OVERVIEW OF UL 2900

MEDICAL DEVICE CYBERSECURITY WORKSHOP

MINNEAPOLIS, MN

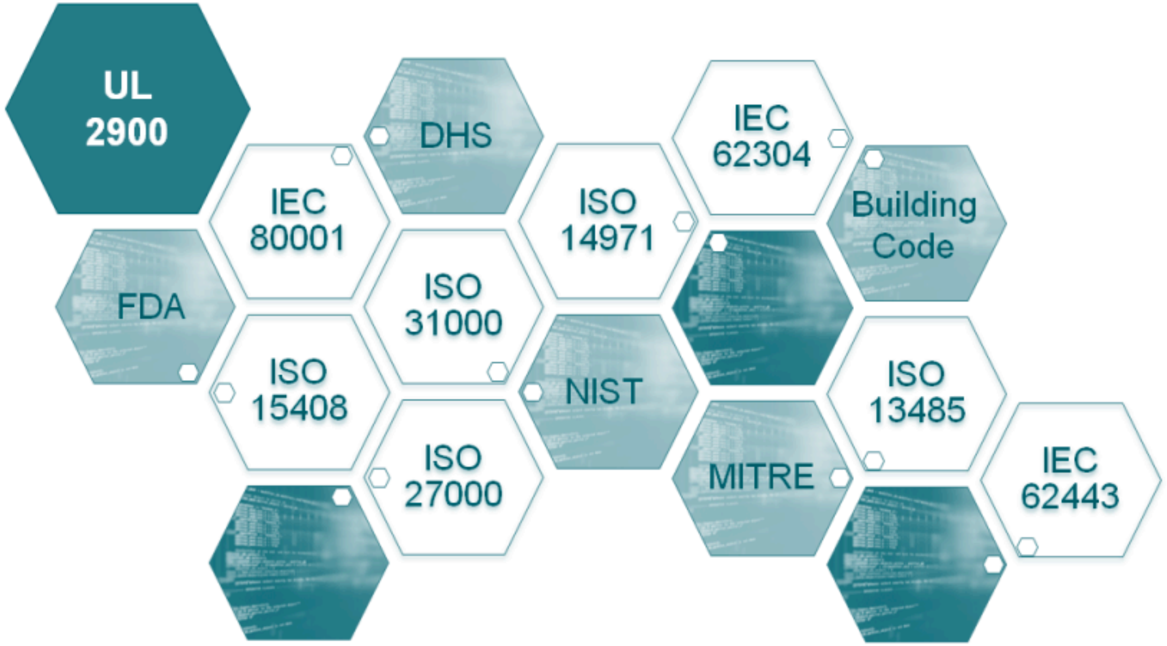
Justin Heyl, BSME
UL | Cybersecurity Commercial Strategies
T: +1 612-618-8797
E: Justin.heyl@ul.com

AN INTRODUCTION TO UL 2900

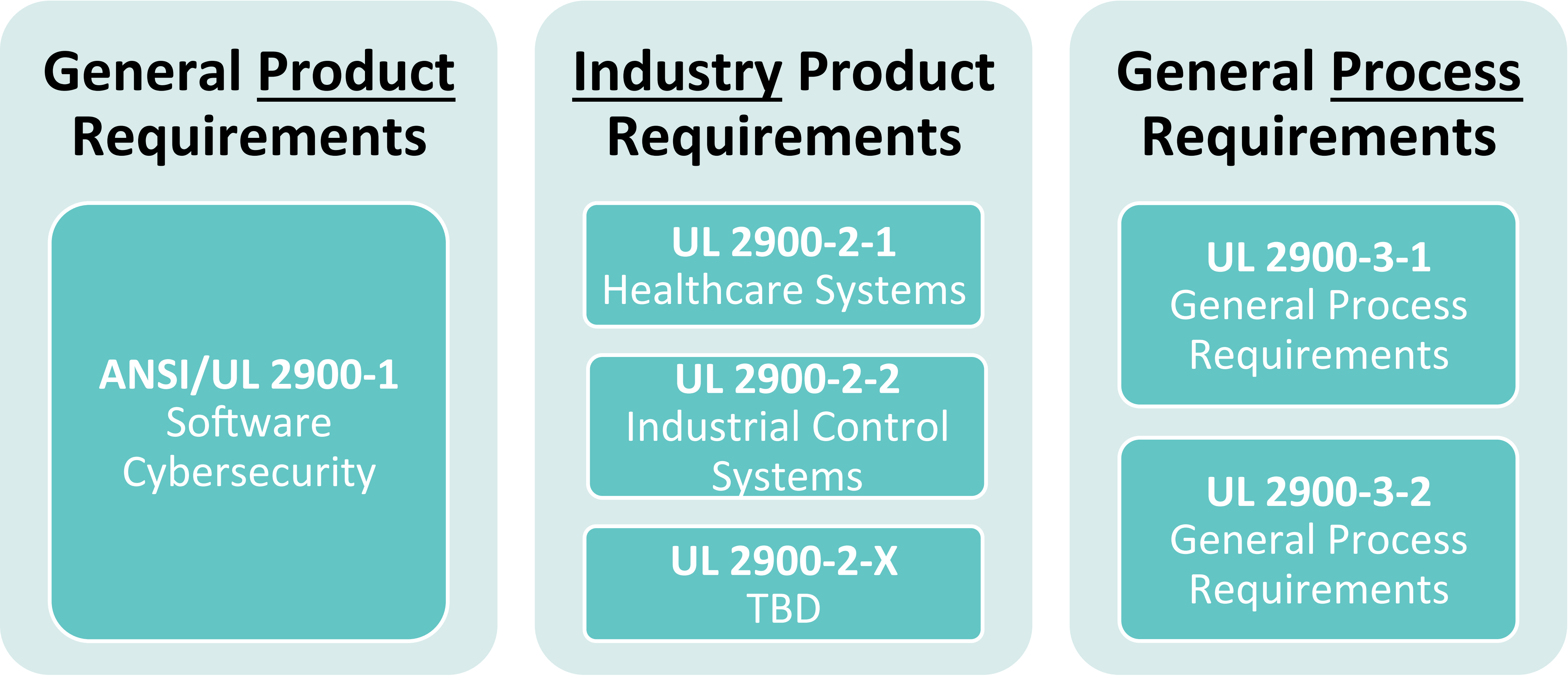
UL 2900

UL 2900 series of standards was developed as part of UL's Cybersecurity Assurance Program which provides manufacturers testable and measureable criteria

- To assess product weaknesses
- To assess vulnerabilities
- To assess security risk controls



OVERVIEW OF UL 2900



General Product Requirements

ANSI/UL 2900-1
Software
Cybersecurity

Industry Product Requirements

UL 2900-2-1
Healthcare Systems

UL 2900-2-2
Industrial Control
Systems

UL 2900-2-X
TBD

General Process Requirements

UL 2900-3-1
General Process
Requirements

UL 2900-3-2
General Process
Requirements

ANSI UL 2900

The American National Standards Institute (ANSI) has granted consensus for UL 2900-1 and UL 2900-2-1.

The FDA has also voted affirmatively to adopt both UL 2900-1 and UL 2900-2-1 as recognized consensus standards.

The US Federal Register notice of FDA Recognized consensus standards was published in August 2017 for UL 2900-1. We anticipate an update to the FR to reflect adoption of UL 2900-2-1, soon.

UL 2900 REFLECTS PREMARKET REGULATORY THINKING

UL 2900-2-1 has direct alignment with FDA Guidance Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Risk Management around assets with respect to threats, and vulnerabilities

Considers core functions of NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, Recover

Cybersecurity Documentation

UL 2900 REFLECTS POSTMARKET REGULATORY THINKING

There is also alignment with Postmarket Management of Cybersecurity in Medical Devices

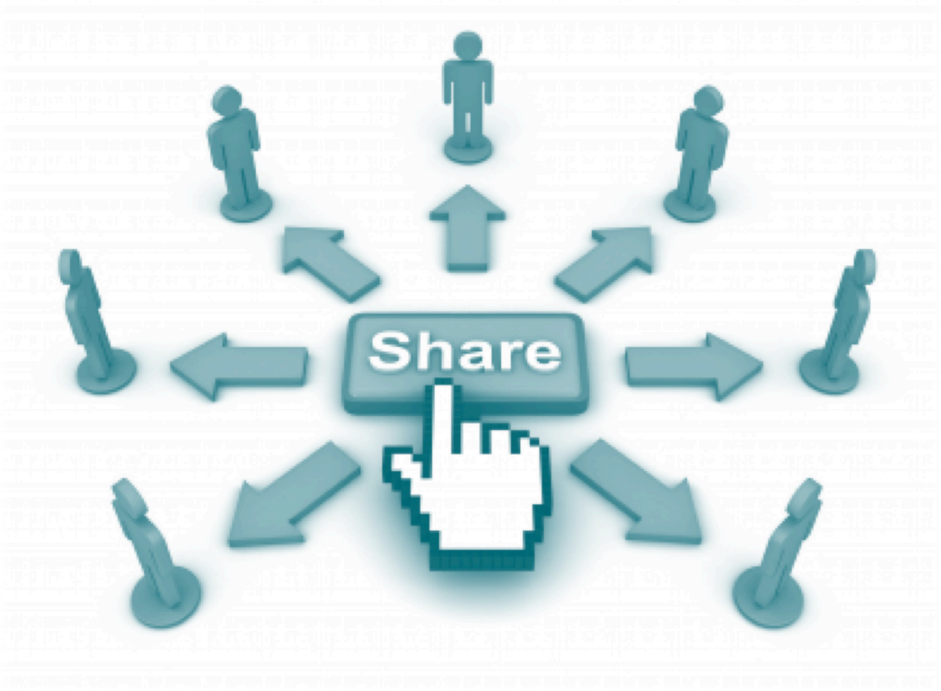
- Risk Management
- Quality Management System Requirements (21 CFR 820 & ISO 13485)
- Use of CVSS in conjunctions with medical device risk management
- Patch management

UL 2900 REFLECTS POSTMARKET REGULATORY THINKING

FDA strongly urges manufacturer participation in ISAO.

UL 2900 has no parallel requirement but does require manufacturers to provide a plan for providing software updates and patches throughout the lifecycle of the product

UL is stringent about manufacturer confidentiality however security transparency is achieved by information shared through the UL 2900 CAP Certificate



ANSI/UL 2900-1 TABLE OF CONTENTS

INTRODUCTION

1. Scope
2. Normative References
3. Glossary
4. Documentation of Product, Product Design and Product Use
5. Product Design Documentation
6. Documentation for Product Use
7. Risk Controls
8. Access Control, User Authentication and User Authorization
9. Remote Communication
10. Sensitive Data
11. Product Management

RISK CONTROLS & RISK MANAGEMENT

12. Vendor Product Risk Management Process

VULNERABILITIES AND EXPLOITS

13. Known Vulnerability Testing
14. Malware Testing
15. Malformed Input Testing
16. Structured Penetration Testing

SOFTWARE WEAKNESSES

17. Software Weakness Analysis
18. Static Source Code Analysis
19. Static Binary and Byte Code Analysis

APPENDICES

A1. Sources for Software Weaknesses

B1. Requirements for Secure Mechanisms for Storing Sensitive Data and Personally Identifiable Data

C1. Requirements for Security Functions

ANSI/UL 2900-2-1 TABLE OF CONTENTS

INTRODUCTION

1. Scope
2. Normative References
3. Glossary

DOCUMENTATION FOR PRODUCT, PROCESSES, AND USE

4. Product Documentation
5. Process Documentation
6. Documentation for Product Use

RISK CONTROLS & RISK MANAGEMENT

6. General
7. Access Control, User Authentication and User Authorization
9. Remote Communication
10. Cryptography
11. Product Management

PRODUCT ASSESSMENT

12. Safety Related Security Risk Management
13. Known Vulnerability Testing
14. Malware Testing
15. Malformed Input Testing
16. Structured Penetration Testing
17. Software Weakness Analysis
18. Static Source Code Analysis
19. Static Binary and Bytecode Analysis

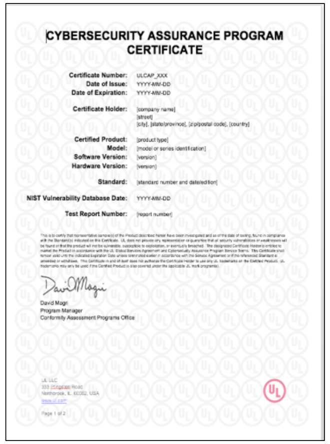
ORGANIZATIONAL ASSESSMENT

20. Lifecycle Security Processes

UL Cybersecurity Assurance Program Details

Vulnerability Assessment aims to evaluate known vulnerabilities of a product.
Known Vulnerability Testing: – All software binaries, including executables and libraries, in a product are assessed for known vulnerabilities at the time of evaluation. The vulnerabilities are identified from the NIST National Vulnerability Database (NVD).
Malware Testing: The product is inspected for malware which may exist in the software deliverables of the product.
Fuzz Testing: All external interfaces and communication protocols of the product is evaluated using generational fuzz testing techniques, if available, and template-based fuzz testing techniques otherwise. The product is evaluated for unexpected behavior based on the customer's specifications.
Robustness Evaluation aims to test the product's resilience against unexpected or malformed input.
Weakness Analysis
○ Common Weakness Enumerations (CWE): The product shall not contain any software weakness identified from CWE/SANS Top 25 Most Dangerous Software Errors, CWE/SANS on the cusp list or OWASP Top 10 2013 web application software weaknesses.
○ Static Code Analysis: Static analysis of all compiled executables and libraries of the product, in order to look for known malware and vulnerabilities
○ Static Binary and Byte Code Analysis: Static binary and byte code analysis of all compiled or intermediate binary executables and libraries of the product.
Penetration Testing: Evaluation of a product to identify vulnerabilities and software weaknesses.
Network Port and Service Testing
Wireless Testing: If a product has wireless communications technologies, the product is evaluated to identify vulnerabilities and software weaknesses through wireless access points.
Risk Assessment: Analysis by the vendor of the security risk(s) for the product.
Common Vulnerability Scoring System (CVSS): Provides a means for prioritizing CVEs in terms of exploit potential.
Common Weakness Scoring System (CWSS): Provides a means for prioritizing CWEs based on their technical impact.
Common Attack Pattern Enumeration and Classification (CAPEC): List of large number of attack patterns which are a description of common methods for exploiting software.
Organizational Assessment
Patch Management
SDLC
Wireless

Disclosure of Results Support the Supply Chain



CYBERSECURITY ASSURANCE PROGRAM CERTIFICATE

Certificate Number: ULCAP_XXX
Date of Issue: YYYY-MM-DD
Date of Expiration: YYYY-MM-DD

Certificate Holder: [company name]
[street]
[city], [state/province], [zip/postal code], [country]

Certified Product: [product type]
Model: [model or series identification]
Software Version: [version]
Hardware Version: [version]

Standard: [standard number and date/edition]

NIST Vulnerability Database Date: YYYY-MM-DD

Test Report Number: [report number]

This is to certify that representative sample(s) of the Product described herein have been investigated and as of the date of testing, found in compliance with the Standard(s) indicated on this Certificate. UL does not provide any representation or guarantee that all security vulnerabilities or weaknesses will be found or that the product will not be vulnerable, susceptible to exploitation, or eventually breached. The designated Certificate Holder is entitled to market the Product in accordance with the UL Global Services Agreement and Cybersecurity Assurance Program Service Terms. This Certificate shall remain valid until the indicated Expiration Date unless terminated earlier in accordance with the Service Agreement or if the referenced Standard is amended or withdrawn. This Certificate in and of itself does not authorize the Certificate Holder to use any UL trademarks on the Certified Product. UL trademarks may only be used if the Certified Product is also covered under the applicable UL mark program(s).

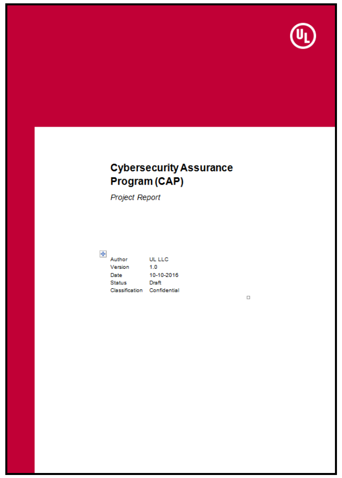
David Magi
Program Manager
Conformity Assessment Programs Office

UL LLC
333 Pfingsten Road
Northbrook, IL 60062, USA
www.ul.com

Page 1 of 2

Public

Manufacturer
Product CM
NVD version
UL DB version
Etc…



Cybersecurity Assurance Program (CAP)

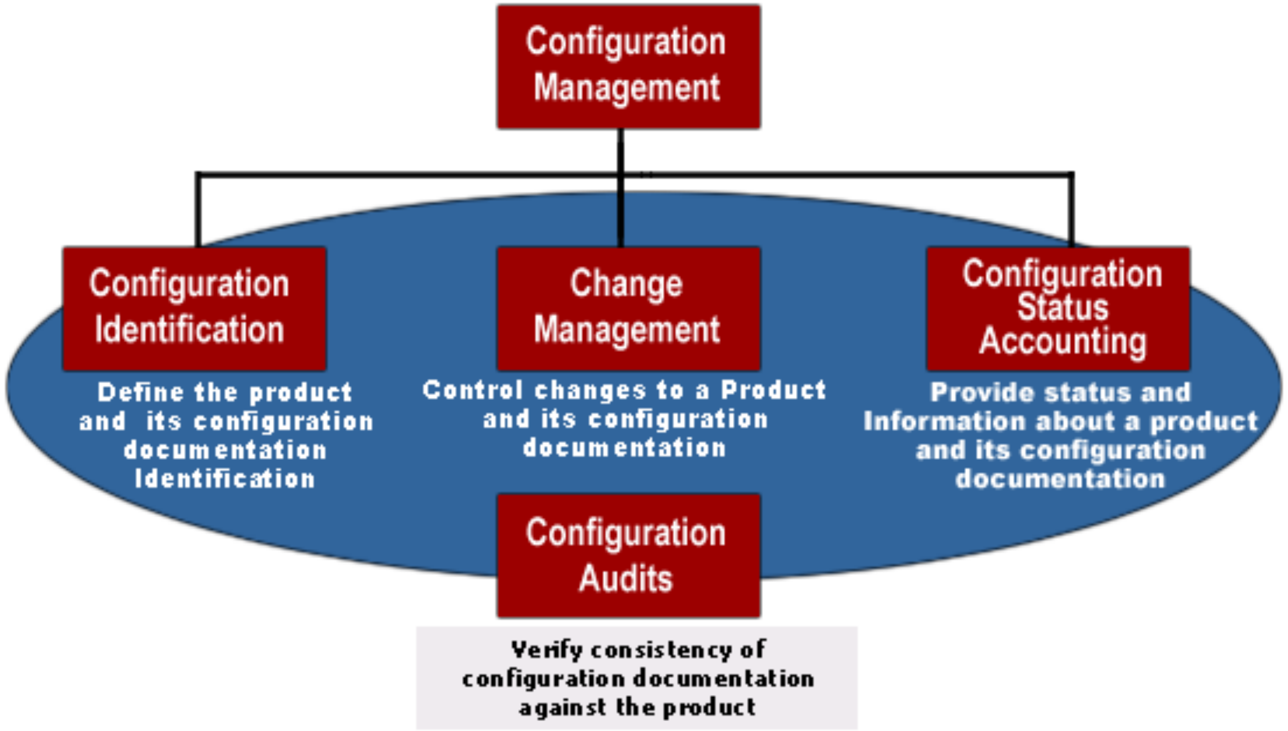
Project Report

Author	UL LLC
Version	1.0
Date	10-10-2016
Status	Draft
Classification	Confidential

Private

Manufacturer
Product CM
Attack surface
Threat model
Vulnerabilities
Security assurance claims, arguments, and evidence
Etc…

DISCLOSURE SUPPORTS SUPPLY CHAIN


Configuration Management

Configuration Identification

Define the product and its configuration documentation Identification

Change Management

Control changes to a Product and its configuration documentation

Configuration Status Accounting

Provide status and Information about a product and its configuration documentation

Configuration Audits

Verify consistency of configuration documentation against the product

http://ops.fhwa.dot.gov/freewaymgmt/publications/cm/handbook/chapter1.htm

- Example CM strategy X.Y; where X represents critical changes and Y represents non-critical changes.

UL 2900 AND FDA GUIDANCE

MAPPING UL 2900 TO FDA GUIDANCE

FDA Guidance Section	General Description	ANSI/UL 2900-1 Clause Reference	UL 2900-2-1 Clause Reference
General Principles	Address cybersecurity during the design and development to affect a more robust and efficient mitigation of patient risks related to cybersecurity	Clause 5	Refer to UL 2900-1
	Identification of assets, threats, and vulnerabilities	Clause 12	Clause 12
	Assessment of the likelihood of threat and/or vulnerability being exploited	Clause 12	Clause 12
	Assessment of residual risk, risk acceptance criteria	Clause 12	Clause 12

MAPPING UL 2900 TO FDA GUIDANCE

FDA Guidance Section	General Description	ANSI/UL 2900-1 Clause Reference	UL 2900-2-1 Clause Reference
Cybersecurity Functions **Identify and Protect**	Security controls depend upon the device's intended use, the presence and intent of its electronic data interfaces, its intended environment of use	Clause 4 Clause 6	Clause 12
	Type of cybersecurity vulnerabilities present, likelihood the vulnerability will be exploited, and the probable risk of patient harm due to a breach.	Clause 12 Clause 13	Clause 12 Clause 13
	Balancing cybersecurity safeguards and usability to ensure that the security controls are appropriate for intended users.	Clause 6	Clause 6
	Security controls should not unreasonably hinder access to a device intended to be used during an emergency situation.		Clause 12
	Justification in the premarket submission for the security functions chosen for their medical devices.		Clause 12

MAPPING UL 2900 TO FDA GUIDANCE

FDA Guidance Section	General Description	ANSI/UL 2900-1 Clause Reference	UL 2900-2-1 Clause Reference
Cybersecurity Functions **Identify and Protect** ***(Limit Access to Trusted Users Only)***	Limit access to devices through the authentication of users	Clause 8	Clause 12.4
	Use automatic timed methods to terminate sessions within the system where appropriate for the use environment	Clause 8	Refer to UL 2900-1
	Consideration of a layered authorization model by differentiating privileges based on the user role	Clause 8	Clause 12.4
	Use appropriate authentication	Clause 8	Refer to UL 2900-1
	Strengthen password protection by avoiding “hardcoded” password or common words	Clause 6, Clause 8	Refer to UL 2900-1
	Limit public access to passwords used for privileged device access	*Organization assessment, future UL 2900-3-1*	
	Physical locks on devices and their communication ports to minimize tampering, where appropriate	Clause 6	Clause 12.4
	Require user authentication or other appropriate controls before permitting software or firmware updates	Clause 11	Clause 12.4

MAPPING UL 2900 TO FDA GUIDANCE

FDA Guidance Section	General Description	ANSI/UL 2900-1 Clause Reference	UL 2900-2-1 Clause Reference
Cybersecurity Functions **Identify and Protect** ***(Ensure Trusted Content)***	Restrict software or firmware updates to authenticated code	Clause 4 Clause 11	Clause 12.4
	Use systematic procedures for authorized users to download version-identifiable software	Clause 11	Refer to UL 2900-1
	Ensure capability of secure data transfer to and from the device, including encryption considerations	Clause 4 Clause 11	Refer to UL 2900-1

MAPPING UL 2900 TO FDA GUIDANCE

FDA Guidance Section	General Description	ANSI/UL 2900-1 Clause Reference	UL 2900-2-1 Clause Reference
Cybersecurity Documentation **Detect, Respond, Recover**	Features that allow for security compromises to be detected, recognized, logged, timed, and acted upon during normal use	Clause 6 Clause 11	Refer to UL 2900-1
	Information to the end user concerning appropriate actions to take upon detection of a cybersecurity event	Clause 12	Refer to UL 2900-1
	Features that protect critical functionality, even in the event of cybersecurity compromise	Clause 12	Refer to UL 2900-1
	Methods for retention and recovery of device configuration by an authenticated privileged user	Clause 15 Clause 16	Refer to UL 2900-1
	Manufacturers may elect to provide an alternative method or approach, with appropriate justification.	Clause 6 Clause 12	Clause 6 Clause 12

MAPPING UL 2900 TO FDA GUIDANCE

FDA Guidance Section	General Description	ANSI/UL 2900-1 Clause Reference	UL 2900-2-1 Clause Reference
Cybersecurity Documentation **Detect, Respond, Recover**	Hazard analysis, mitigations, and design considerations pertaining to cybersecurity, including	Clause 12	Clause 12
	Specific list of all cybersecurity risks that were considered in the design of your device	Clause 12	Clause 12
	Specific list and justification for all cybersecurity controls that were established for your device	Clause 12 *Also verified through Penetration Testing:* *Clause 16*	
	Traceability matrix linking actual cybersecurity controls to the cybersecurity risks	Clause 12	Clause 12
	Summary describing the plan for providing validated software updates and patches as needed throughout the lifecycle of the device	Clause 11	Clause 12 Clause 20
	Summary of controls that are in place to assure that the medical device software will maintain its integrity from the point of origin to the point at which that device leaves the control of the manufacturer		Clause 12
	Instructions for use and product specifications related to recommended cybersecurity controls appropriate for the intended use environment	Clause 6	Clause 12

IN SUMMARY

- The FDA Guidance on the Content of Premarket Submissions for Management of Cybersecurity in Medical Devices includes several recommendations for cybersecurity
  - Security Risk Analysis
  - Security Design Principles
  - Security Documentation in Premarket Submission

- Devices and software intended for the US with network interfaces and/or connectivity requires evidence for the management of cybersecurity in the regulatory submission

THANK YOU!

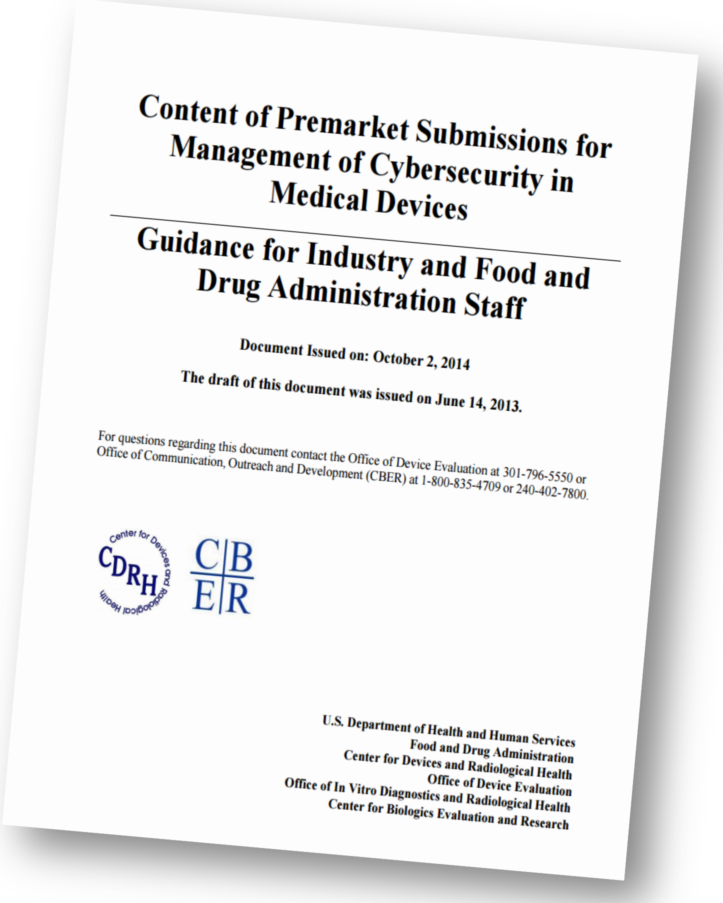
Justin Heyl
Improving your experience and success
Business Development Director
Health Sciences Division
P: 612-618-8797
www.linkedin.com/in/jheyl

APPENDIX:

PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL

The FDA Guidance on Cybersecurity is applicable to any device containing software or programmable logic, including software as a medical device.

Products that generate, store either temporarily or permanent, receive or transport any critical assets should be evaluated for cybersecurity risk.



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

The draft of this document was issued on June 14, 2013.

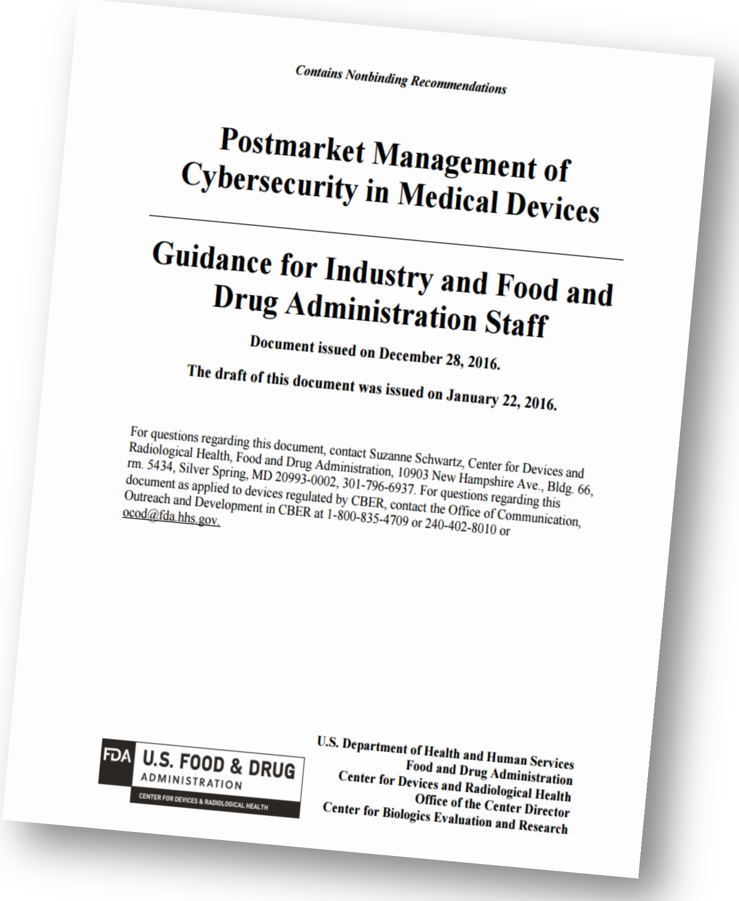
For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Device Evaluation
Office of In Vitro Diagnostics and Radiological Health
Center for Biologics Evaluation and Research

POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES

Guidance provides FDA recommendations for proactively managing cybersecurity for Postmarket devices and software.

The Guidance also clarifies manufacturer’s responsibilities for medical device reporting in the context of cybersecurity management



Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@fda.hhs.gov.

FDA U.S. FOOD & DRUG ADMINISTRATION
CENTER FOR DEVICES & RADIOLOGICAL HEALTH

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of the Center Director
Center for Biologics Evaluation and Research

MANUFACTURER'S RESPONSIBILITIES UNDER FDA GUIDANCE

The FDA does recognize that cybersecurity is a shared responsibility between all stakeholders in the healthcare ecosystem

- Device and software manufacturers
- Healthcare Delivery Organizations (HDO)
- Clinicians and providers
- Patients

MANUFACTURER’S RESPONSIBILITIES UNDER THE GUIDANCES

The FDA has established an expectation that medical devices support cybersecurity by analyzing risks associated with cybersecurity, including:

- Confidentiality
- Integrity
- Availability

MANUFACTURER’S RESPONSIBILITIES UNDER THE GUIDANCES

Manufacturers should address cybersecurity during the design and development of devices by establishing design inputs that inform needed mitigations for cybersecurity

Identify Assets	*Perform security hazard analysis*	*Identify security threats*	*Identify known vulnerabilities in design and technology*
Determine the likelihood of a threat or vulnerability being exploited	*Establish security risk acceptance criteria*	*Identify and implement appropriate risk mitigations*	*Assess residual risk associated with cybersecurity*