webinar we have our partners with us today Sunrise Labs thank you so much for joining us we have great content for you today we're going to be talking about cyber security in 2024 and Beyond there's there's a lot to cover um we have an hour for today's discussion and we are going to be saving some time for Q&A so please make sure to put that um in the Q&A function in the bottom of your screen at any time um questions arise to you um before I turn over to our panel just want to introduce myself I'm Nicole Owens from Mass medic if you're not familiar with our organization we are a medical device trade Association for companies primarily in the New England area um and we work to bolster the ecosystem through education and connection events like this advocacy and awareness all right as I mentioned um we have an awesome um panel for you today our moderator is Dave Hibbert he's the vice president of engineering for Sunrise labs and he's joined by an all our panel including shiv chastian he is the CTO of catellis biosystems and then his team as well from Sunrise Labs Christine Mason director of software and Nick Daniel senior principal software engineer so I'm going to turn it over today for the conversation and enjoy take it away all right thank you Nicole and thank you to mass medic for hosting us today it's certainly an honor to be here and be able to talk about cyber security and you know U just tell us tell people people what we know um so again uh my name is Dave hippard my role at Sunrise Labs is the VP of engineering um I'll just give a be brief overview of my background and then I'll let the rest of the team uh give their background as well but for me uh I've been working in the medical device industry my whole career so about 30 years now a little bit more than that uh I've worked both on the industry side and the services side um so I've worked with you know large manufacturers such as metronic and then services companies such as sun and then as far as different types of Technologies and products that I've worked on so I've spent quite a bit of time in image guided surgery and radiation oncology and kind of combining those two aspects together for positioning and for radiation delivery um I spent a fair amount of time working on parial dialysis and then fair amount of time uh also on insulin delivery looking at different types of pumps and um companion apps to along with those pumps so I'd like to each one of the panel to introduce themselves as well so uh sh maybe you can go next yeah thanks David um thanks Nicole and mass medic for um hosting us today my name is shiv Sabas I'm a CTO of citris um it's a startup Boston based startup it's a h MGH spin-off uh what we do is uh um remove skin in a scarless fashion and believe it or not it requires a lot of datadriven decision making and therefore there is a role for cyber security Even in our application uh as far as I'm concerned uh before that before this startup um I've been in the medical device industry for 20 plus years um I had my own startups I sold one I tanked one and then I had uh large company experiences with metronic leenova Phillips um and then I took a detour to Google and Google I was part of their machine learning team and uh at that time we also started working very closely with the FDA on their cyber security guidance so I've been kind of watching this journey of how cyber security has evolved over these years um I'm very excited to be here thank you Christine you want to go next I'm happy to so I'm Christine n director of software at Sunrise Labs I've been developing medical devices for over 20 years um at various layers of the software stack um but primarily in in the embedded space um the types of devices I've worked on um you know range two class two class three medical devices um with you know battery operated Technologies Wireless and fluid moving devices so in my current role um I work with this software group um to you know develop solutions for our clients and among them uh cyber secure medical devices which uh we're gonna get more into today thank you Christine

all right Nick awesome thank you Dave so my name is Nicholas Daniel I've been working primarily on medical devices but not just only in the medical space for about the last 15 years um my experience as it comes as it pertains to cyber security um I originally started working on devices early in my career that were some of the first generation medical devices to integrate network connectivity and that came with a whole host of challenges of understanding the cyber security space so that I could develop robust solutions to mitigate these risks which took me kind of all over of discovering this since this is primarily before any FDA guidance so hoping today I can share some of my experience and how that pertains to as in my current role where I'm architecting and designing uh secure and robust solutions for medical devices all right well thank you all for being here today um so why don't we go ahead and get started um so just to give a little bit of background information why we thought this was important so cyber security you know every day gains more visibility you see ransomware attacks and other attacks you see just um medical devices having issues problems again being attacked in various different ways and so more scrutiny and um really the whole cyber security field gets more and more complex um with each passing day so the FDA originally drafted some guidance um I think it's been almost about eight years now um but that was sent out as draft there's lots of feedback and a couple revisions that went there uh as well and then finally it was brought into law um in the CFR 8 820 about 14 15 months ago something like that but the final draft didn't really come out into the middle of uh last year so the final drafts final release guidance document really has been out for a few months now maybe six months or so and interestingly even yesterday as we were kind of talking preparing for uh this webinar we saw that they another draft guidance came out and it's really just a supplement to the the document that was released um six months or we go but the one thing that I found interesting in it uh just giving it a quick read is there are some some items where it said the FDA recommends blank or the FDA recommends you submit this document and now there's some of those recommends were changed to musts so again it's becoming more and more uh visible and more and more crucial I think to um the FDA submission and product development overall so with that with that said um i' like to kind of start out and and U maybe kind of start on you know how does one get started in cyber security and how does um what's the best place to start and really about timing so Christine maybe you can talk about a little bit about where to start uh the cyber security in the the product development life cycle and what's what's important and when yeah of course so yeah one of the key takeaways that uh I got from the guidance is that the cyber security should really be integrated into the total product life cycle so when you ask about when we should start um as early as possible um ideally even during um product conceptualization so I think as medical device U manufacturers developers we're used to incorporating safety risk management into um the whole development process and so security risk management really is is a form of you know risk management and so you know tr57 has this great diagram where where it shows security risk management paralleled with safety risk management and how they can affect each other and so um just early in the process we want to be incorporating cyber security so one of the first things you want to consider is your device um security risk profile now that can vary depending on the device um for a for example if you have a device that's let's say in a secure area a hospital it's not Network connected it's only going to be really accessed by doctors and nurses that's going to have a very different security risk profile than something that's a device that's in a patient home where you don't have uh control over the house Network or in a publicly accessed area so

those are things to consider the types of security requirements you want to think about early in the process so you know some of these examples of security requirements could be like you know do you need authentication is there patient data um private patient data that we need to keep confidential do we want to use encryption in our communication protocols so it's always great to incorporate cyber security early on it creates a more um cohesive solution um in architecture and so one of the ways that we can do this is to incorporate cyber security into your quality management system so qms um I think the FDA refers to you know the term secure product development framework but it's really a set of processes that incorporates Security Management into your whole product life cycle and that's going to look different for every organization um with a goal of you know you want to reduce vulnerabilities and make uh safer devices and so if you incorporate let's just say you incorporate cyber security after the fact there's a lot of downsides to that so first of all your your um you don't have a cohesive solution your security measures are more like patches or you know boltons it's it's not going to be um as efficient uh in addition let's say for example you discover you need secure boot you do your analysis too late well with secure boot typically you need encryption keys in your Hardware so that could make you want uh have to uh redesign your Hardware I mean there's a lot of um detriments to that right you've got your schedule your budgets and it's just something you want to incorporate early on so um to bring it back to your question you want to incorporate security um as early as possible okay thank you um so one of the one of the things that Christine mentioned was the environment um so maybe you want to talk about um some of the sort of environmental and maybe physical security concerns and how that could affect your overall architecture uh as you're starting to develop a product yeah sure um so the you know I think as Christine mentioned I think there's a whole bunch of con sitations from an architecture point of view um I think as far as you know physical and environmental are concerned I think you know it again comes down to fundamentally you know the issues around you know Access Control where you actually want to I mean of course everything depends on the type of your product right I think but at the end of the day you know you want to I mean this is more of an issue um when you have um you know essentially data coming out of your device and you essentially have other third parties and other locations where you actually storing your system where I think it kind of gets into a much more interesting conversation as far as you know the actual device is concerned I mean you just have to make sure that you know um there's not you know if somebody really wants to do something physically to your device there's not much you can do to stop it but I think you still want to make sure that you have the right kind of Access Control capabilities from a perspective if you have a software interface to have kind of multiactor authentication some kind of authentication system if you have a physical needs then you have to have something like you know like key cards and biometric access be able to have some sort of surveillance capabilities you know some sort of visitor Management in case of data centers and data that's kind of stored there um when it comes to environmental you know controls you have to you know I mean in general when you think about architecture you have to think about you know Disaster Recovery as just as a as a global principle and I think so I think whether it's related to power backups or whether it's related to climate control or or any kind of fire related issues fundamentally it all Ates back to how do you actually build resilience and redundancy in your system so fundamentally that's kind of what you're trying to do with these en controls so you know that's so that's typically what you have to think about when you're thinking about

environmental controls is you know how do you set up for Disaster Recovery how do you actually plan for backup and storage um how do you so those are the things that you have to kind of keep in mind um when it comes to I would say architectural elements as it pertains to physical and environmental safeguards thank you all right so Nick um kind of expanding on the architecture a little bit um so if you're starting to develop a system architecture and then break that down into a a software architecture what are some of the sort of the key considerations that you're looking at there and you know even in terms of operating systems and just the architecture as a whole yeah absolutely I'm gonna Echo a couple points already made which is understanding the use cases is a really big one um understanding the environments so that you can adequately build build appropriate controls understanding the use cases and the data flow and the purposes for all the data will let you better categorize your assets um doing so will let you better analyze your different attack surfaces and threat vectors um because the goal is the architectural phase is to design Out Security risks if we can design them out then we don't have to come up with unique or novel solutions for mitigations this is why it's so powerful doing this security analysis early is that you can avoid problems holistically which is a great Empower of the architecture which can't those Solutions often can't be bolted on later those ones that really design out the problems um but beyond that there sometimes uh based on the use cases of the device you might not be able to design out those problems uh you that is where you start looking into these security mitigations looking at the different assets you're protecting such as data where the data at rest motion and in use and making sure you're taking all the appropriate steps to control that that might be choosing authentication techniques that meets with your use cases um encrypting the data at storage and hardening your software systems to prevent against these type of attacks great thank you um so one of the other things that Christine mentioned was one of the fda's concepts of the secure framework um do you have any thoughts on how that's set up and um what what are some considerations in terms of that framework yeah so for as far as like the the security risk management Frameworks there's a few out there I I have my own preferences the ones I I typically stand to is uh tr57 that was one actually that Christine had brought up I really like the way they describe the risk management especially as somebody who's very familiar with 14971 which is generic medical device uh management it really puts it in the context of the risk management that we're very familiar with but steps into the space of secure uh cyber security where the probability of initiation is a little different and has to have different considerations so tr57 I think is really good um when it comes to actually conducting your risk assessment the one I draw on is the nist 830 I think it's a nice starting point for diving into all of the uniqueness that cyber security has as it comes to risk assessment so those are the ones that I typically draw to conduct the secure process as well as uh conducting my risk assessments though I will give honorable mentions to the iso 27k uh documents as well as copit and nist 853 there's lots of Frameworks out there I think that uh really to make your own process you really should read them all and understand the pros and cons that they all weigh and you can really make a very robust process and these documents explain not only how but why so those are very good documents okay fantastic um I think one of the things that we've kind of been hinting at here is jumping into one of the early phases which is threat analysis So Christine maybe you can kind of give a little bit overview of um how we connected threat analysis and maybe how we've Incorporated like the N standard into that threat analysis and do some of this for sure so so as for at sunrise for risk assessments for security we use the nist

800-30 that Nick mentioned so that's a guide for conducting risk assessments um as it's pertains to security so this this is a guide that's widely used in um many industry Industries and one that's actually recommended by the FDA so this guide it provides a structured um methodical approach to identify threats evaluate the risks and then um determine what kind of control measures we can put it in place to reduce risk um I see it a lot it's a very analogous to the FMEA process where the FMEA is based on probability um and severity of harms and that determines your risk and so for security risk it's really the exploitability with the with the severity of impacts now those impacts could be safety harms or business or reputation harms too and so uh one of the inputs or the input into the risk assessment is understanding what are your attack surfaces and a good way to figure out um what that is is to develop a threat model so a threat model is typically a diagram um that shows a system view of how that product um what that looks like in it's like ecosystem of use so it's it's going to describe you know what are your external interfaces um showing internal interfaces um where the assets or you know Keys um are located in your system and part of that is defining where your trust boundary is and that's going to depend on the risk profile theice but really what this threat model shows is your attack surfaces what are the entry points into the system and so that's the first step of your risk assessment so once you have your your tax service and I can just go to do a go overview of the kind of the different steps but not going to go into too much detail um so once you have your tax service the next thing is what are your threat sources and so that's identif who are your adversaries um are they outsiders with moderate secure knowledge um maybe they have like wire shark you know uh or do you have to worry about insiders I mean it depends on the risk profile device again it's going to vary um then you're going to identify threat events so think you know examples of this could be like uh denial of service from jamming or some uh sniffing data to read uh critical data U manal attacks things like that and then another Factor are identifying uh predisposing conditions um let's say you have to interface to a legacy system or a different another device and they only provide a certain interface to communicate and that communication is unencrypted well there's nothing you can do about that that's just it's part of the system but it should be factored um into risk so once you have that information um the next thing is determining the likelihood of these of these threat events occurring and you know that that's uh that's a difficult one to that one requires definitely someone with a lot of experience in this area and it can actually change over time depending on um new exploits and uh discovered so with all that information um what comes out of that is risk right you've got the exploitability the impacts and your risk and so at this point are the risks acceptable or unacceptable if they're unacceptable you've got to put in your security control measures um mitigations and you know some some examples of that could be you know adding encryption or doing Integrity checks on critical data or adding passwords to um a bios or the screen actually one of the attack surface you may not think of is a touch screen um worked on products where the service interface is available and if you don't if you can just go in there and you know change critical parameters that that's a definitely a huge concern and so um what comes out of that is is this is it do you have a password as a mitigation and ideally the password is unique to each device so at the end of it you have your residual risk after your mitigations and hopefully um at that point they're all acceptable so that's just kind of an overview of the process that we use here at Sunrise thank you so Nick one of one of the concepts that Christine mentioned was the trust boundary what how do you define a trust boundary and and identify that yeah trust boundaries are a little tricky you have to they're basically setting up a line

where you as a product have considered everything within this boundary as trusted so this as an example if you have a little box and you have external interfaces maybe you draw those trust boundaries just around the internals of your box to the point where we're no we're not going to worry about the security between one particular integrated circuit talking to another integrated circuit so we don't have to encrypt internal communication that might be a place where you draw the trust boundary though your environment in use cases could bury the box at loan might not be the trust boundary or it could extend past the box so if you have two systems that are communicating closely maybe your trust boundary includes both of those systems so it's mostly establishing a line where at this point anybody who crosses this line is considered trusted otherwise you will end up in this infinite Loop of finding your way all the way down to the circuitry of trying to protect those and you'll lose yeah basically diminishing returns after a certain amount thank you um so sh you know when you're creating a a threat model and trying to identify um all the attack vectors what are some of the difficulties that you've seen and um you know are advice that you have to try and make that a little bit easier and gain consensus between all the members because that's any risk management that's always the hardest part I think that's a I mean um I think I think the challenge of I think just building a threat model of course I mean I think um you've said it multiple times everything is use case dependent but I think the few I would say that three in over these years and across many different products um I think there's fundamentally I would say three really critical things that cause difficulty in creating a robust threat model um the first one is just the just the evolving cyber security threat landscape um you know you cannot prevent what you can't predict and uh and which means that your threat model is dynamic in nature you know so today you debate about what you have your product today and what it can do but you don't know what is out there in the in the wild when this product goes out so there's the debate is around how much can we predict uh today about what we're going to expect tomorrow and that's never easy you know uh unless you live in Arizona and you can predict every other day is a sunny day I mean you know that's not the case in cyber security um so there's that issue the second issue which I always find is a is a point of debate and also a point of I think I would say difficulty is as medical device manufacturers as companies go you know we always makes the decision of what do we build and what do we let's say buy so to speak and from that vantage point I think the issue is around you know the complexity in your device and the ability to do interoperability so every time you actually so complexity I defined in terms of the different components inside your medical device system um and every time you have an interface as Christine every time you have an interface now whether it's an internal interface whether you're let's say whether you're actually incorporating a software of unknown Provence inside your product all of these things then create these vulnerability points they create these attack surfaces that that you don't have full control on and you have to rely on your partners to provide the information or have the same level of commitment towards security um so there's so there's that issue of complexity which is I think more about how the system is built and then the other aspect of this is the interoperability with other external system so if you think about it in a healthcare provider setting where you actually have to deal with hospital it now yes we can ensure that our product is essentially secure but then it still has to interface with an EHR and EMR system that the hospital it controls so then having that interoperability again creates that vulnerability point that I think becomes again a topic of discussion of how do we actually create a threat model where we have a product that's let's say has soup components inside the

system has interoperability with external infrastructures so that's I would say the second difficulty in actually creating threat model um and I would say the third one uh which I think is you know is I think is equally important is I would say the I would say the diverse usage environments we talked about how you know you know different usage environments impact uh threat models and that's kind of the I would say the third critical component because you know again as medical devices go you can use them in your home and if you're using it in your home then you're connecting to an insecure uh Network then I think that again creates a vulnerability similar to you know your requirements for the same thing connecting to an hospital it network is different so different usage environments again create different kind of thread models but I would say that I think those three are I would say the top three issues that I've seen that people have debated and I think is there is there a right answer or a wrong answer no it's just very specific to the product depending on which product you actually trying to build and how much is your risk appetite and what is the true you know harm that you identified uh I think defines the path forward um but I would say that those would be in my mind probably the three main I would say difficulties that I kind of trying to summarize across all the products that I've built so far yeah I'm glad you mentioned um you know looking at other systems that may be involved and connected to yours because that that really does make a much more complex system than when you're just putting a product out by yourself so if you're trying to talk to possible information system it really um it really does complicate the issue uh one of the questions that came up while we were talking um I'll thr this one out to Nick but anyone can answer if they want to which is what is mandated by the by the FDA so if you the particular question was around are there standards that are mandated but um we mentioned some of the standards that are uh available uh to help guide you but is anything required and what is required just from a general sort of submission into the FDA yeah so uh the FDA doesn't call out a mandation to follow any particular standard but they are looking for you to follow a process so the standards that I listed like tr57 or ISO 27,1 these These are standards that kind of outly a typic a process that that you could follow um but I think as far as what the FDA is looking for is for you to document and describe your process to make sure you're meeting the intent of the guidance but your process is is kind of up to your own I think pulling these sources from all this information and making a complete story for your process to cover all your concerns is is the most important part yeah I think I'll just add to that is I think that I think something that we're working you know very closely with Sunrise as an example is I think you know so our quality management system essentially I mean like any other quality management system you know has the phase for you know requirements definition risk management right up front but most of the risk management as Christine was alluding to is focused on say safety risk assessment and um but I think having a very specific sop that's targeting cyber security risk assessment specific requirements around cyber security creating those kind of standard operating policies um and then following those policies through design through test um through documentation then kind of is what I think uh Nick alluding to by saying process so that's kind of the process that at least we as cers follow this is kind of how is is what you know companies that are dealing with data that are dealing with cyber security issues are are are doing is to incorporate Sops because at the end of the day Engineers follow you know design control processes if you want to create that attitude and that mindset of security by Design that has to be part of a policy okay uh and the other the other question that came in was kind of a long question so I'll paraphrase it a little bit but um this

question is asking about non-medical software um so maybe it's like n DDS or something like that that's interacting with a medical device uh and would you have different considerations there so I I think the first thing that I would say is the whoever developed the medical device software is certainly responsible for the cyber security of that device um but um I don't know Christine if you have a few thoughts on if you were developing something to interact with a medical device um you know again maybe it's like mpbs or something like that um would you follow the same process um and you know what would you see as maybe some major differences or even maybe there's only minor differences um that's a good question one of the things that I I think would be a little bit different maybe would be um the way you're doing the the risk assessment right so if it's not a medical device maybe you're not as concerned about patient safety right by definition it shouldn't be right but I think the process may be similar yeah I think the I would say the process has to be similar even if you're interfacing with a a medical device um and you're providing the let's say a software backend for example you know that's what the medical device Data Systems are you know that's why they're class one typically um mdds and the the thing though is that I think at the end of the day as I mentioned earlier about interoperability I think the accountability factor for cyber security when you are actually relying on Partners to work with has to be mutually agreed upon so I think you know you have to make sure that the data that's coming into your mdds system is somewhat encrypted right because I think you know you're because the data is getting shipped from a medical device to your mdds system so at least you have to ensure when the data is coming in what kind of controls can you establish for integrity checks as an example so these are things I think you will have to kind of Ensure it happens when the data comes in so I do not necessarily think that it's a different approach to security assessment and Security Management security planning and security incorporation but I think it's just the it becomes a shared responsibility model um where you are actually sharing the responsibility of cyber security with the devices that you're interfacing with and so an example here would be you know like it's the similar example that I can give when I let's say if I build a SAS platform and I'm working I'm developing it on Azure I'm developing it on AWS typically you have a business you know agreement addendums with these kind of companies right and these addendums are essentially the idea of hey I'm using your infrastructure to build my application so we have a shared responsibility for security and and so so that's kind of the idea that kind of that kind of goes along with you know any mdds system even though it's not MediCal software but it's still a a software that is supporting a medical application all right thank you um maybe one last question before we kind of move into the V&V but as we kind of wrap up um talking about sort of developing the product in the development phase that you would go through normally um maybe you can talk a little bit about how often You' sort of go back and revisit your threat model revisit any like known vulnerabilities that type of thing as you go through the development process yeah absolutely so some of the things for me that triggers me to Reit my risk assessment is kind of uh two different factors one is uh presumed use cases and features any changes to the product landscape or definition really should cause you to re-evaluate your risks you could have really changed your risk landscape by modifying use case or the features of the product so that would be stuff if I was making a new Alpha Beta where we or a version two we would re-review and go back through the process the other thing that really informs that is um and and is one of the recommendations of the FDA is to integrate um your monitoring of uh your software of unknown Providence or soup during your

development life cycle and some of the benefits of that is when you start seeing new cves or common vulnerability enumerations which are basically just uh reports of different vulnerabilities that exist in different software systems that if you are ingressing those and analyzing those the development phase they're better adequately describing the landscape of your software so if you see that you might see that that is a higher risk than you originally assumed and has different types of impacts so continuously monitoring for different vulnerabilities or different uh hazards that might exist those can continuously feed back into your risk assessment so ideally this is a continuous process that you're evolving as you get new information as you go all right um Christine sh any last minute comments on the development phase before we kind of hop over to some of the more vulnerability analysis and soup and things like that no I think I think think we covered this SP as well you can move to the next section all right so if we now jump into the EnV right so have your pro uh product process developed um you know you go through the implementation phase and now you're kind of getting into um how you're going to test this so um you know there's a bunch of things that are going to be required uh as part of your submission including an es bomb and vulnerability analysis um so Nick maybe you can talk a little bit about um um you know how do you evaluate soup um how do you find vulnerabilities that maybe in um components that you've Incorporated in whether it's an operating system or you know drivers or whatever that is um how you do vulnerability scanning yeah absolutely um so one of the very first steps is in order for to investigate and determine what kind of vulnerabilities is to really build a catalog of what you got without having an adequate understanding of the composition of your software components it you really won't be able to do a really in-depth analysis so kind of very first steps is looking at your systems and determining all the different software that's over under concern that doesn't necessarily mean software that you've written if you're using off-the-shelf Parts uh off-the-shelf hardware and you're just configuring it those are still points of concern so that we've been calling that the the security bomb for a software bomb uh so building that s bomb is a really important First Step um how you do that is going to be a little bit different per system uh different types of systems such as uh interpreted languages have really nice package managers that will output you a complete manifest of all the packages you're using other systems are a little bit more difficult where they don't use package managers and we have to use something called software composition analysis where we do we do almost open- Source fingerprinting of binary image is to find all the different types of uh soup that are in a system you'd be surprised often sometimes you'll have multiple of the same Library embedded in different parts of your systems all with different vulnerabilities so it's really important to get an accurate understanding of is what in is in your system uh once you have that accurate list one of the uh important thing of continuous monitoring is taking that list and looking to what are the reported an uh vulnerabilities and anomalies with those different libraries those will greatly inform uh how those impact your system uh you really will have to go through it in the first time it might be kind of a big uh list of vulnerabilities to analyze but you need to go through those one by one and understand the impact your system of every vulnerability after you've made that initial pass it may it gets a little easier because you're only looking at changes as they occur over a time uh but you need to do that first initial vulnerability scanning um once you have that es bomb my preference way is there are a lot of great tools out there especially if you generate your sbom into a format that is interoperable with other systems one example example is Cyclone DX that's a really nice format

that allows you to feed your sbom into different systems that can do vulnerability analysis by going to different databases of reported anomalies and ingressing all those data to give you a list of different vulnerabilities which you can then take and do a security analysis of how that impacts your system which is probably the most important part because while you might have a CVSs score or a condom vulnerability uh score that is very high that may not impact your system at all and have no relationship or you might have one that's very low that does directly impact your software and its safety profile so it's very important to go through and enumerate and and look into each one of these vulnerabilities um go ahead oh no as on on top of that there's other types of testing options that you might want to employ to impropriate during development such as uh continuous vulnerability scanning of your software through static analysis testing of the in of your interfaces and even potentially fuzz testing to try to catch boundary conditions so okay thank you um So Christine I don't know if you've have you seen tools for or techniques for storing the sbom um as part of the cyber security work that you've done um yeah what one consideration on on storing esums is you know that is part of your configuration management so um if you've have a configuration management plan um that should be discussed as how you are controlling that and the sbom is really a a blueprint to your software so it's really important to store the sbom in a high integrity secure location with uh limited access um because we you don't want this kind of information getting to the hands of your adversaries and so I I think that's an important consideration on storing as boms um yeah another aspect uh is making sure your sbom is complete you know it's obvious that libraries and packages are should be listed but um you know Docker images drivers firmware loaded on chips um it's it's it's important to think about all the software that's comprised in your system all right um sh I don't know if you can talk a little bit about just when you find some of the vulnerabilities that Nick was talking about like H how do you evaluate them how do you score them how do you how do you decide if it's something you need to address or something you can live with yeah it's a great question I think you know so there's as Nick mentioned so there's the process of I think you know identifying these uh you know these uh vulnerabilities and scoring them and then the other aspect of this is to how do you assess based on the severity and the score how does it impact your system I mean that is something that I think we've discussed a few times in a few different ways is I think it comes down to you know your system security risk so if you have a very well defined security risk plan and risk management and you know what you know if you've done that homework in your initial phase of your design then this is just a mapping exercise this you just look at you know the the the scores that you receive because again you know as Nick mentioned you know these databases exist you know these tools exist you know these tools run through existing vulnerabilities and assess if your system is exposed to it or not and gives you a score and you know you are the best person for your application you know exactly how it's going to impact your system so if you have your risk document you have this V abilities it's a comparison exercise um so I think it's it's it's no different than than the way people assess safety um it's the same process so at least that's that's I would say that's the simplest answer here so comes down to again you know doing your homework upfront and knowing your security vulnerabilities upfront so that when something shows up that sounds bad but it's like ity doesn't impact my system for one reason or the other um so we are not we are not doing any we are not storing any patient data so we're not worried about this encryption issue on the device for example so so it's it's a function of a thing the application okay um so

we're got about 15 minutes left but we before we kind of move on to postmarket I did have one more question for Nick which was um in terms of you mentioned fuzz testing so you know fuzz testing penetration testing so maybe you can define those a little bit and and kind of say what the goals are and is there a particular time where you think those are more important to to do than others or is there times where maybe you can do a lighter version of that testing yeah absolutely there's the since security is such a ever moving evolving topic more and more different testing strategies and testing tools are constantly coming out to help you evaluate the security risk of your product so like I mentioned fuzz testing is a is a great testing tool for interfaces to Just Produce random entropy of data to see how your system responds that doesn't necessarily mean it's it's an exploitable event but you might catch instances where your software misbehaves um so the fuzz testing will take externally interfaces and really just through them through a bunch of variability and make sure they're robust um that is something that can start very early it has really no prec uh preconditions other than you have the interface present in order to fuzz test it and it's one I'd recommend doing early um the other types of testing uh security related obviously when you're making your risk analysis you're going to have a bunch of mitigations that you're going to generate those are all going to be security level requirements and and they need to be tested and verified as well as any of the other requirements in your system so testing those security ones to show that if you have a risk of denial of service which might have additional risks to your product such as delay of therapy or any any other types of risk that those are tested and shown to be implemented um other types of testing I like to do on my product in order to get kind of ahead of the game is to do my own vulnerability scanning so there's open source tools out there such as or a metlo that allows you to point at interfaces and those cves that I was mentioning they also have a great database in these tools along with Python scripts or any other types of scripts that actually will exploit them so you can point these scanning tools at your product and look for the vulnerabilities yourself uh try to find them you might you might be surprised at what you find um but finally when you're getting to the later stages of your product I always recommend going through a third party to do penetration testing um that can be an engagement in varying levels uh you can go everywhere from what I call white box testing all the way to Black Box testing and even with gray box testing in the middle and what I mean by those box metaphors is that you provide the penetration testers with varying amounts of information for your system the goal is to get back as much actionable information as you can so going complete blackbox testing has some downsides of where the per it will take a lot longer but they are equipped with the same knowledge as most people would externally so you might get a more accurate representation but it takes longer providing clear box or gray box testing allows you give them requirements design details libraries which allows them to be more actionable and be more targeted in their testing um that's usually something I save uh and will probably engage periodically uh through the post of the device but those are kind of the varying there's probably more in there that I miss but those are kind of the high Lev ones all right thank you so I one question came in while we were talking I'll just kind of throw this out to whoever wants to to jump in but um the the question was do you have to do threat modeling floods testing or other types of testing if you don't store patient data on your device so I I would recommend um if your device falls into the Cyber device category of the medical devices then yes I I think that those do apply and I also think that fuzz testing even for a non-medical device is a great tool for testing robustness of interfaces to make sure there's a lot of unforeseen

circumstances in the world and with analog systems that you you can't always consider for so I think there are good robust strategies uh regardless of uh the different types of devices so I I would implore to use them they make a better product anyways even outside the cyber security space all right awesome all right well we have a few minutes left so I did want to um you know one last topic that I thought would be beneficial to talk about today is uh postmarket so um so maybe you can Define you know what what do we mean when we say postmarket obviously you've gone through development you've gone through your testing now you just put the do put it out there what what activities are you doing in the post Market um to try and keep the device secure uh as it gets more and more Acceptance in the field yeah so you know postmarket is um you know in this world of as we discussed evolving threat landscape right I think you know post Market is about you know looking at many different aspects of how you you know ensure that the safe use of your device uh and secure use of your device when it's in the wild and that entails a whole bunch of things um it starts by I think our ability to you know continuously monitor uh you know this the product and continuously be up toate with threat intelligence um and being able to know exactly you know if there's a new threat that has come up to be able to have the ability to scan for those understand those and then react to those um through updates and patches so which is essentially kind of the aspect of continu monitoring andth intelligence which is about I think vulnerability modeling monitoring as well as you know making updates and patches um to actually you know um prevent against them or protect against them despite our best efforts you know there's always a situation and that can arise uh and therefore postmarket um surveillance is also about how do you actually respond to incidents and how do you respond and manage those incidents um so having a good incident response plan and having the ability to collaborate with your stakeholders and notify them about breaches about security issues um is the importance of having an incident response plan and management that's one other aspect of this um we talked about these databases on vulnerability how did they come up uh well because when different companies and different folks faced these kind of cyber security threats they had to report right so there's a requirement around regulatory reporting and maintaining compliance so when you actually face a Cy security issue we have to have procedures in place to be able to report these things to the regulatory bodies so that again that adds to the database but also is important for us to be aware of these things and then and I think I would it also is about uh I think training and education um around around these things that I think is also making people aware that you know that you know there is you know we will have to do software updates you know walking into a hospital every 3 months and asking them hey hey I need your system to update the software is not something that anybody likes but that's the reality of the situation but can you do that remotely if you want to do it remotely then how do you want to do it so capabilities like that and things like that is what I would kind of consider consider as um as a postmarket surveillance uh in a broad scham I mean there's many things that have to be considered but I would kind of summarize it in that way right thank you um So Christine so should have talked a lot about the patches so I don't know you know maybe you can just talk a little bit about the process of how you would go about you know verifying a pat right so you you identify a vulnerability you have maybe an incident uh and then you need to get a patch out there so um what's what sort of activities would you revisit as you're preparing that patch um well certainly if you're changing the software you've got to make sure that you're not introducing any additional safety risk associated with that and of course there's going to be a

regression testing too so um that's where we have the the systems approach right with with with um security and safety um actually Nick I remember this the story you told about good example of where that could be but is um you decide you want to add encryption to a communication um interface but in doing that it uses more processing power and if you're on a battery operative device your life of the device is now reduced and that could be a safety risk so it's definitely important to think about um what kind of safety risks or maybe even other security risks that could be there and so ideally if you know automated testing is uh recommended so that when you're doing your regression it's not a huge lift and um looking at the vulnerabilities themselves sometimes the vulnerability is not related to your use case so if you have a library library does a bunch of things but you're only using this uh small intended use that's not affected by the vulnerability in that case to do that analysis um to to not unnecessarily have to do a Patrick because there's always a risk so uh those are some considerations and so um touching on what ship said it's very important to have a plan about how you're going to do the patch and and talking about how often you should be doing these monitorings um I ideally it's a vent driven so because um you know really important point is SEC your security Effectiveness is really correlated with how fast you can fix it so the longer the vulnerability is out there uh the more likely there could be an exploit so being responsive is is really important all right thank you well we're we're starting to get a little bit tight on time so I'll just kind of open it up and see if anyone has any last thoughts they want to uh other say otherwise um Nicole there was a question about um can we provide a list of standards that we mentioned in here so if we can maybe email that out afterward that would be good but but does anyone have any uh final thoughts before we wrap up and if not we'll we'll probably end up wrapping up I think we've gone through a lot there's a lot of areas we didn't touch on today either um you know there's there's a whole series of of postmarket things and submissions to the FDA which we didn't get into but um I hopefully you guys found this um informational and and if you do have questions you can always try and reach back out to Sunrise and we can help you with that uh but I think I'll turn it back over to h Nicole and we'll wrap up till we can finish up by one all right thank you so much what an awesome conversation um Dave is there a good email for folks to reach out to Sunrise if they have any questions uh Barb do you have a generic email that or an email that would be best or do you have a slide you want to flip to maybe that has the contact information there's a slide yep awesome there we go thank you so much everyone for joining us today thank you to our panel um really appreciate your expertise um just want to say thank you to Sunrise Labs um for sponsoring today's content we can't put on these expert panels without support of members like you so really appreciate that um please make sure to check out math.com and uh go to our events tab and see all of the great events we have coming up and we'll see you next time thanks so much take care thank you bye guys bye bye-bye