Cybertrack

Indiana's Local Government Cybersecurity Assessment Program

Quarterly Progress Report for Q1 CY26

April 2026

Joe Beckman, Craig Jackson
Ranson Ricks, Leigh Ann Griffin, George Bailey

---

1 Executive Summary

About Cybertrack. With sponsorship from the Indiana Office of Technology (IOT), Purdue University and Indiana University have partnered to develop Cybertrack: Indiana's Local Government Cybersecurity Assessment Program. Cybertrack is designed to put local organizations in contact with top tier cybersecurity experts and provide them with practical, prioritized advice about doable, proven-powerful cybersecurity fundamentals. Our goal is to make Indiana more secure in the short term and shape our collective cybersecurity strategy and policy for the long term. Cybertrack cybersecurity assessments are available for no fee to Indiana local entities.

Highlights from this Quarter. This report covers 1 Jan - 31 March 2026, including the following highlights. In this quarter, we:

- **Delivered 18 assessment reports**. Cumulatively, we have **completed 196 assessments** over the life of the program.
- **Received 70 applications**, including 9 applications for reassessments, and **onboarded 22** organizations.
- **Found that reassessed organizations demonstrated more measurable progress** in implementing the highly-impactful practices we measure. *See* Section 6.
- **Briefed the Indiana Supreme Court**, including Chief Justice Rush, Justice Slaughter, Justice Goff, and Justice Molter, as well as several of the Court's administrative leaders on the Cybertrack assessment we completed in July 2025. *See* Section 7.
- Continued to receive overwhelmingly positive responses to **post-assessment questionnaires**. *See* Appendix E.
- **Briefed the Indiana Executive Council on Cybersecurity** (IECC) on the basics of the Cybertrack program high-level aggregated data analysis trends across the State. We received vocal positive feedback from CIO Lenard, and representatives of both the Secret Service and Transportation Security Administration (TSA) foot-stomped Cybertrack's emphasis on fundamentals and our evidence-driven calls to action. *See* Section 7.

> **"Your team's work, and the way you presented it, made clear that this was not a checkbox exercise but a thoughtful, evidence-based effort to help make our judiciary measurably safer. … Thank you again for your time, your expertise, and the work you and the broader Cybertrack team are doing to strengthen cybersecurity across Indiana's public institutions."**
>
> **- Chief Justice Loretta Rush**

- **Submitted a whitepaper to IECC leadership** titled "Maximizing Impact," aimed at providing ideas to the Council as it conducts strategic planning. *See* Section 7.
- Hosted personnel from the **Indiana Department of Environment Management** (IDEM) and the **Indiana National Guard** (INNG) as observers in Cybertrack+ onboarding and discovery sessions, deepening our collaboration with these organizations. *See* Section 7.
- Initiated an internal discussion on potential programmatic and methodological expansions and refinements for "**Cybertrack 2.0**." *See* Section 2.

Looking Ahead. Over Q2 CY26, we expect to:

- Conduct a follow-on planning meeting with IDEM.
- Continue recruiting efforts to include pursuing utilities to participate in the Cybertrack+ assessment.
- Release the next Aggregate Analysis & Results Report in early June 2026.
- Participate in IOT's Base Camp and Public Sector Cybersecurity Summit (16-17 June).

Roadmap for this Report. The remainder of this report is broken down by the Cybertrack program's major activity areas: **Sponsor Engagement** (Sec 2), **Recruitment** (Sec 3), **Methodology** (Sec 4), **Assessment Execution** (Sec 5), **Aggregate Analysis & Reporting** (Sec 6), and **Broader Impacts & Relationships** (Sec 7).

The report also includes the following appendices:

- **Appendix A:** Recent and Upcoming Events
- **Appendix B:** Distribution of Implementation Ratings
- **Appendix C:** Distribution of Implementation Ratings (Transformative Twelve)
- **Appendix D:** Geographic Distribution of Cybertrack-Assessed Entities
- **Appendix E:** Responses to Impact and Feedback Questionnaires

2 Sponsor Engagement

The Cybertrack team continued to support IOT's outreach to local governments through frequent participation in IOT's weekly Ideas Exchanges, Town Halls, meetings, and IECC meetings.

In this quarter, the Cybertrack team assisted in developing the Call for Proposals for IOT's cybersecurity Base Camp training day scheduled for 16 June. The Call for Proposals focuses criteria on Cybertrack Calls to Action & the least implemented Musts & Safeguards from Cybertrack Aggregate Analysis & Results reports.

Looking Ahead. As we experience a surge in demand for Cybertrack assessments[1] and reach the final 40% of the funding on the initial Cybertrack award, we've begun organizing our thoughts on the shape of "**Cybertrack 2.0.**" We hope to begin brainstorming with IOT in Q2, so that we are well-ahead of fiscal planning cycles and can respond to the heightened demand in a timely way.

[1] *See*, Section 3 (Recruitment) for more detail.

We are closely managing the use of remaining program funding, which stood at **~$1.6M** at the end of March 2026. Based on an estimated mix of 70% standard and 30% Cybertrack+ assessments, we project that these funds will support **~135 more assessments** (*i.e.*, 90 Standard and 45 Cybertrack+). Ninety-eight applicants (92 standard Cybertrack assessments, 6 Cybertrack+ assessments) are currently awaiting or in the process of assessment. While our no cost extension (NCE) runs through June 2028, at the current usage rate, we anticipate full fund exhaustion during **Q3 FY2028 (January–March 2028)**. And, considering the surge in recruitment discussed in Section 3, we may exhaust the funds at a faster rate if we increase production above the planned 5-6 assessments per month.

We used our annual in-person all hands Cybertrack team meeting to ideate on programmatic and assessment methodology expansions and refinements that would further amplify Cybertrack's impact in years to come. Sources of ideas include feedback we've received from IOT and other key state stakeholders, input received from Cybertrack participants, and the collective experience of our frontline assessors and program managers. Ideas for Cybertrack 2.0 include, but certainly aren't limited to (a) making post-assessment outbriefs standard for all assessments,[2] (b) offering limited post-assessment engagements to accelerate organizations' action on our recommendations, (c) expanding the Cybertrack team to include partner organizations, (d) explicitly expanding and clarifying the scope of organizations that can qualify for an assessment, and (e) including a leadership/elected official engagement activity as part of the larger program.[3]

We had a number of other meaningful interactions with Indiana state stakeholders in Q1. See, Section 7 (Broader Impacts & Relationships) for more.

3 Recruitment

In Q1, Cybertrack received **70 applications** and **onboarded 22 entities** for assessments.

K-12 schools, utilities, and reassessments drove recruitment in this quarter:

- **K-12 Schools:** Our regular engagement with Brad Hagg (Director of Educational Technology at the Indiana Department of Education) and the CTO Council[4] continues to bring applicants to Cybertrack. K-12 recruitment was mostly driven in Q1 by messaging from Brad Hagg to all of IDoE's K-12 IT points of contact via the HECC listserv reminding them of Cybertrack's availability and of the cybersecurity assessment requirements in IC 4-13.1-4-8. Brad's message generated **57 applications** in March. Six applications resulted from Cybertrack's January K-12 "Ask Me Anything" Teams session described in Section 7.
- **Utilities:** Our work recruiting utilities in previous quarters and continued interaction with IDEM produced additional recruits. We received **two Cybertrack+ applications** this quarter, both from municipal governments. We expect the number of applications for Cybertrack+ assessments to continue to grow as the number of entities that can serve as peer references for Cybertrack+ increases and as our work with IDEM develops concrete

[2] Recent post assessment questionnaires suggesting this would be a welcomed feature.
[3] This may include proactive engagement with municipal organizations such as Accelerate Indiana Municipalities (AIM) and Indiana Conference of Mayors (ICOM).
[4] The CTO Council is Indiana's chapter of the Consortium for School Networking (CoSN). Additional information about the CTO council is available at: https://www.indianactocouncil.org/.

recruitment tasks.

- **Reassessments:** Nine of the 70 applications this quarter were for reassessments. As of 31 March 2026, 36% (34/94) of the organizations who qualify for a reassessment have requested one.
- Applications this quarter also included **one municipal government** alongside **two township governments** and **two libraries seeking Cybertrack assessments**.

In Q2, we expect our relationship with IDEM to drive interest in the Cybertrack program. As noted in Sponsor Engagement, members of Cybertrack's leadership team are continuing to work with IDEM to find and implement concrete actions to recruit additional water/wastewater utilities into Cybertrack+.

4 Methodology Research, Development, Refinement, and Training

In this section, we cover activity regarding Cybertrack+ R&D (4.1) and Post-Assessment Findings (4.2).

4.1 Cybertrack+ R&D

We have successfully transitioned from the major development phase of Cybertrack+ into active production assessments. The team has shifted its focus toward refinement and operational efficiency, with a specific concentration on developing new and variant recommendations tailored for operational technology-reliant organizations.

Originally launched in December 2024, Cybertrack+ was driven by the critical and growing cybersecurity threats facing our nation's operational technology-reliant environments, particularly in water and wastewater operations.[5] This assessment is best for organizations with a substantial and/or mission-critical operational technology footprint. It addresses both IT and OT equally well.

4.2 Post-Assessment Findings

The team continued to receive positive feedback from the **post-assessment questionnaires** we developed and placed in production in Project Year 2. These are designed to assess and improve both the quality and participant satisfaction with the assessment experience, and get an initial sense of the program's impact**.** Continuing the theme for early reassessment results, questionnaire data shows that Cybertrack and state-wide initiatives are having an impact. One of the most encouraging and impactful findings is that **more than 87% percent of organizations responded "Yes" to the question "Has your organization taken action on any of the recommendations in the Cybertrack assessment report?"**

[5] https://wisdiam.com/publications/recent-cyber-attacks-water-wastewater/.

Appendix E provides more information about the questionnaires and includes a more comprehensive summary of the positive results we are seeing. The following quotes stood out among the ones we received this quarter:

> "This program is valuable for even the smallest units because even if you can't implement all of the recommendations, it does make you think of your processes and gives tips for simple things that can be done for little to no costs."
>
> *-Julie Elmore, Oakland City Columbia Township Public Library*

> "The Cybertrack team professionally and passionately cares about the municipalities they serve in delivering both a strategic and tactical roadmap that minimizes cybersecurity risk to the organization."
>
> *-City CIO*

> "This has been the best experience when it comes to learning and improvement. All recommendations were easy to follow and I feel I was able to address most right away."
>
> *-Technology Director, K-12*

> "The Cybertrack process was exceptionally well-organized and clearly communicated. It provided the structure we needed to sharpen our focus and effectively narrow down our cybersecurity goals."
>
> *-Assistant Director of Technology Operations, K-12*

5 Assessment Execution Management

We continued to hold monthly multi-organization onboarding sessions. The following table provides metrics including quarterly and cumulative assessed entities by entity type. **At the close of Q1 2026, Cybertrack had delivered 196 reports.** The greater number of assessed entities reflects single assessments performed for multiple entities that share common, centralized IT services. Examples include a county and its largest municipality or a town and its local school district. In Table 1, note that "ReA" references Cybertrack reassessments. For example, we have cumulatively completed 37 assessments of county governments; 8 of those completed assessments were reassessments.

Table 1: Numbers of Onboarded Organizations and Delivered Reports, Q1 2026 & Cumulative

	Q1 2026		Cumulative	
Type of Organization	**Onboarded**	**Report Delivered**	**Onboarded**	**Report Delivered**
Cybertrack Assessment				
County Government	0	1 (1 ReA)	42	37 (8 ReA)
Municipal (City/Town) Government	1	1	51	4 (ReA)
Township Government	0	0	10	7 (0 ReA)
K-12 School District	10	3 (1 ReA)	79	65 (1 ReA)
Library	6	9	34	30 (0 ReA)
Other (e.g., Utilities, Airports, Special Service Districts)	0	0	6	7 (0 ReA)
Subtotal	***17***	***14***	***222***	***189 (13 ReA)***
Cybertrack+ Assessments				
Municipal (City/Town) Government	5	4 (2 ReA)	9	6 (3 ReA)
Other (e.g., Utilities, Airports, Special Service Districts)	0	0	3	1
Subtotal	***5***	***4***	***12***	***7***
Total	**22**	**18**	**234**	**196 (16 ReA)**[6]

6 Aggregate Results & Analysis

The Cybertrack team will release our next Aggregate Results & Analysis Report in 2026, prior to the next Indiana Public Sector Cybersecurity Summit scheduled to begin on 16 June.[7] That report will provide new insights driven by our growing sample size, more in-depth analysis of existing trends, our first analysis of data from Cybertrack+ assessments, and our first quantitative analysis of Cybertrack's impact using reassessment data. We will discuss the nature of Cybertrack's impacts on assessed organizations, and on the cybersecurity ecosystem in which Indiana's local public sector organizations operate. **Appendices B and C** provide a continuation of results reporting since our June 2025 report. Results and trends remain consistent with those reported in June 2024 and 2025.

[6] Four municipalities received their first Cybertrack+ assessment that also served as a reassessment of their original Cybertrack assessments. Because Cybertrack and Cybertrack+ are scoped differently at the CIS Safeguard level, these four assessments were not counted as reassessments in Table 1.

[7] Our last full Aggregate Results & Analysis report (from June 2025) is available at https://incybertrack.org/media/4kejmeyk/cybertrack-aggregate-results-report-june-2025.pdf

Initial Cybertrack Assessments: As shown in Table 1 above, public libraries made up 64% (9/14) of initial Cybertrack assessments completed in Q1. As a group, organizations assessed this quarter exhibited similar cybersecurity profiles to others receiving initial Cybertrack assessments over the life of the program. Average total assessment score for primary assessments this quarter was 34.53 points versus an overall average of 34.54 points.

Reassessments: **Organizations have demonstrated measurable progress in implementing the highly-impactful practices we measure.** On average, since their first Cybertrack assessment, these 13 organizations have increased or refined their implementations by 10.4 points (up from 8.5 points measured at the end of Q4 2025).[8] This average increase can be generally characterized as an increase in implementation level across several Trusted CI Framework Musts, which account for 2.3 points (22.1%) of the average increase, and CIS Safeguards, which account for 8.3 points (79.3%) of the average increase.

These findings serve as a key metric, providing evidence of Cybertrack's positive return on investment for the state. As of this report, there are 10 more reassessments scheduled, being scheduled for onboarding, or in the process of receiving a reassessment.

While today's sample size is small (13 entities), we are closely analyzing these results as they come in: All but one reassessed organization showed overall progress by increasing their total scores; variations in the magnitude of these improvements ranged between 2 and 40 points. Thus far, we can characterize ratings results from reassessed entities generally as showing some progress made on Trusted CI Musts accompanied by progress on several assessed Safeguards. The progress made also broadly follows recommendations made in the entities' initial Cybertrack assessment. That is, these organizations have taken action on the recommendations in their first assessment reports.

Regarding Reassessment Outliers. Notably, we again removed the highest positive score from this average because it is a statistical outlier. That is, the 10.4 average point increase **does not** include one reassessed entity which increased or refined its implementation of evaluated Musts and Safeguards by **40 points**, tripling its ratings score in reassessment! In this case, the assessed entity further developed its implementation by at least one rating level on 5 of 6 Trusted CI Framework Musts, and 19 of 27 CIS Safeguards. On 11 Musts and Safeguards, the entity advanced two ratings levels.

In the case of the entity that did not show overall progress in reassessment, it did show progress in some areas of cybersecurity. The entity progressed in areas of governance as reflected in its Musts ratings, but continued to work on gaps in some key Safeguards, including newly-noted gaps in secure configuration.

Reassessment Case Example. Post-assessment progress varies significantly by entity, but the general pattern is represented in the following case. In this case, the assessed entity received recommendations for action on Must 5 (Leadership), Must 9 (Policy), as well as Must 12 (Budget) and Must 13 (Personnel). CIS Safeguard recommendations focused on securing administrative access (CIS 3.3 & 5.4) through secure configuration (CIS 4.1 - 4.3) and implementation of multi-factor authentication (MFA,CIS 6.3 - 6.5). The assessed entity moved from Not Implementing to

[8] **Implementation Rating Quantification:** Cybertrack uses a four-level ordinal scale (Not Implementing, Developing, Implementing, Optimizing). Progress is quantified numerically, where each step represents an increase of "1". For example, progressing from Not Implementing to Developing is an increase of 1, and from Not Implementing to Implementing is an increase of 2.

Developing on these four Musts, developed and implemented more secure configuration processes, and broadened its implementation of MFA.

Cybertrack+ Assessments: These assessments evaluate all Musts and Safeguards from standard Cybertrack assessments, as well as twelve additional Safeguards to more completely capture cybersecurity control implementations in OT-reliant environments. The first eight organizations assessed using Cybertrack+ averaged a total score of 46.29 out of 138 points (33.5% of the points possible in this type of assessment). This percentage compares to an average of 33.3% of the total points possible achieved by organizations receiving an initial Cybertrack assessment and 40.2% of the total points possible achieved by organizations after reassessment. These results are consistent between initial Cybertrack and Cybertrack+ assessments.

7 Broader Impacts & Relationships

This section highlights the expanding engagements and strategic relationships that the Cybertrack program and its methodology are fostering both across Indiana and at the national level. Over this last quarter:

- Craig Jackson and Joe Beckman briefed the **Indiana Executive Council on Cybersecurity** (IECC) at its January 30th quarterly meeting. The briefing covered the basics of the program, key results, and three critical calls to action based on the results of Cybertrack assessments through CY 2025. We received vocal positive feedback from CIO Lenard. Later in the meeting, representatives of both the Secret Service and Transportation Security Administration (TSA) vocalized their support for Cybertrack's emphasis on fundamentals and our evidence-driven calls to action.

- Considering the fact that IECC is in a forward-looking, strategic planning phase, in March, Craig Jackson and Joe Beckman offered a short whitepaper to IECC leadership entitled, **"Maximizing Impact: Ideas for the Next Phase of the Indiana Executive Council on Cybersecurity."** Based heavily on Cybertrack's findings, the whitepaper recommends (a) focusing on initiatives that directly address evidence-based best practices and empirically-identified needs, (b) prioritizing broadly-applicable initiatives designed to maximize the breadth and depth of impact on cybersecurity capabilities, and (c) orienting initiatives to outcomes and measurable impact.

- Craig Jackson (IU), Kelli Shute (IU) and Matthew Crane (PU) briefed the **Indiana Supreme Court**, including Chief Justice Rush, Justice Slaughter, Justice Goff, and Justice Molter, as well as several of the Court's administrative leaders on the Cybertrack assessment we completed in July 2025. Following the briefing, we received a letter from Chief Justice Rush, including the following statements:

> "Your team's work, and the way you presented it, made clear that this was not a checkbox exercise but a thoughtful, evidence-based effort to help make our judiciary measurably safer. … Thank you again for your time, your expertise, and the work you and the broader Cybertrack team are doing to strengthen cybersecurity across Indiana's public institutions."

- In our continued collaboration with the **Indiana National Guard**, MAJ Christopher Myers (Director of Cybersecurity) participated as an observer on Cybertrack+ assessments and an onboarding meeting. The purpose of the observations was to provide INNG a more complete, hands-on understanding of the assessment methodology and process. Additionally, we anticipate exposure is highly beneficial for both our organizations as we explore ways to collaborate and potentially expand services beyond assessments. Meetings planned for Q2 2026 will focus on how Cybertrack and INNG will coordinate and build awareness of our complementary services.

- Similarly, **Indiana Department of Environmental Management** (IDEM) personnel Travis Goodwin (Security and Counter Terrorism Coordinator, Office of Water Quality), Andrew Dryden (Technical Environmental Specialist, Compliance Branch, Office of Water Quality) observed a Cybertrack+ F4 discovery session in advance of further coordination to discuss concrete steps to promote Cybertrack to Indiana water and wastewater utilities. Meetings planned for Q2 2026 will focus on how Cybertrack will coordinate programming with IDEM.

- Cybertrack hosted an hour-long **"Ask Me Anything" session sponsored by the CTO Council**.[9] The session focused on answering the cybersecurity questions of K-12 IT and district leaders. A second "Ask Me Anything" meeting is scheduled for Wednesday, April 29th.

- We continued our engagements with the **Center for Internet Security** (CIS) and the **UC Berkeley Center for Long-Term Cybersecurity** (CLTC), sharing updates and exploring ways to collaborate on a national scale.

[9] https://www.indianactocouncil.org/

Appendix A: Recent and Upcoming Events and Milestones

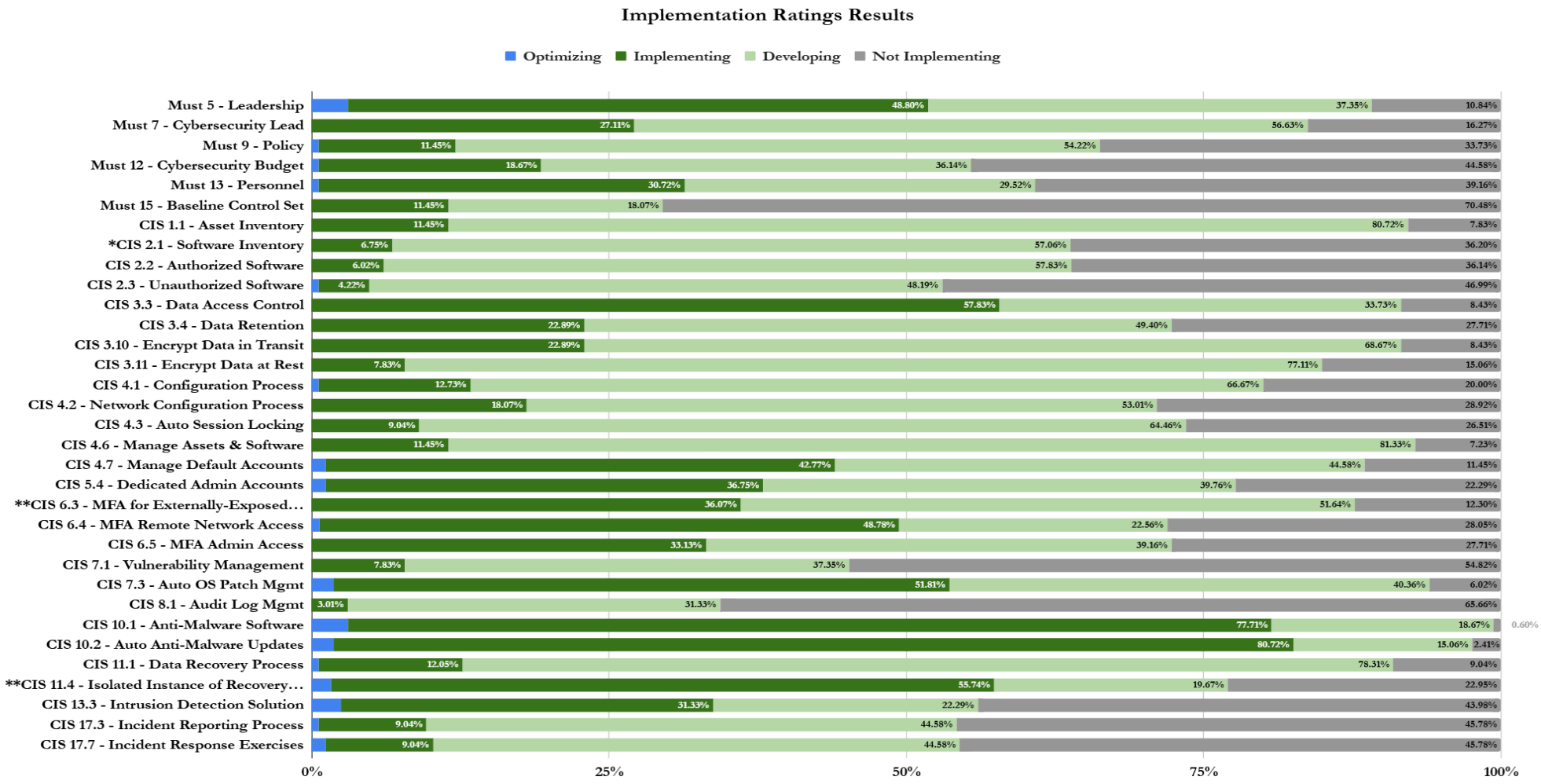
Recent Events

20 Jan	Cybertrack Executive Steering Committee Meeting
30 Jan	Governor Braun's Executive Council on Cybersecurity Meeting

Upcoming Events

20 Apr	Cybertrack Executive Steering Committee Meeting
24 Apr	Governor Braun's Indiana Executive Council on Cybersecurity Meeting
12 Jun	Release Aggregate Results & Analysis Report #4
16 Jun	IOT Bootcamp
17 Jun	IOT Public Sector Cybersecurity Summit

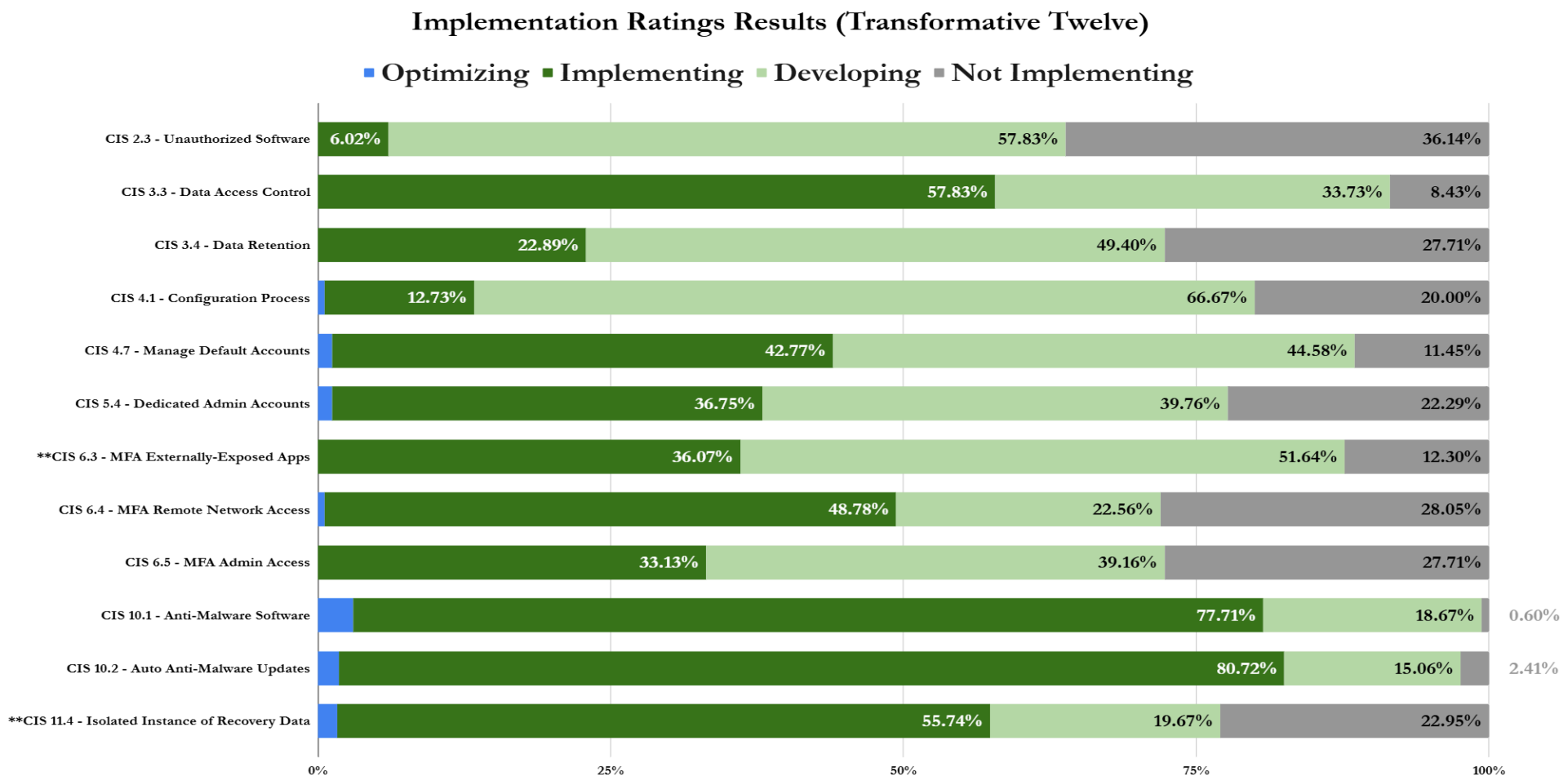
Appendix B: Distribution of Implementation Ratings



* The three Alpha Pilot assessments did not include evaluation of CIS Safeguards 2.1.

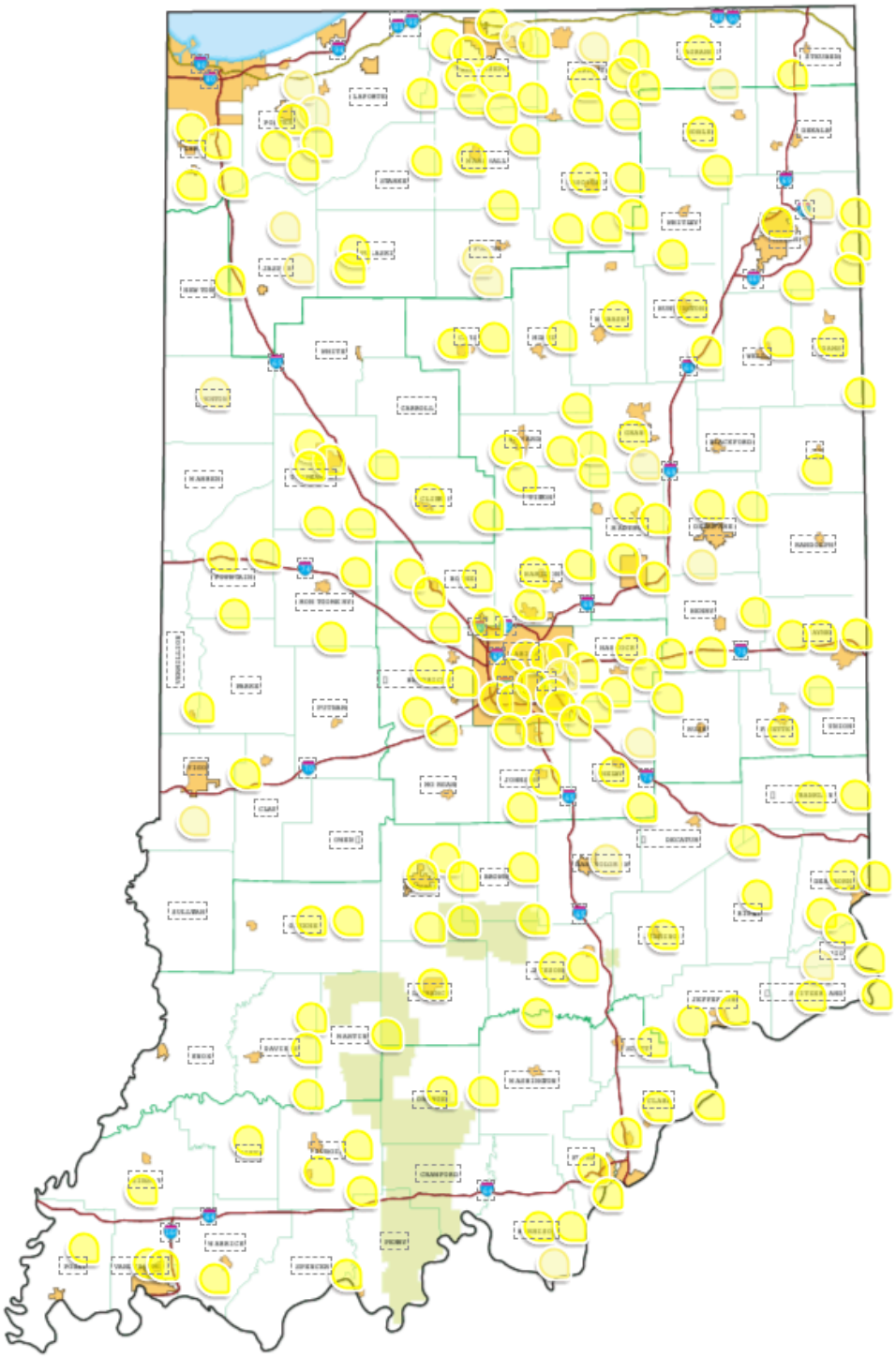
**Cybertrack began assessing Safeguards 6.3 & 11.4 in January 2024. These Safeguards were assessed for thirty-two entities at the time of this report.

Appendix C: Distribution of Implementation Ratings (Transformative Twelve)



**Cybertrack began assessing Safeguards 6.3 & 11.4 in January 2024. These Safeguards were assessed for thirty-two entities at the time of this report

Appendix D: Geographic Distribution of Cybertrack-Assessed Entities through December 2025



Appendix E: Responses to Impact and Feedback Questionnaires

In December 2023, we completed a pilot implementation of our post-assessment **Cybertrack Assessment Impact Questionnaire** with the three Alpha pilot organizations. Because our reassessment cycle would not start until CY2025, with a likely rhythm of no more frequent than every two years, we are using this instrument to determine whether and how our assessments impact the participating entities. We solicit responses from all participating organizations at 6 months following the delivery of their assessment report and at 6-month intervals thereafter.

In February 2024, we rolled out a **Cybertrack Assessment Feedback Questionnaire** to solicit feedback on the assessment process itself. We solicit responses at the time of delivering the assessment report. (We retroactively sent this questionnaire to organizations receiving their assessment reports between October 2023 and January 2024.) Thus far, we've overwhelmingly received positive feedback, and responses have included some great ideas for ways to refine the assessment process even further. We will continue to review the incoming responses for areas of improvement.

The following are highlights from the results:

Questions Asked Only in the Impact Questionnaire	**Results**
Action on Recommendations. Has your organization taken action on any of the recommendations in the Cybertrack assessment report? ("Taking action" includes, but is not limited to, implementing recommendations and/or establishing plans to implement recommendations.)	75 of 86 respondents selected "Yes." 11 respondents selected "No"
Senior Leadership Review**.** Has your organization's most senior leadership reviewed or been briefed on the Cybertrack assessment report?	69 of 86 selected "Yes." 17 respondents selected "No."
Questions asked in both the Impact and Feedback Questionnaires	**Results**
Likely to Recommend? On a scale of 1 to 5 (with 5 being the most positive), how likely would you be to recommend that other Indiana organizations complete a Cybertrack assessment?	115 of 169 respondents selected "5 - Extremely Likely," 45 selected "4 - Likely," 7 selected "3 - Neutral," and 2 selected "4 - Unlikely."
Worth it? On a scale of 1 to 5 (with 5 being the most positive), how much do you agree with the following statement: "The Cybertrack assessment was worth the time and effort our organization put into it."	101 of 169 respondents selected "5 - Strongly Agree," 59 selected " 4 - Agree," 6 selected "3 - Undecided", 2 selected "2 - Disagree."[10], 1 selected "1 "Strongly Disagree"[11]

The following are quotable quotes we've received from participants this quarter:

[10] The LGs that selected "Disagree" commented 1) "It is too complicated and lengthy for most non-computer people to complete accurately" and 2) The report did not provide anything they did not know already and the WDRs were too long.

[11] The respondent felt the effort was not worth it because the value of the report was "downplayed" by leadership.

"This program is valuable for even the smallest units because even if you can't implement all of the recommendations, it does make you think of your processes and gives tips for simple things that can be done for little to no costs."- *Julie Elmore, Oakland City Columbia Township Public Library*

"This has been the best experience when it comes to learning and improvement. All recommendations were easy to follow and I feel I was able to address most right away."

"The assessment was very detailed and helped with implementation of state requirements."

"Excellent!"

"Well worth the time and it went by quickly. Highly recommend.

"Nowhere else can you get a free cybersecurity assessment provided by a team of security professionals from two of Indiana's premier Universities. Thank you Cybertrack!"

"The CyberTrack team professionally and passionately cares about the municipalities they serve in delivering both a strategic and tactical roadmap that minimizes cybersecurity risk to the organization."

"CyberTrack provided a thorough, practical assessment that helped us better understand where our cybersecurity program is strong and where to focus next. The process and final report gave us clear, actionable guidance that we can use with both leadership and staff." - *Sheila Broussard, Systems Administrator, Jasper County Public Library*

"The Cybertrack process was exceptionally well-organized and clearly communicated. It provided the structure we needed to sharpen our focus and effectively narrow down our cybersecurity goals."

The following are selected quotes from previous quarters' responses:

"The assessment report reinforced our strengths and provided a clear roadmap for addressing areas of improvement. Transparency is essential in this process."

"Very friendly team, very thorough assessment."

"... I liked working with the IU and Purdue teams."

"It is great to see the state's top public institutions partnering together and in conjunction with IOT and its partners to provide an important service to give local organizations a leg up."

"There's no magic button...just persistent effort, strategic thinking, and a healthy dose of sarcastic optimism. As a small district, it feels like just a few of us taking on the rest of the world. Programs like this allow us to know we're not alone and help us bridge some of the gaps we may have had."

"It's worth it just to see where you stand. It's easy to get caught up in the day to day and overlook some of these 30,000 foot view items. This helps bring them into the forefront so they can be addressed and documented in a manner that will improve your team and your organization."

"Our Cybertrack experience was incredibly valuable — it gave us the opportunity to review our operational procedures and implement new policies that have strengthened our municipality. We're now more prepared and feel confident in addressing cybersecurity challenges that may arise."

“Even if I am not able to implement everything, the entire process made me more aware of how I am using technology and is making me see areas for improvement.”

“The CyberTrack Assessment provided us with a highly-detailed, CIS Controls-based benchmark that allowed our IT team to pinpoint areas of weakness in our cybersecurity posture. It delivered actionable insights that will significantly enhance the maturity and effectiveness of our cybersecurity program at Franklin Community Schools.”

“This was a good exercise to get a disassociated, object view of current Cyber Security practices.”

“We now have actionable and achievable Musts that we will be able to implement to better protect our Library”

“The Cybertrack assessment offers an invaluable opportunity for organizations seeking to strengthen their defenses against cybersecurity threats. Regardless of where you stand on your cybersecurity journey, the process provides practical insights and actionable feedback designed to help you take clear steps toward being more secure tomorrow than you are today.”

“There is no shortage of offers to perform security assessments on our organization. Cybertrack has the most rational framework I have seen in my twenty-plus years of working in this space. It's imperative that we have regularly scheduled follow-up assessments and continue with Cybertrack for the long term.”

“As the sole technology professional at a small public charter school, I was initially apprehensive about undertaking the CyberTrack assessment. However, I fully recognized its importance to our organization. That said, the comprehensive explanations provided in the WDR, along with access to knowledgeable personnel for any questions I had, made the process seamless. I felt fully supported throughout the process, and I never felt judged for my level of expertise. This assessment report was invaluable to our organization, and it was a privilege to collaborate with the CyberTrack team.” - Caleb Day, Geist Montessori Academy

“Cybertrack was a great opportunity to take a big picture look at my organization's IT infrastructure. It is so easy to get bogged down in the day to day and neglect strategic thinking. Participating in the Cybertrack assessment provided comprehensive look at where my organization is now and provided direction for our future.” - Victoria Smallegan, Nappanee Public Library

“Cybertrack has given us the opportunity to really examine our protocols and pushed us to make some changes to how we manage and maintain the network and our security. They pushed us to be better. 10 out of 10, would recommend.”

“The cybertrack assessment solidified some things that we were in the process of implementing and allows us to have further support moving forward as we can show that these steps are industry based and standardized.”

“We appreciate any and all opportunities to analyze our security posture. This project has given us dedicated time to consider our overall security and we have benefited from this process.”

“We've been able to use this information to reaffirm the steps we are currently taking are in the right direction.”

“The assessment removed the fear of the unknown from leadership and gave them a position to begin planning for the future.”

“The Cybertrack experience forced me to ask questions I should have asked years ago. It opened my eyes to our town's vulnerabilities and gave us concrete steps to get them fixed. I now feel like I'm levels above where I began and can't wait to get started on the recommendations.”

“Cybertrack made the evaluation process seamless, providing clear guidance and support every step of the way. The detailed report we received offered valuable insights, helping us address vulnerabilities and strengthen our cybersecurity posture effectively.” - Matthew Snoeberger, Lewis Cass Schools

“The Cybertrack team put together extensive information for us to use as we begin putting together our cybersecurity stance. Thank you to everyone who had a hand in performing the discovery, putting together the report and sharing the information with our technology team. Looking forward to following up with you!”

“This was a great experience and provided incredible valuable feedback that has led to substantive changes within our organization.”

“We appreciate this free resource to evaluate our Cybersecurity posture.”

“This has been a great review that has improved [our] practices, reinforced areas of strength and pointed out gaps we need to shore up.”

"Your team was so nice and absolutely professional and was so accommodating when answering questions. We can't thank you enough."

“Smart people giving smart feedback.”

“Cybertrack has been an invaluable resource in strengthening our cybersecurity posture. The hands-on experience and practical insights have not only helped to identify our pain points but also empowered us [to] take action to safeguard our digital infrastructure with greater confidence. It's an essential program for any organization serious about cybersecurity.”

“I loved this process as it was like shining a flashlight into the dark world of Cybersecurity and made us realize there was some easy things we could do to better position ourselves.”

“You don't know what you don't know....and even if you do know, it never hurts to have another set of eyes.”

“Very thorough insight into your cyber environment, extremely helpful identifying your cyber strengths and weaknesses.”

“I had an idea where our strengths and weaknesses were, and in some instances, those were what our data supported, but this process helped us understand some of the things we weren't thinking about, and gave us a good list of work to do to be more protected.”

“The assessment was overall a really easy experience especially being a K12 with limited time and resources. They made the process straightforward and efficient. No need for improvement that we can see.”

“Well worth the time and effort. Great learning tool and roadmap to implementation of the (Trusted CI Framework “Musts”) and (CIS Safeguards).”