Cybertrack

Indiana's Local Government Cybersecurity Assessment Program

Quarterly Progress Report for Q4 CY25

January 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, 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 Oct - 31 Dec 2025, including the following highlights:

- Completed R&D on the Cybertrack Operational Technology Expansion Module, resulting in the "**Cybertrack+**" version of the assessment methodology and initiated production assessments. This also included revising or creating toolkit components to facilitate Cybertrack+ assessments (*see* Section 4.1).
- **Completed 178 assessments** as of the close of CY2025 and delivered **22** reports this quarter. This was the most productive quarter since Q3 CY2024.
- Received **18 applications**, including 4 applications for reassessments, and onboarded 28 entities for assessment.
- While these are early results, **10 of the 11 reassessed organizations demonstrated measurable progress** in implementing the highly-impactful practices we measure.
- Participated in both the 6 Oct State of Technology Symposium and 7 Oct Indiana Digital Governance Summit.
- We continued to receive **overwhelmingly positive responses** to post-assessment questionnaires, including the inset quote. *See* **Appendix E** for more.
- Engaged key cybersecurity personnel at **IDEM** and will continue this engagement in January.
- Met with **Indiana National Guard** personnel (US Air Force and Army officers) at Stout Field on 18 December to explore opportunities for collaboration.

> **"The assessment report reinforced our strengths and provided a clear roadmap for addressing areas of improvement. Transparency is essential in this process."**
>
> ***-A Public Library participant***

- Continued our active participation in both the **SLCGP** and **IECC** meetings.

Looking Ahead. Over Q1 CY26, we expect the following milestones and highlights:

- Conduct a follow on meeting with IDEM to continue our collaboration.
- Continue recruiting efforts to include pursuing utilities to participate in the Cybertrack+ assessment.
- Conduct an increased number of reassessments and Cybertrack+ assessments.
- Finalize Memoranda of Understanding (MOU) with key stakeholder organizations to support IU CACR and Purdue cyberTAP efforts to establish CenterLine (*see* Section 7). Continue our active participation in both the SLCGP and IECC meetings. Members of the Cybertrack team will be presenting program updates at the January 30 IECC meeting.

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, SLCGP meetings, and IECC meetings[1].

Cybertrack's leadership team engaged cybersecurity contacts from the Indiana Department of Environmental Management (IDEM) on 15 December. With the Cybertrack+ assessment (enhanced for OT-reliant environments) moving into production, we used this initial meeting to present the Cybertrack program and Cybertrack+ assessment methodology to the following IDEM personnel: Jason House (Compliance Branch Chief, Office of Water Quality), Travis Goodwin (Security and Counter Terrorism Coordinator, Office of Water Quality), and Andrew Dryden (Technical Environmental Specialist, Compliance Branch, Office of Water Quality). We started discussing how Cybertrack and IDEM can work together to bring Cybertrack to Indiana's water and wastewater utilities. We plan to host another virtual meeting in January 2026 to lay out the "how" of working together to promote Cybertrack+ to IDEM's population of utilities. It was a very positive engagement, and we're excited about this collaboration.

[1] In addition to these direct engagements with IOT, Cybertrack worked to build Indiana's local cybersecurity community by engaging, networking with, and supporting other programs with missions supporting local cybersecurity. This work is discussed below in Section 7, Broader Impacts & Relationships.

3 Recruitment

In this quarter, we received **18 applications** and **onboarded 28 entities** for assessment. Three areas of engagement drove recruitment in Q4:

- **K-12 Schools:** Our regular engagement with Brad Hagg (Director of Educational Technology at Indiana Department of Education) and the CTO Council[2] continues to bring applicants to Cybertrack through outreach performed by Brad, the Council, and members of the Cybertrack Team. In Q4, members of the Cybertrack team hosted two breakout sessions at the Hoosier Educational Computing Coordinators conference (HECC) on 6 November, both of which featured Cybertrack heavily.
- **Libraries:** We continued to bring public libraries into Cybertrack from our 19 August presentation to the Indiana Library Federation. Applications from libraries came from library representatives who attended the presentation, as well as from those made aware of Cybertrack by their peers.
- **Utilities:** Our work recruiting utilities in previous quarters continued to bear fruit in Q4. The Cybertrack+ assessment moved from its pilot phase into production in Q4, which has provided an increasing number of entities that can serve as peer references for Cybertrack+.
- Reassessments: Four of the 28 entities this quarter were Reassessments.

In the next quarter, we expect the following two initiatives to drive interest in the Cybertrack program.

- **IDEM Engagement:** As noted in Sponsor Engagement, members of Cybertrack's leadership team have engaged key cybersecurity personnel at IDEM and will continue this engagement in January.
- **The "Tarmac County" Report:** The Cybertrack Team produced a sample Cybertrack report and corresponding Executive Summary for a fictional Tarmac County. A number of stakeholders have asked for something like this *fictional, but realistic* example Cybertrack Assessment Report. We're hopeful this salient representation of the report deliverable will tip the value proposition balance for some potential recruits.
- As of this report, there are **10 additional organizations that will complete reassessments in Q1 2026**.

4 Methodology Research, Development, Refinement, and Training

In this section, we cover the **Cybertrack+ (Operational Technology Expansion Module)** (Sec 4.1), **Operational Technology Training for our Assessors** (Sec 4.2), **Addressing the Use of AI in Responding to Written Discovery Requests (WDRs)** (Sec 4.3), and **Post-Assessment Findings** (Sec 4.4).

[2] 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/.

4.1 Cybertrack+: OT Module R&D

In Q4, we completed R&D on the **Cybertrack Operational Technology Expansion Module, resulting in the "Cybertrack+" version of the assessment methodology** and initiated production assessments. Development of Cybertrack+ began in December 2024, driven by the critical and growing cybersecurity threats facing our nation's operational technology-reliant environments, particularly in water and wastewater operations.[3] This assessment is best for organizations with a substantial and/or mission-critical operational technology footprint. It addresses both IT and OT equally well.

Cybertrack+ expands the assessment standard to include 13 CIS Safeguards not already being assessed as part of the original methodology. To select these additional Safeguards, we followed the same research methodology used to discover the Transformative Twelve (T12).[4] This research uncovered the "OT22," *i.e.*, twenty-two CIS Safeguards proven highly impactful for OT systems. (Nine of these were already being assessed.) For more, see Section 2.1.2 of our June 2025 Aggregate Analysis & Results Report.[5] Together with the T12 and considering overlaps between the two sets, we refer to the full set as the **Sturdy 30**. All 30 of these controls are **empirically-proven and relevant to both IT and OT systems, with some having particularly strong utility for traditional IT and others for OT**.

The team successfully completed a second Cybertrack+ pilot in October 2025. Additionally, at no cost to the State, we completed a third pilot in September 2025 via Trusted CI[6] for an NSF Major Facility. Leveraging lessons learned from these pilots, we shifted our focus to toolkit and process refinements. The following refinements were required to allow our team to deliver the new OT-enhanced assessments with efficiency and consistency:

- **Modified Application and Screening:** We modified our application process to help organizations select the most appropriate assessment for their technology footprint and to alleviate oversubscription.
- **Onboarding Process:** We established a separate Cybertrack+ onboarding process, placing emphasis on organizations answering Written Discovery Request (WDR) questions for both IT and OT.
- **Enhanced Discovery:** We updated the WDRs to include the additional CIS Safeguards required for OT environments.
- **Discovery Assistance:** We developed and standardized an approach for meeting with and

[3] https://wisdiam.com/publications/recent-cyber-attacks-water-wastewater/.
[4] For more on the methodology, *see* https://www.lawfaremedia.org/article/the-difficulties-of-defining-secure-by-design.
[5] https://incybertrack.org/media/4kejmeyk/cybertrack-aggregate-results-report-june-2025.pdf.
[6] Trusted CI is the NSF Cybersecurity Center of Excellence is supported by the National Science Foundation under Interagency Agreement #A2407-049-089-064206.0, [https://www.trustedci.org/].

aiding assessment recipients during the discovery phase.

- **Outbrief:** We developed a standardized approach for planning, recruiting participation for, and conducting outbriefs after report delivery. This includes a highly templated slide presentation designed to drive engaging discussions regarding assessment report recommendations.
- **Assessment Team Tooling:** We expanded the functionality of the Implementation Ratings Adjudicator, developed new or expanded rating rubrics for the CIS Safeguards, and revised the Assessment Report Template for Cybertrack+.
- **Streamlined Facilitation:** We developed a distinct, tailored facilitation process, including new templates for Discovery Assistance and Post-Assessment Outbriefings.
- **Communication:** We developed and integrated new communication templates to support stakeholder engagement throughout the enhanced assessment lifecycle.
- **Workflow Integration:** We are currently integrating revised, comprehensive workflows directly into the Work Breakdown Structure (WBS).
- **Finalized Additional Cost per Assessment:** Via effort tracking during our pilots, we have determined the additional cost per assessment is $3,700. The major factors contributing to this increase include the separate onboarding process, the preparation and facilitation of two additional meetings, and the effort required to assess the additional 13 CIS Safeguards. The total cost for a Cybertrack+ assessment is $14,500 (compared to $10,800 for standard Cybertrack assessments).

4.2 Operational Technology Training for our Assessors

While our team possesses deep expertise in OT security, we are implementing an upskilling plan to bring our entire assessor cadre to a high level of practical OT security knowledge.

We are conducting team-wide technical training during the next quarter. As we bring the full team up to high proficiency, we are staffing all Cybertrack+ engagements with at least one already-established advanced expert in OT.

4.3 Addressing the Use of AI in Responding to Written Discovery Requests (WDRs)

We recently identified instances where organizations utilized artificial intelligence (AI) to generate responses for their Written Discovery Requests. This practice has contributed to responses that do not reflect the technical or operational realities of the specific environment. We will continue to monitor this emerging trend and are evaluating potential guidance and strategies to help organizations provide authentic, evidence-based responses.

We will be adding an AI-use discussion to onboarding sessions. This would explicitly address the risks of AI and stress that the assessment's value relies on authentic responses.

4.4 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?"**

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

> "The assessment report reinforced our strengths and provided a clear roadmap for addressing areas of improvement. Transparency is essential in this process."[7]
>
> *-A Public Library*

5 Assessment Execution Management

We continued to hold monthly multi-organization onboarding sessions. The following tables provide metrics including quarterly and cumulative assessed entities by entity type. The total of 178 reports were delivered to 190 assessed entities. 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.

Table 2: Numbers of Onboarded Entities and Delivered Reports, Q4 2025 & Cumulative

	Q4 2025		Cumulative	
Type of Entity	**Onboarded**	**Report Delivered**	**Onboarded**	**Report Delivered**
County Government	3	3	39	36
Municipal (City/Town) Government	4	4	47	45
Township Government	0	0	7	7
K-12 School District	10	6	67	63
Library	10	8	28	21
Other (e.g., Utilities, Airports, Special Service Districts)	0	1	7	6
Total	28	22	**195**	**178**

[7] We interpret the respondent as saying that it is important to be honest with the CT assessors.

6 Aggregate Analysis & Reporting

The Cybertrack team anticipates releasing our next aggregate results and analysis report in 2026, immediately prior to the next expected Indiana Public Sector Cybersecurity Summit.[8] That report will provide new insights driven by our growing sample size of entities, 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. **Appendices B and C** follow and provide a continuation of results reporting since our June 2025 report. Results and trends remain consistent with those reported in June 2024 and 2025.

Early Results from Reassessments:

We continue to be encouraged by results from early reassessments. Ten of the 11 **reassessed organizations have demonstrated measurable progress in implementing the highly-impactful practices we measure.** On average, since their first Cybertrack assessment, these organizations have increased or refined their implementations by 8.5 points.[9] This average increase can be generally characterized as an increase in implementation level across several Musts, which account for 1.6 points (18.8%) of the average increase, and Safeguards, which account for 6.9 points (81.1%) of the average increase.

All but one reassessed organization showed progress; variations in the magnitude of these improvements ranged between 2 and 40 ratings points. Of course, we're still looking at a small sample size (11 entities), and we'll continue to update these results as our sample grows. Thus far, we can characterize ratings results from re-assessed 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.

Notably, we've removed a (positive) outlier from this average: That is, the average increase **does not** include one reassessed entity that was assessed as having 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 their 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.

Case Example. 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

[8] 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

[9] **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.

(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 Developing on these four Musts, developed and implemented more secure configuration processes, and widened its implementation of MFA. Though some of the Safeguards that were subject to Cybertrack's recommendations were fully implemented at the time of the entity's reassessment, most recommendations from the entity's initial assessment had only been partially implemented.

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 additional organizations scheduled, being scheduled for onboarding, or in the process of receiving a reassessment.

7 Broader Impacts & Relationships

Finally, the Cybertrack methodology and overall program continued to garner broader national attention and to support growing relationships. Over this last quarter:

- IU CACR and Purdue cyberTAP continued our effort to establish **CenterLine**, a highly collaborative, jointly-run center dedicated to improving community cybersecurity across Indiana's critical infrastructure, including water/wastewater, defense critical infrastructure, and local government. The vision for CenterLine is two-fold:
  (a) to expand the success of Cybertrack and
  (b) to localize the successful Trusted CI model to meet Indiana's most pressing cybersecurity needs. CenterLine will offer assessments and consulting, training and education, guidance and tools at scale, and community building forum.
- To establish momentum and demonstrate community demand, we are actively working with key stakeholder organizations to establish **MOUs.** These agreements will formalize communication and mutual support now, and provide a framework for future governance once an oversight committee is established. The Indiana National Guard is among stakeholder organizations that resonate with the CenterLine concept and plan to execute an MOU.
- We met with Indiana National Guard personnel (US Air Force and Army officers) at Stout Field on 18 December to explore opportunities for collaboration. Major Christopher Myers provided an overview of capabilities and resources the National Guard has for assisting state and local governments. Our team conducted an in-depth Cybertrack program discussion.
- We continued our collaborative relationship with **UC Berkeley's Center for Long-Term Cybersecurity (CLTC)**, advising their Public Interest Cybersecurity program on their research agenda and efforts to deepen community engagement at a regional/multi-state scale.
- We continued our discussions with the Center for Internet Security (CIS), providing information on the **Cybertrack+ methodology** and our assessment approach. We are exploring potential partnerships.

Appendix A: Recent and Upcoming Events and Milestones

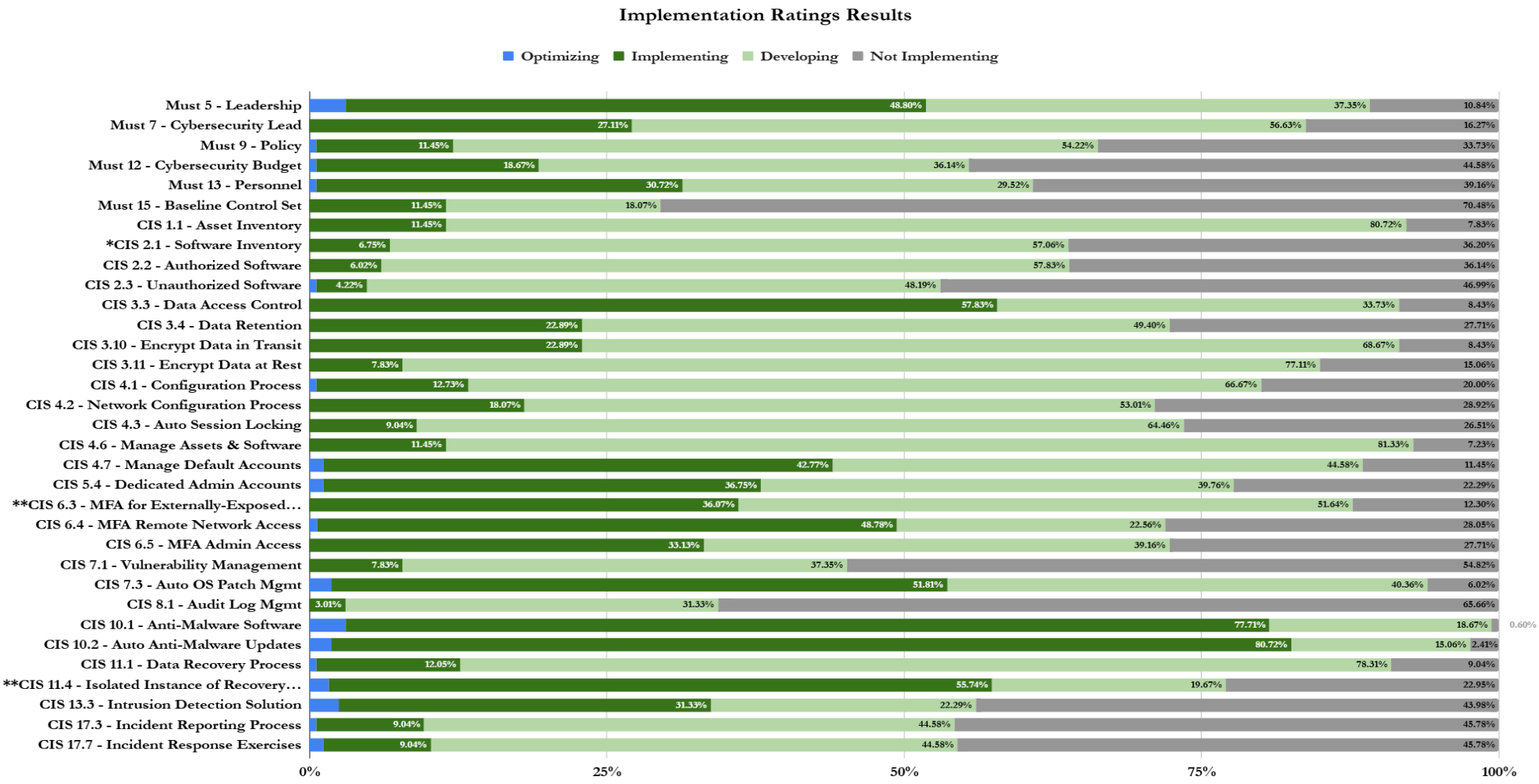
Recent Events

3 Oct	Cybertrack+ Pilot #2 Assessment Report Delivery
6 Oct	IOT 2025 Local Government IT Symposium
7 Oct	Indiana Digital Governance Summit
20 Oct	ESC Meeting
20-24 Oct	NSF Cybersecurity Summit
31 Oct	Governor Braun's Executive Council on Cybersecurity Meeting
4 Dec	SLCGP Mtg
15 Dec	IDEM Meeting/Partnership Development
18 Dec	INNG Stout Field Visit

Upcoming Events

20 Jan	ESC Meeting
30 Jan	Governor Braun's Executive Council on Cybersecurity Meeting
TBD	IDEM Follow Up Meeting
19 Feb	SLCGP Meeting

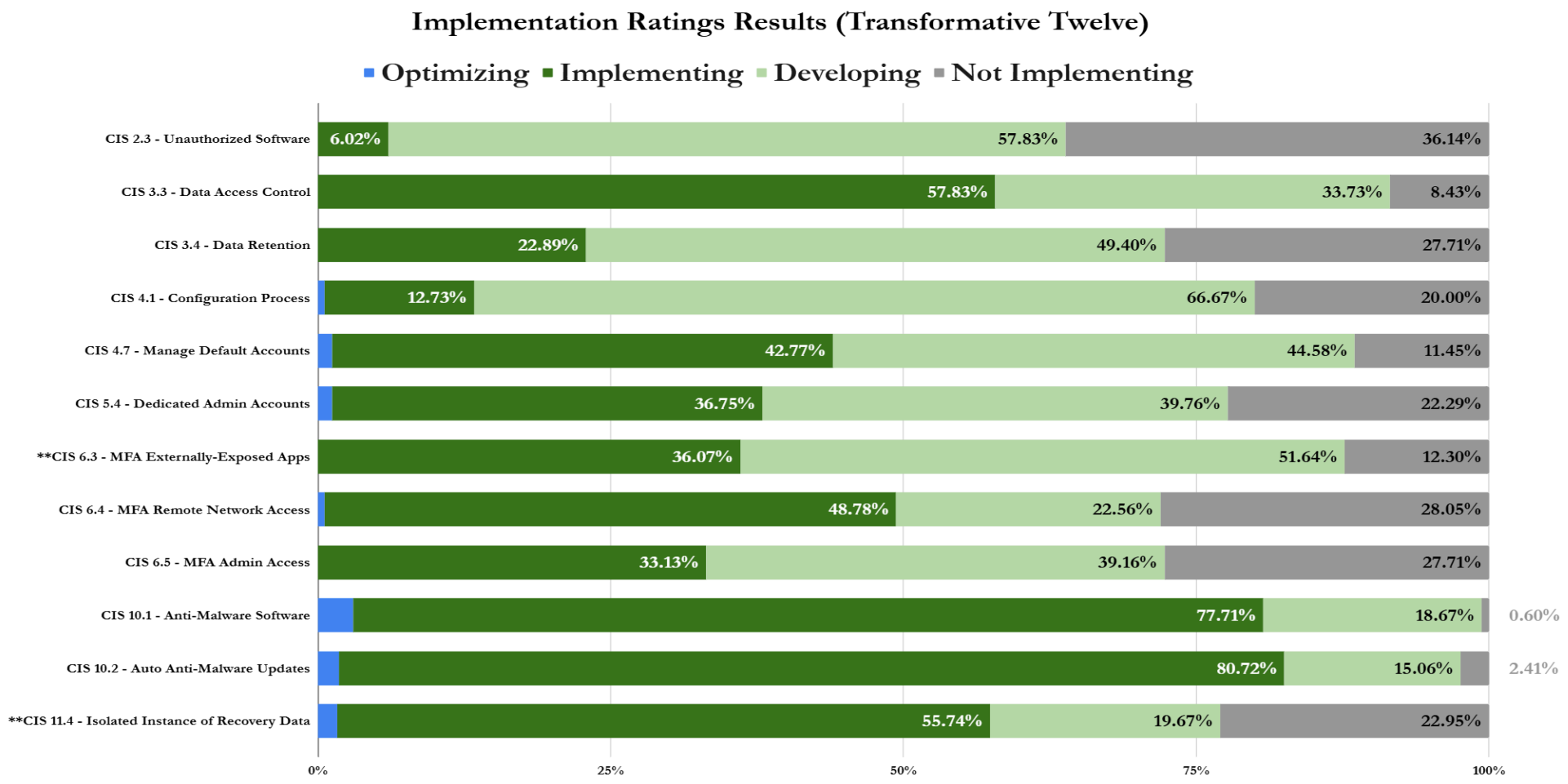
Appendix B: Distribution of Implementation Ratings



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

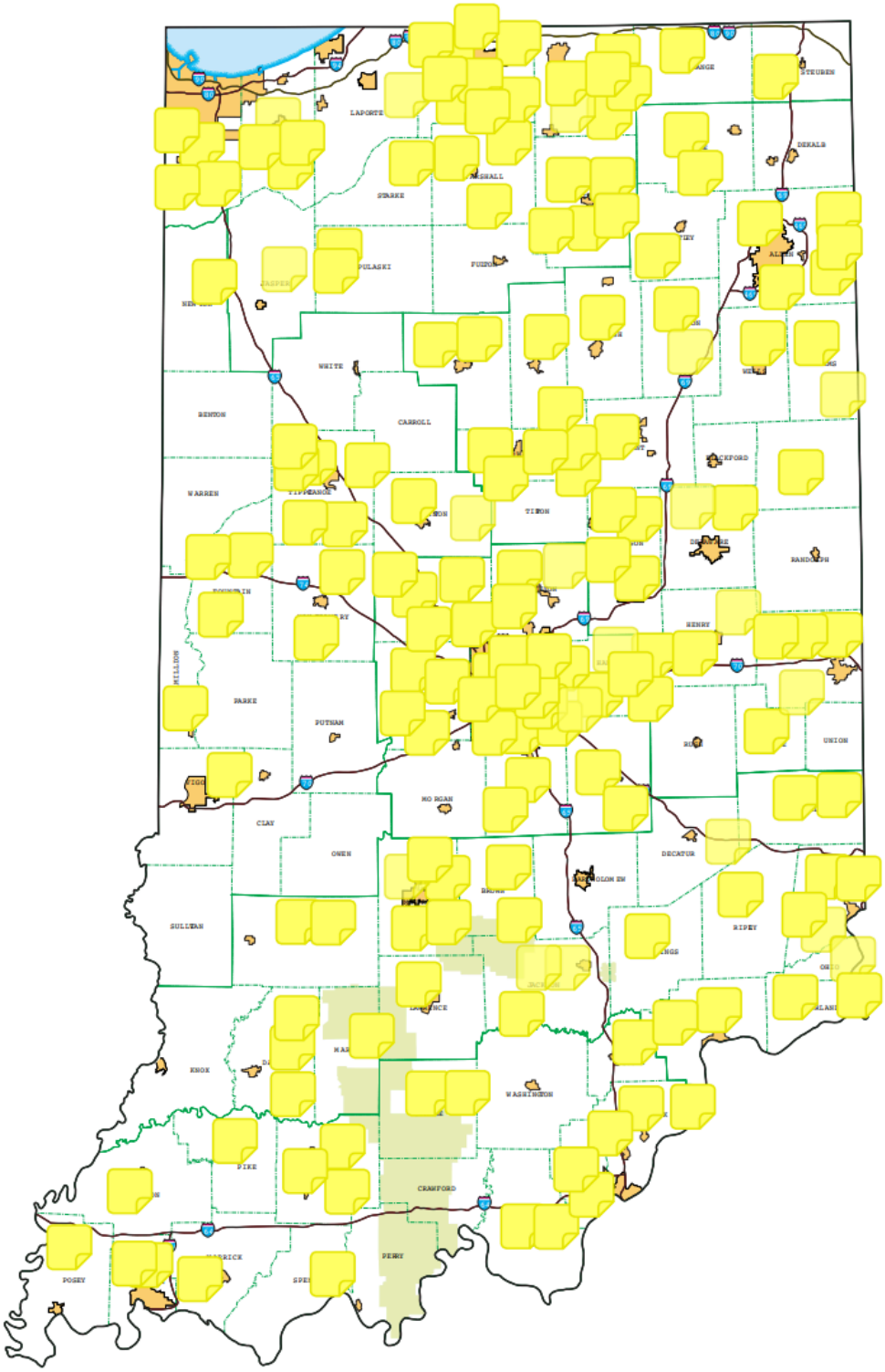
**Cybertrack began assessing Safeguards 6.3 & 11.4 in January 2024. These Safeguards were assessed for thirty-two entities at the time of this report.

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.) As of this report, we have 68 total responses from 166 solicitations (a 40% response rate). 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.)	69 of 79 respondents selected "Yes." 10 respondents selected "No"
Senior Leadership Review**.** Has your organization's most senior leadership reviewed or been briefed on the Cybertrack assessment report?	62 of 79 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?	98 of 147 respondents selected "5 - Extremely Likely," 41 selected "4 - Likely," 6 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."	86 of 147 respondents selected "5 - Strongly Agree," 53 selected " 4 - Agree," 5 selected "3 - Undecided", 2 selected "2 - Disagree."[10]

[10] The participants 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.

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

> "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."

The following are selected quotes from previous quarters' responses:

> "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).”