OMBU
ENTERPRISES, LLC

3 Forest Ave.
Swanzey, NH 03446
Phone: 603-209-0600
Fax: 603-358-3083
www.OmbuEnterprises.com
Dan@OmbuEnterprises.com

On June 14, 2013, CDRH & CBER issued a draft guidance document entitled *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*

The draft guidance (starting at line 135) says, "Manufacturers should define and document the following components of their cybersecurity risk analysis and management plan as part of the risk analysis required by 21 CFR 820.30(g):

- Identification of assets, threats, and vulnerabilities;
- Impact assessment of the threats and vulnerabilities on device functionality;
- Assessment of the likelihood of a threat and of a vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies;
- Residual risk assessment and risk acceptance criteria.

Starting at line 210, the guidance asks for, "Hazard analysis, mitigations, and design considerations pertaining to intentional and unintentional cybersecurity risks associated with your device …"

It also asks (starting at line 217) for, "A traceability matrix that links your actual cybersecurity controls to the cybersecurity risks that were considered … "

The requested items are part of the risk analysis in 820.30(g). However, neither the guidance nor 820.30(g) have a defined method for performing risk analysis, although the QSR preamble discusses the elements that constitute an appropriate risk analysis.

In our opinion, the guidance document would be better if it followed the structure of ISO 14971:2007. A model for this approach is the June 22, 2011 draft guidance *Applying Human Factors and Usability to Optimize Medical Device Design*.

The human factors guidance provided a list of hazards for consideration, offers a risk reduction option priority order that is specific to the kinds of hazards, and provides a flow chart (Figure 3) for addressing use related hazards.

This guidance should take a similar approach. While taking care not to be prescriptive, the framework of ISO 14971:2007 provides a useful model. Augmenting it with hazard lists, *etc*. will provide the kind of information necessary for a robust submission.

The points below address some specific issues in the cybersecurity draft guidance.

Identify known and foreseeable hazards in normal and fault conditions (This is four possible combinations.)

The likelihood of a threat is the probability, while the “impact assessment of the threats and vulnerabilities on device functionality” is the severity. These combine to provide the estimated risk, called determination of risk levels in the draft guidance.

Risk acceptance criteria are important and should be stated in the same terms as risk estimation, *i.e.*, specify the combinations of probability and severity that are acceptable and, by inference, those that require risk reduction.

The documentation should include, “A specific list of all cybersecurity hazards and hazardous situations considered in the design of your device”. The guidance uses the word risk, defined as the combination of probability and severity.

The documentation should include, “A traceability matrix that links your actual cybersecurity controls to the cybersecurity hazardous and hazardous situation that were considered” The comment above about the use of the word risk applies. In addition, ISO 14971:2007 requires implementation verification, which links to “actual cybersecurity controls”.

In summary, the guidance would be better if it followed the ISO 14971:2007 using the correct terms and information flow. In addition, it could augment information (such as a hazard list) that applies to the cybersecurity case. This would improve the ability of firms to use the existing risk management structure.