The MARYLAND
HEALTH CARE COMMISSION

Cybersecurity

A Self-Assessment Readiness Tool

May 18, 2017

(Version 1.0)

Introduction

In response to an increase in cyber threats, health care organizations (organizations) are encouraged to assess their cybersecurity readiness. Cybersecurity readiness is essential for organizations to maintain their information technology (IT) system(s), sustain operations, protect against current and future cybersecurity threats, and respond to and recover from a cyber-attack. Cybersecurity is not limited to the cyber-environment, but encompasses the people, processes, policies, and technology that contribute to an organization's overall cybersecurity readiness. In response to growing cybersecurity concerns, the Maryland Health Care Commission (MHCC), in collaboration with stakeholders, developed a *Cybersecurity Self-Assessment Tool* (tool) to assist organizations with assessing their cybersecurity readiness.

This tool uses select elements from the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).[1] The NIST CSF was developed through a collaborative process with experts in the federal government and private sector to create standards for assessing cybersecurity risks. Users of the tool are encouraged to review the NIST CSF to learn more about the cybersecurity safeguards recommended by NIST at: www.nist.gov/cyberframework.

The tool consists of a series of self-evaluation statements intended to help organizations identify potential gaps in cybersecurity readiness. The statements are grouped into people, processes, policies, and technology and each statement contains industry best practices source information adopted by the NIST CSF. *Results from the tool can help inform organizations about the adequacy of existing cyber protections and does not constitute legal advice.*

Instructions

Assess the organization's cybersecurity readiness by selecting the option that most accurately reflects the organization's readiness for meeting best practices:

Implemented: Formal processes are established and standardized across the organization.

Needs to be implemented: Formal processes have not been adopted by the organization.

Not applicable: Not applicable to the organization.

[1] The Cybersecurity Self-Assessment Tool uses the functions, categories, and subcategories developed by NIST. Descriptions in this document contain language used in the "Framework for Improving Critical Infrastructure Cybersecurity Version 1.0" developed by NIST. A copy of the document can be accessed at: www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

#	People	Process	Policy	Technology
1	Cybersecurity[2] roles and responsibilities have been identified and communicated to employees and third-parties[3] • Sample compliance: Business Associate Agreements executed with third parties, and employee roles detailed in Employee Handbook and training ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source[4]: ID.AM.6	The organization has mapped how information and data moves through the organization • Sample compliance: Workflow charts for communication and data transmission processes ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.AM.3	The requirements and protocols for response and recovery have been identified and communicated to employees and third-parties • Sample compliance: Cybersecurity incident response, business continuity, and disaster recovery plans, documented roles and training for employees, Business Associate Agreements for third-parties ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.BE.5	Physical devices, information technology systems (IT systems)[5], and software owned by the organization have been inventoried • Sample compliance: Catalogue of all computers, mobile devices, electronic medical devices, printers, scanners, fax machines, copiers, any machines stored off site that are accessed virtually by the organization, programs installed on computers, and electronic health record systems ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.AM.1, ID.AM.2

[2] The technologies, processes, and practices that are designed to protect the cyber environment of a practice's critical infrastructure.
[3] Include suppliers, customers, and partners that provide information system development, information technology services, outsourced applications, and network and security management.
[4] See Reference Information on page 18.
[5] Composed of the computers, mobile devices, electronic medical devices, printer, copiers, scanners, fax machines, and machines that are stored outside of the organization that are accessed virtually (virtual machines).

#	People	Process	Policy	Technology
2	The mission, objectives, and activities of the organization have been established and communicated to employees and third-parties, as appropriate • Sample compliance: Company Operation Manual, Employee Handbook, and memorandums of understanding, Business Associate Agreements, and contracts executed with third-parties ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.BE.3	The importance of all IT systems, software, data, and employee and third-party roles to the organization's operation are established • Sample compliance: Business impact analysis and risk assessments to identify the impact and criticality to the organization's operations for all hardware, devices, data, and software ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.AM.5	Cybersecurity policies are continuously tested to determine their usefulness against new and emerging threats and how well they comply with industry best practices, which are continuously improved through incorporation of lessons learned • Sample compliance: Mock drills, business impact and disaster recovery reports are generated and reviewed, and IT Operations Manual are updated with lessons learned ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: DE.DP.3, DE.DP.2, DE.DP.5, PR.IP.7	A catalogue of any IT systems that are not owned by the organization exists and is kept up to date • Sample compliance: A catalogue of all computer devices, wireless networks, and cloud services that includes information on ownership and maintenance ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.AM.4

#	People	Process	Policy	Technology
3	All senior organization leaders computer system security personnel, employees, and third parties have received training and demonstrate understanding of their role in protecting against, detecting, and responding to cybersecurity events[6] • Sample compliance: Employee Handbook, position requirements, employee training program including testing and exercises, signed contracts, memorandums of understanding, Business Associate Agreements ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.AT.1, PR.AT.2, PR.AT.3, PR.AT.4, PR.IP.11, DE.DP.1, RS.CO.1	There is an established baseline level for normal operation of the IT system network[7] and how information and data is transmitted • Sample compliance: IT system manuals describing purpose and function, chart outlining how data gets communicated through IT systems ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: DE.AE.1	Personnel understand the legal and regulatory requirements governing cybersecurity • Sample compliance: HIPAA and HITECH, privacy and security, and ethics training for all employees and third-parties ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.GV.3	The IT systems, the network, software, and third party activity is monitored and scanned to detect malicious and unauthorized code, and identify unauthorized access • Sample compliance: Vulnerability scans, testing to find vulnerability a cyber attacker could use to gain unauthorized access to the system (penetration testing), and reviews of IT system access audit logs are conducted to detect computer viruses, worms, JavaScript, and VBS Script, and to identify personnel, connections, devices, and software ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: DE.CM.1; DE.CM.4; DE.CM.5 DE.CM.6 DE.CM.7, DE.CM.8

[6] Any type of incidence that raises concern or indicates that suspicious activity is occurring, which includes alerts, breaches, attacks, disruptions, abnormal activity, etc.
[7] The method for how IT systems are connected to the internet, including local area network (LAN), wireless local area network (WLAN or Wi-Fi), System Area Network, Storage Area Network.

#	People	Process	Policy	Technology
4	Employees and third parties with access to information technology systems and software demonstrate understanding of their roles and responsibilities for safeguarding the physical system and electronic access to information • Sample compliance: Employee Handbook, position requirements, employee training program including testing and exercises, signed contracts, memorandums of understanding, Business Associate Agreements ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.AT.5	The organization knows its role in the industry and this has been communicated to all employees and relevant third-parties • Sample compliance: Evaluation of potential effects from an interruption in critical business operations is conducted and result disseminated to all employees and third-parties ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.BE.1;ID.BE.2	Cybersecurity risks are addressed in governing and risk management policies • Sample compliance: IT Operations and Employee Handbooks include cybersecurity ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.GV.4	All information and data that is stored, transmitted, or accessed by the organization is protected from unauthorized access • Sample compliance: IT Operations Manual includes information on converting data to code (encrypting), establishing firewalls, and information is included in Employee Handbook and training, and contracts with third-parties ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.GV.1, PR.DS.1, PR.DS.2, PR.DS.5
5	Periodic review of employee IT system activity log[8] to inspect Internet use, e-mails, file downloads and use of portable external devices • Sample compliance: Audits of IT system logs and e-mail accounts ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: DE.CM.3	The organization has identified and documented known cybersecurity threats and the potential impact of unauthorized access to information, and used this information to determine organization's level risk • Sample compliance: Business impact analysis, and IT risk assessment report ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.RA.1, ID.RA.4, ID.RA.5	Internal and external cybersecurity threats are formally documented • Sample compliance: Risk assessment that addresses personnel, unlocked doors, unsecured devices, computer viruses, phishing scams, and hackers ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.RA.3	The IT systems network has the capacity to ensure data and software is always able to be accessed and used • Sample compliance: Use of a calculator to determine amount of data that can be transferred in one second ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.DS.4

[8] Report of all activity of any IT system that includes information on the user, time/date stamp, what information was accessed and duration.

#	People	Process	Policy	Technology
6		All roles and responsibilities for managing cybersecurity processes are coordinated to avoid duplication and are aligned to the employees position • Sample compliance: IT Operations Manual, Employee Handbook, and Business Associates Agreements outline roles and responsibilities of all employees and third-parties ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.GV.2	The organization has established formal risk management policy approved by senior management • Sample compliance: Risk Management Framework[9] is completed, incorporated into Operational Manual, and approved by senior management ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.RM.1	All IT systems, software, and data is scanned to identify who sent it and/or where it came from, and assess how likely the source is to be reputable • Sample compliance: Use of firewalls, virus scans, email spam filters, verifying identity of a source, authorization and converting data to a codes is outlined in IT Operations Manual ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.DS.6
7		The organization has identified and prioritized all activities essential for its' operation • Sample compliance: Evaluation of potential effects from an interruption in critical business operations is conducted and results are disseminated to all employees and third-parties for all organization activities and IT systems ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.BE.4	All users and devices undergo a standard approval process prior to use and their system identities and credentials are managed by designated authorized personnel • Sample compliance: IT Systems Operation Manual outlines requirements for user names, passwords, and application access ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.AC.1	Any IT system that is used for testing and development are separated from the IT systems that carry out daily operations of the organization • Sample compliance: Use of internal firewalls and having separate internet connections ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.DS.7

[9] Provides the steps to select the appropriate methods to effectively manage the organization's risk based on the specific activities of the organization. More information can be found at: csrc.nist.gov/groups/SMA/fisma/framework.html.

#	People	Process	Policy	Technology
8		All cybersecurity events are identified, linked to other relevant information to understand the impact to the organization, and to provide processes to mitigate the threat • Sample compliance: Virus scans, audit logs of internet activity, and penetration testing to identify new threats, database of results from all business impact analysis, risk assessment, and disaster recovery reports ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: DE.AE.3, RS.MI.3, PR.IP.12	Remote access[10] is managed through formal approval and credentialing based on the role of the employee or third-party • Sample compliance: IT Systems Operation Manual outlines access requirements for each role and security procedures for encryption when accessing data and information using a virtual private network (VPN), remote desktop, or remote data base ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.AC.3	Consistent procedures for development and acquisition of IT systems and software are used • Sample compliance: IT Operations Manual outlines the process analyzing, designing, developing, testing, installing, maintaining, evaluating, and disposing of IT systems and software ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.IP.2

[10] Access to an IT system, such as an office computer or virtual machine, from another IT system at a different location.

#	People	Process	Policy	Technology
9		Cybersecurity events are categorized by how much of a threat and impact to the organization, and this information is used to establish acceptable levels of risk for cybersecurity threats and prioritize responses based on impact to the organization's operations • Sample compliance: Analysis to determine risk level by both the probability and the impact of the threat occurring, business impact analysis conducted and results incorporated into cybersecurity incident response, and disaster recovery, and business continuity plans ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.RM.3, RS.AN.4, ID.RA.6	Permissions for users, devices, and software access to organization IT systems, equipment, and files is limited to only what is necessary to perform job functions or ensure normal functioning • Sample compliance: Configuring IT system's user profiles and software based on role, key cards and fobs limiting access to sensitive areas/materials ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.AC.3, PR.PT.3	IT systems are protected by limiting changes to the system, software installation, connection of external devices, monitoring electronic communications, and users of the system • Sample compliance: Encrypting of information during storage and transmission, virus scans, monitoring of email and Internet use, limiting ability to install software to dedicated IT employees, blocking external devices, such as flash drives and smart phones, from connecting to a computer or network ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.IP.1, PR.IP.3, PR.AC.5, PR.PT.2, PR.PT.4
10		The organization has identified, documented, and shared with employees and relevant third-parties an acceptable level of risk for organizational operations • Sample compliance: Risk assessment is completed and results included in Employee Handbook and training ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: ID.RM.2	IT systems are audited for any unauthorized access by a user or software • Sample compliance: Audit logs of IT system access are generated and reviewed ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.PT.1	Maintenance and repair of IT systems and software is conducted by authorized individuals, vendors, and tools, and documented • Sample compliance: List of approved vendors and tools, limiting the authorization to conduct maintenance and repairs to designated IT individuals, Including IT maintenance procedures in Employee Handbook and training ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.MA.1, PR.MA.2

#	People	Process	Policy	Technology
11		The environment outside of IT systems is monitored for unauthorized access • Sample compliance: Security personnel, key cards and fobs for access, and auditing of access logs, visitor sign in/out logs ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: DE.CM.2	Access to areas outside of the IT system is restricted, especially in areas where computers, devices, and files that contain sensitive information are kept • Sample compliance: Use of key cards/fobs and lock and key to restrict physical access, employee ID badges, and visitors required to sign in and be escorted while on the premises ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.AC.2	
12		System back-ups are implemented, tested, and updated • Sample compliance: IT Operations Manual outlines the process and frequency of system back-up and testing ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.IP.4	IT systems and data removal, transfer, storage, and destruction is standard throughout the organization • Sample compliance: IT Operations Manual, and Employee Handbook and training addresses the removal, transfer, and storage of systems and data, and the process for overwriting, de-magnetizing, or shredding data ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.DS.3, PR.IP.6	

#	People	Process	Policy	Technology
13		The organization shares information with third-parties about how the organizations chose, implements, and uses the technology to protect against a cybersecurity event • Sample compliance: Information sharing through, participation in online forums, writing product reviews, and case studies ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.IP.8	All personnel and third-parties demonstrate adherence to established policies and regulations when using IT systems and software • Sample compliance: Employee policy includes steps for taking action for non-compliance, and agreements, contracts, memorandums of understanding are executed with third-parties, detail responsibilities, and termination clause for non-compliance ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.IP.5	
14		The organization has developed response and recovery plans that address cybersecurity, is able to execute plans during or after an event, and continuously updates these plans to address new cybersecurity threats and incorporate lessons learned • Sample compliance: Cybersecurity incident response, business continuity, and disaster recovery plans are in place and updated ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: PR.IP.9, PR.IP.10, RS.RP.1, RS.IM.1, RS.IM.2, RC.RP.1, RC.IM.1, RC.IM.2	Criteria have been established to report cyber-attacks, monitor compliance with reporting, and remedy non-compliance with reporting policies • Sample compliance: Cybersecurity response and disaster recovery plans; Employee Handbook outlines training, documentation of counseling, and/or termination procedures for non-compliance ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: RS.CO.2	

#	People	Process	Policy	Technology
		Employees and third-parties are able to respond effectively to a cyber-attack • Sample compliance: Employees are trained on recovery and response protocols, mock drills, and competency evaluations ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: RS.CO.4	Procedures have been established to manage public relations after a cyber-attack • Sample compliance: Operations Manual, cyber incident response, disaster recovery, and business continuity plans, and Employee Handbook include public relations procedures ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: RC.CO.1	
15		Notifications from detection systems, such as virus software, intrusion detection systems, or security management systems, are evaluated to understand how an attack would be carried out and the appropriate response • Sample compliance: Risk assessment and business impact analysis conducted for each event, analysis to determine risk level by both the probability and the impact of the threat occurring, and the level at which to trigger an alert ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: DE.AE.2, DE.AE.5, RS.AN.1		

#	People	Process	Policy	Technology
16		The organization is able to contain cybersecurity events to minimize the impact • Sample compliance: Use of firewalls to separate the network used for patient information, Internet browsing and email, and guest use to stop the attack from spreading throughout the IT system ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: RS.MI.1, RS.MI.2		
17		Information is collected following a cyber-attack and analyzed to understand type, entry point, and root cause of a cyber-attack • Sample compliance: Business impact analysis and disaster recovery reports ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: RS.AN.3		

#	People	Process	Policy	Technology
18		The impact to all aspects of the organization following a cyber-attack is assessed and results are reported • Sample compliance: Business impact analysis and disaster recovery reports ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: DE.AE.4, RS.AN.2		
19		Information pertaining to cybersecurity processes, testing, threats, and attacks are received and shared with appropriate employees and third-parties • Sample compliance: Communication plan included in Operations Manual, cybersecurity plans and cybersecurity incident reports are disseminated to employees and third-parties, participation in online forums, stakeholder advisory groups, and information sharing sessions ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: DE.DP.4, RS.CO.3, RC.CO.3, RS.CO.5, ID.RA.2		

#	People	Process	Policy	Technology
20		A strategy is in place to repair the organization's reputation following a cybersecurity event • Sample compliance: Disaster recovery plan, public relations strategies that include sharing remediation actions ☐ *Implemented* ☐ *Needs to be implemented* ☐ *Not applicable* Source: RC.CO.2		

About the score

The score is meant to serve as an indicator of an organization's cybersecurity readiness.

1. Count the number answered "Implemented" and the number answered "Not Applicable" and enter them below.

Implemented	#
Not applicable	#

2. Take the total number of questions in the tool minus those answered "Not Applicable" to get the "Total questions for scoring."

51	−	# Not applicable	=	Total questions for scoring

3. Calculate your "Readiness Percent" by dividing the number "Implemented" from the total answered above.

# Implemented	÷	Total questions for scoring	=	Readiness percent

4. Circle the "Readiness Percent" on the scale below.

Readiness Indicator											
Readiness Percent	**0%**	**10%**	**20%**	**30%**	**40%**	**50%**	**60%**	**70%**	**80%**	**90%**	**100%**
	Partial					**Moderate**					**Advanced**

Readiness Indicator Levels

Partial: Minimal development of processes have been established by the organization.

Moderate: Some processes have been established by the organization.

Advanced: Formalized processes have been developed by the organization to address leading cybersecurity risks.

Resources

1. *Baldrige Cybersecurity Excellence Builder-DRAFT*, National Institute of Standards and Technology. Available at: www.nist.gov/sites/default/files/documents/2016/09/15/baldrige-cybersecurity-excellence-builder-draft-09.2016.pdf
2. *Security Risk Assessment Tool,* HealthIT.gov. Available at: www.healthit.gov/providers-professionals/security-risk-assessment-tool
3. *Framework for Improving Critical Infrastructure Cybersecurity Version 1*, National Institute of Standards and Technology. Available at: www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
4. *Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology Special Publication 800-53 Revision 4. Available at: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
5. *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework,* Health and Human Services. Available at: www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf

Reference Information

Items in the tool include source information from the NIST CSF, which can be accessed here: www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. By referencing the NIST CSF, users of the tool can identify the originating industry standard(s) that provide the framework for the NIST CSF. Identification of the standards was a result of collaboration between the federal government and private sector.

About MHCC

The MHCC is an independent regulatory agency whose mission is to plan for health system needs, promote informed decision-making, increase accountability, and improve access in a rapidly changing health care environment by providing timely and accurate information on availability, cost, and quality of services to policy makers, purchasers, providers and the public. The MHCC is responsible for advancing health information technology statewide and fostering innovation in a way that balances the need for information sharing with the need for strong privacy and security policies.

Acknowledgements

The MHCC appreciates the contribution made by members of the Maryland Hospital Association, MedChi, The Maryland State Medical Society, LifeSpan Network, and Health Facilities Association of Maryland in developing and testing the tool. Stakeholder engagement throughout the process was laudable.