STARFISH ANALYSIS

FDA Cybersecurity Draft Guidance

Empowering Medtech Innovation®

StarFish MEDICAL

The FDA released a new Cybersecurity draft guidance on April 2022. It is intended to replace the current final guidance from 2014 which is well overdue an update. The draft guidance significantly expands requirements for cybersecurity activities and documentation for medical devices. The intention is to align medical device development with current best practices from other industries. This white paper reviews these new requirements and considers their impact on medical device developments.

Introduction

The current finalised guidance on Cybersecurity was released in 2014 and is 9 pages long. This new draft guidance expands to a hefty 49 pages. The FDA tried to update this guidance in 2018 but it did not progress beyond draft due to the number of comments received.

The current guidance covers the following documentation requirements:

- Risk assessment
- Traceability matrix
- Software updates plan
- Software integrity controls
- Device instructions for use covering cybersecurity (no specific guidance on content)

The process guidance only spans 2 pages with the steps: Identify, Protect, Detect, Respond and Recover. However, they include recommendations for applicable standards which could be followed to help implement this process.

This draft guidance describes recommendations regarding cybersecurity information to be submitted for devices under the following premarket submission types:

- Premarket Notification (510(k)) submissions;
- De Novo requests;
- Premarket Approval Applications (PMAs) and PMA supplements;
- Product Development Protocols (PDPs);
- Investigational Device Exemption (IDE) submissions; (with a note that content is expected to be less mature)
- Humanitarian Device Exemption (HDE) submissions.

This guidance document is applicable to devices that contain software (including firmware) or programmable logic, as well as software as a medical device (SaMD). It is important to note this guidance is not limited to devices that are network-enabled or contain other connected capabilities; hence, it needs to be considered for a wider range of products than previously covered.

It is important to note that they state that this guidance is not limited to devices that are network-enabled or contain other connected capabilities; hence, it needs to be considered for a wider range of products than previously covered.

The FDA also acknowledge that the term “medical device system” includes the device and systems such as health care facility networks, other devices, and software update servers to which it is connected.

Why The Guidance Has Been Rewritten

The FDA provided the following explanation as to why the guidance has been rewritten:

"Events across the healthcare sector have stressed the importance of cybersecurity to patient safety. The WannaCry ransomware affected hospital systems and medical devices across the globe. Vulnerabilities identified in commonly used third-party components, like URGENT/11 and SweynTooth, have led to potential safety concerns across a broad range of devices and clinical specialties. In 2020, a ransomware attack on a German hospital highlighted the potential impacts due to delayed patient care when a cybersecurity attack forced patients to be diverted to another hospital.

The rapidly evolving landscape, an increased understanding of emerging threats, and the need for capable deployment of mitigations throughout the total product lifecycle (TPLC) warrants an updated, iterative approach to device cybersecurity"

This guidance now sits alongside an expanded range of software guidances including:

- "Postmarket Management of Cybersecurity in Medical Devices,"
- "Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software"
- "Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices."

New approach

In this guidance the FDA introduces the concept of a Secure Product Development Framework (SPDF). This is a set of processes that reduce the number and severity of vulnerabilities in products throughout the device lifecycle.

They state that:

- *Using an SPDF is one approach to help ensure that QSR requirements are met. Because of its benefits in helping comply with QSRs and cybersecurity, FDA encourages manufacturers to use an SPDF, but other approaches might also satisfy QSR requirements.*

Which ties in with the revised title of the guidance "*Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*" compared to the previous "C*ontent of Premarket Submissions for Management of Cybersecurity in Medical Devices*".

They also give specific details of an expanded list of Submission Documentation, with the understanding that device cybersecurity design and documentation is expected to scale with the cybersecurity risk of that device and not with the software safety classification.

Required documentation:

- Risk Management documentation
  - o including: threat modeling, SBOM, security assessment of unresolved anomalies, security risk management plan/report, post market risk management & metrics
- Security Architecture
  - o including: implementation of security controls, security "views"
- Cybersecurity testing documentation
- Labelling
- Vulnerability Management Plan(s)

Security Risk Management

As per the current final guidance, security risk management is still a key focus for this guidance, and like other guidances preceding this one, both from the FDA and other regulators. It acknowledges that the process for performing security risk management is a distinct process from performing safety risk management as described in ISO 14971:2019.

While safety risk management focuses on physical injury or damage to property or the environment, security risk management may include not only risks that can result in patient harm. It may also include those risks that are outside of FDA's assessment of safety and effectiveness, such as those related to business or reputational risks.

FDA recommends that device manufacturers conduct both a safety risk assessment per ISO 14971:2019 and a separate, accompanying security risk assessment to ensure a more comprehensive identification and management of patient safety risks. However, these processes should also ensure that risk control measures for one type of risk assessment do not inadvertently introduce new risks in the other.

In addition to the security risk assessment, which is detailed in the current final guidance, this draft guidance also identifies other topics under the heading of risk management:

Threat Modeling:

Threat modeling includes a process for identifying security objectives, risks, and vulnerabilities across the system, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system throughout its lifecycle.

The guidance states that the threat model should:

- *identify system risks and mitigations as well as inform the pre- and post-mitigation risks considered as part of the security risk assessment;*
- *state any assumptions about the system or environment of use (e.g. hospital networks are inherently hostile, therefore manufacturers are recommended to assume that an adversary controls the network with the ability to alter, drop, and replay packets); and*
- *capture cybersecurity risks introduced through the supply chain, manufacturing, deployment, interoperation with other devices, maintenance/update activities, and decommission activities that might otherwise be overlooked in a traditional safety risk assessment processes.*

An interesting point to note is that the guidance indicates that Threat Modeling activities can be performed and/or reviewed during design reviews.

3rd Party Software & SBOMs:

The FDA's guidance "Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software" details the specific requirements for OTS software, but in the new draft guidance on Cybersecurity, they go further into the details of software which may be not fully OTS, but is developed by a 3rd party.

The guidance indicates that as part of configuration management, device manufacturers should have custodial control of source code through source code escrow and source code backups. If this control is not available based on the terms in the supplier agreements, the manufacturer should include in premarket submissions a plan of how the third-party software component could be updated or replaced should support for the software end.

This is an interesting concept that could be well understood when there is a specific client / supplier relationship, and these terms can be discussed and negotiated. However, when the vendor becomes a larger organisation than the procurer, the negotiation of terms becomes harder. It is difficult to see how this could be implemented when negotiating with the likes of Microsoft, Apple or Amazon.

This version of the guidance also introduces the concept of a Software Bill of Materials (SBOM), a term that is growing in popularity. The guidance explains that an SBOM helps facilitate risk management processes by providing a mechanism to identify devices that might be affected by vulnerabilities in the software components, both during development (when software is being chosen as a component) and after it has been placed into the market throughout all other phases of a product's life. Certainly, many parties are already implementing this approach as the benefits from a traceability perspective appear obvious for them.

Now, the FDA also requests that for third-party components with known vulnerabilities, device manufacturers should provide further information in premarket submissions, such as:

- A safety and security risk assessment of each known vulnerability; and
- Details of applicable safety and security risk controls to address the vulnerability. If risk controls include compensating controls, those should be described in an appropriate level of detail.

This is a new set of activities and documentation not previously requested.

Security Assessment of Unresolved Anomalies:

The FDA's Premarket Software Guidance recommends that device manufacturers provide a list of software anomalies (e.g., bugs or defects) that exist in a product at the time of submission. For each of these anomalies, FDA recommends that you conduct an assessment of the anomaly's impact on safety and effectiveness, and consult the Premarket Software Guidance to assess the associated documentation recommended for inclusion in such device's premarket submission.

The criteria and rationales for addressing the resulting anomalies with security impacts should be provided as part of the security risk assessment documentation in the premarket submission.

Security Risk Management Documentation:

In terms of summarising the security risk management process and outputs, the FDA are now looking for a security risk management report to be part of the submission, same as a product safety related risk management report is required.

The guidance states that the security risk management report should:

- summarize the risk evaluation methods and processes, detail the security risk assessment, and detail the risk mitigation activities undertaken as part of a manufacturer's risk management processes; and
- provide traceability between the security risks, controls and the testing reports that ensure the device is reasonably secure.

This suggests an expectation of a report which is similar to that produced for safety risk.

Total Product Lifecycle (TPLC) Security Risk Management (or Post Market Risk Management)

The FDA recommends that the risk management documentation account for any differences in the risk management for devices in the field (e.g., marketed devices or devices no longer marketed but still in use). For example, if an update is not applied automatically for all devices, then there will likely be different risk profiles for differing software configurations of the device. The FDA recommends that vulnerabilities be assessed for any differing impacts for all potential configurations or versions to ensure patient risks are being accurately assessed.

To demonstrate the effectiveness of a manufacturer's processes, the FDA recommends that a manufacturer track and record the measures and metrics below, and report them in premarket submissions and PMA annual reports:

- Percentage of identified vulnerabilities that are updated or patched (defect density).
- Time from vulnerability identification to when it is updated or patched.
- Time from when an update or patch is available to complete implementation in devices deployed in the field

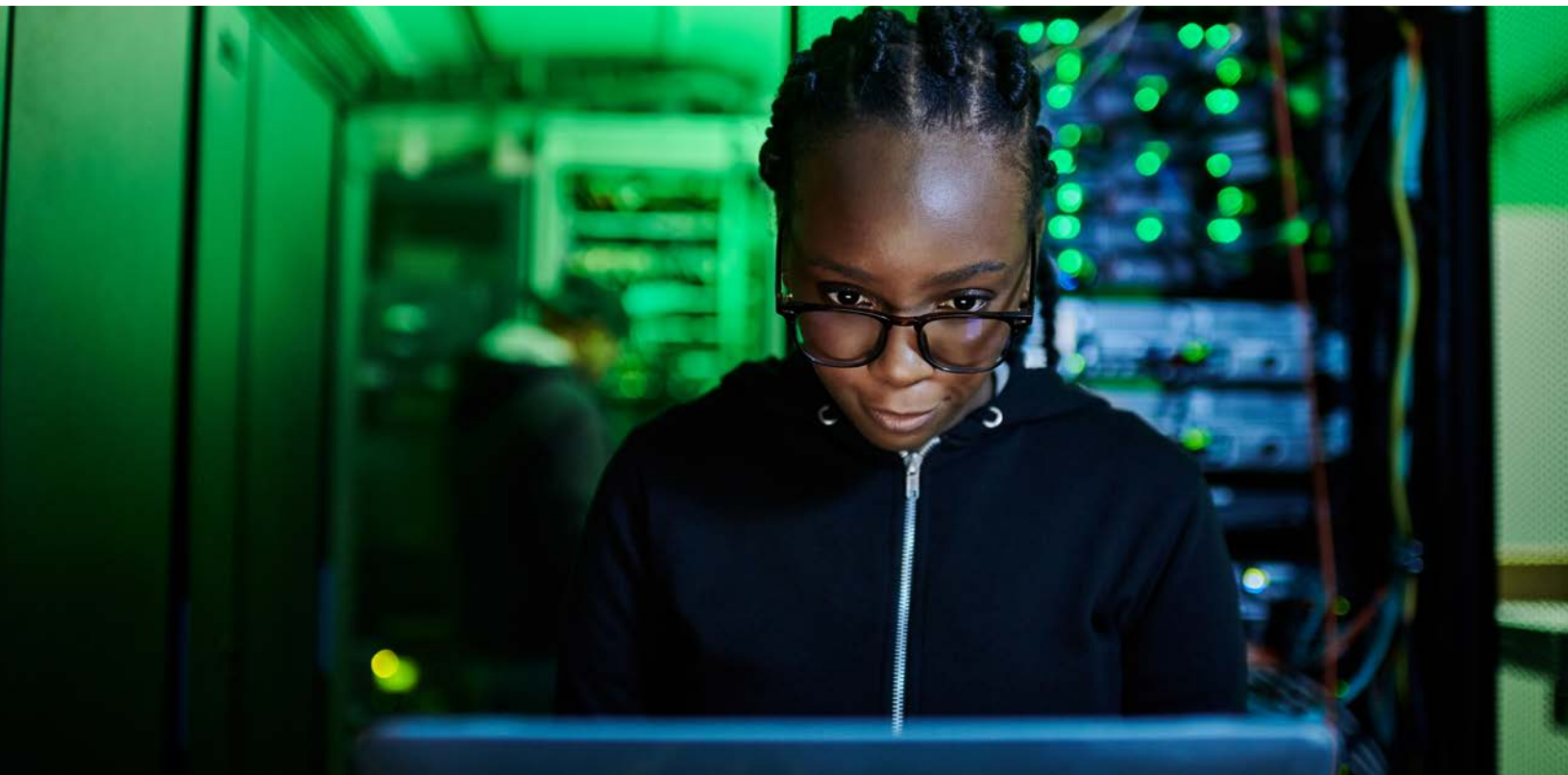
As these are new metrics, this will need to be considered in updates to QMS processes to capture this data and make sure those processes are implemented prior to when they need to start collecting data. It is always hard to data mine after the moment has passed.

Security Architecture:

Those following IEC 62304 for their software development processes probably already have a software architecture on hand. However, in this guidance, the FDA are now also looking for a Security Architecture document.

As detailed above in the risk management section, manufacturers are responsible for identifying cybersecurity risks. Within the context of security architecture, the new draft guidance reminds that we should be considering both the devices and the systems in which we expect those devices to operate. These risks may include those introduced by device reliance on hospital networks, cloud infrastructure, or "other functions" (as defined in FDA's guidance "Multiple Function Device Products: Policy and Considerations", e.g. patient records management, web interfaces, billing functions etc.).

A security architecture, like a system architecture, defines the system and all end-to-end connections into and/or out of the system. Analysis of the entire system should be performed to understand the full environment and context in which the device is expected to operate.



Also, as with a system architecture, a security architecture should be core as to how the device is developed to ensure security by design. This means that requirements for security should be included within the main design inputs for the product from other stakeholders. The FDA recommends that this approach is integrated into design & development procedures.

The security architecture should also include details about the implementation of security controls:

The FDA recommends that an adequate set of security controls will include, but not necessarily be limited to, controls from the following categories:

- Authentication;
- Authorization;
- Cryptography;
- Code, Data, and Execution Integrity;
- Confidentiality;
- Event Detection and Logging;
- Resiliency and Recovery; and
- Updatability and Patchability

As always, the FDA is looking for manufacturers to include documentation in their premarket submissions demonstrating that the security controls for the categories above have (1) been implemented, and (2) been tested in order to validate that they were effectively implemented.

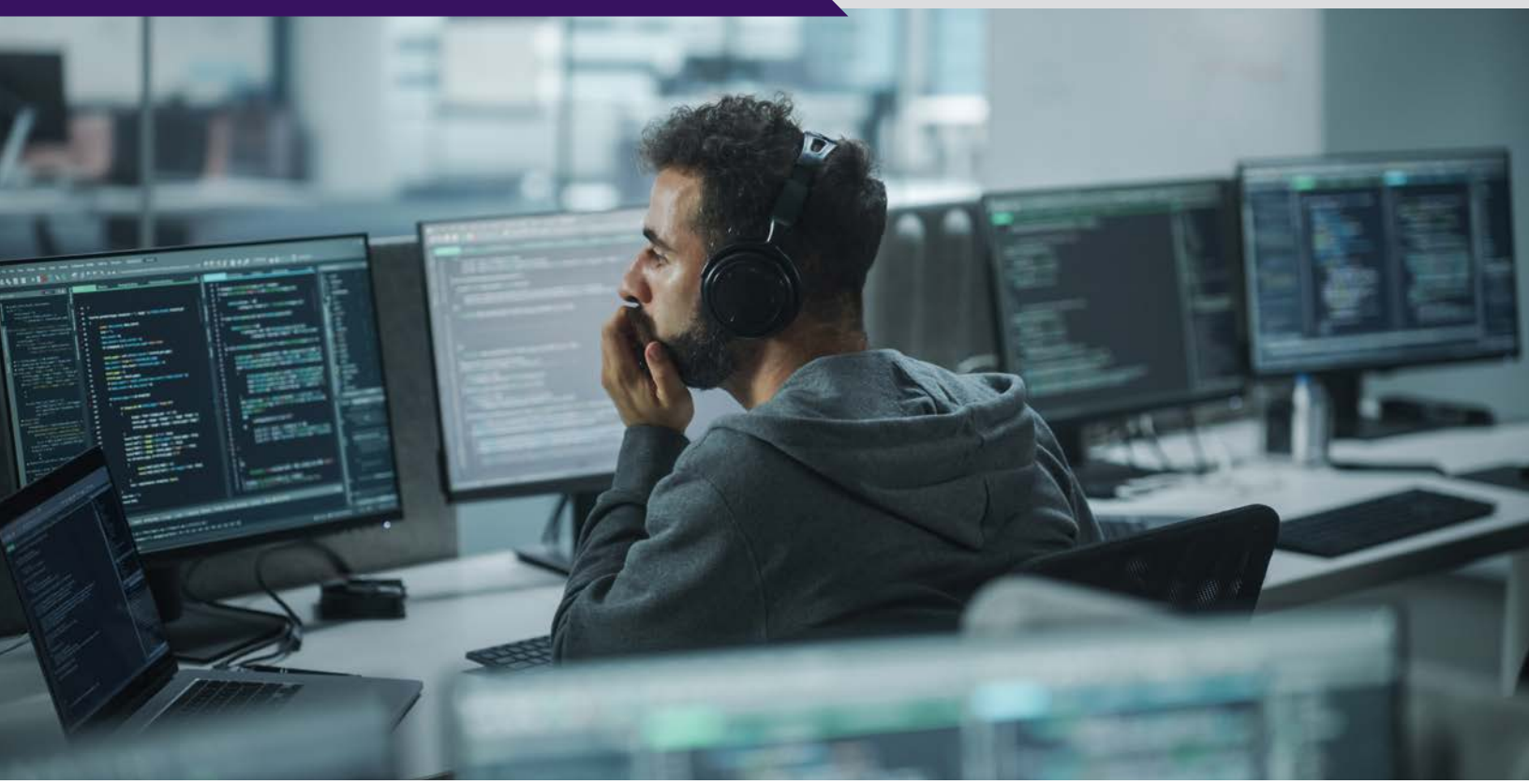
The FDA recommends this security architecture information in the form of "views". The FDA recommends providing, at minimum, the following types of views in premarket submissions:

- Global System View;
- Multi-Patient Harm View;
- Updateability/Patchability View; and
- Security Use Case View(s)

These security architecture views should:

- Identify security-relevant system elements and their interfaces;
- Define security context, domains, boundaries, and external interfaces of the system;
- Align the architecture with (a) the system security objectives and requirements, (b) security design characteristics; and
- Establish traceability of architecture elements to user and system security requirements

Fortunately for us, the FDA recognises this is a new concept and provides further detailed information on these "views" and what needs to go into them in Appendix 2 of the guidance.



Cybersecurity Testing

Cybersecurity testing, and in particular penetration testing, has been routine in other security related industries for some time. Anyone who is implementing an Information Security Management System (ISMS) for ISO27001 alongside their QMS will be familiar with this sort of testing. The current final guidance does not explicitly require any testing; however, it can be used to prove the effectiveness of the risk controls which are required.

In this guidance the FDA is more explicit about the specific testing required to be included in submissions. Some of these requirements and documentation will be generated or captured as part of the risk management process, some during verification and software validation; and some will need specific cybersecurity testing to be carried out.

FDA recommends that the following types of testing, among others, be provided in the submission:

- *Security requirements*
  - *Manufacturers should provide evidence that each design input requirement was implemented successfully.*
  - *Manufacturers should provide evidence of their boundary analysis and rationale for their boundary assumptions.*

- *Threat mitigation*
  - *Manufacturers should provide details and evidence of testing that demonstrates effective risk control measures according to the threat models provided in the system, use case, and call-flow views.*
  - *Manufacturers should ensure the adequacy of each cybersecurity risk control (e.g., security effectiveness in enforcing the specified security policy, performance for maximum traffic conditions, stability and reliability, as appropriate).*

- *Vulnerability Testing (such as section 9.4 of ANSI/ISA 62443-4-1)*

  Manufacturers should provide details and evidence of the following testing pertaining to known vulnerabilities:

  - *Abuse case, malformed, and unexpected inputs,*
    - *Robustness*
    - *Fuzz testing*
  - *Attack surface analysis,*
  - *Vulnerability chaining,*
  - *Closed box testing of known vulnerability scanning,*
  - *Software composition analysis of binary executable files, and*
  - *Static and dynamic code analysis, including testing for credentials that are "hardcoded," default, easily-guessed, and easily compromised.*
- *Penetration testing*

The testing should identify and characterize security-related issues via tests that focus on discovering and exploiting security vulnerabilities in the product. Penetration test reports should be provided and include the following elements:

- *Independence and technical expertise of testers,*
- *Scope of testing,*
- *Duration of testing,*
- *Testing methods employed, and*
- *Test results, findings, and observations.*

We find it interesting that the FDA goes as far as indicating that cybersecurity testing should be performed at regular intervals (e.g., annually) to ensure that potential vulnerabilities are identified and able to be addressed prior to their ability to be exploited.

Labelling

In this guidance, the FDA expands upon their labelling expectations, specifically detailing 15 key points that they will be looking for in product labelling, either on the device itself or in the instructions for use.

Vulnerability Management Plans

Cybersecurity doesn't stop once the product submission has gone in. Vulnerabilities are continually being identified and manufacturers need to manage the safety and security of their devices throughout their lifetime in the field. The FDA have defined a document called a Vulnerability Management Plan which will lay out how a manufacturer will carry out this process. This will need to be included as part of premarket submissions so that the FDA can assess whether the manufacturer has sufficiently addressed how to maintain the safety and effectiveness of the device after marketing authorization is achieved.

The guidance details that vulnerability management (or communication) plans should include the following elements:

a) Personnel responsible;

b) Sources, methods, and frequency for monitoring for and identifying vulnerabilities (e.g., researchers, NIST NVD, third-party software manufacturers, etc.);

c) Periodic security testing to test identified vulnerability impact;

d) Timeline to develop and release patches;

e) Update processes;

f) Patching capability (i.e., rate at which update can be delivered to devices);

g) Description of their coordinated vulnerability disclosure process; and

h) Description of how manufacturer intends to communicate forthcoming remediations, patches, and updates to customer.

Key Definitions:

- **Authentication** – the act of verifying the identity of a user, process, or device as a prerequisite to allowing access to the device, its data, information, or systems, or provision of assurance that a claimed characteristic of an entity is correct.
- **Authorization** – the right or a permission that is granted to a system entity to access a system resource.
- **Cryptography** – the discipline that embodies the principles, means, and methods for providing information security; including confidentiality, data integrity, non-repudiation, and authenticity.
- **Encryption** – the cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used.
- **Exploitability** – the feasibility or ease and technical means by which the vulnerability can be exploited by a threat.
- **Threat** – any circumstance or event with the potential to adversely impact the device, organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Threats exercise vulnerabilities, which may impact the safety or effectiveness of the device.
- **Threat modeling** – a methodology for optimizing system, product, network, application, and connection security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system.
- **Vulnerability** - a weakness in an information system, system security procedure(s), internal control(s), human behavior, or implementation that could be exploited.

Conclusions / Main Considerations:

With the increase in concern about cybersecurity in this connected world, the FDA is looking to bring their expectations for cybersecurity content up to date. This brings a lot more focus on the topic. Whilst this is a draft guidance, I feel this is likely to be reflective of what the FDA is going to expect. The draft guidance is defining industry best practices already considered the baseline in wider information security fields, and applying it to medical devices.

Going forward, this will become a more significant task within projects and needs to have sufficient resources allocated in order to prepare sufficiently convincing documentation for submissions. This documentation can't be done after the fact at the time of creating the submission. They will be looking for it to be integrated from day one in product requirements and throughout the development process and into post market activities.

It should be noted that when the comment period on this draft guidance closed in early July 2022, a significant quantity of comments had been received, including a large number of responses from campaign groups, in particular those using diabetes monitors. Hence, we will wait and see if this guidance progresses is rewritten again as the 2018 guidance was. We hope that it will move forward as the 2014 guidance is now significantly out of touch with current best practices and does not give the level of detailed guidance to make appropriate design decisions.

AUTHOR:
Helen Simons
Senior QA/RA Specialist

Helen Simons has over 15 years experience in product development. She has worked on a wide range of Medical Device and IVD products, from inhalers and injection devices to phototherapy devices and ventilators. Her experience includes project managing product developments and providing quality and regulatory guidance to both internal teams and clients for the US, EU and Canadian markets. Providing detailed insight into the regulatory requirements for those markets, Helen's expertise includes business improvements and building effective and efficient quality systems. Prior to joining StarFish Medical, Helen worked at companies including Sagentia, Cambridge Design Partnership, and GHD. She holds a Master's Degree in Engineering from Durham University, Durham, England.