Response to NIST Workshop and Call for Position Papers[1] on Standards and Guidelines to Enhance Software Supply Chain Security[2]

Food & Drug Administration (FDA), Center for Devices and Radiological Health (CDRH) May 26, 2021

Cybersecurity is crucial for medical device safety and effectiveness. Critical functions are shifting from on-premises software infrastructure to distributed and remote infrastructure, including newly essential cloud services depended upon during the diagnosis and treatment of disease. Publicly noted cybersecurity incidents in 2021 include ransomware disabling the Irish Healthcare Service[3], ransomware disrupting a hospital for weeks[4], and a fundamentally new problem where ransomware remediation disrupted the cloud services necessary for critical function of cancer radiation therapy rather than simply disrupting electronic health record systems and other, more traditional hospital IT infrastructure[5]. Such increasingly common ransomware incidents highlight the ungraceful failure of perimeter-based firewalls and the safety consequences of not separating OT from IT by design.

This document is targeted towards providing relevant responses to the National Institute of Standards and Technology (NIST) call for position papers[6] to fulfill the President's Executive Order (EO) on Improving the Cybersecurity of the Federal Government (EO 14028), issued on May 12, 2021[7]. It highlights existing FDA guidance documents and international standards on the science of cybersecurity for the premarket review of medical device manufacturing and post-market surveillance of cybersecurity incidents and vulnerabilities. FDA urges NIST and the National Telecommunications and Information Administration (NTIA) to continue with and enhance their present approaches to the development of standards and guidelines for Operational Technology (OT) security by leveraging experts from across the public and private sectors. Increasing communications on existing science and engineering principles, standards, and guidance can translate into improvements in OT cybersecurity, which has a fundamentally different risk management calculus from traditional IT cybersecurity. This document summarizes established FDA practices and efforts presently underway for OT cybersecurity in the greater medical device security ecosystem and highlights the five areas NIST identified.

1. NIST's question on criteria for designating "critical software"

Software supply chain security is one essential part of managing risk to patients. The need for effective cybersecurity to ensure safe and effective medical devices has become more important with the increasing use of wireless, Internet- and network-connected devices, portable media (e.g., USB or CD), and the frequent electronic exchange of medical device-related health information. As a result, it is critical to our healthcare system that software that meets the definition of device in section 201(h) of the Federal Food, Drug, and Cosmetic Act (FDCA)[8] remains safe and effective, including cybersecure. In addition,

---

[1] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/workshop-and-call-position-papers

[2] For questions about this document, contact CDRH's Division of Digital Health at DigitalHealth@fda.hhs.gov or Kevin Fu, PhD (Acting Director, Medical Device Cybersecurity, FDA CDRH) at kevin.fu@fda.hhs.gov; Matthew Hazelett (Cybersecurity Policy Analyst, FDA CDRH), Suzanne Schwartz, MD, MBA (Director, Office of Strategic Partnerships & Technology Innovation), or Jessica Wilkerson, JD (Cyber Policy Advisor, FDA CDRH).

[3] https://www.nytimes.com/2021/05/20/technology/ransomware-attack-ireland-hospitals.html

[4] https://www.sandiegouniontribune.com/news/health/story/2021-05-14/scripps-ransomware-shutdown-hits-the-two-week-mark

[5] https://www.ajc.com/news/investigations/cyberattack-disrupts-cancer-care/EJWYPB3KNNEMDAJK2FW2HFULLM/

[6] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/workshop-and-call-position-papers

[7] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[8] On December 13, 2016, the Cures Act was enacted (Pub. L. 114-255) and amended the FDCA to state that the term device does not include software functions excluded pursuant to section 520(o)(1) of the FDCA. FDA made conforming edits to our classification regulations based upon this change in the FDCA (See 86 FR 20278).

software that does not meet the definition of device, but which supports or is relied on by devices, such as third-party software necessary to achieve the intended use of devices, hospital network software, programs, applications, mobile devices, cloud services, and certain Electronic Health Records (EHRs)/Electronic Medical Records (EMRs) where medical devices pull/push data directly as part of their intended use, are also critical to assuring devices are safe and effective. Safe and effective devices are essential to effective patient care and healthcare delivery, and thus, software is "critical software" generally (i) where it meets the definition of device and (ii) where the software is necessary for the safe and effective use of a device.

FDA has issued several guidance documents focused on software-related matters, including FDA regulation of and policies on Software as a Medical Device (SaMD) and Software in a Medical Device (SiMD), that may inform the definition of critical software[9]. The greater academic research community recognizes that the notion of software can extend into domains such as firmware in circuit boards, sensors, Central Processing Units (CPUs), Graphics Processing Units (GPUs), and peripherals; software abstracted behind the APIs of cloud services; software radios; and other software-reconfigurable hardware. Academic research community consensus papers on critical software include the Computing Community Consortium (CCC) white paper on embedded security and the MForesight white paper on OT security for manufacturing[10].

2. NIST's question on standards and guidelines for federal purchasing

There are many medical device security standards and guidelines to consider for purchasing decisions of acquiring technologies.

- FDA created the Joint Security Plan (JSP) in partnership with co-leads from Healthcare Delivery Organizations (HDOs) and Medical Device Manufacturers (MDMs) via the Healthcare Sector Coordinating Council (HSCC) for considering a total product lifecycle (TPLC) approach for medical device manufacturing[11].
- An FDA Fact Sheet dispels myths and communicates facts on FDA's role in medical device cybersecurity[12].
- FDA co-leads the International Medical Device Regulators Forum (IMDRF) and the JSP. These groups are working on coordination of the Software Bill of Materials (SBOM) intended to harmonize and bring greater consistency for cybersecurity across global medical device regulatory

[9] See Final FDA guidance on Software as a Medical Device (SAMD): Clinical Evaluation, December 2017 https://www.fda.gov/regulatory-information/search-fda-guidance-documents/software-medical-device-samd-clinical-evaluation; Final FDA guidance on Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act, September 2019 https://www.fda.gov/regulatory-information/search-fda-guidance-documents/changes-existing-medical-software-policies-resulting-section-3060-21st-century-cures-act; Final FDA guidance on Off-The-Shelf Software Use in Medical Devices, September 2019 https://www.fda.gov/regulatory-information/search-fda-guidance-documents/shelf-software-use-medical-devices; Final FDA guidance on Policy for Device Software Functions and Mobile Medical Applications, September 2019 https://www.fda.gov/regulatory-information/search-fda-guidance-documents/policy-device-software-functions-and-mobile-medical-applications; Final FDA guidance on Deciding When to Submit a 510(k) for a Software Change to an Existing Device, October 2017 https://www.fda.gov/regulatory-information/search-fda-guidance-documents/deciding-when-submit-510k-software-change-existing-device; Draft FDA guidance on Clinical Decision Support Software, September 2019 https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-decision-support-software. When final, this guidance will represent FDA's current thinking on this topic

[10] https://cra.org/ccc/wp-content/uploads/sites/2/2020/05/CCC_Embedded_Security_Report_final.pdf and http://mforesight.org/projects-events/cyber-security-for-manufacturers/

[11] See https://healthsectorcouncil.org/the-joint-security-plan/

[12] https://www.fda.gov/media/123052/download

frameworks[13].

- FDA guidance on medical device cybersecurity includes the final 2014 premarket guidance[14], the final 2016 post-market guidance[15], and FDA's proposed thinking in a draft 2018 premarket guidance to update the 2014 guidance[16]. FDA is targeting a late 2021 issuance for the revised draft premarket guidance for public comment.
- Existing general standards for medical device security include the Association for the Advancement of Medical Instrumentation (AAMI) TIR57 (Principles for medical device security - Risk management)[17], AAMI TIR97 (Principles for medical device security - Postmarket risk management for device manufacturers)[18], AAMI draft standard SW96 (Medical Devices - Application of security risk management to medical devices), and IEC/ANSI/ISA 62443-4-1 (Security for industrial automation and control systems: Secure product development lifecycle requirements)[19] among others resources[20].
- FDA has identified new premarket statutory authorities that would mitigate vulnerabilities throughout the total product lifecycle of medical devices. FDA's Medical Device Safety Action Plan of 2018[21] and the HHS FY20 and FY21 Congressional budget justifications[22] outline plans to consider potential new premarket statutory authorities to require firms to take steps on medical device security software updates and SBOM. These documents may be helpful to NIST when selecting standards, best practices, and guidelines acceptable for the development of software for purchase by the federal government per EO 14028, in particular Section 4(e)(i, ii, ix, and x).
- The HHS FY21 Congressional budget justification states: "Currently, there is no statutory requirement (pre- or post-market) that expressly compels medical device manufacturers to address cybersecurity. This proposal would advance medical device safety by ensuring FDA and the public have information about the cybersecurity of devices. Specifically, FDA seeks to require: that devices have the capability to be updated and patched in a timely manner; that premarket submissions to FDA include evidence demonstrating the capability from a design and architecture perspective for device updating and patching; a phased-in approach to a Cybersecurity Bill of Materials (CBOM), a list that includes but is not limited to commercial, open source, and off-the-shelf software and hardware components that are or could become susceptible to vulnerabilities; and that device firms publicly disclose when they learn of a cybersecurity vulnerability so users know when a device they use may be vulnerable and to provide direction to customers to reduce their risk. The proposal also seeks to improve proactive responses to cybersecurity vulnerabilities."

---

[13] See IMDRF/CYBER WG/NG60, Final document Principles and Practices for Medical Device Cybersecurity, issued March 2020; http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf

[14] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0

[15] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

[16] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices. When final, this guidance will represent FDA's current thinking on this topic.

[17] FDA has the ability to recognize certain consensus standards and provides a Supplementary Information Sheet in such circumstances which identifies the extent of FDA's recognition. Please see https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfstandards/detail.cfm?standard__identification_no=34082

[18] FDA has the ability to recognize certain consensus standards and provides a Supplementary Information Sheet in such circumstances which identifies the extent of FDA's recognition. Please see https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/detail.cfm?standard__identification_no=40251

[19] https://www.isa.org/products/ansi-isa-62443-4-1-2018-security-for-industrial-au

[20] https://www.fda.gov/media/123070/download

[21] https://www.fda.gov/media/112497/download

[22] FY2021 https://www.fda.gov/media/135078/download and FY2020 https://www.fda.gov/media/121408/download

3. *NIST's question on guidelines outlining security measures that shall be applied to the federal government's use of critical software*

We concur with NIST's goals of developing software-related standards and guidelines called for by EO 14028, especially for SBOMs and science-driven security testing. In FDA's 2018 draft premarket guidance on "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices,"[23] FDA proposed thinking on regulatory approaches for SBOMs, legacy software policies, and manufacturer responsibilities for providing regular software security updates. FDA's proposed recommendations emphasized SBOMs (then called Cybersecurity BOMS (CBOMs) to cover 3rd party systems and components with cybersecurity concerns regardless of a particular software or hardware embodiment) should include (1) traditional software (including firmware), (2) programmable logic, and (3) hardware. The draft guidance also outlined how CBOMs should enumerate commercial, open source, and off-the-shelf software and hardware components that are or could become susceptible to vulnerabilities. An SBOM is a part of a CBOM, which further includes risk management of hardware-centric third-party cybersecurity risks. In FDA's 2018 draft guidance[24], FDA proposed certain key elements of an SBOM for medical devices in support of consistency and standardization.

The AAMI TIR57 is an FDA recognized consensus standard on principles for medical device security - Risk management. The principles derive from the IEEE paper, "The Protection of Information in Computer Systems,"[25] which provides eight critical design principles for trustworthy software: (1) economy of mechanism, (2) fail-safe defaults based on permission, not exclusion, (3) complete mediation with every access checked for authority, (4) open design principle: do not depend on ignorance of attackers or security by obscurity, (5) separation of privilege, (6) the principle of least privilege (POLP) whereby a system uses the least privileges necessary to complete a function (e.g., user vs. root/supervisor), (7) least common mechanism to limit share resources that leads to side channel vulnerabilities (e.g., Spectre/Meltdown), and (8) psychological acceptability for usable security and privacy. NIST could consider this IEEE paper in thinking how to close the gap for OT cybersecurity in the federal government's use of critical software.

4. *NIST's question on initial minimum requirements for testing software source code*

FDA stood up threat modeling bootcamps[26] via a partnership with MITRE and MDIC[27]. Threat modeling provides a blueprint to strengthen security through the TPLC of the devices, thereby ensuring improved safety and effectiveness of medical products. Threat modeling helps to lay the groundwork for science-driven penetration testing and other downstream security testing as identified in the 2018 draft premarket guidance[28]. Both the 2018 draft FDA premarket guidance and AAMI TIR57 discuss the need for static and dynamic code analysis, penetration testing, and other technology to manage medical device security risk. Penetration testing is a point-in-time assessment against current, known security risks. Security testing carries the most scientific value[29] for yet unknown vulnerabilities when tied directly to design requirements and an explicit, refutable threat model and clinically relevant OT cybersecurity risks rather than solely

---

[23] See https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices. When final, this guidance will represent FDA's current thinking on this topic.
[24] *Ibid*
[25] Saltzer and Schroeder. "The protection of information in computer systems," In Proc. IEEE, 63(9), 1975.
[26] https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
[27] https://mdic.org/project/medical-device-cybersecurity-threat-modeling/
[28] See https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices. When final, this guidance will represent FDA's current thinking on this topic..
[29] Herley and van Oorschot. "SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit," In Proc. IEEE Symp. on Security & Privacy, 2017. https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/scienceAndSecuritySoK.pdf

unstructured searches for known vulnerabilities. Testing to failure (crashworthiness) rather than testing to "seems to work" produces more meaningful understanding of the limits of intrusion tolerance and graceful failure.

5. NIST's question on guidelines for software integrity chains and provenance

FDA has been involved with and supportive of the NTIA Multistakeholder work on SBOM since its inception. Many medical device and healthcare stakeholders, including FDA, have been instrumental in developing the schemas, formats, and other outputs from the NTIA process, and many such stakeholders are beginning to adopt these outputs. FDA would therefore strongly support NIST closely examining the NTIA work as part of their exploration of guidelines for software integrity chains provenance. FDA's post-market guidance on cybersecurity[30] recommends manufacturers adopt a coordinated vulnerability disclosure policy and practice. The FDA has recognized AAMI TIR97 and ISO/IEC 29147:2014 (Information technology — Security techniques — Vulnerability disclosure)[31] for techniques of vulnerability disclosure.

[30] See FDA's final guidance https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

[31] https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-1:v1:en