NH Forum on Strengthening Cybersafety Skills & Systems

Opportunities for Collaboration

Tuesday September 6th, 2023
2:00-4:00PM Eastern
Welcome and thanks!

Panelists:

Denis Goulet  NH’s Chief Information Officer and Commissioner of Information Technology (and immediate past president, NASCIO)

Bob McLaughlin  Executive Director, National Collaborative for Digital Equity

Stephanie Turek  Assistant Vice President, Coordinated Services, Granite United Way, 211

Gerry Hanley  Executive Director, Skills Commons and MERLOT

Discussant  Michael Klein, Infrastructure Fellow, Office of Educational Technology, US Department of Education
Aims of the Webinar

Explore stellar opportunities for collaboration among state leaders to strengthen cybersafety systems and skills

• (USDOC) Federally-funded state digital equity and BEAD planning
• (DHS) Federally funded state & local cybersecurity system building
• (FCC) 211 Help Desks to point callers and visitors to essential human services
• (USDOL) Repositories of curated open educational resources for economic inclusion: SkillsCommons and MERLOT
• (ED) Statewide and local initiatives to grow digital literacy & cybersafety skills
State initiatives to build cybersecurity state & local systems
State digital equity planning & implementation

• 5 key metrics
• Metric #4: building cybersafety skills
• Metric #5: strengthening inclusiveness & accessibility of web portals to essential public resources/services
• State’s DHS-supported cybersecurity initiative
• 211 Help Desk
211 Help Desk

- Unique role of NH’s (and the nation’s) 211 Help Desks
- Strengths and limitations of NH’s 211 service
- Opportunities to strengthen the 211 service
Visitors to NH 211 & their Concerns

<table>
<thead>
<tr>
<th>211 NH 2022 Totals</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Calls to 2-1-1</td>
<td>73,588</td>
</tr>
<tr>
<td>211 Website Visits</td>
<td>46,706</td>
</tr>
<tr>
<td>Total contacts</td>
<td>160,831</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Top Calls - 2022</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Tax Related Inquiries</td>
<td>10109</td>
</tr>
<tr>
<td>Homeless Related Referrals</td>
<td>9741</td>
</tr>
<tr>
<td>SUD Related Referrals</td>
<td>8886</td>
</tr>
<tr>
<td>Utility Assistance Referrals</td>
<td>6551</td>
</tr>
<tr>
<td>COVID-19 Related Inquiries*</td>
<td>4739</td>
</tr>
<tr>
<td>Rent Assistance Referrals</td>
<td>4651</td>
</tr>
<tr>
<td>All Other Inquiries</td>
<td>28911</td>
</tr>
</tbody>
</table>

*There were 6,941 additional COVID-19 related calls that were routed to Maximus call centers.
Commonly Encountered Concerns

- Tax Related Inquiries: 14%
- Homeless Related Referrals: 13%
- SUD Related Referrals: 12%
- Utility Assistance Referrals: 9%
- Rent Assistance Referrals: 6%
- COVID-19 Related Inquiries: 7%
- All Other Inquires: 39%
SkillsCommons and State Digital Equity & Cybersafety initiatives

Dr. Gerry Hanley
Executive director

SkillsCommons & MERLOT
Accessibility, Access, and Inclusiveness

Not "Reinventing the Wheel" with Available Resources From SkillsCommons

Gerry Hanley, Ph.D.
Executive Director, MERLOT and SkillsCommons
Director, Cal State University Long Beach Center for Usability in Design and Accessibility
Professor Emeritus, Department of Psychology, CSULB
Speed and Effectiveness will be Key to Successful Use of Digital Equity Act Funds

• Leveraging NH CIO leadership and IT programs
• Leveraging NH 211 leadership and programs

• Resources from Federal Programs are available for immediate use.
  • SkillsCommons: US Dept of Labor’s TAACCCT funded free and open library for workforce development
Accessibility, Access, and Inclusiveness

• **Accessibility:** Everyone including those with disabilities are able to access and use the digital content with equal effectiveness.
  - Support United Way’s 211 website strategies to be WCAG (Web Content Accessibility Guidelines) compliant.
  - All the online resources referenced by United Way’s 211 website need to be WCAG compliant
    - SkillsCommons and CAST created a free and open “Accessibility Self-Service Support Center”
    - There are technology tools and companies that bring exceptional expertise and capabilities.
Build Capacities for Accessibility

Accessibility Checkpoints and Instruction Guide

The Accessibility Checkpoints

These checkpoints are meant to be used as a guide to improve the accessibility of a digital document. It is recommended to check if the document should be uploaded to the SkillsCommons repository.

Instruction Guide for Completing Checkpoints

This instruction guide provides explanations and examples for each checkpoint.

Accessibility Evaluation Manuals

The Accessibility Evaluation Manual contains checklists for accessibility that contain short descriptions of each checkpoint and materials provided to evaluate a document.

Reading Order - Digital resource layout

10. Reading Order - Digital resource layout

The reading order for digital resource content logically corresponds to the visual layout of the page when rendered by assistive technology.

Resources & Examples

To be accessible to non-visual readers, content must be marked up such that a logical path that excludes secondary material (e.g., endnotes, sidebars, charts, etc.) and orders the primary content can be followed by assistive technology.

“Best Practices in Organizing OER Content”

BC Open Textbook Accessibility Toolkit (BCcampus and CAPER-BC)

The resource below contains technical references with generic explanation of reading order and examples depending on the OER file type.

EPUB3 Accessibility Guidelines (International Digital Publishing Forum)

Checking Logical Reading Order with CommonLook PDF (NetCentric Technologies) Note this is from a commercial vendor
Accessibility, **Access**, and Inclusiveness

**Access:** Providing FREE and OPEN access to user-friendly resources

- Both time and money are barriers to access the resources
- Service providers can offer some of their resources free and open
  - SkillsCommons created an “Open Licensing Support Center” in collaboration with Creative Commons with a free online course.
  - SkillsCommons partnered with [CSULB Center for Usability in Design and Accessibility](#) to provide examples and guidelines on how to reuse, revise, remix open educational resources to be more user-friendly for your users.
Build Capacities to Leverage & Create OER

Reuse “as is” OER

Reuse “as is” = no modifications were made to the original material(s). Materials accessed/downloaded from SkillsCommons and used “as is.”

View Reuse Showcase

Revise and Reuse OER

Revise and Reuse = Edits to the content, branding, scope, and sequence applied, while keeping authoring technology of the original material(s).

View Revise & Reuse Showcase

Makeover OER

Makeover = Innovative technologies applied to original material(s) transforming them into more usable, UDL, and effective resources(s).

View Makeover Showcase
Accessibility, Access, and Inclusiveness

• Inclusiveness: There are many dimensions of inclusiveness that creates opportunities for diverse communities to achieve equitable outcomes through processes that recognize and give agency to the diverse communities.

• Economic Inclusiveness: SkillsCommons can support your community members’ workforce readiness skills for jobs with sustainable living wages.

• Digital Inclusiveness: SkillsCommons’ sister program, MERLOT provides free and open learning resources to develop people’s digital literacy skills so they can “live online”
Build Capacities for Inclusiveness

Industry Sector Training Materials

Explore the FREE and OPEN library of materials designed for education and industry in recruitment, training and occupations across Ohio:

Machining Career Pathway

Ohio Wages as reported on makingohio.com. Click on *“* for Job Requirements.

- **PRODUCTION TECHNICIAN** $37,662
- **MACHINE OPERATOR** $39,834
- **MACHINIST 1** $41,126
- **MACHINIST 2** $53,482
- **TEAM LEAD** $53,482
- **ENGINEERING TECHNOLOGIST** $61,809
- **CNC PROGRAMMER** $59,882
- **MACHINE SHOP SUPERVISOR** $70,087
- **MANUFACTURING ENGINEER** $86,326

Career Descriptions

Explore Machining careers at CareerOneStop

- Machine Feeders and Loaders
- Office Machine Operators, Except Computer
- Continuous Mining Machine Operators
- Saw Machine Operators and Tenders
- Core Drill, Automated Tuber, and Office Machine Repairers
Capabilities Maturity Model: Sustainability Strategy for Digital Equity Act Investments

Characteristics of the Maturity levels:

- **Initial (Level 1)**: Processes unpredictable, poorly controlled and reactive.
- **Managed (Level 2)**: Processes characterized for projects and is often reactive.
- **Defined (Level 3)**: Processes characterized for the organization and is proactive. (Projects tailor their processes from organization's standards)
- **Quantitatively Managed (Level 4)**: Processes measured and controlled
- **Optimizing (Level 5)**: Focus on process improvement
Maturing Capabilities Begins With Where People Are Today

• **Principles of CMM**
  - Assess what level your organization is currently functioning and identify the next level “up”.
  - You can’t skip level.
  - Your established level of operations functions as the foundation for the next level of operations.
  - You have to practice the operational policies, not just declare policies about how you want to operate.
  - Maturing operational capabilities requires the professional development and persistence of staff.
  - Gradual progress should be celebrated with regular recognition.
Collaboration at the State Level is Essential for Sustainability and Success

SkillsCommons has identified exemplary practices for state level strategies for coordinating many partners required to solve complex problems.

https://support.skillscommons.org/paving-pathways/
US Dept. of Education’s support for state and local digital equity & cybersafety initiatives

Michael Klein
Infrastructure Fellow
Office of Educational Technology
US Department of Education
Why should we be concerned about K-12 cybersecurity?
1,619 K-12 Cyber Incidents Between 2016-2022

Hackers leak 500GB trove of LAUSD ransomware attack
data

Des Moines Public School year after school
district approves ransomware

Samantha Hernandez
Des Moines Register

Published 11:45 a.m. CT Jan. 10, 2023 | Updated 3:07 p.m. CT
Pillar 1: Defend Critical Infrastructure

WH National Cybersecurity Strategy

“We will give the American people confidence in the availability and resilience of our critical infrastructure and the essential services it provides.”

ANCD Kemba Walden: “We expect school districts to go toe-to-toe with transnational criminal organizations largely by themselves. This isn't just unfair; it's ineffective. The biggest and most capable and best positioned actors in our digital ecosystem can and should shoulder a greater share of the burden for managing cyber risk and keeping us all safe. And that includes the federal government.”
What steps are we taking right now?
Step 1: Elevate Importance of K-12 Cyber
Step 2: Establish a GCC to enable coordination

The Department will launch a Government Coordinating Council (GCC) to coordinate activities, policy, and communications between federal, state, local, tribal, and territorial governments that strengthen the cyber defenses and resilience of K-12 schools.

What this means: By facilitating ongoing collaboration between all levels of government and the education sector, the GCC will be a key first step in the Department’s strategy to protect schools and districts from cybersecurity threats and for supporting districts in preparing for, responding to, and recovering from cybersecurity attacks.

Impact:
• Fulfills #1 recommendation from the October 2022 GAO Report.
• Brings ED closer to other sectors like Election Infrastructure and Healthcare that already have GCCs with robust engagement
Step 3: Provide Actionable Guidance

K-12 DIGITAL INFRASTRUCTURE BRIEF:
DEFENSIBLE & RESILIENT
High-Impact Recommendations

Prioritization of the greatest risks and mitigations can begin to address these challenges. Many malicious cyber actors gain initial access in one of three ways:¹⁴

1. Compromising valid accounts, often with weak or stolen credentials
2. Phishing users with a malicious link or attachment
3. Exploiting unpatched known vulnerabilities in public-facing applications

In October 2022, ED, the U.S. Department of Homeland Security, the U.S. Department of Justice (DOJ), and the U.S. Department of Health and Human Services (HHS) jointly released a 1-page set of Cybersecurity Action Steps for the K–12 Community, which details steps that districts can take to dramatically reduce their cybersecurity risk and potential liability:

1. Enable Multi-Factor Authentication (MFA)
2. Use strong, unique passwords for every account
3. Recognize and report phishing
4. Update your software
NORTH DAKOTA'S WHOLE-OF-STATE APPROACH TO CYBER

In April 2019, State Bill 2110 made North Dakota (ND) "the first state to authorize a central, shared service approach to cybersecurity strategy across all aspects of state government including state, local, legislative, judicial, K-12 education and higher education." This whole-of-state approach empowered the state Chief Information Security Officer and North Dakota Information Technology (NDIT) to address third-party risk in several ways:

- **NDIT’s Joint-Cybersecurity Security Operations Center (JCSOC)** protects endpoints and networks across ND and enables collaboration with at least 10 other states.

- **Lower Insurance Costs:** Entities that adopt NDIT cybersecurity shared services receive a 4 percent reduction in cost from the North Dakota Insurance Reserve Fund, the state insurance entity.

- **Third-Party Risk Assessment:** As of July 2023, all ND state agency vendors will be required to undergo a third-party risk management assessment in order to sell products or services to any of the 57 ND state agencies. Fast track options for vendors with one of three recognized cloud security certs: FedRAMP, StateRAMP, HITRUST.
Identify: Free Action to Take

If you only do one thing...

Mitigate Known Exploited Vulnerabilities (CPG 1.E)

Cybersecurity threats can feel overwhelming given limited resources in terms of time, staff, and funding. CISA and ED strongly encourage organizational cybersecurity leaders to focus on identifying and mitigating known exploited vulnerabilities: the small subset of vulnerabilities that are being actively exploited in the wild and have clear remediation actions to mitigate against that immediate harm.

As a state or district cybersecurity leader, the highest-impact action you can take to address this challenge (for Free!):

- Sign up for CISA’s Cyber Hygiene Vulnerability Scanning. Vulnerability scanning helps secure internet-facing systems from weak configurations and known vulnerabilities and encourages the adoption of best practices. SEAs and local educational agencies (LEAs) that enroll get a weekly vulnerability scan and report, and, importantly, they are automatically enrolled in CISA’s Ransomware Vulnerability Warning Pilot.
Detect: Example

Connecticut’s Approach to No-Cost Cybersecurity Services

In addition to providing accessible and equitable pricing for broadband to 100 percent of the school districts in Connecticut, the Connecticut Education Network (CEN) includes a number of cybersecurity services at no additional cost. CEN provides

- Distributed Denial of Service (DDoS) monitoring and mitigation protections,
- inline and remote Children’s Internet Protection Act (CIPA) filtering for all K–12 districts and libraries (which expanded to include 1:1 device initiatives during emergency remote learning and throughout the pandemic), and
- DNS firewall.
Detect: Free Action to Take

*If you only do one thing...*

Join the Multi-State Information Sharing and Analysis Center (MS-ISAC)

MS-ISAC is a CISA-funded Information Sharing and Analysis Center (ISAC) operated by the Center for Internet Security designed to serve as the central cybersecurity resource for the nation's state, local, territorial, and Tribal (SLTT) governments, including educational institutions. Members receive direct access to a suite of services and informational products including cybersecurity advisories and alerts, vulnerability assessments, incident response support, secure information sharing, tabletop exercises, a weekly malicious domains/IP report, and more. To learn more about the MS-ISAC program, email directly at info@msisac.org or visit their website at [www.cisecurity.org/ms-isac](http://www.cisecurity.org/ms-isac).
North Carolina’s Joint Cyber Task Force

North Carolina’s whole-of-state approach provides a powerful example that combines

- information sharing,
- mandatory incident reporting, and
- real-time incident response in support of K–12 schools.

In January 2021, North Carolina built a Joint Cybersecurity Task Force that includes the FBI, National Guard, SEA, and school districts. The task force is authorized by the governor and the legislature to mobilize the National Guard and deploy a strike force to support districts immediately upon learning of a cybersecurity incident, which all school districts and local governments are required to report based on the state’s new incident reporting law. “The IT Strike Team is a group of volunteers and members of the North Carolina Local Government Information Systems Association (NCLGISA), an association of local government IT professionals. Strike team members volunteer their time and skills and, along with the National Guard, serve as boots on the ground to provide on-scene response and recovery services.”
Respond: Free Action to Take

If you only do one thing...

Get to Know Local CISA and FBI Points of Contact

Cyber Incident Response is a Team Sport. There are many federal, state, regional, and local resources to support you as you navigate what may be one of the most challenging experiences of your career. In terms of federal support for incident response, your two most important points of contact are your local FBI field office and your CISA regional Cyber Security Advisor. If you are not sure how to find CISA or FBI help locally, contact your CISA regional office or local FBI field office.
Bonus High-Impact Free Action to Take

If you only do one thing...

Run a Tabletop Exercise with your District Leadership Team (CPGs 1.F, 4.A)

As a district leader focused on buying down cybersecurity risk, there is no bigger bang for your buck than running a 60–90-minute tabletop exercise with your executive leadership team. Drills and exercises offer a way of making infrastructure visible to the community so everyone can understand their role in protecting it and what to do in case it fails.

CISA and ED have developed K–12-specific tabletop exercises that you can use immediately or modify to meet specific needs. CISA’s K–12 Schools Tabletop Exercise Package features a scenario where a threat actor targets district employees through phishing emails. Ransomware compromises the computer system with multiple impacts including exfiltration of students’ PII, loss of school HVAC system control, and media inquiries. In the REMS-TA Cybersecurity Tabletop Exercise, you should imagine that you are a member of your school’s emergency planning team and that you have access to only the resources and systems you currently have in place. You will discuss your response to a hypothetical cybersecurity incident, specifically a data breach that occurs because of malware.
Q & A with our panelists

Panelists:

Denis Goulet    NH’s Chief Information Officer and Commissioner of Information Technology (and immediate past president, NASCIO)

Bob McLaughlin  Executive Director, National Collaborative for Digital Equity

Stephanie Turek Assistant Vice President, Coordinated Services, Granite United Way

Gerry Hanley    Executive Director, Skills Commons and MERLOT

Discussant:    Michael Klein, Infrastructure Fellow, Office of Educational Technology, US Department of Education
Framing the Challenge