Nationwide Cyber Security Review 2018, 2019 & 2020: 689368

Created Date: 9/29/2020 11:44 AM Last Updated: 2/5/2021 11:42 AM

Instructions

Review the following steps to complete this questionnaire:

1) Utilize the save button found in the upper left hand corner periodically throughout the survey.

2) Answer the required questions in the **General Information** section of the survey.

3) Complete the survey by answering **all** of the questions in the following tabs listed below: Demographics, Identify, Protect, Detect, Respond, Recover, Cybersecurity Automation & Orchestration Capabilities, and Post Survey Questions.

4) You can add comments or attach supporting evidence to each question by clicking on the sticky note icon located to the right of the question.

5) You can view question clarification by selecting the question mark icon located to the left of the question. Also included within this icon is a link to a policy template, if applicable.

6) When you have completed the assessment, change the Status within the Submit Self-Assessment section to Submit.

7) After you have completed the survey, you will be able to gain access to various reports specific to your entity. To access your results, utilize the dashboard found on the main homepage.

OMB Reference: OMB Control Number: 1670-0040, OMB Expiration Date: 11/30/2022

General Information

Questionnaire ID:	689368	**Year:**	2020
Organization:	New York - Friendship Central School District	**Due Date:**	12/31/2020
Progress:	142 of 142 Completed	What does your organization need to comply with? (Can select multiple answers below)	
Progress Status:	100%	**Compliance Drivers:**	N/A

Submit Self-Assessment

Submit Self-Assessment:	Please note: It's important to make sure the survey is completed in full prior to changing the status to "Submit". Once the status is changed, your findings are generated and the survey is locked.	In Progress

Maturity Scale

The Nationwide Cyber Security Review utilizes the below response scale which allows participants to indicate how formalized the cybersecurity activities are within their organization.

Optimized: Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.

Tested and Verified: Your organization has formally documented policies. standards, and procedures. Implementation is tested and verified.

Implementation in Process: Your organization has formally documented policies, standards, and procedures, and is in the process of implementing and aligning this documentation to a formal security framework and/or methodology.

Partially Documented Standards and/or Procedures: Your organization has a formal policy in place and began the process of developing documented standards and/or procedures to support the policy.

Documented Policy: Your organization has a formal policy in place.

Informally Done: Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.

Not Performed: Activities, processes and technologies are not in place to achieve the referenced objective.

Completion Tracking

Completion Tracking (ID):	100 %	**Completion Tracking (RC):**	100 %
Completion Tracking (PR):	100 %		
Completion Tracking (DE):	100 %		
Completion Tracking (RS):	100 %		

Demographics

(CSF) Demographics

(NCSR)Demo 1: Cybersecurity Governance:	How would you categorize your cybersecurity governance structure?	Hybrid - Information security governance/policy authority and decision making is distributed between a central body and individual sub-organizations
(NCSR)Demo 2: Cybersecurity Governance:	How would you categorize your cybersecurity implementation and operations?	Hybrid - Information security implementation and operations authority and decision making is distributed between a central body and individual sub-organizations
(NCSR)Demo 3: Cybersecurity Governance:	Who are you answering the NCSR on behalf of?	Your organization only
(NCSR)Demo 4: Executive Cyber Reporting:	Is executive cyber reporting mandated, optional, or non-existent within your organization?	Optional
(NCSR)Demo 5: Cyber Security Executive Mandates/ Policies:	If applicable, select all policy/mandate details that apply to your organization:	My organization has formally adopted a set of policies and standards. My organization is subject to Executive Mandates/Laws/Statutes/Legislation.
(NCSR)Demo 6: Security Framework:	Which control frameworks and/or security methodologies are your organization's information security controls based on? Select all that apply.	NIST Cyber Security Framework
(NCSR)Demo 7: FTE Size:	How many full-time equivalent (FTEs) employees/contractors are there in your organization?	50 to 99
(NCSR)Demo 8: IT FTE:	How many full-time equivalent employees are there in your IT?	2 to 5
(NCSR)Demo 9: Security FTE:	How many full-time equivalent employees have security related duties?	2 to 4
(NCSR)Demo 10: IT Outsourcing:	What part of your IT operation is outsourced?	Between 50% and 75%
(NCSR)Demo 11: Security Outsourcing:	What part of your security operation is outsourced?	Between 50% and 75%
(NCSR)Demo 12: Grant Program:	My organization is completing the NCSR due to receiving funds from the following grant program (select all that apply):	I am not taking the NCSR as part of the SHSP or UASI grant requirement
(NCSR)Demo 13: Fiscal Year:	My organization was awarded the applicable grant funds specific to the following fiscal year(s). Select all that apply.	Not Applicable

Paperwork Reduction Act

The public reporting burden to complete this information collection is estimated at 2 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and the completing and reviewing the collected information. The collection of information is voluntary. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number and expiration date. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to DHS/NPPD/CS&C, 245 Murray Lane, SW, Mail Stop 0612, Arlington, VA 20598-0640 or SLTTCyber@HQ.DHS.GOV ATTN: PRA [OMB Control No. 1670-0040].

Identify

(CSF) Identify.Asset Management		
ID.AM-1:	Physical devices and systems within the organization are inventoried.	Tested and Verified
ID.AM-2:	Software platforms and applications within the organization are inventoried	Tested and Verified
ID.AM-3:	Organizational communication and data flows are mapped	Tested and Verified
ID.AM-4:	External information systems are catalogued	Tested and Verified
ID.AM-5:	Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	Tested and Verified
ID.AM-6:	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Implementation in Process

(CSF) Identify.Business Environment		
ID.BE-1:	The organization's role in the supply chain is identified and communicated	Tested and Verified
ID.BE-2:	The organization's place in critical infrastructure and its industry sector is identified and communicated	Tested and Verified
ID.BE-3:	Priorities for organizational mission, objectives, and activities are established and communicated	Tested and Verified
ID.BE-4:	Dependencies and critical functions for delivery of critical services are established	Tested and Verified
ID.BE-5:	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	Tested and Verified

(CSF) Identify.Governance		
ID.GV-1:	Organizational cybersecurity policy is established and communicated	Implementation in Process
ID.GV-2:	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	Implementation in Process
ID.GV-3:	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	Tested and Verified
ID.GV-4:	Governance and risk management processes address cybersecurity risks	Implementation in Process

(CSF) Identify.Risk Assessment		
ID.RA-1:	Asset vulnerabilities are identified and documented	Implementation in Process
ID.RA-2:	Cyber threat intelligence and vulnerability information is received from information sharing forums and sources	Implementation in Process
ID.RA-3:	Threats, both internal and external, are identified and documented	Tested and Verified
ID.RA-4:	Potential business impacts and likelihoods are identified	Tested and Verified
ID.RA-5:	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Tested and Verified
ID.RA-6:	Risk responses are identified and prioritized	Tested and Verified

(CSF) Identify.Risk Management Strategy		
ID.RM-1:	Risk management processes are established, managed, and agreed to by organizational stakeholders	Tested and Verified
ID.RM-2:	Organizational risk tolerance is determined and clearly expressed	Tested and Verified
ID.RM-3:	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	Implementation in Process

(CSF) Identify.Supply Chain Risk Management		
ID.SC-1:	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	Implementation in Process
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	Tested and Verified
ID.SC-3:	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	Tested and Verified
ID.SC-4:	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	Tested and Verified
ID.SC-5:	Response and recovery planning and testing are conducted with suppliers and third-party providers	Tested and Verified

Protect

(CSF) Protect.Access Control		
PR.AC-1:	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	Tested and Verified
PR.AC-2:	Physical access to assets is managed and protected	Tested and Verified
PR.AC-3:	Remote access is managed	Tested and Verified
PR.AC-4:	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Tested and Verified
PR.AC-5:	Network integrity is protected (e.g., network segregation, network segmentation)	Tested and Verified
PR.AC-6:	Identities are proofed and bound to credentials and asserted in interactions	Tested and Verified
PR.AC-7:	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Implementation in Process

(CSF) Protect.Awareness and Training		
PR.AT-1:	All users are informed and trained	Tested and Verified
PR.AT-2:	Privileged users understand roles & responsibilities	Tested and Verified
PR.AT-3:	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	Tested and Verified
PR.AT-4:	Senior executives understand roles & responsibilities	Tested and Verified
PR.AT-5:	Physical and cybersecurity personnel understand their roles and responsibilities	Tested and Verified

(CSF) Protect.Data Security		
PR.DS-1:	Data-at-rest is protected	Tested and Verified
PR.DS-2:	Data-in-transit is protected	Tested and Verified
PR.DS-3:	Assets are formally managed throughout removal, transfers, and disposition	Tested and Verified
PR.DS-4:	Adequate capacity to ensure availability is maintained	Tested and Verified
PR.DS-5:	Protections against data leaks are implemented	Tested and Verified
PR.DS-6:	Integrity checking mechanisms are used to verify software, firmware, and information integrity	Tested and Verified
PR.DS-7:	The development and testing environment(s) are separate from the production environment	Tested and Verified
PR.DS-8:	Integrity checking mechanisms are used to verify hardware integrity	Tested and Verified

(CSF) Protect.Information Protection Process and Procedures		
PR.IP-1:	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	Tested and Verified
PR.IP-2:	A System Development Life Cycle to manage systems is implemented	Implementation in Process
PR.IP-3:	Configuration change control processes are in place	Tested and Verified
PR.IP-4:	Backups of information are conducted, maintained, and tested	Implementation in Process
PR.IP-5:	Policy and regulations regarding the physical operating environment for organizational assets are met	Tested and Verified
PR.IP-6:	Data is destroyed according to policy	Tested and Verified
PR.IP-7:	Protection processes are improved	Tested and Verified
PR.IP-8:	Effectiveness of protection technologies is shared	Implementation in Process
PR.IP-9:	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	Implementation in Process
PR.IP-10:	Response and recovery plans are tested	Implementation in Process
PR.IP-11:	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	Tested and Verified
PR.IP-12:	A vulnerability management plan is developed and implemented	Implementation in Process

(CSF) Protect.Maintenance		
PR.MA-1:	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	Tested and Verified
PR.MA-2:	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Tested and Verified

(CSF) Protect.Protective Technology		
PR.PT-1:	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Implementation in Process
PR.PT-2:	Removable media is protected and its use restricted according to policy	Tested and Verified
PR.PT-3:	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	Tested and Verified
PR.PT-4:	Communications and control networks are protected	Tested and Verified
PR.PT-5:	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Tested and Verified

Detect		
(CSF) Detect.Anomalies and Events		
DE.AE-1:	A baseline of network operations and expected data flows for users and systems is established and managed	Tested and Verified
DE.AE-2:	Detected events are analyzed to understand attack targets and methods	Tested and Verified
DE.AE-3:	Event data are collected and correlated from multiple sources and sensors	Tested and Verified
DE.AE-4:	Impact of events is determined	Tested and Verified
DE.AE-5:	Incident alert thresholds are established	Implementation in Process
(CSF) Detect.Security Continuous Monitoring		
DE.CM-1:	The network is monitored to detect potential cybersecurity events	Tested and Verified
DE.CM-2:	The physical environment is monitored to detect potential cybersecurity events	Tested and Verified
DE.CM-3:	Personnel activity is monitored to detect potential cybersecurity events	Tested and Verified
DE.CM-4:	Malicious code is detected	Tested and Verified
DE.CM-5:	Unauthorized mobile code is detected	Tested and Verified
DE.CM-6:	External service provider activity is monitored to detect potential cybersecurity events	Tested and Verified
DE.CM-7:	Monitoring for unauthorized personnel, connections, devices, and software is performed	Tested and Verified
DE.CM-8:	Vulnerability scans are performed	Tested and Verified
(CSF) Detect.Detection Process		
DE.DP-1:	Roles and responsibilities for detection are well defined to ensure accountability	Implementation in Process
DE.DP-2:	Detection activities comply with all applicable requirements	Implementation in Process
DE.DP-3:	Detection processes are tested	Implementation in Process
DE.DP-4:	Event detection information is communicated	Implementation in Process
DE.DP-5:	Detection processes are continuously improved	Implementation in Process

Respond		
(CSF) Respond.Response Planning		
RS.RP-1:	Response plan is executed during or after an event	Partially Documented Standards and/or Procedures
(CSF) Respond.Communications		
RS.CO-1:	Personnel know their roles and order of operations when a response is needed	Implementation in Process
RS.CO-2:	Incidents are reported consistent with established criteria	Implementation in Process
RS.CO-3:	Information is shared consistent with response plans	Implementation in Process
RS.CO-4:	Coordination with stakeholders occurs consistent with response plans	Implementation in Process
RS.CO-5:	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	Implementation in Process
(CSF) Respond.Analysis		
RS.AN-1:	Notifications from detection systems are investigated	Implementation in Process
RS.AN-2:	The impact of the incident is understood	Implementation in Process
RS.AN-3:	Forensics are performed	Implementation in Process
RS.AN-4:	Incidents are categorized consistent with response plans	Implementation in Process
RS.AN-5:	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	Implementation in Process
(CSF) Respond.Mitigation		
RS.MI-1:	Incidents are contained	Implementation in Process
RS.MI-2:	Incidents are mitigated	Implementation in Process
RS.MI-3:	Newly identified vulnerabilities are mitigated or documented as accepted risks	Implementation in Process
(CSF) Respond.Improvements		
RS.IM-1:	Response plans incorporate lessons learned	Implementation in Process
RS.IM-2:	Response strategies are updated	Implementation in Process

Recover		
(CSF) Recover.Recovery Planning		
RC.RP-1:	Recovery plan is executed during or after a cybersecurity incident	Implementation in Process
(CSF) Recover.Improvements		
RC.IM-1:	Recovery plans incorporate lessons learned	Implementation in Process
RC.IM-2:	Recovery strategies are updated	Implementation in Process
(CSF) Recover.Communications		
RC.CO-1:	Public relations are managed	Implementation in Process
RC.CO-2:	Reputation is repaired after an incident	Implementation in Process
RC.CO-3:	Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	Implementation in Process

Cybersecurity Automation & Orchestration Capabilities

Cybersecurity Automation & Orchestration

(Automation) Question 1:	Security Information and Event Management (SIEM) tools are fully implemented, monitored, and managed.	Yes
(Automation) Question 2:	Identity and Access Management (IAM) tools are fully implemented, monitored, and managed.	Yes
(Automation) Question 3:	Two factor authentication has been fully implemented.	No
(Automation) Question 4:	Mobile Device Management (MDM) tools are fully implemented for the administration of mobile devices.	Yes
(Automation) Question 5:	Vulnerability assessment tools are fully implemented, monitored, and managed.	Yes
(Automation) Question 6:	Intrusion Defense System (IDS) tools are fully implemented.	Yes
(Automation) Question 7:	Intrusion Prevention System (IPS) tools are fully implemented.	Yes
(Automation) Question 8:	End point protection tools are fully implemented to monitor and analyze network endpoints.	Yes
(Automation) Question 9:	Automated tools are used to manage physical IT assets (i.e., inventory and tracking of all software or hardware within an IT environment).	Yes
(Automation) Question 10:	Automated tools are used to manage and control removable media.	Yes
(Automation) Question 11:	Automated tools are used to encrypt sensitive data in transit between networks.	Yes
(Automation) Question 12:	Automated tools are used to create and maintain baseline configuration/change control information.	Yes
(Automation) Question 13:	Automated tools are used to conduct and test system backups.	Yes
(Automation) Question 14:	Penetration tests are performed to exploit identified vulnerabilities.	Yes
(Automation) Question 15:	Antiviral tools are implemented, monitored, and managed.	Yes
(Automation) Question 16:	Automated methods are used to integrate disparate security systems.	Yes

Post Survey Questions

General

(Post Survey) Question 1:	What are your top 5 security concerns?	Conflicting federal rules and requirements Lack of sufficient funding Lack of legislative support Increasing sophistication of threats Emerging technologies
(Post Survey) Question 2::	If your organization supports any sector considered part of the U.S. critical infrastructure, please select the applicable sector(s). Critical infrastructure is defined as "infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." Details located here: https://www.cisa.gov/critical-infrastructure-sectors	Not Applicable
(Post Survey) Question 3::	Do your organization's IT operations (specifically information security) support election operations within the jurisdiction?	No
(Post Survey) Question 4::	What describes your motivation to take NCSR? Select all that apply.	Compliance Requirement (Example - Policy or Regulatory)
(Post Survey) Question 5:	Please enter your organization's zip code.	14739

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				