovered vulnerabilities.
368	General	Clarify or remove: "sufficiently minor"	We believe the standard should not use subjective terminology. Instead, objective and measurable terms should be used.
376	General	Clarify or remove: "not adequately and promptly mitigated."	We believe the standard should not use subjective terminology. Instead, objective and measurable terms should be used.
383-384	General	Delete: "DWG reserves the right to institute random audits of the developer by DWG personnel and/or DTSec-approved labs"	We do not believe developer audits should be addressed in the standard because this process is intended to result in a product-specific certificate, rather than a process-specific certificate.
398	General	Additional information should be included to addresses how disputes between parties are handled.	N/A

Comments on DTS Protection Profile for Connected Diabetes Devices (CDD)

Line Number	**Type of comment** (General/ Technical/ Editorial)	**Comment/Proposed Change**	**Rationale**
General	General	AdvaMed represents manufacturers of medical devices, diagnostic products, and health information systems that are transforming health care through earlier disease detection, less invasive procedures, and more effective treatment. Our members range from the smallest to the largest medical technology innovators and companies.	N/A
General	General	We recommend that DTS rely on FDA's final guidance document titled, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," and draft guidance titled, "Postmarket Management of Cybersecurity in Medical Devices," for managing cybersecurity risks associated with medical devices. We do not believe a separate standard for connected diabetes devices is appropriate.	While we appreciate the importance that the DTS has placed on cybersecurity safety and the efforts that they have undertaken to focus on this critical issue, the FDA has issued premarket (finalized in October, 2014) and postmarket (draft released in January, 2016) guidance documents concerning the management of medical device cybersecurity. These documents rely heavily on a risk-based approach to cybersecurity management, use concepts such as essential clinical performance and controlled versus uncontrolled risk, and incorporate concepts from FDA-recognized standards such as IEC 60601-1:2005 and ISO 14971:2007. The proposed DTSec documents, however, do not reference a similar cybersecurity risk management approach, nor do they provide direction for assessing risks based on their influence on the essential clinical performance of a device. Moreover, the DTSec documents are based almost exclusively on standards, such as ISO/IEC 15408-1, ISO/IEC 15408-2, and ISO/IEC 15408-3, which are not recognized by FDA. Given these significant differences, we believe that manufacturers and interested stakeholders should follow the cybersecurity management processes outlined in the FDA guidance documents.
General	General	The "Protection Profile for Connected Diabetes Devices (CDD)"	While we appreciate that DTS drafted the Protection Profile

Line Number	Type of comment (General/ Technical/ Editorial)	Comment/Proposed Change	Rationale
		indicates that simple devices, such as bG meters, must meet the same security requirements as complex systems, such as an artificial pancreas. We believe, instead, that the process should focus on assessing the risk to the device's essential clinical performance by considering the exploitability of the vulnerability and the severity of the health impact to patients if the vulnerability were exploited.	specifically for CDDs, simple devices, such as bG meters, do not require their own cybersecurity standard because they do not hold protected health information or personally identifiable information. Such simple devices undergo a self-security check during start-up, and cybersecurity management is controlled through good engineering practices (rather than lab accreditation), which can be subject to regulatory review. Because the DTSec and Protection Profile do not apply a risk-based approach to cybersecurity management, the Protection Profile document applies the same security requirements to all CDDs. This is unreasonable because a particular vulnerability is not necessarily the same across all device types and does not necessarily have the same influence on essential clinical performance. As FDA has stated, "[t]he presence of a vulnerability does not necessarily trigger patient safety concerns, rather it is the impact of the vulnerability on the essential clinical performance of the device that might trigger patient concerns." FDA Draft Guidance, Postmarket Management of Medical Device Cybersecurity, p. 12, lines 351-55. DTSec and the Protection Profile for CDD do not adhere to this approach.
35	Editorial	Clarify or remove: "and government accrediting bodies."	There are no other references to government accrediting bodies within the document. As a result, this phrase should be deleted, or additional clarity should be provided.
127	Technical	Replace: "testing" with "activities" "Independent testing laboratory that evaluates the TOE against its ST by analyzing documentation and performing ~~testing~~activities such as vulnerability assessment."	Vulnerability assessments involve more than just testing (*e.g.*, identifying, quantifying and prioritizing vulnerabilities).
127	Editorial	Sort the table and glossary alphabetically by Terminology	N/A

Line Number	Type of comment (General/ Technical/ Editorial)	Comment/Proposed Change	Rationale
130	Technical	Replace: "life-saving" with "therapeutic" "Medical devices used for monitoring and managing diabetes provide ~~life-saving~~therapeutic benefits to patients"	A "life-saving" device implies a higher level of criticality. Diabetes devices generally are considered therapeutic.
142-143	Technical	Delete: "transferring BG readings to a PC via USB cable"	This phrase implies that the USB connection is within scope for the evaluation.
148	General	We suggest providing a specific definition and examples of diabetes data management applications. Examples include applications that enable users to move data to external systems (such as EMRs) or applications that enable healthcare professionals to review patient data. Additionally, if these types of items are expected to conform to the PP, we would recommend considering an alternate structure for Mandatory and Optional Security objectives. If they are not expected to conform to the PP, then this also needs to be made clear (*see also*, comment on Line 364).	Data management applications typically exist as a part of a connected system, allowing users to move data to external systems (such as EMRs) or allow professionals to review patient data. These systems generally carry a lower risk profile as they are not used for immediate treatment, such as an insulin infusion device. Safety may not be a primary concern, but security remains a critical concern. Aspects such as protected communication and strong cryptography are critically important to ensure safe handling and transport of patient data in these systems. However, ensuring integrity of software, firmware and physical protections of the device are security objectives that are more appropriate for physical devices that users interact with. Additionally, because the majority of these systems are connected to the internet, currently optional objectives in the PP, such as User Authentication, should be mandatory.
148-151	Editorial	Revise to: "Examples of a CDD that should claim conformance to this Protection Profile include simple blood glucose monitors (BGM), more sophisticated BGMs – e.g. with larger displays and audio functions, Continuous Glucose Monitors (CGMs), remote controllers of other CDDs and insulin delivery devices."	Insulin pumps are specifically identified, but this may unintentionally exclude "smart" insulin pens or patches.
151-152	Technical	Replace "that make the overall system secure" with "that would still need to be evaluated together as a TOE." "A closed loop artificial pancreas (AP) system may be a TOE itself or may be comprised by evaluated TOEs ~~that make the overall system secure~~that would still need to be evaluated together as a TOE."	A system of secure devices is not necessarily secure. The security of the system itself should be evaluated.

Line Number	Type of comment (General/ Technical/ Editorial)	Comment/Proposed Change	Rationale
156-157	Technical	Delete or clarify: "The CDD provides essential services, such as protected wireless communications to a companion device, to support the operation of the device."	We believe the standard should not use subjective terminology. Instead, objective and measurable terms should be used.
161	Editorial	Delete: "general"	We believe the standard should not use subjective terminology. Instead, objective and measurable terms should be used.
179-181	Technical	Replace: "each TOE must satisfy the requirements in this PP (and derived ST) and will be evaluated independently against its ST" with "the system must satisfy the requirements in this PP (and derived ST) for the system and the level of authentication requisite with the given use case, and each TOE will be evaluated independently against its ST if they can also operate stand-alone; independent of the system." "While multiple TOEs may interact in a larger system – for example, a BGM communicating wirelessly with an insulin pump – ~~each TOE must satisfy the requirements in this PP (and derived ST) and will be evaluated independently against its ST~~the system must satisfy the requirements in this PP (and derived ST) for the system and the level of authentication requisite with the given use case, and each TOE will be evaluated independently against its ST if they can also operate stand-alone; independent of the system."	As drafted this sentence seems to remove "system security" from the scope of this document. Independent of the security of its components, "system security" should be the principal focus of an assurance standard.
191-193	Technical	Replace "then the full device and its software would need to be evaluated against this PP/ST" with "then the functions and the services of the smartphone that are used by the TOE would need to be evaluated against this PP/ST" "If a commercial-off-the-shelf smartphone is used directly for safety-relevant control (for example, as the controller in a closed-loop AP), ~~then the full device and its software would need to be evaluated against this PP/ST~~then the functions and the services of the smartphone that are used by the TOE would need to be evaluated against this PP/ST."	If the system has the necessary capability to operate securely in a hostile environment, then the environment does not need to be secure.
193-197	Editorial	Delete the sentence starting with: "At time . . . ."	This sentence is not necessary.

542

Line Number	Type of comment (General/ Technical/ Editorial)	Comment/Proposed Change	Rationale
203	Technical	Replace "they must be separately validated against the related assurance standards" with "they should be validated based on their use in the TOE"	A separate validation of device components is unreasonable.
207	Editorial	We recommend changing the title of Section 1.4 to: "Executive Overview"	The current title is confusing.
233-234	Technical	Revise this paragraph to address IEEE 11073 profiles.	This paragraph does not take into consideration IEEE 11073-10417 glucose, 10425 insulin pump, and 10419 continuous glucose profiles. These approved IEEE standards define device data exchange including (remote) control. The CGM profile defines authorization as part of "command and control."
137	General	Delete: "privacy"	Lines 274-277 states, "this PP does not include requirements associated with confidentiality protection of user data," which implies that privacy is not within the scope of the PP.
259	Editorial	Add "n": "stolen"	N/A
278	General	Remove Sections 1.4.2 and 7.	The protection profile should concentrate on security requirements. Security Assurance Requirements are addressed in the standard.
285	General	Describe the penetration test process, who specifies the plan and criteria, and how its completeness is judged.	Further clarity is needed.
290	General	Insert: "to harm the patient" "If none of the penetration test attacks are successful to harm the patient"	N/A
292	General	Define a process that enables objective evaluation of the penetration test results, including: Who scores penetration test results; what are the evaluation criteria; how do we judge critical vs non-critical; how is subjectivity removed.	N/A
312, 315	Technical	Delete: "network eavesdropping from lines"	Lines 274-277 states, "this PP does not include requirements associated with confidentiality protection of user data," which

543

Line Number	Type of comment (General/ Technical/ Editorial)	Comment/Proposed Change	Rationale
			implies that privacy is not within the scope of the PP.
328	Technical	The T.PHYSICAL section should be out-of-scope.	The focus on the DTSec and the PP are on multi-point networked CDDs. If an attacker gains physical access to a device, there are numerous additional threats that are realized. However, requiring manufactures to design and develop mitigations against threats that require physical access would entail imposing substantive burdens on the clinical usability of the device. DTSec should be limited to "networked" security, not physical security.
347	General	Replace: "properly authenticated network peer" with "network peer"	A properly authenticated network peer is a trusted partner that is not expected to act maliciously. If a network peer is acting maliciously, then it is not authenticated properly.
364	Editorial	Clarify the application of the PP to diabetes related data management applications. If applicable, provide an alternate structure for mandatory and optional security objectives that is appropriate for diabetes related data management applications.	*See* comments to line 148.
371	Technical	Delete: "and confidentiality" "Ensure the integrity ~~and confidentiality~~ of data transiting . . . ."	This is unnecessary if data privacy is not the goal.
378, 380	Editorial	Replace: "shall"	Use of "shall" implies the phrase is a requirement.
380	General	Delete: "any"	We believe the standard should not use subjective terminology. Instead, objective and measurable terms should be used.
388	Technical	Section 4.2.1 (User Authentication) should apply only to devices where alteration of data and/or settings could potentially cause user harm.	N/A
389	General	Delete: "Loss of confidentiality of user data"	This phrase conflicts with multiple statements throughout the document, such as line 315.
394	Technical	Delete: 4.2.2 OP.HW_PHYSICAL	This section deals with physical security, which should be out of scope.

Line Number	Type of comment (General/ Technical/ Editorial)	Comment/Proposed Change	Rationale
404-406	Technical	Delete: Section 4.3.1	It is not clear what the user is supposed to do, including how they would "eliminate the risk" for data corruption, or any data transferred beyond the TOE. The actions that need to be taken by the user do not belong in this document since this document is not intended for end users.
407-411	Technical	Delete: Section 4.3.2.	This section places the burden on the user to contribute to the assurance standard. Such a mechanism cannot be verified by testing.
437-438	Technical	Delete: FCS_COP_EXT.1.2	There is no known quality metric for entropy.
449-456	Technical	We recommend deleting the application note.	This statement is too specific for this section of the document.
460	Technical	We suggest renaming this section to: "Basic Data Integrity" or "Basic Data Validity"	This section is titled "data authentication" but it discusses validity (*i.e.*, integrity). Validity is not the same as authentication which goes to the source of the data and repudiation.
460	Technical	Indicate this section is optional when the data is limited to use of basic reporting and non-critical operations.	This section calls for authentication and integrity checking of data (including BG values). There currently is no industry "source of trust" to verify signatures, revocations, etc. Without such a mechanism in place, there is a risk of hindering open-innovation in combining data.
465-470	Technical	Replace with: "a non-cryptographic mechanism such as a CRC could be acceptable depending on presence of additional security precautions such as use of memory locks, OTP technology, proprietary communications protocols, etc."	Blanket dismissal of CRCs is not reasonable across all possible CDDs, particularly given technology restrictions present for various CDDs that would preclude usage of signatures. It should be possible to pass the evaluation of the CDD against the PP/ST with suitable explanation for why the additional security precautions are adequate.
467-468	Technical	Replace: "Signatures must leverage a manufacturer-trusted hardware-protected root of trust to guard against tampering of the data" with: "If possible, signatures should leverage a manufacturer-trusted hardware-protected, root of trust to guard against tampering of the data"	While a desirable goal for security, this is frequently not possible for an embedded device. Currently, processors available for embedded devices do not provide root-of-trust.
469	Technical	Replace: "In particular, a non-cryptographic mechanism such as a CRC does not meet the intent of this requirement"	In embedded systems, it may not always be practical to validate the data using a cryptographic mechanism. This change would allow for

Line Number	Type of comment (General/ Technical/ Editorial)	Comment/Proposed Change	Rationale
		with: "It is suggested that a cryptographic mechanism be used to validate the data whenever possible."	the possibility to use a non-cryptographic mechanism for validating data where justified.
486-490	General	Delete: FDP_IFF.1.3 & 1.4 & 1.5.	N/A
497-498	General	Delete reference to buffer overflow: "Both connections should protect against implementation flaws~~, such as buffer overflows,~~ that could be . . ."	This is inappropriate for the section.
510	Technical	Delete: "immutable firmware"	The immutable firmware requirement negates OTA updates, a desirable security feature. It also assumes that there will be an immutable part of the software, which is not correct.
511-512	Technical	Replace: "Signatures must leverage a manufacturer-trusted, hardware-protected root of trust to guard against tampering" with: "If possible, signatures should leverage a manufacturer-trusted hardware-protected, root of trust to guard against tampering"	While a desirable goal for security, in an embedded design this is frequently impossible to accomplish. Hardware root of trust is not always available in a device.
513-514	Technical	Replace with: "a non-cryptographic mechanism such as a CRC could be acceptable depending on presence of additional security precautions such as use of memory locks, OTP technology, proprietary communications protocols, etc."	Blanket dismissal of CRCs is not reasonable across all possible CDDs, particularly given technology restrictions present for various CDDs that would preclude usage of signatures. It should be possible to pass the evaluation of the CDD against the PP/ST with suitable explanation for why the additional security precautions are adequate.
522	General	Replace: "are" with "and"	N/A
521-534	Technical	Delete: FTP_ITC.1.1.	We suggest removing this section since there is no trusted pipe.
525-526	Technical	Delete: FTP_ITC.1.2	It is unclear who is permitted to initiate communications that does not impact security.
527-528	Technical	Delete: FTP_ITC.1.3	BTLE defines the list of functions with or without security mode 1 or 3 enabled, so this section is not needed.
529-530	Technical	Delete: FTP class	There is nothing distinct about using BTLE security mode level 1 or level 3. This section is not applicable for the on-body network.

549
550

Line Number	Type of comment (General/ Technical/ Editorial)	Comment/Proposed Change	Rationale
565 and 570	General	Replace: "User authentication should not get in the way of life-critical operation" with: "User authentication shall be used in cases where it's justified based on risk benefit analysis."	Diabetes device operations are generally not life critical.
575	General	We recommend removing this discussion because it discusses physical access to the device.	N/A
592	General	Delete: Sections 1.4.2 and 7.	We believe the protection profile should concentrate on the security requirements. Security assurance requirements are appropriately addressed in the standard.
600	General	Define the approval process of the ST, including the timing and the criteria.	Additional larity is needed.
604	General	We recommend including the option for the device manufacturer to self-certify, resulting in a lower level tier of DTSec approval (*e.g.*, Basic or Silver).	N/A
646; 718	Technical	Line 646 states, ADV_TDS.4, while line 718 states, ADV_TDS.3. These references should be consistent.	N/A
766	Technical	Delete: A.PHYSICAL	This section deals with physical security, which should be out of scope.
775	Technical	Delete: OP.HW_PHYSICAL	This section deals with physical security, which should be out of scope.

RESPONSE:

Thank you for your detailed comments. We believe you have some misconceptions about DTSec, which is understandable given its nascent status. We will strive to correct those misconceptions here, referring and responding to specific entries from your comment form. The following responses are made to your comments about the standard.

Comment #1 (Line = General): N/A

Comment #2 (Line = General): As FDA has been involved in the steering of DTSec from its inception, it has always been DWG's intent that DTSec be consistent with FDA guidance. Reference has been made to DTSec's recommendation that existing recognized standards (e.g. IEC 62304) be leveraged to improve the economies of evaluations performed under DTSec. Furthermore, it is absolutely the case that risk assessment, which as you point out is central to FDA guidance for cybersecurity best practices, is also central to the DTSec approach. Per your recommendation, we have added a section in the standard that attempts to make this link clearer. As such, we have made the following change to the standard in response to your feedback:

- **Addition of section 1.2, "Role of DTSec in Medical Device Safety Risk Assessment", to the standard. This section explains the importance of cybersecurity risk assessment in perspective of an overall safety risk assessment program and provides detailed examples of how the DTSec program helps fulfill the spirit of common regulatory guidance in cybersecurity risk assessment (uses FDA premarket guidance as the example).**

It is also a misconception that DTSec does not adopt a risk-based approach. The DTSec protection profile and security target require a risk assessment that considers the threat model of a specific product type and essential clinical performance. This risk assessment takes as input risk assessments already performed in advance by product developers but also considers the important inputs of caregivers, patients, regulators, and independent cybersecurity experts. For example, in considering the threat of unauthorized physical access to blood glucose monitors, our risk assessment determined that user authentication, while desirable from a purely theoretical security standpoint to counter this threat, could pose additional safety risks to essential clinical performance. For this reason, user authentication was rendered optional in the protection profile, allowing for the security target to include or not include such controls depending on the specific I/O interface capabilities, threat model, and essential clinical performance parameters of a particular product.

With respect to the comment that "the DTSec documents are based almost exclusively on standards that are not recognized by FDA, such as ISO/IEC 15408-1, ISO/IEC 15408-2,

and ISO/IEC 15408-3", please note that ISO 15408 is the only internationally accepted standard for information/computer security evaluation. It is widely used in US government and many other governments. As FDA has been involved in the steering of DTSec since its inception, the DWG fully expects FDA to recognize the DTSec standard and its use of ISO 15408 as the framework for specifying and evaluating security requirements, especially since there does not exist an alternative ratified international framework for specifying and evaluating security requirements of arbitrary devices and software.

Comment #3 (Line = General): This is a misconception. As described above, a risk-based approach is used to create PPs and STs authored under the DTSec standard. In particular, different CDDs will require different STs based on their risk assessments, and therefore there is no requirement nor expectation that disparate CDDs will have the same security requirements, although of course it is possible that two CDDs can have very similar STs (requirements) if the product capabilities, threat models, and risk assessments are themselves very similar.

Comment #4 (Line number = General): The standard itself does not specify implementation details; the scope of wired vs. wireless networks applies to security requirements specified in the PP and STs (yet to be written). For the PP document, it is was DWG's expectation that wireless networks would be supported. However, there is no reason why wired networks, if a diabetes device used one, could not be supported by the PP. Therefore, while we leave the use of "wireless" whenever it is used by example, we are making the following changes to the PP to remove any unnecessary mention of "wireless" that might be construed to limit the potential scope of the PP:

- **Line 156: Replace "wireless" with "network"**
- **Line 273: Replace "wireless" with "network"**
- **Line 324: Replace "wireless" with "network"**
- **Lines 372-386: Delete these lines**
- **Line 449: Delete "wireless"**
- **Lines 629-630: Delete "that utilize local/short-range wireless networks (e.g. Bluetooth)"**

Comment #5 (Lines 35-38): There are plenty of standards created by industry consortia that are not ANSI certified. We discussed whether it would be appropriate for DTS to develop DTSec with a number of government authorities, including FDA, and were assured that it was acceptable. FDA's involvement in steering DTSec is further evidence of this. Finally, we would like to point out that DTSec is an international standard, in no way limited only to use within the United States; as such, it is not clear that ANSI certification would help or hinder DTS' mission of promulgating improved security standards across the entire medical world.

Comment #6 (Line 120): We do not agree with your suggestion that point-to-point networks should be out-of-scope. We are intentionally leaving network details unspecified in the PP and expect the ST to be specific about the network types supported by a specific product under evaluation. There are numerous diabetes devices that allow a single point-to-point network connection and will be supported by (future) derived STs.

Comment #7 (Line 122): Same response as previous.

Comment #8 (Lines 143-144): Assurance via independent evaluation is the reason why DTSec exists, so it makes no sense to remove this. The digital world has proven beyond doubt that the high level of security assurance needed for critical systems (such as medical devices) cannot be reliably obtained simply by relying on the product developer to do the right thing. Independent evaluation following a standardized framework is the only proven method for achieving the requisite level of security assurance. We do believe that security requirements should be treated differently from other requirements. In the avionics world, assurance requirements for software safety in a digital flight control system are extremely different from other software requirements of the system. In particular, in the United States, general functional requirements are tested by the product developer, but independent safety validation of flight-critical electronics must be performed by FAA representatives. In a medical device, every single time a device is used for normal operation (e.g. in clinical trials), some assurance is derived from the fact the device performed normally and safely. However, these same tests do not provide significant assurance against security risks. Across the medical device manufacturer community today, cybersecurity experience, expertise, and maturity is far lower than the well-established experience, expertise, and maturity in clinically-related safety concerns. Today, security assurance can only be obtained by rigorous vulnerability analysis and testing by security experts. Taking the approach of simply trusting the product developer to build in and hire the required security expertise is simply too dangerous in today's world. We do believe that manufacturers who demonstrate, via DTSec evaluation, a consistent level of experience, expertise, and maturity should be treated favorably with respect to the burden of proof and rigor required in future evaluations, but this trust must be earned over time rather than assumed at the start.

Comment #9 (Lines 148-150): Same response as previous.

Comment #10 (Line 152): We see no reason to limit the scope of DTSec as proposed. Any device that can fulfill its associated PP and ST requirements can be certified under DTSec.

Comment #11 (Lines 215-216): The lifecycle of ST is defined in the ISO 15408 standard. However, if you have specific improvement suggestions, we are happy to consider them.

Comment #12 (Line 218): Approval of STs is covered in section 2.4 of the standard. The standard is intentionally not prescriptive regarding the authorship and timing of ST creation relative to product development because this varies based on numerous factors (including the maturity of the product family, how different instances are from other instances, availability of similar STs, etc.). There is a long history of ST development in the computer security world, and the timing of ST development has always been variable.

Comment #13 (Line 235): We agree that security risk is but one part of an overall system risk analysis and that PP/ST authors must consider general system risk when performing the security risk analysis that results in a selection of security requirements for the ST/PP. As mentioned in the response to comment #2, we have endeavored to clarify the relationship between DTSec security requirements derivation and the overall safety risk process.

Comment #14 (Line 242): We are making the following fix:

- **Line 242 (standard): Delete "threats"**

Comment #15 (Lines 246-248): Vulnerability assessment at the required assurance level of the PP is necessarily tied to a particular device implementation. It would not be feasible to protect against moderate attack potential threats without examining the detailed design and implementation details of the product. This fact is well established in similar security standards, for example with smart card financial systems. With respect to your mention of "copyright concerns", we do not see how copyright is relevant; please be more specific.

Comment #16 (Line 252): No IEC 62304 audit is required under DTSec; this paragraph is simply stating that such an audit and its associated assurance artifacts, if available, may help to reduce the assurance generation burden when evaluating security under DTSec.

Comment #17 (Line 257): By definition, certification under DTSec would apply to products after their certification date; not clear on the intended point here. There is no requirement that a certification only be applied to devices placed in commerce. In theory, a product can be certified under DTSec and then never placed into commerce.

Comment #18 (Line 258): We agree that the word "consistent" is not particularly valuable in this context. We are making the following change in the standard:

- **Line 258: Delete the word "consistent"**

Comment #19 (Line 259): This statement is non-normative discussion intended to frame potential future assurance program enhancements. The normative assurance program is defined in subsequent section "Assurance Maintenance Program" that does require an analysis of security-relevant changes. However, the point is taken that the commentary is unnecessary and potentially misleading, and therefore, we are making the following change to the standard:

- **Lines 257-263: Delete this paragraph**

Comment #20 (Line 260): No longer relevant as the entire paragraph has been deleted per previous comment.

Comment #21 (Line 267): We agree with the comment; the standard should not be overly prescriptive regarding attack potential as we can conceive of PP/STs for which a wide range of attack potentials may be appropriate. We are therefore making the following change to the standard:

- **Line 265: Delete "high-criticality"**
- **Line 266: Change "a custom" to: "an" - editorial change, unnecessary modifier**
- **Line 267-268: Change "moderate to high potential attack threats" to: "levels of attack potential consistent with associated assessed security risk of that product or component"**
- **Line 268: Delete "custom" – editorial change, unnecessary modifier**

Comment #22 (Lines 268-270): Agreed that "and more" is unnecessary and redundant. We are therefore making the following change to the standard:

- **Lines 269-270: Change "specific selection of assurance requirements, and more." to: ", and specific selection of assurance requirements."**

Comment #23 (Lines 272-273): Agreed that the comment should be cleaned up. We are therefore making the following change to the standard:

- **Lines 272-273: Change ", or devices that are not exposed to such attack threats (e.g. non-networked devices used only within hospitals)." to: "or devices not at risk of exposure to moderate or higher potential attackers."**

Comment #24 (Lines 278-284): We do want to encourage evaluation of components in order to reduce the cost/scope of product evaluations. But in contrast to your comment, DTSec does not require this; it is simply an efficiency opportunity. If a product developer uses third party components for security functionality not already certified under DTSec, then the evaluator must apply resources to evaluating those components.

Comment #25 (290): It is a misconception that the DWG is being solely relied upon to have the requisite expertise and capabilities to carry out the cybersecurity activities associated with DTSec. While DWG includes a wide range of cybersecurity perspectives and expertise, DTSec relies on expert independent laboratories, which are accredited to have the requisite expertise and capabilities to consider threats and evaluate security requirements that are acknowledged to be rapidly evolving. In fact, we counter-argue that relying on a medical device vendor to have the requisite internal expertise and capabilities is far riskier. Participation in ISAOs, while a good idea, is not sufficient to ensure that product developers have the requisite expertise and knowledge to ensure sufficient product security. Security design, architecture, and especially testing, is very different from safety-based development that has been well institutionalized in medical device manufacturers. DTSec, by way of independent evaluation and feedback, will encourage product developers to gain the requisite experience, but in no way can we assume that vendors should be expected to possess it a-priori, even if they are active participants in ISAOs.

Comment #26 (Lines 295-297): DTSec scheme relies on a consensus working group of many stakeholders to ensure quality and a balanced approach to all concerns. While we are open to audit by regulatory bodies, our preferred approach is to actually have those regulatory bodies be directly involved in the scheme, rendering an audit moot/superfluous. Should a non-participatory regulatory body require an audit of DWG activity in order to allow use of DTSec in the body's jurisdiction, then DWG would be required to permit such audit in order to serve that jurisdiction. Therefore, we do not see a need to add explicit audit of DWG to the standard at this time. We remain open to recommendations from FDA, Health Canada, and other regulatory bodies regarding this concern.

Comment #27 (Line 298): Lab fees for device evaluation are set by the labs. Current rough ranges for price and schedule for diabetes devices, based on the cost-sensitive approach taken from the start by DWG, give us confidence of economic viability, but each evaluation

will be priced based on assurance artifacts availability, complexity, and other factors. Supply and demand will also factor into pricing. There is currently no plan for DTS to levy fees for approval of labs themselves (to be listed as approved labs under DTSec).

Comment #28 (Lines 306-307): There does not today exist an international standard for qualifying labs for moderate+ attack potential vulnerability assessment on medical devices, and therefore, we feel the standard requires some amount of flexibility here. If and when an accreditation process exists for all required DTSec lab skills, this can be removed.

Comment #29 (Line 320): Same response as previous.

Comment #30 (Line 330): This sentence is unnecessary and editorial, so we accept your suggestion and will delete the sentence in the standard:

- **Lines 328-330: Delete the last sentence in this paragraph**

Comment #31 (Line 331): There are too many variables to be able to put specific timelines into the standard. Security certification throughout history as shown that time scales vary based on many factors, including supply and demand, complexity of products, responsiveness of the product developer, etc. It is in everyone's interest to ensure time scales meet commerciality requirements and are not an impediment to commerciality.

Comment #32 (Line 333): We will make the following change to the standard:

- **Line 333: Delete the word "successfully"**

Comment #33 (Lines 337-338): The process defined here is the same as every other security evaluation scheme we are aware of. There must be an entity ("scheme") to oversee the labs, manage changes to the standard, and ensure consistency of application of the standard and results. As of now, DWG serves as the "scheme". Other examples include NIAP as the scheme for US national security common criteria certification, NIST CMVP as the scheme for US FIPS 140-2 crypto module certification, and EMVCo as the scheme for certifications to its standards in the area of secure payment transactions.

Comment #34 (Lines 344-347): As independent assurance is the goal of this standard, there must be a way for all stakeholders to know when a product has been evaluated under the standard.

Comment #35 (Line 348): We admit this is subjective, but we do not feel there can be a simple objective formula. Other schemes enforce a time limit and force re-evaluation at the end of the timeframe, but DWG feels an arbitrary time limit may allow products deemed unworthy of the DTSec certification to improperly remain certified and also may force manufacturers who are doing a great job to spend money for re-evaluation that is unnecessary.

Comment #36 (Lines 360-361): We think the reviewer misunderstands the point of this sentence. The standard is stating that only approved STs can be used in DTSec evaluations. An ST that has not been approved by the scheme can not be used for DTSec evaluations as there would be no way to ensure it has met the same standard of quality needed. We are open to clarify if you have a specific suggestion, but we think the current language is sufficiently clear.

Comment #37 (Line 362): We agree and will clarify this point in the standard:

- **Line 381: Add the following sentences to the paragraph ending on this line:**
  "DWG advocates prompt mitigation of vulnerabilities (e.g. via an authorized software update if such updates are supported by the manufacturer) that may directly impact patient safety. Notification of DWG regarding vulnerabilities in evaluated products should not be treated as higher priority than the clinical mitigation required for patient safety."

Comment #38 (Line 368): To your point, security often requires a risk-based approach, and DWG must examine the inputs to assess risk and make a determination. This implies some level of subjectivity.

Comment #39 (Line 376): To your point, security often requires a risk-based approach, and DWG must examine the inputs to assess risk and make a determination. This implies some level of subjectivity.

Comment #40 (Lines 383-384): These audits would be used to examine artifacts associated with the specific evaluated product only, and the current wording makes this clear as it refers to the product (vs. process).

Comment #41 (Line 398): Like any other scheme (of which we are aware), disputes are handled by the scheme. There must be some authority, although the scheme in our case is managed by a wide range of stakeholders to help ensure a balanced approach to disputes, unlike some other schemes that are dominated by a single stakeholder (e.g. a government-run scheme with only government members).

The following responses are made to your comments about the PP.

Comment #1 (Line = General): N/A

Comment #2 (Line = General): Covered by same response to same comment in previous section of comments about the standard.

Comment #3 (Line = General): Covered by same response to same comment in previous section of comments about the standard.

Comment #4 (Line 35): We think the term is self-explanatory and appropriate but acknowledge that it may be good to add regulatory bodies as well, as regulatory bodies are often independent from accrediting bodies.

- Line 35: After "evaluators" add: ", government regulatory bodies,"

Comment #5 (Line 127): Suggestion accepted:

- **Line 127: Change "performing testing" to: "performing activities"**

Comment #6 (Line 127): Suggestion accepted:

- **Line 127: Sort alphabetically by Term**

Comment #7 (Line 130): Your word is more general, and therefore, we accept the suggestion.

- **Line 130: Change "life-saving" to "therapeutic"**

Comment #8 (Lines 142-143): We do not agree that the mention of USB implies the cable is within scope.

Comment #9 (Line 148): The scope of the PP was carefully considered by DWG, and we do not think it appropriate to add these examples. Products that do not fit the profile defined by this PP may still be evaluable under DTSec, using a different yet-to-be-written PP or a custom ST.

Comment #10 (Lines 148-151): We do not intend to exclude any devices that may conform to the PP yet do not want to overly complicate the informative content. The specific list of examples was carefully considered by DWG.

Comment #11 (Lines 151-152): We agree this should be clarified:

- **Change the last sentence to: "A closed loop artificial pancreas (AP) TOE may be a single CDD from a single manufacturer or may be comprised of multiple DTSec-evaluated CDDs from multiple manufacturers (example depicted in Figure 2):"**

Comment #12 (Lines 156-157): We think the examples make this clear. If you have specific suggestions, please advise.

Comment #13 (Line 161): We do not agree that this is a subjective term that needs to be changed.

Comment #14 (Lines 179-181): We do not intend to place any preference on "system" level assurance, per your recommendation, vs. assurance for specific devices. A manufacturer of a CDD should wish to have the CDD-specific assurance offered by DTSec independently of how the CDD may be used in a larger system.

Comment #15 (Lines 191-193): We appreciate the intent of your comment and are making the following change:

- **Lines 193-198. Replace the existing 6 lines with the following: "these safety-relevant portions of the smartphone (hardware, software) would be in scope for evaluation and need to be sufficiently protected from non-safety relevant portions of the smartphone. The precise specification of the scope, evaluation boundary, and security requirements would be codified in the ST."**

Comment #16 (Lines 193-197): Replaced as described in previous comment.

Comment #17 (Line 203): Comment generally accepted:

- **Lines 202-203: Change: "they must be separately validated against the related assurance standards (PPs and/or STs). It" to: "it"**

Comment #18 (Line 207): Thank you for the suggestion, however, this section and its intended focus was a specific request from FDA, so we prefer to keep the spirit of the current title.

Comment #19 (Lines 233-234): These are non-normative sections and your request implies a normative requirement. No change.

Comment #20 (Line 137): While privacy is not a specific target goal of the PP, we believe the statement as stated is accurate in that an improperly secured CDD can present privacy risks in some cases. Privacy is a future potential target of DTSec PPs. This information is non-normative.

Comment #21 (Line 259): Thank you for this error correction:

- **Line 259: change "stole" to "stolen"**

Comment #22 (Line 278): Incorrect. The PP addresses security assurance requirements.

Comment #23 (Line 285): This section is non-normative. Evaluation generally follows ISO 18045 as described elsewhere, although AVA_VAN.4 requires a level of creativity and experience that cannot be described in a standard.

Comment #24 (Line 290): Direct harm of a patient is not the only reason why an evaluation would fail. There is a term in security called "defense-in-depth" wherein we strive for improved security at many levels to reduce the overall probability of a successful attack (which could cause harm).

Comment #25 (Line 292): Subjectivity cannot be completely removed from safety risk assessment.

Comment #26 (Line 312, 315): Network eavesdropping deterrence is not intended as a privacy control but rather as a control to prevent an attacker from learning protocols or uncovering critical data that could later be used to aid in attacks against the TOE. Information flow confidentiality is important for security of some key agreement protocols, for example.

Comment #27 (Line 328): PPs attempt to define all relevant threats, even those that are not handled by the TOE (handled by the environment instead). In addition, some physical threats can be economically handled by TOEs and can effectively reduce safety risks of an overall system.

Comment #28 (Line 347): This is incorrect. A peer can be authenticated and still be malicious (if malware is installed on a phone that is otherwise authenticating properly).

Comment #29 (Line 364): Same response as your comment for Line 148.

Comment #30 (Line 371): See comment #26.

Comment #31 (Line 378, 380): Objectives are not purely informational; they are the specific objectives from which requirements are derived. "Shall" does not seem inappropriate in this context.

Comment #32 (Line 380): Deleting "any" would create a sentence with incorrect grammar. Leaving as-is.

Comment #33 (Line 388): This is an optional requirement because the risk assessment performed when creating the ST should determine if this is necessary.

Comment #34 (Line 389): While confidentiality of user data is not a primary goal of the PP, the optional user authentication component if included would help address this issue.

Comment #35 (Line 394): Out-of-scope and optional are different. We want to allow for ST/TOEs that implement additional capabilities if their risk assessments deem them necessary, even if they are not required in the PP.

Comment #36 (Lines 404-406): It is customary under ISO 15408 to enumerate related environmental objectives, despite not being part of the TOE. It helps stakeholders understand that potentially important threats must be countered with something other than the TOE itself.

Comment #37 (Lines 407-411): This objective would not be part of TOE evaluation but still pertinent to overall system security and therefore useful for inclusion as described in previous comment.

Comment #38 (Lines 437-438): This is not correct. Entropy quality is evaluated in security systems - for example, mobile devices validated under NIAP. While not every aspect of high quality cryptographic implementation is included in the PP, poor entropy is a common failure case, which is why modern NIAP PPs include it as well.

Comment #39 (Lines 449-456): Most of the application note shows examples and is therefore not too specific (and this is non-normative, anyway). We think it helps readers understand intent of the requirement.

Comment #40 (Line 460): The titles come from directly from ISO 15408.

Comment #41 (Lines 465-470): The application note is non-normative. In theory, an ST could be created specifying a CRC if the risk assessment deems it acceptable. However, in the collective opinion of DWG, a CRC is unlikely to be acceptable because it cannot protect against malicious modifications, which is the purpose of this requirement.

Comment #42 (Lines 467-468): The comment is incorrect: some embedded devices do indeed support HW root of trust. However, we acknowledge that a combination of controls may make a signature check acceptable even without a complete HW root of trust chain:

- **Line 467: Change "must" to "should"**

Comment #43 (Line 469): Please see response to comment #41.

Comment #44 (Lines 486-490): This format follows ISO 15408.

Comment #45 (Lines 497-498): We do not understand why you think this is not relevant.

Comment #46 (Line 510): The firmware should be immutable. The memory may be modifiable via authenticated FOTA, but the FOTA image itself is immutable.

Comment #47 (Lines 511-512): See comment #42

Comment #48 (Lines 513-514): See comment #41

Comment #49 (Line 522): Accepted:

- **Line 522: Replace "are" with "and".**

Comment #50 (Lines 521-534): This is an important requirement of the PP.

Comment #51 (Lines 525-526): This is an important requirement of the PP.

Comment #52 (Lines 527-528): This is an important requirement of the PP.

Comment #53 (Lines 529-530): This is an important requirement of the PP.

Comment #54 (Line 565, 570): We think many diabetes devices are life-critical and that the description is appropriate.

Comment #55 (Line 575): Disagree, these are optional requirements and may be leveraged for some STs.

Comment #56 (Line 592): Assurance requirements are a critical part of the PP.

Comment #57 (Line 600): The ST process is defined in the standard, not in the PP.

Comment #58 (Line 604): We do not agree that self-evaluation is sufficient at this time – it does not provide developer-independent assurance to all relevant stakeholders. Self-certification is an oxymoron.

Comment #59 (Lines 646-718): Agree with recommendation:

- **Line 646: Change ADV_TDS.4 to ADV_TDS.3**

Comment #60 (Line 766): See previous comments: environment assumptions and threats are intentionally part of the PP even if they are out of scope of TOE evaluation.

Comment #61 (Line 775): Same as previous.

FDA comments below

Dear Dr. David Klonoff,

Thank you for your patience. Cybersecurity is a Center priority and we appreciate DTSec's efforts. The following comments are in-line with the general level feedback provided via email on October 16, 2015 and reflect FDA's role in the DTSec standard effort as a non-voting member. The following feedback is not a roadmap for standard recognition. Standard recognition is an entirely separate domain. More importantly, implementation of the standard is more important than recognition of a standard.

We understand the common criteria approach of ISO 15408; the segregation between your standard's derivation of security functional requirements and generation of a protection profile and the separate process of implementing those security functional requirements at the security target level. At the Center, medical devices are reviewed for safety and effectiveness for a specific device at the security target level; therefore, we cannot comment on the adequacy of a general protection profile as mitigations of all types of risk (e.g. clinical) at the security target or specific device level.

1) Diabetes devices don't follow a single risk profile, rather there are different levels of risk associated with different diabetes devices. Therefore, we recommend encouraging a risk-based approach to cybersecurity profiles. These risks may be addressed in a security target.

2) Devices are constantly evolving in design (especially software-centric devices); threats to device cybersecurity evolve in response to device introduction to market, to software updates and/or to changes in device hosting (for example, apps on a mobile platform affected by OS updates). Therefore, we recommend clarifying how the certification program will provide the necessary processes to account for evolution of the devices in a timely manner to address these threats. We also recommend clarifying how accredited labs would ensure that they are testing for the most up-to-date or device-specific vulnerabilities.

3) The "Standard" document appears more like a Technical Report (or even a Guide) for the use of the referenced ISO/IEC standards in the 15408 series, ISO/IEC 18045 and IEC 62304. Technical guides can be a viable tool that could be referenced under any of the reference recognized FDA consensus ISO/IEC standards as well as the specific device standards.

4) The Protection Profile document is more robust; however, it is unclear given items 1, 2, 3, above, that the protection profile would result in a sufficient baseline of security for a security target, which is the level of specificity that would be reviewed in a 510(k) or PMA submission.

5) The assurance domain of the common criteria approach is also incorporated into your standard model. The main differentiation from the ISO 15408 is the amount of control

DTSec intends to exert over the process. For example, assurance section language suggests the intent to exert ambiguous control over device design. There are many appropriate ways to go about designing a device, and device design evolves with new research, new processes, and new technologies. Specifying one design approach may also stifle innovation. Therefore, we do not recommend specifying specific approaches to device design in the standard.

Response to FDA feedback below:

Thank you for this valuable feedback.

We agree with your assessment that the ST is the ultimate arbiter of the proper, risk-based security requirements for a particular device and that the current standard and PP are unable to predict the proper selection of derived requirements for any future ST. The standard and PP are intended to provide the framework and some of the heavy lifting, but as you point out, the ST process is a critical part of the overall defined process/framework.

1. You point out that devices do not follow a single risk profile (no one-size fits all) and that a risk-based approach be used in cybersecurity profiles and addressed in the security target. We fully agree and will clarify this in the standard.

Changes to standard made in response:

- **Addition of section 1.2, "Role of DTSec in Medical Device Safety Risk Assessment", to the standard. This section explains the importance of cybersecurity risk assessment in perspective of an overall safety risk assessment program and provides detailed examples of how the DTSec program helps fulfill the spirit of common regulatory guidance in cybersecurity risk assessment (uses FDA premarket guidance as the example). Specific mention is made of the role of the ST as a risk-based approach in determining security controls for a specific device.**

2. In regards to your recommendation to ensure new threats are properly addressed in the standard: we agree and have added the following new text in the "Assurance Maintenance Program" section of the standard.

Changes to standard made in response:

- **Addition of the following 3rd paragraph in section 2.5, "Assurance Maintenance Program":**

Recognizing that threat actors and techniques rapidly evolve, DWG reserves the right to request the submission of an assurance maintenance request form to specifically address new threats that the DWG and/or applicable DTSec-approved labs feel may invalidate an active approval. The above process for product modifications will be used by DWG to determine, by working with appropriate stakeholders including the developer, whether product changes and re-evaluation are necessary.

In regards to your recommendation that we clarify how accredited labs ensure they are testing for the most up-to-date threats and vulnerabilities, we do not believe a change is needed because the standard/PP already reference the CC's Common Methodology standards document, which explains the overall approach for vulnerability assessment at the PP's moderate attack potential, including the requirement that evaluators examine current public sources of vulnerability information as part of the overall assessment activity.

3. Thank you for this commentary; changes to standard/PP: N/A

4. We agree that the ST is required for the complete picture of security requirements. We hope we've made that clear with our explanation of the documents and phases in the standard. No change proposed.

5. We agree the standard should not be prescriptive of product design, and the PP has been written to be as non-prescriptive as possible with respect to security implementation, allowing maximum flexibility in design while still conforming to the PP. For example, the PP requires a secure channel between the TOE and peer, but does not specify design and implementation details (e.g. Bluetooth vs. some other wireless technology, Bluetooth security mode, version, pairing mode, etc.). However, the balance between a PP and ST ensures that we can provide multi-stakeholder (including manufacturers, caregivers, and patients) guidance intended to help developers make better design decisions with respect to security. If a vendor makes a design decision to leave any form of data protection whatsoever, we also want to avoid that. So we understand and appreciate your concern – it is in fact the exact reason why we adopted the combination of PP and ST to guide developers with higher-level requirements while still giving them design and implementation flexibility at the ST level. Furthermore, the standard does not ***require*** the use of the PP. If a product has threats and objectives that based on a risk assessment are not consistent with the PP, then a custom ST, that is not compliant to the PP at all, can be used. Thus, the existence of the PP in no way limits design possibilities; rather, it is meant to help developers reduce cost and time in performing the task of risk-based security specification for similar devices. Also, in this scenario of using a custom ST, if a developer is unable to allow involvement of the full DWG community in providing ST input (because of confidentiality concerns), then a custom ST process will miss out on the multi-stakeholder risk assessment process utilized in the PP. Select members of the DWG and the evaluator may be the sole stakeholders working with the developer to finalize the ST. This approach increases the risk of an inferior ST and a longer and more expensive evaluation process. The DWG feels that the standard and its PP/ST process provide the best balance of multi-stakeholder involvement while retaining reasonable design and implementation flexibility. Based on your feedback, however,

we will add clarification to the standard regarding the use of custom STs and a desire to not unnecessarily constrain product design and implementation.

Changes to standard made in response:

- **Addition of the following final paragraph in section 1:**
  This standard also allows for DWG-approved custom STs (not derived from any DWG-approved PPs) for complete CDD products, although this is generally discouraged unless the product fails to map to an existing DWG approved PP. In the same way that the PP follows a multi-stakeholder, risk-based approach to deriving an appropriate set of security threats, objectives, and requirements, a custom ST ***shall*** be carefully created so as to consider a maximum practical selection of DWG stakeholder perspectives (e.g. product developer, regulators, evaluators, caregivers, independent security experts, professional organizations, etc.). In addition, the development process for custom STs, like all other STs, should strive not to constrain product design and implementation freedom while defining, via a risk-based approach, the product's security objectives and requirements.