Public Schools of North Carolina
State Board of Education
Department of Public Instruction

# Report to the North Carolina General Assembly

## Public Schools Cybersecurity Study

*HB 1030 Sec. 8.17*

**Date Due: --- December 15, 2016**

Report # 35

DPI Chronological Schedule, 2016-2017

## STATE BOARD OF EDUCATION

SBE VISION: Every public school student will graduate ready for post-secondary education and work, prepared to be a globally engaged and productive citizen.

SBE MISSION: The State Board of Education will use its constitutional authority to lead and uphold the system of public education in North Carolina.

**WILLIAM COBEY**

Chair :: Chapel Hill – At-Large

**A.L. COLLINS**

Vice Chair :: Kernersville – Piedmont Triad Region

**DAN FOREST**

Lieutenant Governor :: Raleigh – Ex Officio

**JANET COWELL**

State Treasurer :: Raleigh – Ex Officio

**JUNE ST. CLAIR ATKINSON**

Secretary to the Board :: Raleigh

**BECKY TAYLOR**

Greenville – Northeast Region

**REGINALD KENAN**

Rose Hill – Southeast Region

**AMY WHITE**

Garner – North Central Region

**OLIVIA OXENDINE**

Lumberton – Sandhills Region

**GREG ALCORN**

Salisbury – Southwest Region

**TODD CHASTEEN**

Blowing Rock – Northwest Region

**WAYNE MCDEVITT**

Asheville – Western Region

**ERIC DAVIS**

Charlotte – At-Large

**PATRICIA N. WILLOUGHBY**

Raleigh – At-Large

## NC DEPARTMENT OF PUBLIC INSTRUCTION


**June St. Clair Atkinson, Ed.D., State Superintendent**

**301 N. Wilmington Street :: Raleigh, North Carolina 27601-2825**




**Inquiries or complaints regarding discrimination issues should be directed to:**


Dr. Rebecca Garland, Deputy State Superintendent
6368 Mail Service Center, Raleigh, NC 27699-6368 :: Telephone: (919) 807-3200 :: Fax: (919) 807-3388


**Visit us on the Web :: www.ncpublicschools.org**


M0816

# NC Department of Public Instruction
# Public Schools Cybersecurity Study

Public Schools of North Carolina
State Board of Education
Department of Public Instruction

Submitted by:

Michael Nicolaides, Chief Information Officer
NC Department of Public Instruction

December 2016

This page left intentionally blank

# Table of Contents

# 1. Executive Summary

In its 2015-2016 Session, the General Assembly directed the North Carolina Department of Public Instruction (NCDPI) to conduct a study on cybersecurity in North Carolina public schools, including charter schools. A bidirectional approach was used to develop the study. This two-pronged strategy is summarized as follows:

- A secure web-based survey was developed by NCDPI Information Technology (IT) staff through research of leading organizations and advice of technical experts in this discipline. Answers to questions by school districts and charter schools were analyzed; results are incorporated in the study.
- Meetings and interviews were conducted with oversight and cognizant State and related organizations, leaders and interested parties. Relevant information and insights were organized and incorporated in the study.

From a general perspective on a statewide level, key observations are:

- **Schools vary significantly in their portfolios of cybersecurity capacity -** Survey findings suggest that cybersecurity policies and practices are being implemented in an ad hoc fashion that vary considerably across school districts and charter schools without clear prioritization. As such, there are missed opportunities for implementing low cost/high value practices for improving cybersecurity.
- **Small school districts and charter schools are the most vulnerable** – In general, small school districts and charter schools do not have the infrastructure and personnel resources in place to support data security, indicating they are the most vulnerable to handle cybersecurity events.
- **The majority of school districts and charter schools surveyed are not prepared for a significant disaster or cybersecurity event** – The majority of school districts and charter schools do not have plans and resources in place for ensuring continuity of operations in response to a significant disaster or cybersecurity event.
- **Loss of federal funding for Internet content filtering and firewall services -** Due to changes made in 2015 to the eligible services list for the federal E-rate Program, schools are no longer eligible to receive a federal funding which was used to cover approximately 70% of the cost for their Internet content filtering and firewall services.
- **School districts and charter schools are not mandated to follow the guidelines established in the North Carolina Statewide Information Security Manual** - The North Carolina Statewide Information Security Manual is both comprehensive and detailed, and it is an excellent reference source for assisting school districts and charters in evaluating their level of maturity for cybersecurity and in developing and implementing their controls.

## Key recommendations resulting from this study are:

- **Develop common templates and prioritization guidelines** – Provide State-level guidance and support for documents that can be used by all school districts and charter schools to increase their security posture.
- **Publish a quarterly information security newsletter** – Enhance awareness of the needs for cybersecurity practices and offer information that will assist districts and charter schools in the development and operation of their policies and capabilities.
- **Employee Cyber Awareness Training** – Increase professional development for public school employees across the state by providing cyber awareness training. The annual recurring cost for this is estimated at $500,000.
- **Require school districts and charter schools to follow the guidelines established in the North Carolina Statewide Information Security Manual** – The North Carolina Statewide Information Security Manual is developed, issued and updated by the State's Department of Information Technology and it is the foundation for information technology security in State government. Currently, school districts and charter schools are encouraged, but not required, to adopt the manual.
- **Provide regional cybersecurity specialists** – Regionally organized cybersecurity specialist teams, composed of experienced and knowledgeable experts, should be formed to provide advisory services to school districts and charter schools regarding the methodologies, techniques and tools for implementing and operating local security programs. The annual recurring cost for these personnel is estimated at $996,000.
- **Make available State funding for Internet content filtering and firewall protection** - A replacement source of funding should be found for monies lost due to the recent removal of federal E-rate funds for content filtering and firewall protection. State funds needed to replace the lost federal subsidy are $5.5 million.

This study was comprised of two sections. The first section is a high-level summary of results identified from the survey and various meetings and interviews. The second section of this study is provided in a separate addendum and it includes the detailed findings regarding security which, due to their sensitivity, should be kept confidential as provided in North Carolina General Statute 132-6.1(c).

## 2. Background

This report is required by Section 8.17 of NC SL 2016-94 (HB 1030) that states the following:

> "The Department of Public Instruction shall conduct a study on cybersecurity in North Carolina public schools, including charter schools. As part of the study, the Department may request local school administrative units and charter schools to submit a summary of their current policies and procedures on cybersecurity practices and procedures to protect student and employee personally identifiable data. By December 15, 2016, the Department shall report the results of the study to the General Assembly in accordance with G.S. 120-29.5."

The purpose of the study is to ascertain the maturity level of cybersecurity policies, procedures and capabilities for enabling the following:

- Confidentiality of records to provide for safekeeping.
- Privacy of student and employee data to comply with applicable laws and regulations.
- Integrity of processes to ensure accuracy of information and reports.
- Availability of physical and other resources to assist in the recovery from natural disasters and other untoward events.

The study was a review of current policies, procedures and technologies implemented within North Carolina school districts and charter schools. It was not designed to perform threat analyses or evaluate risk mitigation strategies.

# 3. Overall Approach for Conducting the Study

A bidirectional approach was used to develop the study. This two-pronged strategy is summarized as follows:

- A secure web-based survey was developed by NCDPI Information Technology (IT) staff through research of leading organizations and advice of technical experts in this discipline. Answers to questions by school districts and charter schools were analyzed and results incorporated in the study.
- Meetings and interviews were conducted with personnel from oversight and cognizant State and related organizations and interested parties. Relevant information and insights were organized and incorporated in the study.

The development, analysis and identification of results of the survey involved a time-consuming and important part of the study. Representatives from the following groups provided resources, direction and oversight for the survey development and implementation work.

- NCDPI Technology Services
- North Carolina School Boards Association
- MCNC
- Department of Information Technology Services (DIT) Enterprise Security and Risk Management office

A significant part of the approach for performing the study consisted of conducting various meetings and interviews. Stakeholders for these discussions and interactions included personnel from the following organizations:

- The North Carolina Governor's Office
- The North Carolina Lt. Governor's Office
- The North Carolina Department of Information Technology
- The William & Ida Friday Institute for Educational Innovation at the NCSU
- MCNC
- The University of North Carolina School of Government

These meetings led to additional information and findings that were pertinent to the overall observations and recommendations of the study.

# 4. Conducting Surveys

## Methodology Employed for Conducting Surveys

To perform the surveying portion of the study, NCDPI IT staff created a secure online cybersecurity survey and issued it to all Local Education Agencies (LEAs) and charter schools.

The survey was developed with close coordination and detailed input from personnel representing the above organizations. NCDPI and MCNC maintained close contact with school districts and charter schools as they responded to the survey to assist them with clarifications as needed in order to provide appropriate responses to the survey.

The survey was distributed to the technology directors of LEAs and charter schools. Pre-survey notification emails were sent via two NCDPI Weekly Messages to the State's LEA Superintendents and Charter School Directors. These messages identified that the survey was being conducted in response to House Bill 1030. Additionally, they established the purpose and timeframe for the survey. Participants were notified of the survey via an email which explained the purpose of the survey and provided a Web link that allowed individual secure access. Multiple reminder emails were sent out during the survey implementation.

The security domains and specific questions in the survey were derived from two primary sources. The first was the U.S. Department of Education established Privacy Technical Assistance Center (PTAC). PTAC resources are geared towards public education and are dedicated to promoting cybersecurity and privacy best practices. The two specific PTAC documents used were the Data Security Checklist and the Data Governance Checklist. The second main source was the Center for Internet Security (CIS). This highly respected non-profit is dedicated to enhancing cybersecurity readiness and response among public and private sector entities.

Using the above mentioned documents, NCDPI staff developed survey questions around the following function areas as identified in the National Institute of Standards and Technology (NIST) – Cybersecurity Framework document. The function areas organize basic cybersecurity activities at their highest level. These functions are:

**Identify**

This function area addresses subjects pertaining to identifying risks to data and infrastructure. Topics covered in this function include asset management, data governance, risk assessment, and management, strategy and vulnerability management processes.

**Protect**

This function addresses security pertaining to the protection of data and infrastructure. The focus of this function includes topics such as access control, security awareness and training and protective technologies.

**Detect**

This function addresses continuous monitoring of data and infrastructure. Some of the topics for this function include use of automated tools for malware defense and vulnerability management tools and processes.

**Respond**

This function addresses responding to a data security event. The topics for this area includes incident response planning and Continuity of Operations Planning.

**Recover**

This function addresses recovering from a data security event. The topic for this area is data breach notification.

Multiple questions pertaining to each function area were included in the survey. A detailed list of the survey questions is included in the confidential addendum as Appendix A (confidential per North Carolina General Statute 132 -6.1(c)).

The results of the survey were broken out by school districts of large, medium, small and charter school enrollments. District size was determined based on the 2015-16 average daily membership (ADM).

School districts are represented according to the size of the district based on the same criteria used previously by NCDPI, as follows:

- Small – Student enrollment of less than 12,000
- Medium – Student enrollment between 12,000 and 25,000
- Large – Student enrollment of greater than 25,000

All questions were fixed-response on a six-anchor scale reflecting the level of cybersecurity maturity.

Permissible responses for each survey item were list as follows.

0. Not Implementing = No policy, procedures or technology implemented
1. Emerging / Developing = Informal policies, procedures or technology implemented
2. Operationalized = Formalized policies, procedures or technology implemented
3. Optimized = Formalized policies, procedures or technology implemented which include quality control efforts such as auditing effectiveness

4. Not Applicable = did not pertain to the environment
5. Compensating Control = had implemented alternate security measures that met the intent of the identified controls

Additional instructions were provided for each question to assist in selecting the appropriate answer.

## Key Analysis Results from Conducting Surveys

Responses were received from 109 of the 115 school districts and 130 of the 158 charter schools. The survey received a strong response rate; however, the unfortunate events of Hurricane Mathew occurred shortly before the launching of the survey. Some school districts and charter schools that were affected by the hurricane were not able to participate in the survey.

A list of school districts and charter schools surveyed, as well as an indication of which schools responded to the survey, is included in the Addendum as Appendix B (confidential as provided in North Carolina General Statute 132 -6.1(c)). Survey questions asked about a range of cybersecurity policies and practices. Detailed analysis is included in the Addendum as Appendix A (confidential as provided in North Carolina General Statute 132 -6.1(c)).

# 5. Conducting Meetings and Interviews

As the work on the survey part of the study progressed, NCDPI IT staff recognized the need to gather additional information from pertinent sources outside of the school districts and charter schools. We conducted meetings and interviews with cognizant organizations, interest groups, State government leaders and other individuals with expertise in cybersecurity to add to and confirm the observations and insights gleaned from the survey exercise.

## General Observations from Meetings and Interviews

**Loss of federal funding for Internet content filtering and firewall services**

Internet content filtering and firewall services, which provide protection to our students from inappropriate and malicious content, have historically been bundled with the Internet services provided to all school districts and charter schools. All services in the bundle were E-rate eligible and subsidized by 70%. However, in 2015, changes were made to the Eligible Services List for the E-rate program which made bundled Internet content filtering and firewall services no longer eligible to receive a subsidy.

While NCDPI is currently covering these expenses with funds from the connectivity budget, the costs are rising due to increased usage. Loss of these services would dramatically increase the risk to school districts and charter schools. Additional funding will be required to cover the gap.

**School districts and charter schools are not mandated to follow the guidelines established in the North Carolina Statewide Information Security Manual**

The North Carolina Statewide Information Security Manual is both comprehensive and detailed in the guidance it offers for developing and implementing controls for information technology security. It is an excellent reference document for districts and charters to self-evaluate their level of maturity for cybersecurity and to develop and implement the appropriate controls.

# 6. Recommendations from the Study

### 6.1. Develop Common Templates and Prioritization Guidelines

The results of this survey indicate a need for state-level guidance and support to schools in both prioritizing and implementing important cybersecurity policies and practices. Policy templates and guidance documents will be drafted by NCDPI staff to help educate district and charter school IT personnel and provide assistance for improving their security postures. Initial efforts will begin addressing the major problems identified in the survey. The first step will be to characterize cybersecurity policies and practices in terms of both cost and importance. The Center for Internet Security has provided a "top 20" list of small actions for cybersecurity defense, focused specifically on low cost/high value solutions. This guidance will be drawn upon in the creation of these templates and guidelines.

### 6.2. Publish a Quarterly Information Security Newsletter

The results of the survey and communications with district and charter school personnel also revealed a lack of awareness about the importance and relevance of many key cybersecurity practices. This suggests on-going communication and awareness building efforts are needed. Further, cybersecurity is a rapidly changing subject area. School districts and charter schools need additional support in keeping up-to-date on the latest threats, available solutions, and best practices. NCDPI will begin drafting a quarterly security newsletter to communicate trends and hot topics within the realm of cyber and information security for school districts and charter schools. As part of the newsletter process, the districts and charter schools will be solicited for topic ideas to ensure relevance to them.

### 6.3. Provide Cybersecurity Awareness Training

The survey revealed that many districts and charter schools do not have a formalized cyber awareness training program for their employees. To increase professional development for public school employees across the state, we recommend providing required initial (upon hiring) and annual cyber awareness training. The annual recurring cost for this is estimated at $500,000.

### 6.4. Require school districts and charter schools to follow the guidelines established in the North Carolina Statewide Security Manual

The North Carolina Statewide Information Security Manual is the foundation for information technology security in North Carolina. It sets out the statewide information security standards required by N.C.G.S. §147-33.110, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets.

Requiring school districts and charter schools to adhere to the requirements established in the security manual would provide a unified security framework from which they could formalize their security programs. Adopting the statewide security guidelines and standards will allow the schools to focus on primarily implementing, auditing and remediating against deficient controls, instead of having to develop and establish separate policies. The manual addresses, among other topics:

a. Encryption
b. Configuration Management
c. Vulnerability Management
d. Data classification and handling
e. Account Management/Account Access
f. Media Protection
g. Risk Assessment
h. Incident Response

### 6.5. Provide Regional Cyber Security Specialists

In light of the limited IT security expertise in many schools, survey results suggest the need for experienced and knowledgeable regional staff to support school districts and charter schools in reducing risk to cybersecurity threats. To help implement the items above and to establish more fully the importance of cybersecurity within K-12 education, NCDPI proposes the creation of a regionally organized cybersecurity specialist team. These security specialists will conduct ongoing security assessments and provide technical assistance for developing and implementing security plans, policies, processes and best practices. This group would also facilitate the sharing of information regarding security and its best practices among school districts and charter schools. The annual recurring cost for these personnel is estimated at $996,000.

### 6.6. Provide State Funding for Internet Content Filtering and Firewall Protection

Due to changes made in 2015 to the Eligible Services List for the federal E-rate Program, public schools are no longer eligible to receive a federal subsidy, which was used to cover approximately 70% of the cost for their Internet content filtering and firewall services.

The 2016-2017 projected cost of Internet content filtering and firewall services is $5.5 million, and the cost of these services grows in conjunction with the growth of internet utilization. With no E-rate discount for these services, NCDPI will need to acquire additional annual funding in order to continue providing these critical security features to North Carolina schools.

# 7. Supporting Documents

Statewide Information Security Manual

- https://ncit.s3.amazonaws.com/s3fs-public/documents/files/SISM-2-2016.pdf

The PTAC Data Security Checklist and Data Governance Checklists can be found at the following links

- Data Security: http://nces.ed.gov/programs/ptac/pdf/ptac-data-security-checklist.pdf
- Data Governance: http://nces.ed.gov/programs/ptac/pdf/data-governance-checklist.pdf

The Critical Security Controls for Effective Cyber Defense can be found at the following link

- https://www.cisecurity.org/critical-controls.com

Cybersecurity in K-12 education: Schools face increased risk of cyber attacks

- http://fedscoop.com/cybersecurity-in-k-12-education-schools-around-the-country-face-risk-of-cyber-attacks

NIST Cyber Security Framework

- https://www.nist.gov/document-3764