WHAT MEDICAL DEVICE VENDORS CAN LEARN FROM PAST CYBERSECURITY VULNERABILITY DISCLOSURES

An analysis of ICS-CERT cybersecurity disclosures reveals device vendors reported a more than 5-fold increase in disclosed advisories since the FDA released their Cybersecurity Guidance, a potential sign of vendors recognizing the benefits of vulnerability sharing.

Background:

In December 2016, the FDA released a guidance document entitled Postmarket Management of Cybersecurity in Medical Devices, in which the FDA makes several recommendations to medical device vendors and healthcare delivery organizations on how to manage the cybersecurity risk that connected medical devices introduce. One of the recommendations is for device vendors to participate in cyber risk information sharing, in which information about security vulnerabilities is shared with the medical device community via Information Sharing Analysis Organizations (ISAO). Two of the presumed benefits of vulnerability sharing are that 1) industry stakeholders have the information necessary to minimize their cybersecurity risk and 2) enable the larger community to understand and be proactive about emerging risk potential.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has played a critical role in bringing visibility to emergent vulnerabilities by building a repository for medical device manufacturers to communicate with customers. Whether you're a VP, Director, Engineering & Research Professional, or anyone else involved in ensuring cybersecurity best practices are maintained in medical devices, this may inform decisions around product cybersecurity.

*This is an updated version of our 2018 whitepaper analyzing trends in cybersecurity vulnerability disclosures that includes disclosures through 12/31/2019.

A Note On The Inclusion of Vendor Names:

It should be noted that the authors of this paper consider the inclusion of a specific medical device vendor's name in the list of companies below to be a positive indicator of their active management of cybersecurity risk. No piece of technology is completely devoid of cybersecurity risk, and so any manufacturer of a technology product should be expected to have to deal with managing cybersecurity vulnerabilities in their products from time to time. Medical device vendors who actively disclose and address cybersecurity vulnerabilities should not necessarily be seen as negligent for having a cybersecurity vulnerability, but rather should be applauded for embracing the disclosure and sharing process.

SECTION I: DATA

The ICS-CERT Advisory Database was analyzed to find all advisories related to medical devices. In total, 78 advisories were released between October 2013 (issuance of first medical device advisory by ICS-CERT) and December 2019, consisting of a total of 179 cybersecurity vulnerabilities. Advisories were extracted and divided into two time frames—before and after the FDA Postmarket Management of Cybersecurity in Medical Device Guidance (which was finalized on December 28, 2016). Among the data points examined is the Common Vulnerability Scoring System (CVSS) score that has been assigned to vulnerabilities within an advisory.

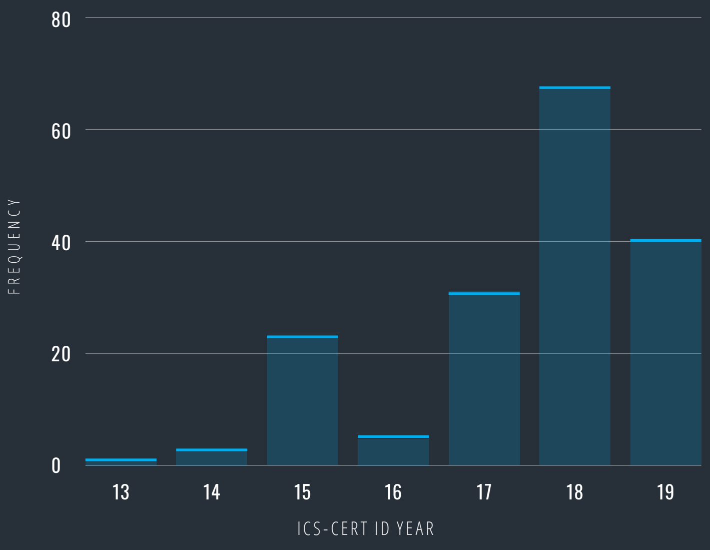
VULNERABILITY DISCLOSURE FREQUENCY

	Oct. 2013 – Dec. 2016	Jan. 2017 – Dec. 2019
Number of Advisories	12	66
Total Vulnerabilities Disclosed in Advisories	37	142
Average Vulnerabilities Per Month	.95	3.94
Companies (advisories issued)	Animas, Baxter, Carefusion (2), Hospira (5), Philips (2), Smiths Medical	Abbott Laboratories (2), B. Braun, BeaconMedaes, Becton, Dickinson and Company (7), Biosense Webster Inc./Johnson & Johnson, BMC, Boston Scientific, Carestream, Change Healthcare (2), Dräger, ENEA/Green Hills Software/ITRON/IP Infusion/Wind River, Ethicon Endo-Surgery/ Johnson & Johnson, Fujifilm, GE (2), i-SENS, Medtronic (9), Natus Medical, Inc., Philips (20), Qualcomm Life, Roche, Siemens (3), Silex Technology/GE Healthcare, Smiths Medical, St. Jude, Stryker, Vyaire
Mean Vulnerabilities CVSS Score	7.3	6.83

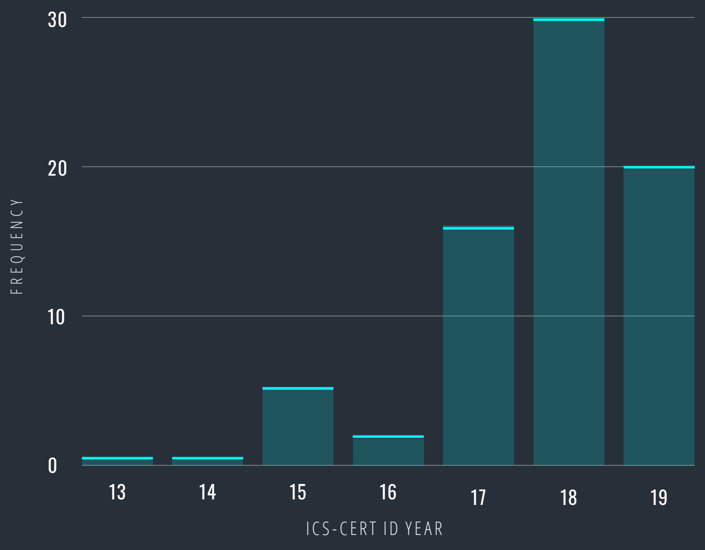
For the period after the FDA guidance was issued it is noted that the version of CVSS methodology used was consistently version 3.

Note that during 2019 one vulnerability stood out as being unique, ICSMA 19-274 (Urgent/11), as it described a set of vulnerabilities of a third party software product rather than an actual finished medical device. We did not change our methodology because of this single occurrence, but wanted to clarify this to the readers' benefit.

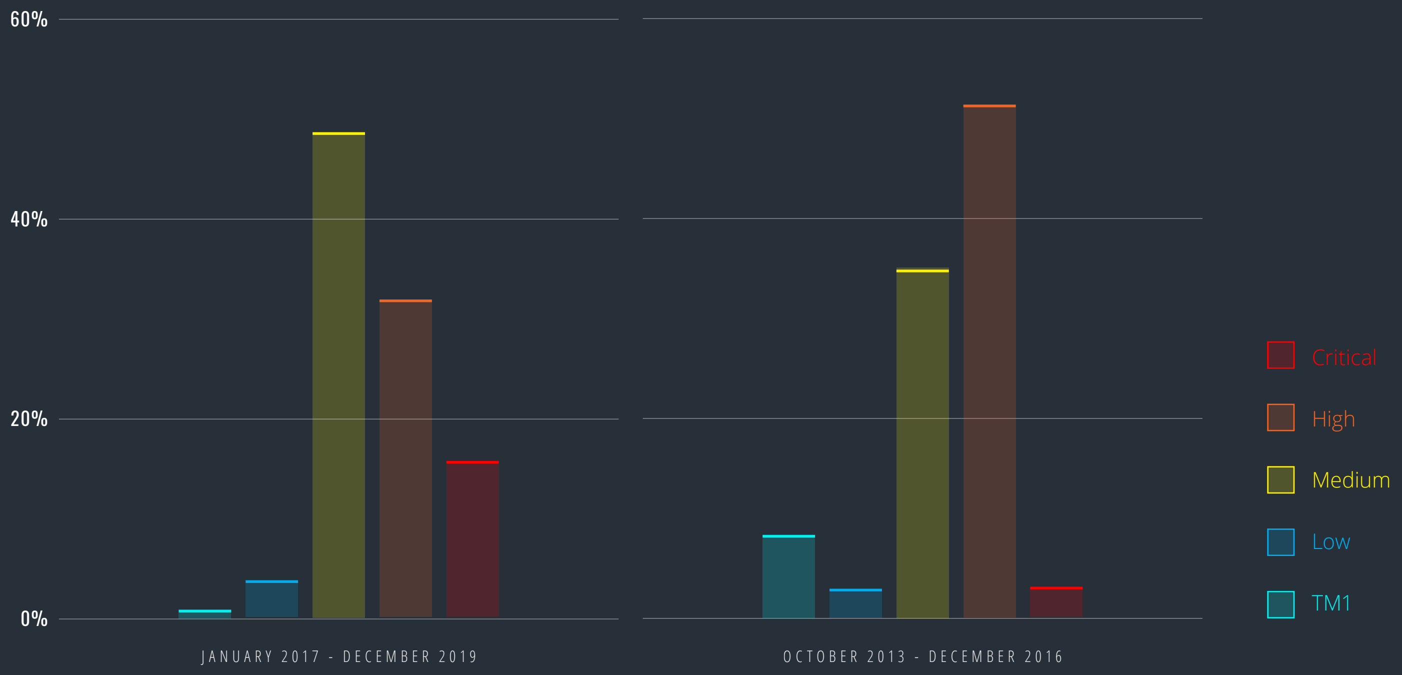
VULNERABILITY FREQUENCY VS. ICS-CERT ID YEAR



ADVISORY FREQUENCY VS. ICS-CERT ID YEAR



Since the release of the FDA Postmarket Guidance, the number of published vulnerabilities has remained high with an average of 3.94 vulnerabilities being released per month, compared to 0.95 per month prior to December 2016. Specifically, applying the National Vulnerability Database (NVD) criteria, details of which are included in Appendix A, the number of vulnerabilities disclosed were expressed as a percentage of the total vulnerabilities disclosed for a time period. The timing of FDA guidance demonstrates a pivot point after which there was a large increase in critical & medium disclosures, along with a decrease in high risk vulnerabilities disclosed.



TM1 - These line items within an advisory were excluded as they did not include the detailed CVSS score, had too many CWEs to assess as a collective or did not reference a related CVSS version in scoring.

VULNERABILITY CAUSES

We attempted to sort the disclosures into eight categories of technological root causes. While many of the vulnerabilities have aspects of multiple categories, we've attempted to match each common weakness enumeration (CWE) (or common vulnerability exposure (CVE) if a CWE was not referenced in the advisory) with one category. (Please see Appendix B for an explanation of each category.)

Attributed Root Cause	Oct 2013-Dec 2016 Totals	Jan 2017-Dec 2019 Totals
Code Defect	5	45
Encryption	8	10
O.S. Vulnerability	1	10
System Configuration	4	12
Third Party Library	3	4
Third Party Encryption		2
User Authentication	16	55
Misc		4
Grand Total	37	142

SECTION II: OBSERVATIONS ABOUT DISCLOSURE FREQUENCY

DISCLOSURES REMAIN HIGH

Subsequent to the FDA guidance release there was an increase of advisories as well as vulnerabilities with the number of advisories being 5.5 times higher and the number of vulnerabilities 3.8 times higher. A hypothesis presents itself here—has there been an increase in the number of vulnerabilities manifesting in devices? Or has the assistance of the FDA helped the industry move up the cybersecurity maturity curve? It is evident that the increase is attributable to the diligent persistence and willingness to partner that medical device manufacturers have worked to implement.

For example, Philips, the only medical device manufacturer to issue an advisory in 2013, has issued 22 advisories: two advisories with one vulnerability each before the FDA guidance and 20 advisories collectively including 42 vulnerabilities since. The trend to disclose more is perhaps demonstrative of a maturity in product security assessments.

FEWER DISCLOSURES IN 2019 THAN 2018

One would expect the number of disclosures to steadily increase, or at least remain at the same high level, until the vast majority of manufacturers have mature disclosure policies in place. The decrease in frequency may have a number of reasons, for one, it could be a sign that the FDA's "carrot" approach to motivating manufacturers to adopt voluntary disclosure practices is not having the intended effect, which could explain the FDA's comments that they may be considering a "stick" approach in the future.

SOME COMPANIES HAVE YET TO ISSUE AN ADVISORY

Comparing the list of companies who have made disclosures against a list of device vendors ranked by market cap, 11 of the top 40 medical device vendors have ever made a vulnerability disclosure through the ICS-CERT system. In reviewing the product offerings of the top 40 medical device vendors it was noted that only 12 seem to not offer a product that in some capacity uses a computer or is connected to a health system. That leaves 17 top medical technology vendors offering connected devices that have never made a disclosure.

There are three main (valid) reasons a medical device vendor would never have made a disclosure.

1. Their device is not network-enabled / computerized
2. Their devices have no vulnerabilities
3. They have never been made aware of or discovered a vulnerability

Further, of the 66 advisories since December 2016, more than half (36) came from three companies alone, demonstrating a high degree of security maturity with these organizations.

Vendors who have yet to issue an advisory due to reasons (2) and (3) should continue to ensure their product development protocols include proper cybersecurity premarket and postmarket monitoring.. We also suggest that vendors in this situation to consider collaboration with a cybersecurity company, perhaps through a formal "Bug Bounty" program, like those described here.

To address reason (3), device vendors should publish coordinating disclosure processes online in the event someone needs to alert the vendor of a vulnerability. Of the top 40 medical device vendors, 13 have published a vulnerability disclosure process and provide a PGP Public Key to encrypt email submissions. Of those 13 with disclosure processes, 7 have not made a vulnerability disclosure through the ICS-CERT database, revealing that a previous vulnerability disclosure is not perceived as a prerequisite for developing a vulnerability disclosure process.

There are other ways the healthcare community is normalizing disclosures. At DEFCON 27, a notable annual hacking conference that takes place in Las Vegas, the biohacking village welcomed attendees to test the security of medical devices in the Medical Device Lab. Medical device vendors were given the opportunity to bring in devices for the participants to test. Upon entering the Medical Device Lab, attendees sign a form agreeing that if they find a vulnerability in a device, they will disclose it to prioritize patient safety and help device vendors improve the security of their devices. This kind of collaboration between medical device manufacturers and the hacker community demonstrates a shift in healthcare culture in which sharing and discussing vulnerabilities is not something to conceal, but something to encourage. Changing the culture surrounding vulnerability disclosures may contribute to the changes in participation rates.

CERTAIN CLASSES OF DEVICES ARE UNDER-REPRESENTED IN LIST OF ADVISORIES

There are certain classes of medical devices that are conspicuously absent from the collection of ICS-CERT advisories. One would expect to see a uniform cross section of the networked medical device market represented in the database, yet the advisories tend to focus on specific device classes, like pacemakers, insulin and infusion pumps, and imaging systems. Outside of advisories issued by GE and Philips, there seemed to be a under-representation of advisories relating to other classes of devices, including but not limited to surgical robotics, diagnostics, radiation oncology, PACS systems and clinical decision support systems. We expect to see advisories affecting these classes of devices in the future.

SECTION III: OBSERVATIONS ABOUT VULNERABILITY CAUSES

USER AUTHENTICATION IS A COMMON PROBLEM

Vulnerabilities attributed to user authentication and code defects each covered 73.5% of the vulnerabilities included in the ICS-CERT advisories after January 1, 2017, an increase from 62.5% in the period prior. It is possible that user authentication vulnerabilities are the most commonly reported because it's **literally the first thing a penetration tester would interact with**. If this is true, we would expect to see future advisories focus on deeper "layers" of the technology stack as medical device cybersecurity matures. Possible areas of focus for future advisories include network communications and data storage.

MANY ADVISORIES LACK TECHNICAL DETAIL

One of the assumed goals of cybersecurity Information Sharing is to enable medical device vendors to learn from, and avoid the cybersecurity vulnerabilities found in other vendors' medical devices. In order to learn from a cybersecurity vulnerability disclosure, one needs sufficient technical information on the source of the vulnerability in order to avoid that same mistake in one's own product. Many of the ICSMA advisories lack sufficient engineering detail to achieve this goal.

The technical granularity offered in an advisory is a combination of CVSS vector scoring and the detail in a CVE detail report. In some instances like CVE-2017-2852, a referenced TALOS report provides tactically useful information. However, this granularity appears to be the exception, rather than the norm. The type of information needed for an engineer to determine implementable changes is rarely seen in these advisories. Furthermore, the timeline from identification, assessment and publication makes it challenging for medical device manufacturers to learn from disclosures and implement changes without giving a threat actor ample time to exploit.

ROLE OF RESEARCHERS

Of the 179 vulnerabilities assessed, 114 explicitly referenced a researcher being involved in the identification of the vulnerability. While the role of researchers can be controversial, their attribution to 64% of the vulnerabilities assessed confirms their presence in the ecosystem. This is not meant to imply that researchers were not involved in other ICS-CERT vulnerability disclosures, only that researchers were referenced in 28 vulnerabilities prior to FDA guidance and 86 since the guidance was issued.

CONCLUSIONS FROM DATA ANALYSIS

1 Various mediums to provide disclosures to the community will dilute the ability to determine a holistic view of device security at a particular health system.

2 Hyperbolic headlines will continue to disincentivize medical device vendors from disclosing more than the minimum absolutely required.

3 The volume of data being available through the software bill of materials, while reflective of a more robust software supply chain management practice, is not yet usable by HDOs.

4 Collaborative relationships with security researchers will bolster the frequency of vulnerability disclosures from medical device vendors.

PREDICTIONS & EXPECTATIONS

1 A single source of reference should be endorsed as part of the regulatory guidance to ensure vendors are equally incentivized, and not negatively penalized, for sharing vulnerability disclosures proactively.

2 HDOs will not be able to digest, action and respond to data shared by vendors. Increased reliance on security by design compared to patching.

3 Certain device types will continue to not report on vulnerabilities as they cannot be readily accessed by researchers / rely heavily on HDO firewall configuration / mitigations.

DISCLOSURES

The authors of this paper are employed by MedCrypt Inc, a medical device cybersecurity software developer.

Thank you.

Axel Wirth, CSS
axel@medcrypt.com

Vidya Murthy
vidya@medcrypt.com

Kate Schneiderman
kate@medcrypt.com

Published Jan, 2020

APPENDIX A

ASSESSMENT ON CVSS VERSION IMPACT

CVSS transitioned from version 2.0 to version 3.0 during the period from October 2013 to December 28, 2016, the details of which are outlined below.

CVSS V3 RATINGS

1. Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9.
2. Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.
3. Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-8.9.
4. Vulnerabilities will be labeled "Critical" severity if they have a CVSS base score of 9.0-10.0.

CVSS V2 RATINGS

1. Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9.
2. Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.
3. Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

The advisories under review were bucketed into qualitative ranges based on the NVD criteria outlined below. Where a version of CVSS was not referenced or hundreds of vulnerabilities were included in a single advisory (see TM1 in raw data), these were excluded from the assessment.

Timeline Relative to FDA Guidance	Critical	High	Low	Medium	TM1	Grand Total
Jan 2017- Dec 2019	13	27	2	42	1	85
Oct 2013 - Dec 2016	1	19	1	13	3	37
Grand Total	14	46	3	55	4	122

The assessment of the new version by Omar Santos, Cisco, predicted in 'The Evolution of Scoring Security Vulnerabilities', an increase in high and critical findings under version 3. The medical device advisories demonstrated a shift in more medium categorizations between version 2 and 3 (see table below). This may be an indicator that even with an increase in vulnerabilities reported, the reported vulnerabilities were lower risk, perhaps further corroborating alignment with fewer technical findings.

	Version 3 Count	Version 3 Percentage	Version 2 Count	Version 2 Percentage
Critical	23	16%		
High	47	32%	17	61%
Medium	72	49%	10	36%
Low	5	3%	1	4%

Specifically as outlined in Appendix B, the common vulnerabilities (CWE IDs) anticipated to cause increases are buffering and user authentications, which are notably attributed as the root cause for many of the medical device advisories.

APPENDIX B

DESCRIPTION OF VULNERABILITY CAUSE CATEGORIES

Code Defect: Can be described as imperfect implementations of otherwise secure software designs. An example of a code defect would be a Buffer Overflow. Many of these defects can be identified in the verification and validation process using tools like Static Code Analysis and Fuzz Testing.

Encryption: The lack of encryption of sensitive data, or vulnerabilities in the way this encryption is implemented, can leave devices and data vulnerable to attack. Common examples are storing user credentials in plain text, storing encryption keys in an insecure fashion, or vulnerabilities discovered in the underlying encryption software and algorithms.

Operating System Vulnerability: Many medical devices include computers running retail operating systems, like Microsoft Windows. These operating systems are regularly found to have vulnerabilities unrelated to the medical device itself, but that can affect the function of the device if left unpatched. One example would be the March 2017 "EternalBlue" vulnerability in Microsoft Windows handling of SMB transactions.

User Authentication: Failure to require user authentication for critical functions, or vulnerabilities in the way users are authenticated, can leave devices susceptible to attack. One common example is the use of "hard-coded" user credentials used across a fleet of devices.

System Configuration: Connected medical devices and their underlying software systems can be designed "securely", but configured in a way that leaves a device susceptible to attack. A common example is failing to disable unnecessary OS services and block all unused ports.

Third Party Library: Medical devices frequently rely on third party software for critical functions, which can be found to have vulnerabilities. One example would be a medical device including a version of a database server application found to have a publicly disclosed vulnerability.

Third Party Encryption: Use of a third party hard- or software component that demonstrated a weakness related to its encryption algorithm. (e.g. OpenSSL)

Miscellaneous: Disclosures that did not fit into one of the above categories were labeled "Miscellaneous."

APPENDIX C

DECREASE IN CVSS MEAN

Three instances of hardcoded account passwords were noted across two vendors, as outlined in the table below. Hospira issued their disclosure in June 2015, and GE in March 2018, and as evident in the table below the ratings were consistent regardless of CVSS version and timing before or after the FDA guidance was issued. The CVSS Vector String has been included as well, as it represents the value assigned to each metric as the vulnerability was assessed. The difference in the hardcoded password between the vulnerabilities can be attributed to the change in version and questions included by CVSS.

Code	Vendor	Product Description	CVSS Score	Vulnerability Description	CVSS vector string
ICSA15-125-01B	Hospira	Infusion System	10 (v.2)	Hardcoded accounts may be used to access the device	AV:N/AC:L/Au:N/C:C/I:C/A:C
ICSA15-161-01	Hospira	Infusion System	10 (v.2)	Hard-coded accounts may be used to access the device.	AV:N/AC:L/Au:N/C:C/I:C/A:C
CSMA18-037-02	GE	Imaging Services	9.8 (v.3)	The affected devices use default or hard-coded credentials.	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A second comparative to assess seemingly similar vulnerabilities released by different vendors with different scores was noted, upon inspection of the CVSS vector string, to have different values for multiple metrics (highlighted in yellow below).

Code	Vendor	CVSS Score	Description	CVSS vector string
18-165-01	Natus Medical	10	A specially-crafted packet takes advantage of the way the program parses data structures and may cause a buffer overflow, which may allow remote execution of arbitrary code.	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
18-156-01	Philips	8.2	The vulnerability exposes an "echo" service, in which an attacker-sent buffer to an attacker-chosen device address within the same subnet is copied to the stack with no boundary checks, hence resulting in stack overflow.	AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:L/A:H

APPENDIX D

NIST-CSF TO ICS-CERT ROOT CAUSES

Understanding guidance for issuing an advisory is at the discretion of the vendor, the NIST-CSF leading industry methodology was assessed against the root causes in the ICS-CERT advisories in this whitepaper. By understanding the diversity of NIST-CSF subcategories resulting in vulnerabilities, 10 unique subcategories out of 108 subcategories were related to the root causes identified.

Advisory Root Causes	**NIST-CSF Subcategory**
Code Defect	PR.DS-4: Adequate capacity to ensure availability is maintained
Encryption	PR.DS-1: Data-at-rest is protected
Encryption	PR.DS-2: Data-in-transit is protected
Operating System Vulnerability	DE.CM-4: Malicious code is detected
System Configuration	DE.CM-4: Malicious code is detected
System Configuration	DE.CM-5: Unauthorized mobile code is detected
Third Party Library	ID.RA-3: Threats, both internal and external, are identified and documented
Third Party Encryption	ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
User Authentication	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
User Authentication	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi- factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
Misc (noted to be mostly physical access)	PR.AC-2: Physical access to assets is managed and protected
Misc (noted to be mostly physical access)	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events