NEW YORK STATE
REGIONAL INFORMATION CENTERS

K-12 CYBERSECURITY PLANNING

RIC ONE RECOMMENDATIONS AND TOOLS

THIS RESOURCE WAS DEVELOPED BASED ON THE
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
PROTECTING OUR FUTURE REPORT

APRIL 2023

THIS PAGE INTENTIONALLY BLANK

REPORT BACKGROUND AND OVERVIEW

The K-12 Cybersecurity Act directed the Cybersecurity and Infrastructure Security Agency (CISA) to report on cybersecurity risks facing schools. The report includes details about challenges facing the sector, field recommendations, and helpful resources. In this RIC One resource, we summarize CISA's recommendations related to cybersecurity planning and infuse related guidance from the RICs.

CISA Report: *Protecting Our Future: Partnering to Safeguard K-12 Organizations From Cybersecurity Treats (January 2023)*

KEY RECOMMENDATIONS

The CISA report includes 3 key recommendations highlighted to the right. The remainder of this resource is primarily focused on the first recommendation (Strategically Mature the District's Security Posture and Plan). The continuum below introduces a strategy aligned with this recommendation.

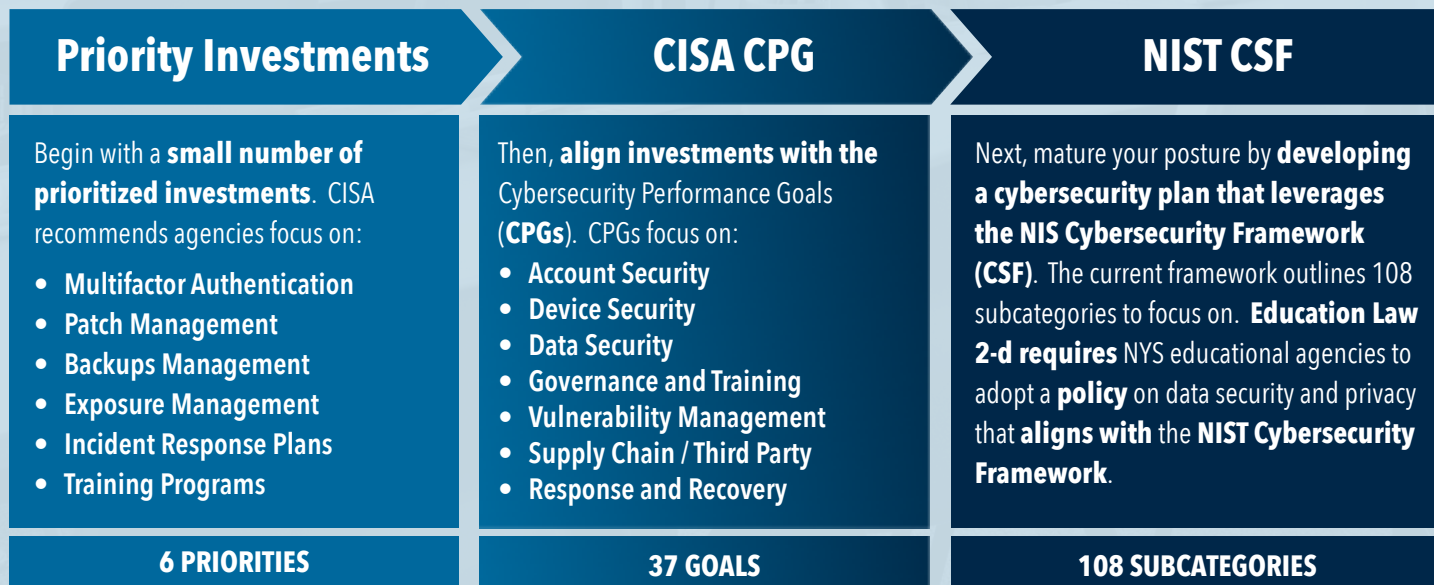**STRATEGICALLY MATURE THE DISTRICT'S CYBERSECURITY POSTURE AND PLAN**

RECOGNIZE AND ACTIVELY ADDRESS RESOURCE CONSTRAINTS

FOCUS ON COLLABORATION AND INFORMATION SHARING

MOVE THROUGH THE K-12 SECURITY MEASURES CONTINUUM TO MATURE THE DISTRICT'S SECURITY POSTURE

As educational agencies have limited resources, CISA outlines a three step process to support districts in maturing their cybersecurity posture. First, school districts focus on a small number of prioritized investments. Next, districts progress to Phase 2 and develop a plan that aligns with the 37 Cybersecurity Performance Goals (CPG). Finally, in Phase 3, the plan is further developed to align with the NIST CSF. As Part 121 of the Commissioner's Regulations require agencies to adopt a policy that aligns with the NIST CSF Version 1.1, this suggested maturity continuum is particularly helpful to New York State school districts and BOCES. The diagram below provides more information about the three step process. Additionally, on subsequent pages each phase is reviewed in more detail.

Priority Investments ⟩ CISA CPG ⟩ NIST CSF

Priority Investments	CISA CPG	NIST CSF
Begin with a **small number of prioritized investments**. CISA recommends agencies focus on: • **Multifactor Authentication** • **Patch Management** • **Backups Management** • **Exposure Management** • **Incident Response Plans** • **Training Programs**	Then, **align investments with the** Cybersecurity Performance Goals (**CPGs**). CPGs focus on: • **Account Security** • **Device Security** • **Data Security** • **Governance and Training** • **Vulnerability Management** • **Supply Chain / Third Party** • **Response and Recovery**	Next, mature your posture by **developing a cybersecurity plan that leverages the NIS Cybersecurity Framework (CSF)**. The current framework outlines 108 subcategories to focus on. **Education Law 2-d requires** NYS educational agencies to adopt a **policy** on data security and privacy that **aligns with** the **NIST Cybersecurity Framework**.
6 PRIORITIES	**37 GOALS**	**108 SUBCATEGORIES**

IMPLEMENT HIGHEST PRIORITY SECURITY CONTROLS

In Phase 1, school districts and BOCES can start to mature their cybersecurity posture by implementing a small number of strategic controls. CISA identifies six important controls in the Protecting Our Future report. These recommended priority areas are described below. To support educational agencies in building on this important first step, each control is aligned to Phase 2 and 3 cybersecurity resources/frameworks (CISA CPG and NIST CSF).

1 IMPLEMENT MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) is a method of logging into a system with two unique forms of verification (or factors) that are used to confirm the user. MFA is highly effective at protecting accounts and data, as generally bad actors (or criminals) are not able to bypass the second authentication requirement. Districts can develop strategic MFA implementation plans that prioritize highest risk systems, such as virtual private networks, and high-priority accounts.

| CISA CPG 1.3 | NIST CSF PR.AC-7 |

2 PATCH MANAGEMENT

Districts should prioritize patch management, as it is one of the most cost-effective practices an organization can adopt to enhance the agency's security posture. Specifically, technology staff should patch known vulnerabilities in a timely manner. It is particularly important to apply patches to those systems that house sensitive data. Districts can leverage CISA's free Vulnerability Scanning service to receive weekly reports on vulnerabilities.

| CISA CPG 5.1 | NIST CSF PR.IP-12 |
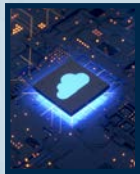
3 BACKUPS MANAGEMENT

School districts should back up all critical systems, audit backups for completion, and test the restoration of data. Backups should be stored offline and disconnected from the network. Isolating backup servers prevents the spread of malware to these servers via compromised domain credentials. These practices should be documented in the district's incident response plan.

| CISA CPG 7.3 | NIST CSF PR.IP-4 |

4 EXPOSURE MANAGEMENT

Cyber attackers use tools similar to search engines to locate and exploit Internet-connected systems. Districts should ensure that solutions accessible via the internet are not exploitable. Appropriate compensating controls should be implemented to prevent abuse related to services that must be exposed. Districts should have plans in place to support routine assessment and mitigation of these exposures.

| CISA CPG 2.1 & 5.4 | NIST CSF PR.IP-12 |

5 INCIDENT RESPONSE PLANS

A Cyber Security Incident Response Plan is a documented procedure that prepares organizations to quickly and efficiently identify, respond to and remediate cybersecurity and data issues. These plans must be appropriately maintained and tested. Districts can use table top exercises to strengthen the response team's readiness and the district's security posture.

| CISA CPG 7.2 | NIST CSF PR.IP-9 |

6 TRAINING PROGRAMS

Robust cybersecurity plans focus on process, people, and technology. Staff and students need security awareness training. Additionally, employees must be educated regarding laws and district policies that protect sensitive information. In New York State this best practice is required. Specifically, the Part 121 regulations require that training be provided annually to all staff and officials with access to protected data.

| CISA CPG 4.3 | NIST CSF PR.AT-1 |

CYBERSECURITY PERFORMANCE GOALS (CPGs)

During Phase 2, districts further develop cybersecurity plans using CISA's Cybersecurity Performance Goals (CPGs). CISA, in partnership with NIST, developed this set of security practices to supplement the NIST CSF. The NIST CSF is a more complex and comprehensive framework. In Phase 2, agencies with limited cybersecurity expertise, resources, and capabilities develop a plan aligned with CISA's 37 security practices (CPGs) before developing a plan aligned with the 108 NIST CSF controls. The 37 CPGs are listed below. CISA has additional resources available to support agencies using the CPGs. These resources include recommendations about each CPG. Additionally, details about the cost, impact, and complexity are provided. To access more information and tools related to each of the goals visit: **https://www.cisa.gov/cross-sector-cybersecurity-performance-goals**.

ACCOUNT SECURITY

#		
1.1	Detection of Unsuccessful Login Attempts	PR.AC-7
1.2	Changing Default Passwords	PR.AC-1
1.3	Multi-Factor Authentication	PR.AC-7
1.4	Minimum Password Strength	PR.AC-1
1.5	Separating User and Privileged Accounts	PR.AC-4
1.6	Unique Credentials	PR.AC-1
1.7	Revoking Credentials for Departing Employees	PR.AC-1

DEVICE SECURITY

#		
2.1	Hardware and Software Approval Process	PR.IP-3
2.2	Disable Macros by Default	PR.IP-1&3
2.3	Asset Inventory	ID.AM-1
2.4	Prohibit Connection of Unauthorized Devices	PR.PT-2
2.5	Document Devices Configurations	PR.IP-1

DATA SECURITY

#		
3.1	Log Collection	PR.PT-1
3.2	Secure Log Storage	PR.PT-1
3.3	Strong and Agile Encryption	PR.DS-1&2
3.4	Secure Sensitive Data	PR.DS-1,2,5

GOVERNANCE AND TRAINING

#		
4.1	Organizational Cybersecurity Leadership	ID.GV-1&2
4.2	OT Cybersecurity Leadership	ID.GV-1&2
4.3	Basic Cybersecurity Training	PR.AT-1
4.4	OT Cybersecurity Training	PR.AT-2,3,5
4.5	Improving IT and OT Cybersecurity Relationship	ID.GV-2

VULNERABILITY MANAGEMENT

#		
5.1	Mitigating Known Vulnerabilities	PR.IP-12, ID.RA-1, DE.CM-8, RS.MI-3
5.2	Vulnerability Disclosure / Reporting	RS.AN-5
5.3	Deploy Security.txt Files	RS.AN-5
5.4	No Exploitable Services on the Internet	PR.PT-4
5.5	Limit OT Connections to Public Internet	PR.PT-4
5.6	Third-Party Validation of Cybersecurity Control Effectiveness	ID.RA-1&3

THIRD PARTY

#		
6.1	Vendor/Supplier Cybersecurity Requirements	ID.SC-3
6.2	Supply Chain Incident Reporting	ID.SC-1&3
6.3	Supply Chain Vulnerability Disclosure	ID.SC-1&3

RESPONSE AND RECOVERY

#		
7.1	Incident Reporting	RS.CO-2&4
7.2	Incident Response (IR) Plans	PR.IP-9&10
7.3	System Back Ups	PR.IP-4
7.4	Document Network Topology	PR.IP-1

OTHER

#		
8.1	Network Segmentation	PR.AC-5, PR.PT-4, DE.CM-1
8.2	Detecting Relevant Threats and TTPs	ID.RA-3, DE.CM-1
8.3	Email Security	PR.DS-1,2,5

NIST CYBERSECURITY FRAMEWORK (NIST CSF)

During Phase 3, districts develop a cybersecurity plan that leverages the NIST Cybersecurity Framework. These plans align with the 108 NIST CSF controls, define a target maturity state, and identify actions that will be implemented to mature the district's security posture. Educational agencies are required by the Part 121 regulations to adopt a policy that aligns with NIST CSF. Below is a list of security practices developed by the RICs that align with the framework. To further explore the CSF visit: https://www.nist.gov/cyberframework.

IDENTIFY		
	ID.AM-1	Physical Devices Inventoried
	ID.AM-2	Softwares and Systems Inventoried
	ID.AM-4 ID.AM-5	System Criticality Ratings and Requirements Documented
	ID.AM-3	Data Flows Documented
	ID.AM-6	Staff Responsibilities Documented
	ID.GV-2	Third-Party Responsibilities Documented
	ID.BE-I-5	Business Environment Documented
	ID.GV-1	ED Law 2-d Policy Adopted
	ID.GV-3	Complaint Practices Documented
	ID.GV-4	Security Meetings Structure
	ID.RA-1	Vulnerabilities Documented
	ID.RA-2	Cyber Alerts Received
	ID.RA-3-6	Risk Registry is Maintained
	ID-RM-1	Risk Management Processes Documented
	ID-RM-2-3	Risk Tolerance Documented
	ID.SC-1-5	Third-Party Risk Management Processes Defined
	ID.SC-3	Contractual Safeguards Implemented

PROTECT		
	PR.AC-1 PR.AC-4 PR.AC-6	On/Off-boarding Processes Documented
		System Account Managers Identified
		Permissions Assigned Based on Duties
	PR.AC-2	Critical Infrastructure Physically Protected
	PR.AC-3	Remote Access Processes Established
	PR.AC-5	Network Traffic Appropriately Segmented
	PR.AC-7	MFA- Privileged Accounts and Functions
	PR.AT-1-5	Training Plans Established
	PR.AT-3	Third-Party Responsibilities in Contract Terms

PROTECT		
	PR.DS-1	Encryption - Portable Devices
	PR.DS-2	Encryption - Externally Accessible Systems
	PR.DS-3	Asset Management Process
	PR.DS-4	Redundant Equipment and Processes
	PR.DS-5	Data Masking Techniques Applied
	PR.DS-6	Anti-malware and Preboot Protections
	PR.DS-7	Separate System Test Environments
	PR.DS-8	Hardware Examined Prior to Installation
	PR.IP-1	System Baseline configurations documented
	PR.IP-2	System Life Cycle Best Practices Followed
	PR.IP-3	Change Control Process Documented
	PR.IP-4	System Backups Performed, Logged & Tested
	PR.IP-5	Environmental Controls in Server Rooms
	PR.IP-6	Data Destruction Procedures Established
	PR.IP-7-8	Data Security Improvement Plan Maintained
	PR.IP-9-10	Incident Response Plan Developed and Tested
	PR.IP-11	On-boarding Training Developed
	PR.IP-12	Vulnerability Management Plan Defined
	PR.MA-1-2	Maintenance Log Maintained
	PR.PT-1	Critical System Logs Reviewed
	PR.PT-2	Removable Media Protocols Documented
	PR.PT-3	Systems Configured - Only Necessary Capabilities
	PR.PT-4	Multi-layered Network Protections
	PR.PT-5	Resiliency Mechanisms

NIST CYBERSECURITY FRAMEWORK (NIST CSF)

DETECT		
DE.AE-1	Environment Baselines Established	
DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5	Detected Events Analyzed	
	Event Data Aggregated and Correlated	
	Event Impact Determined	
	Alert Thresholds Established	
DE.CM-1	Network Monitored	
DE.CM-2	Physical Environment Monitored	
DE.CM-3	Personnel Activity Monitored	
DE.CM-4 DE.CM-5	Malicious Code Detected	
	Unauthorized Mobile Code Detected	
DE.CM-6 DE.CM-7	Service Provider Activity Monitored	
	Connections, Devices, Software Monitored	
DE.CM-8	Vulnerability Scans Performed	
DE.DP-1	Detection Responsibilities Established	
DE.DP-2	Detection Activities Match Requirements	
DE.DP-4	Event Detection Communicated	
DE.DP-3 DE.DP-5	Detection Processes Tested	
	Detection Processes Improved	

RESPOND		
RS.RP-1	Response Plan Executed During/After Incident	
RS.CO-1 RS.CO-4	Personnel Know Roles When Response is Needed	
	Stakeholders Coordination Consistent with Plans	
RS.CO-2	Incidents Reported Consistent with Criteria	
RS.CO-3 RS.CO-5	Information Shared Consistent with Plans	
	Voluntary Information Sharing Occurs	
RS.AN-1 RS.AN-2 RS.AN-3	Notifications Investigated	
	Incident Impact Understood	
	Forensics Perrformed	
RS.AN-4	Incidents Categorized Consistent with Plans	
RS.AN-5	Vulnerabilities Management Plan Documented	
RS.MI-1 RS.MI-2 RS.MI-3	Incidents Contained and Mitigated	
	Vulnerabilities Mitigated/ Accepted Risk Documented	
RS.IM-1 RS.IM-2	Response Plans Incorporate Lessons Learned	
	Response Strategies Updated	

NIST CYBERSECURITY FRAMEWORK
VERSION 1.1

5 FUNCTIONS

23 CATEGORIES

108 SUBCATEGORIES

RECOVER		
RC.RP-1	Recovery Plan Executed During/After Incident	
RC.IM-1 RC.IM-2	Response Plans Incorporate Lessons Learned	
	Response Strategies are Updated	
RC.CO-1	Public Relations Managed	
RC.CO-2	Reputation Repaired After Incident	
RC.CO-3	Recovery Activities Communicated	

RIC
one
TWELVE REGIONAL INFORMATION CENTERS
WORKING AS ONE

RIC one

NEW YORK STATE
REGIONAL INFORMATION CENTERS

APRIL 2023