Cybertrack Report:
Aggregate Results & Analysis from 216 Assessments (May 2023 - May 2026)

Indiana's Local Public Sector Cybersecurity Assessment Program

June 2026

Joe Beckman, Purdue University Technical Assistance Program
Cory Gleyze, Indiana University Center for Applied Cybersecurity Research
Craig Jackson, Indiana University Center for Applied Cybersecurity Research
Ranson Ricks, Indiana University Center for Applied Cybersecurity Research
Kelli Shute, Indiana University Center for Applied Cybersecurity Research

Table of Contents

About Cybertrack. With sponsorship from the Indiana Office of Technology (IOT), Purdue University and Indiana University have partnered to develop Cybertrack: Indiana's local public sector cybersecurity assessment program. Cybertrack is designed to put local public sector 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 public sector organizations.

The primary deliverable of each assessment is a report that includes evaluations of organizational cybersecurity fundamentals and safeguards, actionable recommendations, and explanations thereof. The recommendations emphasize the individual local public sector organizations cybersecurity strategies, focusing on short-term priorities.

Purdue University and Indiana University are two of the nation's leading universities in cybersecurity, with complementary technical and programmatic strengths as well as common commitments to practical cybersecurity and the value of cybersecurity assessments. For additional information about Cybertrack, visit the program's website: https://incybertrack.org or contact: Joe Beckman, beckmanj@purdue.edu or Ranson Ricks, rjricks@iu.edu.

Acknowledgements. The Cybertrack Team thanks the Indiana local public sector organizations that assisted in developing our assessment process by serving as pilot organizations. The report authors also acknowledge the critical eyes of and strong suggestions from Cybertrack team member Matthew Crain. Cybertrack is supported by funding from the Indiana Office of Technology (IOT). The views expressed in this report do not necessarily reflect the views of IOT or any other organization.

Roadmap for the report. Following the Executive Summary, Section 2 (Methodology) describes the Cybertrack assessment methodology, including what we assess, why and how we assess it, and how we aggregated and analyzed the data from those assessments. Section 3 (Results) provides an overview of the aggregated assessment results to date. Section 4 (Analysis) analyzes our results, highlighting noteworthy patterns and themes. Finally, Section 5 (Conclusion) offers perspectives on our results and future directions of the Cybertrack program.

1 Executive Summary

This is the fourth report of aggregate assessment results and analysis from Cybertrack, Indiana's Local Public Sector Assessment Program. The program serves a diverse set of Indiana's local public sector organizations, including counties, cities, towns, K-12 school districts, utilities, and more. This report covers aggregated results from Cybertrack's 216 assessments. In April 2026, the Cybertrack program hit a milestone when we delivered our 200th Cybertrack assessment report. Today, more than 200 Indiana public sector organizations including counties, municipalities, K-12 schools, libraries, and utilities have received the most powerful, most practical, most doable cybersecurity advice from leading cybersecurity experts. The Cybertrack Program is ongoing, but these results offer some clear views into the current state of cybersecurity for Indiana's local government organizations, now including its operational technology (OT)-reliant environments and analysis of progress made by organizations since their original assessments roughly 18 months ago. This program's work should inform how we move forward as a community. One of Cybertrack's primary goals is to inform Indiana's local government cybersecurity policy and strategy. This report supports that goal.

Since our June 2024 report, we've expanded Cybertrack's scope of work to deepen our assessment of local operational technology-rich environments, such as water, wastewater, and other utilities. We are now also reassessing organizations previously assessed by the program to measure longitudinal change and trends and to track our impact. In both cases, we modified or built new assessment instruments to be able to provide these new services. For the first time, this report contains results and analysis supported by these expanded services.

Though the sample size of OT-reliant (Cybertrack+) assessments does not yet support definitive analysis, our results so far exhibit trends similar to our initial Cybertrack assessments. Like other local organizations, the organizations supporting Indiana's OT-reliant, critical infrastructure also struggle to: 1) build awareness among organizational leadership of cybersecurity risk in support of implementing basic governance and risk management practices, 2) implement even the most fundamental, powerful cybersecurity controls, and 3) apply sufficient knowledge and effort to do so.

Cybersecurity gains shown in reassessments show that these organizations are making strong progress on cybersecurity, although progress varied significantly on individual reassessments. Nearly fifty-eight percent of the ratings points gained in reassessment were achieved through actions taken by these organizations in response to recommendations provided on their initial Cybertrack assessment. Notably, one reassessed organization increased or refined its implementation of evaluated Musts & Safeguards by 40 points, tripling its ratings score in reassessment! In this case, free response data from the organization's reassessment questionnaire combined with these ratings data illustrate the power to make exceptional progress on cybersecurity when leadership, resources, and expert guidance are aligned and brought to bear.

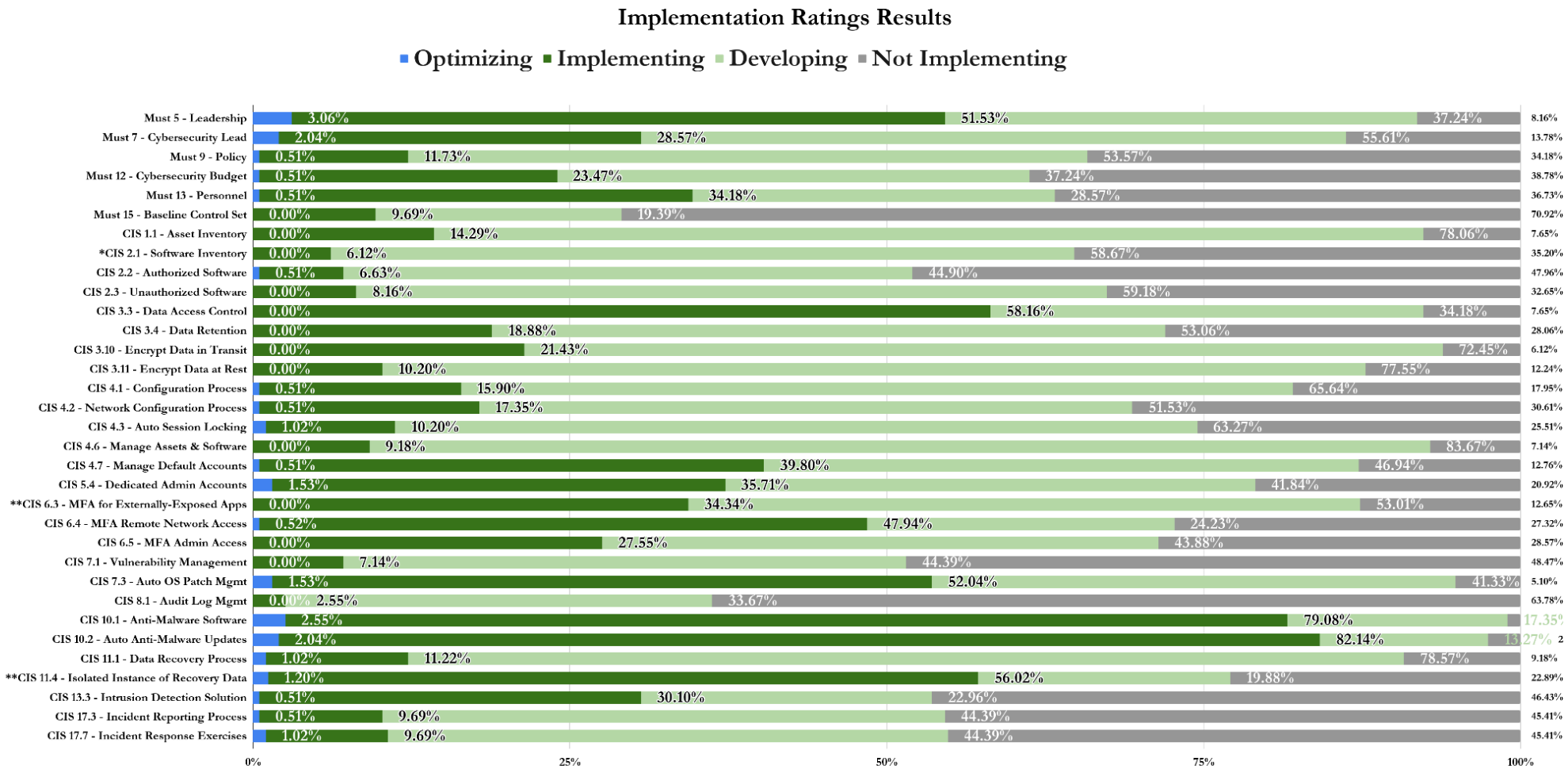
Considering that Cybertrack is focused on cybersecurity practices proven to be among the most powerful, these results remain sobering and show that Indiana's local public sector organizations, including those in critical OT-reliant environments, continue to have a long way to go in basic cybersecurity capability.[1] They continue to need help. The results of 216 assessments continue to support three imperatives, first described in our June 2024 report and highlighted below. These organizations and the supporting community need to:

[1] *See* Figures 1 & 2 below, as well as Figure 4 on p. 18.

A. **Increase leadership involvement and implement basic governance and decision making practices.** Our results show that organizations need functioning cybersecurity programs at the organizational level if they are going to successfully implement the detailed, technical cybersecurity controls that are the focus of most cybersecurity standards. Aggregate results on many assessed Trusted CI Framework Musts, which are foundational pillars of a functional cybersecurity program, were concerning. Basic formalization of cybersecurity governance, policy, budgets, and personnel resource allocation is rare. Indiana local government organizations should prioritize these organizational fundamentals. They are necessary to support sound decision making and cybersecurity investment.
B. **Address the most glaring gaps in evidence-based control implementation.** Our results continue to show that most Indiana local government organizations are struggling to implement even the most fundamental, powerful cybersecurity controls. Our research narrowed the 153 CIS Safeguards down to a list of 27, including 12 of the most empirically proven as powerful. Investing in these Safeguards, including the Transformative Twelve discussed in Section 2.1 (Assessment Methodology), will significantly reduce organizations' cybersecurity risk exposure. Across all Cybertrack-assessed Safeguards, assessed organizations generally received Not Implementing or Developing ratings, including on Transformative Twelve Safeguards, including very powerful controls like secure configuration and multi-factor authentication.
C. **Address the expertise and effort gap.** Program participants most frequently cited insufficient availability of cybersecurity-knowledgeable personnel as a key weakness or barrier to advancing their cybersecurity. Ways to address this gap include training existing staff, hiring new staff, engaging private sector firms, and further developing and engaging public sector / public interest resources (*e.g.*, public universities, IOT, the State and Local Cybersecurity Grant Program committee, CIS, CISA, other local governments). Intentional expansion, coordination, and vetting of these approaches and resources are necessary. Current federal policy means that—more than ever—Indiana needs to rally its own resources to turn the corner on cybersecurity.

In Cybertrack's results, we see reasons for optimism. Organizations that have completed reassessments have shown strong progress on cybersecurity. We've also heard strong positive feedback on the assessment experience, including the highly prioritized nature of our recommendations, as well as strong interest in finding ways to progress as individual organizations and as a community. The Cybertrack Team and our institutions look forward to continuing this work with Indiana's local public sector organizations and stand ready to expand our efforts.

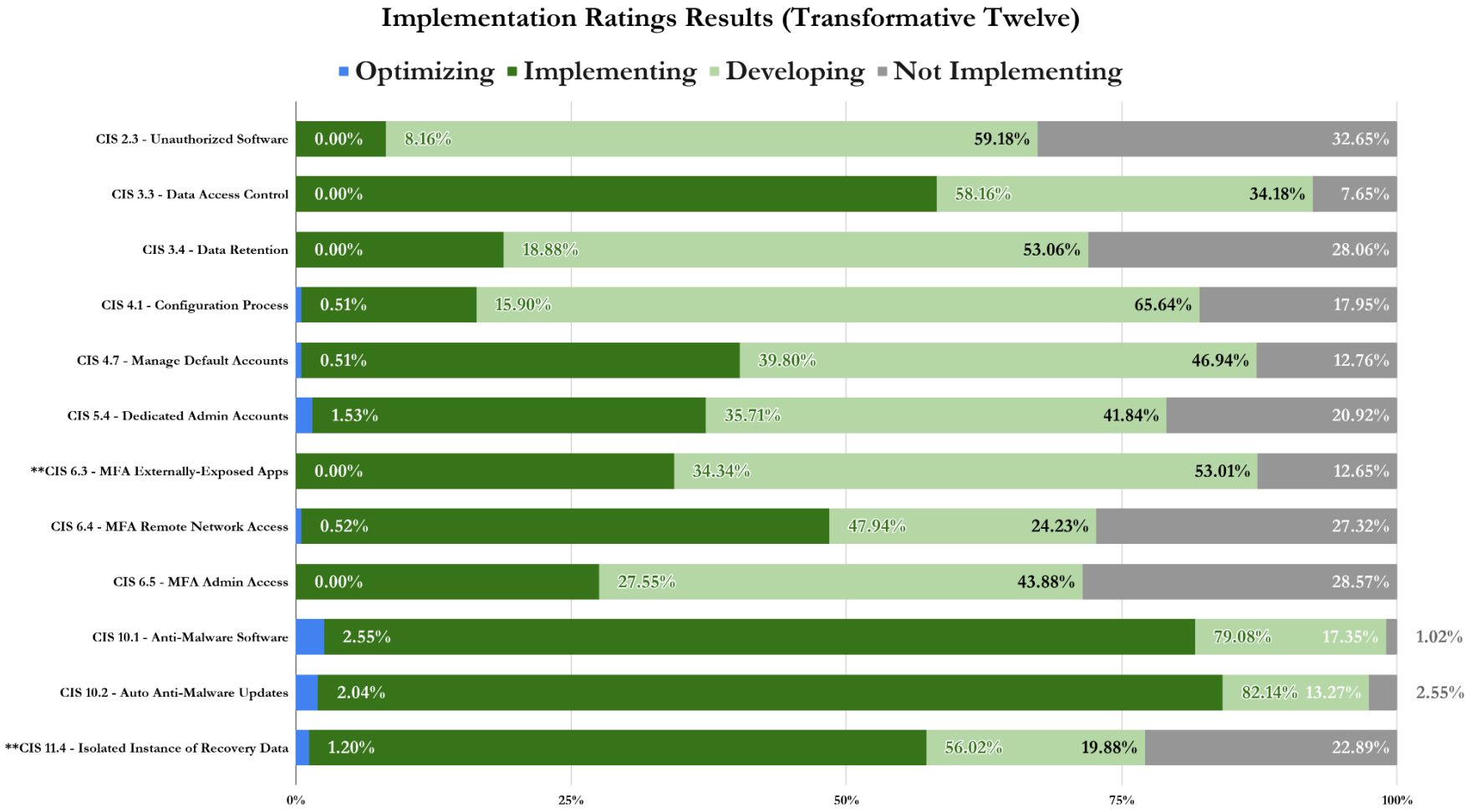
Figure 1. Distribution of Implementation Ratings: Current Cybertrack & Cybertrack+ Assessments



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

**Cybertrack began assessing Safeguards 6.3 & 11.4 in January 2024. These Safeguards were assessed for 172 organizations at the time of this report.

Figure 2. Distribution of Implementation Ratings for Current Cybertrack & Cybertrack+ Assessments (Transformative Twelve)



**Cybertrack began assessing Safeguards 6.3 & 11.4 in January 2024. These Safeguards were assessed for 172 organizations at the time of this report.

2 Methodology

This section describes the Cybertrack assessment methodology, including what we assess, why and how we assess it, and how we aggregated and analyzed the data from those assessments.

2.1 Assessment Methodology

2.1.1 The Core Methodology

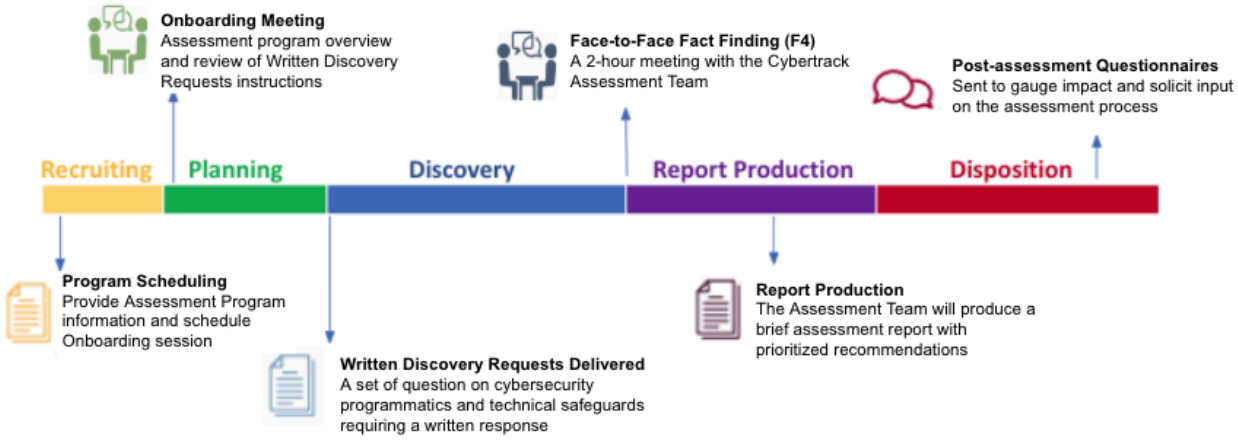
We built the Cybertrack assessment methodology by leveraging the Indiana University Center for Applied Cybersecurity Research's (IU CACR) expertise in cybersecurity assessment methodology development and Purdue's experience conducting CSET-based[2] assessments of public sector organizations. The combined assessment approach draws heavily from the US Navy's PACT cybersecurity assessment methodology[3] and both institutions' extensive experience conducting assessments. The methodology is designed to be standardized, highly efficient, and effective at helping public sector organizations prioritize the most doable, impactful actions while also building an overarching picture of cybersecurity across the state.

Assessment Process. Each Cybertrack Assessment follows a standardized process (Figure 3). After expressing interest, representatives of public sector organizations attend an Onboarding Meeting where Cybertrack Team members explain the assessment process and where personnel from the organizations can ask questions. After the Onboarding Meeting, the local organization identifies its personnel who will be directly involved in the assessment (the "LG-Team"), and the Cybertrack Team delivers our standardized Written Discovery Requests (WDRs). These WDRs call for written responses and are focused on a subset of the Trusted CI Framework Musts and CIS Safeguards discussed later in this section, as well as basic data characterizing the public sector organization (*e.g.*, type, population, number of endpoints).

[2] CSET is software developed by the United States Department of Homeland Security, Cybersecurity & Infrastructure Security Agency to facilitate organizational cybersecurity assessments. https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr.

[3] This methodology was developed by IU personnel and is based heavily on more than dozen prior assessments for the NSF Cybersecurity Center of Excellence and the US Navy. It has been successfully used in a wide range of environments. For more about PACT, *see* https://cacr.iu.edu/initiatives/.

Figure 3. Cybertrack Assessment Phases



Each Cybertrack assessment leverages a two-person Assessment Team (one member from IU CACR and one member from Purdue cyberTAP), with a total effort allocation of 30 hours per assessment. After the LG-Team completes and returns responses to the WDRs, the Assessment Team completes an initial analysis followed by a Face-to-Face Fact Finding (F4) meeting with the LG-Team (and any other local organization's invitees). The F4 is a 2-hour meeting designed to clarify relevant facts and help the Assessment Team identify the highest priority actions the organization can take, which appear in the Assessment Report.

Each assessment report includes implementation ratings (*see* Section 2.2) for each Must and Safeguard we assess and a small number of well-supported, highly actionable recommendations. Each recommendation has Facts, Recommendation Detail, and Rationale sections. The recommendations consider individual, local cybersecurity environments and capabilities, with a particular focus on short-term priorities.

After the report is delivered and time is allowed for the local organization to review and consider the report, the Cybertrack Team follows up with post-assessment questionnaires every six months to gauge impact and solicit input that can improve the assessment process.

Assessment Scope and Standards. The Cybertrack assessment's scope and focus is on the organizational cybersecurity governance and resourcing as well as security controls supporting its information, information technology, and operational technology.[4]

This assessment is **focused on the most proven, most impactful, most fundamental organizational (aka "programmatic") "Musts" and "Safeguards."** The programmatic Musts were selected from the Trusted CI Framework.[5] The Safeguards were identified via research and

[4] Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. *See* https://csrc.nist.gov/glossary/term/operational_technology.
[5] https://www.trustedci.org/framework.

alignment to federal grant programs, mapped to, and ultimately selected primarily from, Implementation Group 1 of the CIS Controls v8.[6] The Musts & Safeguards covered in this assessment are listed in **Appendix A**.

The **Trusted CI Framework** is a minimum standard for cybersecurity programs developed by Trusted CI,[7] the NSF Cybersecurity Center of Excellence, with significant contributions from IU CACR team members. The Trusted CI Framework supports the goals for Cybertrack assessments because, unlike other cybersecurity frameworks, the Trusted CI Framework is focused entirely on organizational cybersecurity fundamentals, aka "programmatics." It consists of 16 "Musts," organized under four pillars: Mission Alignment, Governance, Resources, and Controls. **Each Must represents a foundational requirement for a competent cybersecurity program**. We selected 6 of the most fundamental Musts for inclusion in this assessment (*e.g.*, whether leadership is involved in cybersecurity decision making; whether the organization has a cybersecurity lead role; whether the organization has a cybersecurity budget).

The **CIS Controls** are a list of high-priority, highly effective defensive actions that provide a 'must-do, do-first' starting point for every enterprise seeking to improve their cyber defense."[8] They are 1) highly prioritized; 2) updated frequently; 3) described in sufficient detail for organizations to implement them; and 4) developed by a collaborative and open process informed by a diverse group of cybersecurity practitioners. They apply to a broad range of organizations, including local public sector organizations. They map readily to the controls in many other cybersecurity standards (*e.g.*, NIST CSF, NIST 800-53, SOC 2). Each Control is broken down into "Safeguards" that describe specific actions that organizations should take to implement the Control. **Implementation Group 1 (IG1)**[9] is a set of 56 Safeguards that "represents a minimum standard of information security for all enterprises"[10] and helps all organizations deal with the most common types of real-world attacks.

With efficiency and impact in mind, in order to downselect further, the IU Team conducted research to identify an evidence-based, even more highly prioritized subset of CIS Safeguards. We set out to identify "gold standard" systematic studies whose results point to a small set of proven high-power controls. To meet this "gold standard," we had to develop confidence in the validity of the methodology used in each candidate source. As such, we considered and eliminated a number of sources that lacked any publicly available documentation of their methodology. Ultimately, we found three studies that qualified: (a) the CIS Community Defense Model v2.0;[11] (b) the Microsoft Digital Defense Report;[12] and (c) the Australian Signals Directorate's Essential Eight.[13] Notably, each of these three studies used a different methodology. We mapped the identified controls to the appropriate CIS Safeguards and scored them: Safeguards received a score for each appearance in a gold standard study. Thus, those Safeguards that appear in more gold standard studies received a higher score.

---

[6] https://www.cisecurity.org/controls.
[7] https://www.trustedci.org/.
[8] https://www.cisecurity.org/controls/cis-controls-faq.
[9] https://www.cisecurity.org/controls/implementation-groups/ig1.
[10] https://www.cisecurity.org/insights/white-papers/establishing-essential-cyber-hygiene.
[11] https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0.
[12] https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2021.
https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022.
[13] https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight.

This research resulted in a top-scoring group of 12 IG1 Safeguards. We validated this **"Transformative Twelve"** (*See* Table 1 below) via independent IU and Purdue subject matter expert analysis and confirmed the very high presence of these Safeguards in other standards (*e.g.*, NIST).

As a result, we have high confidence that the core set of specific controls we're assessing are truly fundamental and impactful. This is not to say that these are the only controls that are worth implementing. Moreover, much-needed future research may result in a somewhat different top-scoring group. However, in the context of a cybersecurity landscape where some "standards" include hundreds of controls, and most lack prioritization or evidentiary grounding, we see building real confidence in any subset as a victory for practicality.[14]

Table 1: The Transformative Twelve

2.3	Address Unauthorized Software
3.3	Configure Data Access Control Lists
3.4	Enforce Data Retention
4.1	Establish and Maintain a Secure Configuration Process
4.7	Manage Default Accounts on Enterprise Assets and Software
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts
6.3	Require MFA for Externally-Exposed Applications
6.4	Require MFA for Remote Network Access
6.5	Require MFA for Administrative Access
10.1	Deploy and Maintain Anti-Malware Software
10.2	Configure Automatic Anti-Malware Signature Updates
11.4	Establish and Maintain an Isolated Instance of Recovery Data

To the Transformative Twelve, we added a small number of additional IG1 Safeguards based on the Cybertrack Team's analysis of particular relevance to local public sector organizations, contemporary attack patterns (*e.g.*, prominence of ransomware), as well as inventory controls that scored lower in the CIS Community Defense Model for methodologically technical reasons (as opposed to any evidence that they are not truly critical). Finally, we added a handful of Safeguards that map to "cybersecurity best practices" emphasized in the federal State and Local Cybersecurity Grant Program[15] but were not already included via our research. All said, Cybertrack assesses 27 of CIS's 153 Safeguards, including 23 of IG1's 56.

Implementation Ratings. Much of the Results and Analysis that follow focuses on implementation ratings for the Musts & Safeguards we assess. We developed a common implementation rating scale, as well as a rating rubric for each Must and Safeguard we assess:

[14] For more discussion of the Transformative Twelve and Trusted CI Framework, *see* https://www.lawfaremedia.org/article/the-difficulties-of-defining-secure-by-design.
[15] https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program.

Optimizing: The evidence showed that the organization is implementing the fundamental elements of this Must or Safeguard and has taken action to fortify or refine its implementation (*e.g.*, for greater effectiveness, efficiency, or programmatic resilience).

Implementing: The evidence showed that the organization is implementing the fundamental elements of this Must or Safeguard, with no significant gaps across its environment.

Developing: The evidence showed that the organization is implementing some, but not all of the fundamental elements of this Must or Safeguard, *or* there exist significant gaps in the implementation within the environment.

Not Implementing: Discovery produced little or no evidence that the organization is implementing any of the fundamental elements of this Must or Safeguard.

Not Rated: We use this when we do not provide a rating for a Must or Safeguard. Reasons may include not having enough information to be confident in our rating or the Must or Safeguard being inapplicable to the organization receiving the assessment.

"Fundamental elements" are the minimum requirements for us to confidently say that the assessed organization is implementing the Must or Safeguard.

A "significant gap" is a gap in the implementation of a Must or Safeguard of sufficient scale or concern to warrant further consideration. These include cases where other Must or Safeguard implementations do not mitigate the risk presented by the gap. The "as to warrant further consideration" language is intentional: The identification of a significant gap does not necessarily mean that gap should or necessarily can be closed. An example might be multi-factor authentication being implemented for remote access but only for a small subset of the relevant systems.

When evaluating the evidence provided, we follow these guidelines:

1. We assume that respondents' factual statements are truthful and accurate.
2. We assume that respondents have not intentionally omitted important facts.
3. Unless called for explicitly, we do not consider respondents' statements of opinion when determining implementation ratings.

2.1.2 Reassessments

In February 2025, Cybertrack reached a significant milestone—marking two years since the program conducted its first assessments. According to our workplan, this also signaled the time for the first cohort of alumni to undergo reassessment. Reassessments are critical to Cybertrack's goals because they assist local public sector organizations by providing feedback on the actions taken and process made since their previous assessment and by providing prioritized next steps in their cybersecurity journeys. Reassessments help these organizations drive action, as well as record and celebrate progress on their cybersecurity programs. In aggregate, data from reassessments provide feedback to

Cybertrack and IOT about the impacts the program makes on cybersecurity in the local public sector organizations we assess. The longitudinal information about the implementation of cybersecurity fundamentals provided by reassessment data for a wide swath of Indiana public sector organizations tells us what methods are working and how they affect change.

To ensure that reassessments achieved these ends, we conducted new R&D and a reassessment pilot. This included the development and use of an intake questionnaire designed to 1) gather high-level information about the organization's progress since its last Cybertrack assessment and 2) help our Assessment Teams prepare for the reassessment. The reassessment questionnaire focuses specifically on actions that the organization took in response to the recommendations provided in its previous report. The questionnaire responses inform the Cybertrack team if action was taken on each previous recommendation, whether the organization encountered any barriers to implementation of each recommendation, and how the organization achieved their successes. Other than the addition of the reassessment questionnaire, the assessment process remains the same as the process used to conduct initial Cybertrack assessments. The resulting Cybertrack report produced for reassessments are similar to those produced for initial Cybertrack, but contain critical information about cybersecurity progress made since the initial assessment.

We completed two reassessment pilots in July 2025, and have since completed nine additional reassessments. We reengage with Cybertrack alumni organizations for reassessment once 18 months have elapsed since an organization's last assessment.

2.1.3 Cybertrack+ Assessments

Beginning in December 2024, we began development on the **Cybertrack+ Assessment.** While not the sole motivator, a major driver of this new development was the very present cybersecurity threats facing water / wastewater operations.[16] The April 2024 cybersecurity attack on the wastewater treatment facility in Tipton, Indiana further emphasized the need for strong operational cybersecurity in Indiana's critical OT environments.[17] The team again evaluated numerous sources and analyzed the following six (6) evidence-based sources to identify the most proven-impactful cybersecurity controls for OT-rich environments. These six sources are:

[16] https://wisdiam.com/publications/recent-cyber-attacks-water-wastewater/.
[17] Ibid.

- Dragos' "Threat Perspective: United States Water & Wastewater"[18]
- CPNI's "United Kingdom OT Security Principles - A good practice guide"[19]
- MS-ISAC's "Public Water & Wastewater Sector Face Mounting Threat"[20]
- NSA/CISA Joint Advisory: "NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems"[21]
- USDHS/NCCIC's "Seven Steps to Effectively Defend Industrial Control Systems"[22]
- Water ISAC's "12 Cybersecurity Fundamentals for Water and Wastewater Utilities"[23]

The team followed the same research methodology used to discover the Transformative Twelve.[24] A defining design principle of Cybertrack and part of its success hinges on focusing organizations' limited resources on the most empirically-proven cybersecurity practices. The analysis identified the 22 CIS Safeguards listed in **Table 2** below. Notably, research resulted in a set of controls with substantial overlap with those addressed by the American Water Works Association (AWWA) Cybersecurity Risk Management Tool[25] and the EPA Water Cybersecurity Assessment Tool (WCAT).[26,27] Of these 22 Safeguards, 9 were already being assessed in standard Cybertrack assessments, while 13 were new to Cybertrack. As such, in March 2025 we developed 13 new rubrics and enhanced the 9 already existing with helpful details regarding their applicability to OT-reliant environments. We expanded the assessment standard to include the 13 CIS Safeguards not already being assessed as part of the original methodology. 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 environments and others for OT-reliant environments.In September 2025, this assessment methodology was put into production and branded as Cybertrack+.

[18] https://www.dragos.com/resources/infographic/5-critical-controls-for-world-class-ot-cybersecurity-infographic/.
[19] https://nsarchive.gwu.edu/sites/default/files/documents/5023726/United-Kingdom-Government-Security-for.pdf.
[20] https://learn.cisecurity.org/public-water-and-wastewater-Sector-face-mounting-cyber-threat.
[21] https://media.defense.gov/2020/jul/23/2002462846/-1/-1/0/OT_ADVISORY-DUAL-OFFICIAL-20200722.PDF.
[22] https://www.cisa.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf.
[23] https://www.waterisac.org/system/files/articles/WaterISAC_12%20Fundamentals_FULL%2012%20High%20Res.pdf.
[24] For more on the methodology, *see* https://incybertrack.org/methodology.
[25] https://cybersecurity.awwa.org/.
[26] https://www.epa.gov/cyberwater/cybersecurity-assessments#:~:text=EPA%3A%20Water%20Cybersecurity%20Assessment%20Tool%20and%20Risk%20Mitigation%20Template.
[27] Cybertrack assessments with the OT module will cover at least 65% of what's covered in the AWWA tool and its associated guidance and at least 70% of the EPA guidance. The quantification is approximate, as the mapping exercise requires both linguistic and technical interpretation.

Table 2: Twenty-Two Proven-Impactful Safeguards for OT

CIS Safeguard	Existing Cybertrack-Assessed Safeguard	T12 Safeguard	New to Cybertrack
1.1: Establish and Maintain Detailed Enterprise Asset Inventory	√		
2.1: Establish and Maintain a Software Inventory	√		
4.1: Establish and Maintain a Secure Configuration Process	√	√	
5.2: Use Unique Passwords			√
6.3: Require MFA for Externally-Exposed Applications	√	√	
6.4: Require MFA for Remote Network Access	√	√	
6.5: Require MFA for Administrative Access	√	√	
6.8: Define and Maintain Role-Based Access Control			√
7.2: Establish and Maintain a Remediation Process			√
7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets			√
7.7 Remediate Detected Vulnerabilities			√
11.1: Establish and Maintain a Data Recovery Process	√		
11.5: Test Data Recovery			√
12.2: Establish and Maintain a Secure Network Architecture			√
13.3: Deploy a Network Intrusion Detection Solution	√		
13.4: Perform Traffic Filtering Between Network Segments			√
13.5: Manage Access Control for Remote Assets			√
13.6: Collect Network Traffic Flow Logs			√
17.1: Designate Personnel to Manage Incident Handling			√
17.4: Establish and Maintain an Incident Response Process			√
17.5 Assign Key Roles and Responsibilities (IN IR PLAN)			√
17.7: Conduct Routine Incident Response Exercises	√		

2.2 Approach to Data Analysis

Data collected for analysis are taken from completed WDRs, final implementation ratings for each Must and Safeguard for each assessed organization, and publicly-available information. Where multiple layers of data are captured for analysis, multiple worksheets within the workbook are used to store data. Those data are related to each other using referencing formulae within the workbook.

Some of the more structured or categorical data (*e.g.*, implementation ratings, organization type, municipal spending information) are used directly in the analysis. Most of the data used, including those from WDRs and assessment ratings, are coded to facilitate our analysis. Our analysis relies heavily on assessment teams' assessment ratings, which are coded as shown in the table below.

Table 3: Implementation Ratings Coding System

Rating	Code
Not Rated	N/A
Not Implementing	0
Developing	1
Implementing	2
Optimizing	3

We adopted a numerical coding method for the implementation rating system, enabling us to generate rating metrics.[28] These metrics include intermediary aggregate scores for both the assessed Trusted CI Musts and the assessed CIS Safeguards and, ultimately, an overall assessment rating score for each organization for both the Musts and the Safeguards.

For all assessment types we begin our analysis by generating basic descriptive statistics (mean and variance) for each implementation rating across all organizations. The team also generates a bar graph for each Must and Safeguard that shows the percentage of organizations that achieved each implementation rating. We perform basic statistical comparisons. The team validates calculations and results by having a second team member validate the formulae used in calculations. We perform more advanced statistical comparisons, such as regression and analysis of variance (ANOVA) analyses, using SAS version 9.4, by assessment type.

To derive results and analyze the local public sector organizations' free-form responses collected in the WDR, our team developed coding systems to preprocess this qualitative data for analysis. Data entered into the analysis workbook are checked by the analyst entering the data, then re-checked by

[28] We do not provide numerical scores to assessed organizations as part of their assessment report. For individual organizations, these scores could be misleading for a number of reasons, including the fact that not all Musts & Safeguards are equally powerful. The purpose of the numerical scoring system is solely to facilitate our analysis of aggregate results across the assessed population sample.

another member of the team before the analysis begins. The Cybertrack analysis team breaks various statements into their individual elements related to the question being answered and then groups into categories with similar responses. We then analyze these categorized data. The results of those analyses are shown in this report.

When analyzing data from reassessments, we also compare results of our analysis with those from the organization's prior assessment using the same coding methods. For each Must & Safeguard, scores achieved during the organizations' prior Cybertrack assessment are subtracted from those achieved during reassessment. This difference indicates the magnitude and direction of changes made by the organization since its previous Cybertrack assessment. Some organizations reassessed in this first 20 received initial assessments that evaluated fewer Safeguards. (As noted in Section 3.2, Cybertrack assessed fewer CIS Safeguards prior to January 2024.) In cases where reassessed organizations are evaluated on fewer Safeguards on their initial assessment, total Safeguards scores for reassessment are calculated by adding scores for all 27 currently evaluated Safeguards. Where comparisons are made between reassessed ratings scores and those from the initial assessment, scores for Safeguards not initially assessed are not compared.

In some cases (three, so far), organizations that initially received a Cybertrack assessment chose to receive a Cybertrack+ assessment in reassessment. In these cases, we evaluate their progress since the initial assessment by focusing only on ratings evaluated as part of both assessments. Because the scope of the Cybertrack+ assessment (which includes OT-reliant aspects of the organization such as water and wastewater utilities) is broader than a Cybertrack assessment, comparisons between initial and reassessed ratings are not exact. We detail this issue and its impacts on ratings and ratings comparisons in our analysis of reassessments in Section 4.1.2 below.

3 Results

This section provides an overview of the aggregated results from the 216 assessments of local public sector organizations performed through the Cybertrack program. We begin by refining the basic characteristics of this population of organizations and sample-to-date [Table 4] discussed in our first three reports[29] released in November 2023, June 2024, and June 2025 respectively. Then, we summarize the aggregated results of the implementation ratings across the Musts & Safeguards we assess [Figures 1 & 2] in the context of our larger sample size of assessed organizations.

According to the 2022 United States Public Sector Annual Survey and Census of Governments,[30] 2,649 local government organizations exist in the State of Indiana. These organizations include: "counties, cities, townships, special districts (such as water districts, fire districts, library districts, mosquito abatement districts, and so on), and school districts."[31] Of these, 1,662 are general purpose governments (*e.g.* counties, cities, and other municipalities)[32] that served as the primary governing organization. The remaining 987 local governmental organizations include K-12 school districts and special service governing bodies, among others. These local government organizations represent the majority of the public sector organizations that Cybertrack serves. The 2022 United States Census estimates Indiana's population to be 6,833,037 people.

[29] https://incybertrack.org/reports/.
[30] https://data.census.gov/table/GOVSTIMESERIES.CG00ORG01?q=local+governments+in+Indiana.
[31] https://www.census.gov/programs-surveys/gus/about.html.
[32] https://www2.census.gov/programs-surveys/gus/datasets/2017/2017_gov_org_meth_tech_doc.pdf.

Data collected for each assessed organization includes demographic information including the type of local public sector organization (*e.g.*, county, town, city) and its population. Table 4 below classifies assessed organizations by the type of local organization. Nearly all (22 of 23) of the organizations we assessed between the March 2023 start of this program and November 2023 were county or municipal governments. In total, Cybertrack assessed 38 county governments, which represents 41% of all Indiana counties. Since November 2023, the Cybertrack team has assessed a more diverse sample of organization types. The county, municipal, and township governments assessed by the Cybertrack program to date represent more than 5% of Indiana's local governments, but these organizations serve 55% of Indiana's total population. One hundred twenty-nine assessed organizations (59.4%) were "rural" as defined by The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2022 Homeland Security Grant Program[33] (*i.e.*, they serve a population of 50,000 or fewer people).

Notably, Cybertrack assessed 10 Indiana water / wastewater utilities since our June 2025 report. By bringing Cybertrack+ assessments into production, Cybertrack has deepened its ability to assess operational technology-reliant environments – a key component of Indiana's critical infrastructure.

[33] https://www.fema.gov/grants/preparedness/homeland-security/fy-22-nofo.

Table 4: Cumulative Number of Assessed Organizations by Type of Organization

Type of Organization	Number of Org Type As of November 2023	Number of Org Type As of May 2024	Number of Org Type As of May 2025	Number of Org Type As of May 2026
Cybertrack Assessment				
County Government	12	22	29	38 (8 ReA)
Municipal (City/Town) Government	10	27	39	49 (4 ReA)
Township Government	0	2	6	6 (0 ReA)
K-12 School District	0	20	52	75 (5 ReA)
Library	1	2	9	32 (0 ReA)
Other (*e.g.,* Utilities, Airports, Special Service Districts)	0	3	4	6 (0 ReA)
Subtotal	***23***	***76***	***139***	***206 (17 ReA)***
Cybertrack+ Assessments				
Municipal (City/Town) Government	N/A	N/A	N/A	7 (3 ReA)
Other (*e.g.,* Utilities, Airports, Special Service Districts)	N/A	N/A	N/A	3
Subtotal	N/A	N/A	N/A	***10***
Total	**23**	**73**	**139**	**216 (20 ReA)**[34]

Basic descriptive analysis of the implementation ratings follows and provides additional context to the data displayed in **Figure 1** above.

3.1 Results from Public Sector Organizations' Initial Cybertrack Assessments

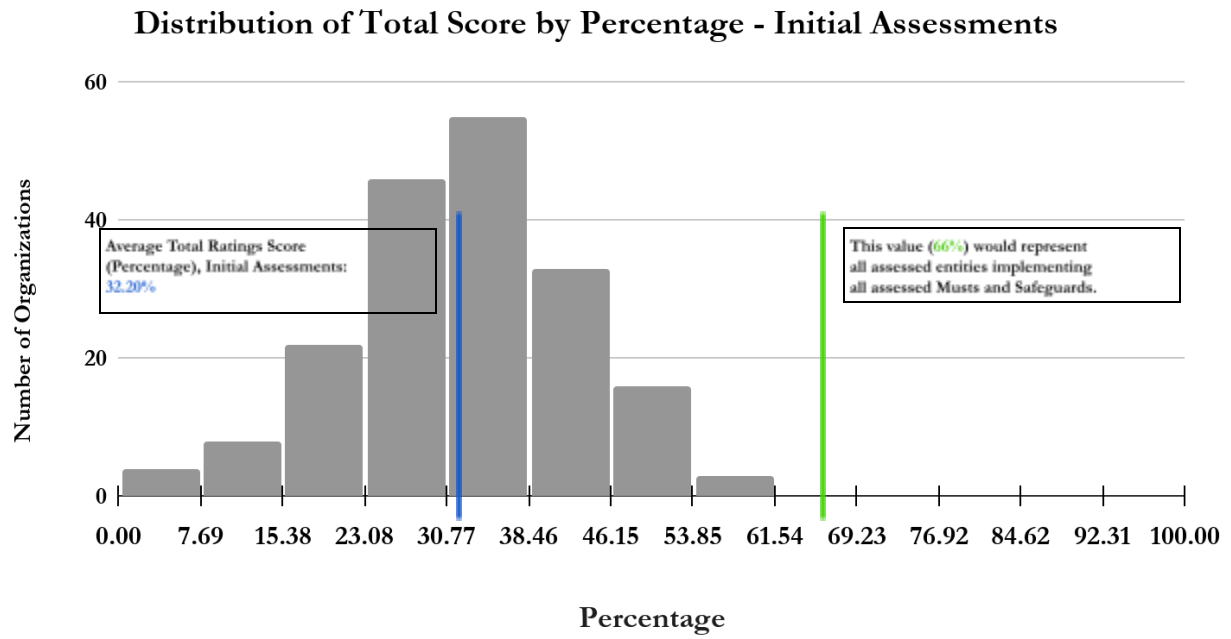
Using the implementation ratings coding system described in Section 2.2, total scores for assessed organizations ranged from 1 to 60 points. Due to the January 2024 addition to our assessment of CIS Safeguards 6.3 "Require MFA for Externally-Exposed Applications"[35] and 11.4 "Establish and Maintain an Isolated Instance of Recovery Data,"[36] organizations assessed after December 2023 can

[34] Three municipalities received their first Cybertrack+ assessment that also served as a reassessment of their original Cybertrack assessments.
[35] Center for Internet Security. (2021, May). *CIS Critical Security Controls Version 8*. cissecurity.org/controls. p. 22.
[36] Center for Internet Security. (2021, May). *CIS Critical Security Controls Version 8*. cissecurity.org/controls. p. 33.

be assessed up to six points more than those organizations assessed prior. For example, an organization that was assessed to be developing all Musts & Safeguards would score 31 points through December 2023 but 33 points since. An organization that was implementing all Musts & Safeguards would score 62 points through December 2023 and 66 since. The maximum possible assessment rating score, which represents an Optimizing rating on all assessed Musts & Safeguards, was 93 prior to December 2023 and is now 99.

The following results and analysis discuss general trends in the assessment data, but the results of individual assessments varied widely. While the risk exposure of an organization scoring 1 point differs greatly from an organization scoring 60 points, organizations with similar scores may well have very different postures. This is due in part to the fact that not all Musts & Safeguards are equally powerful. That said, the graph below shows the distribution of initial assessment total scores.

Figure 4: Distribution of Assessment Total Scores (Number of Organizations (Y) x Ranges of Percentage of Total Score (X) - Initial Assessments



The average total score for organizations assessed **before** the addition of Safeguards 6.3 and 11.4 to the assessment (n=44) was 27.68 out of 93 possible points[37] for each of the 31 assessed Musts & Safeguards. The average total score for all organizations assessed **after** the addition of Safeguards 6.3 and 11.4 to the assessment (n=145) was 33.17 out of 99 possible points. Overall, the 189 organizations completing initial assessments included in this report again averaged 0.97 points per assessed Must & Safeguard – slightly below a Developing implementation rating. For the 6 assessed Trusted CI Musts, organizations averaged 5.47 points or 0.92 points per Must, also nearly identical to our June 2025 result. For CIS Safeguards only, organizations averaged 0.97 points per Safeguard – also quite similar to our June 2025 result. Both before and after the additions of Safeguards 6.3 and

[37] Three assessed organizations received no rating for CIS Safeguard 2.1. One assessed organization received no rating for CIS Safeguard 4.1.

11.4 to the assessment, organizations reached approximately one point per Safeguard, or a Developing rating, in general. Additionally, implementation continues to be the lowest for the following Safeguards:

- CIS 2.1: Establish and Maintain a Software Inventory
- CIS 2.2: Ensure Authorized Software is Currently Supported
- **CIS 2.3: Address Unauthorized Software**
- CIS 7.1: Establish and Maintain a Vulnerability Management Program
- CIS 8.1: Establish and Maintain an Audit Log Management Program
- CIS 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents
- CIS 17.7: Conduct Routine Incident Response Exercises

Of particular note is the fact that Safeguard 2.3 (**bolded above**) is a member of the Transformative Twelve discussed in Section 2.1.

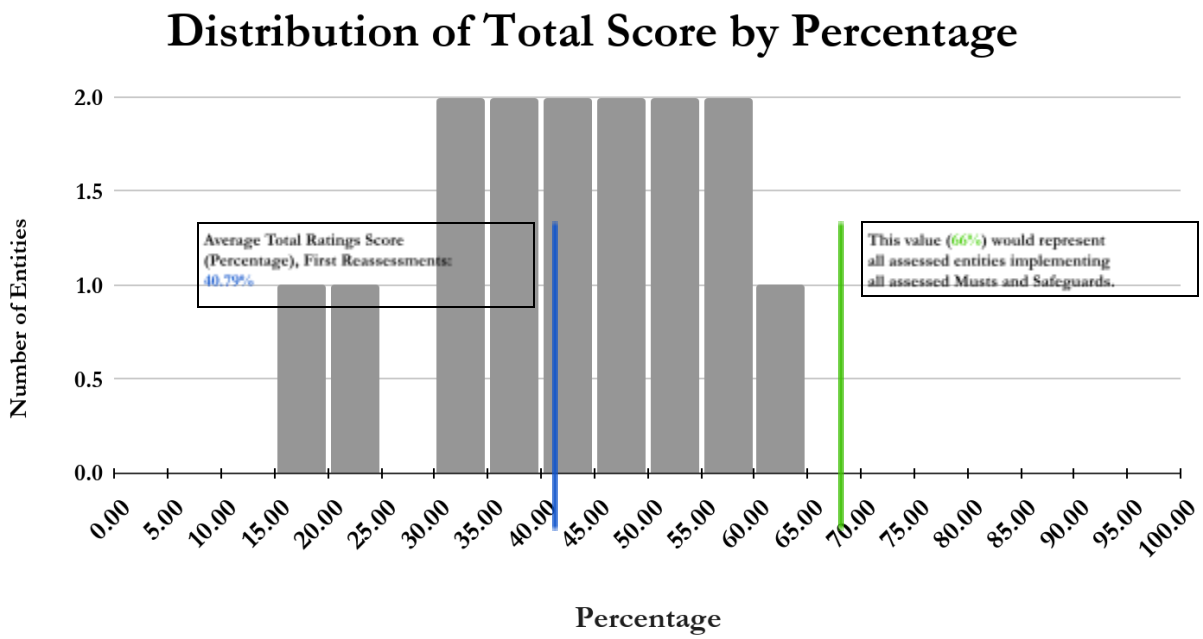
Cybertrack's sample of assessed organizations facilitated a comparison of total assessment rating score by type of organization. We found no statistically significant differences in total score by type of organization. However, we did note that K-12 school districts scored highest, on average, among organization types where more than five organizations have been assessed. The mean total rating score for assessed K-12 organizations was 35.07 points. All other organizations combined averaged 30.02 points. Also of interest, K-12 organizations' scores varied less (a range of 8.74 points) versus a range of 11.19 points for all others. This difference in mean total rating score became statistically significant since our June 2024 report.

3.2 Results from Cybertrack First Reassessments

Cybertrack has reassessed 20 organizations since beginning reassessments in September 2025. As in the initial assessments, we used the implementation ratings coding system described in Section 2.2 in first reassessments (organizations' second overall assessment). Total scores for reassessed organizations ranged from 19 to 60 points. All first reassessments were evaluated using the same 99-point scale currently used for initial assessments, where we evaluate six Trusted CI Musts and 27 CIS Safeguards. An organization that was assessed to be developing all Musts & Safeguards would score 33 points. An organization implementing all Musts & Safeguards would score 66 points. The maximum possible assessment rating score, which represents an Optimizing rating on all assessed Musts & Safeguards, is 99 points.

The following results and analysis discuss general trends in the assessment data. As noted earlier, the results of individual assessments varied widely. The chart below shows the distribution of reassessment total scores.

Figure 5: Distribution of Assessment Total Scores (Number of Organizations (Y) x Ranges of Percentage of Total Score (X), First Reassessments



The average total score for organizations receiving first reassessments (n=20) was 40.79 out of 99 possible points for each of the 33 assessed Musts & Safeguards. Overall, the 20 organizations completing first reassessments averaged 1.24 points per assessed Must & Safeguard – significantly above a Developing implementation rating. For the 6 assessed Trusted CI Musts, organizations averaged 1.19 points per Must. For CIS Safeguards only, organizations averaged 1.24 points per Safeguard. Implementation was the lowest for the following Safeguards:

- CIS 2.2: Ensure Authorized Software is Currently Supported
- **CIS 3.4: Enforce Data Retention**
- CIS 4.6: Securely Manage Enterprise Assets and Software
- CIS 7.1: Establish and Maintain a Vulnerability Management Process
- CIS 8.1: Establish and Maintain an Audit Log Management Program
- CIS 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents
- CIS 17.7: Conduct Routine Incident Response Exercises

Of particular note is the fact that Safeguard 3.4 (**bolded above**) is a member of the Transformative Twelve discussed in Section 2.1.

Because of the relatively small number of first reassessments performed, we did not compare aggregate ratings by type of organization.

At a more granular level, all but three reassessed organizations demonstrated overall progress from their first assessment; variations in the magnitude of these differences ranged between -3 and 40

ratings points. Of course, we're still looking at a small sample size (20 organizations), and we'll continue to update these results as our sample grows. Thus far, we can characterize ratings results from reassessed organizations generally as showing some progress made on Trusted CI Musts accompanied by progress on several assessed Safeguards.

The cybersecurity progress made by reassessed organizations broadly follows recommendations made in the organizations' initial Cybertrack assessment. In our recommendations on reassessed organizations' initial assessments, we referenced 228 individual Musts & Safeguards. Reassessments have shown that the organizations made progress on 93 of the 228 (40.8%) recommended safeguards. Nearly sixty percent (57.9%) of the points gained in aggregate on reassessments are attributed to Musts & Safeguards that were cited in recommendations in the organization's initial assessment.

In the case of the organizations that did not show overall progress in reassessment, each showed progress in some areas of cybersecurity. In one case, an organization progressed in areas of governance as reflected in increased Musts ratings but continued to work on gaps in some key Safeguards, including newly-noted gaps in secure configuration. In another, the organization made gains on some technical controls, but progress on governance and programmatics issues were slower to bear fruit.

Assessment progress varies significantly by organization, but the general pattern is represented in the following case. In this case, the assessed organization 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 organization moved from Not Implementing to Developing on these four Musts, developed and implemented more secure configuration processes, and expanded its implementation of MFA. Though some of the Safeguards that were referenced in Cybertrack's first report recommendations were fully implemented at the time of the organization's reassessment, most recommendations from the organization's initial assessment had only been partially implemented. Reassessed organizations cited time and budget most frequently by far as barriers to additional progress.

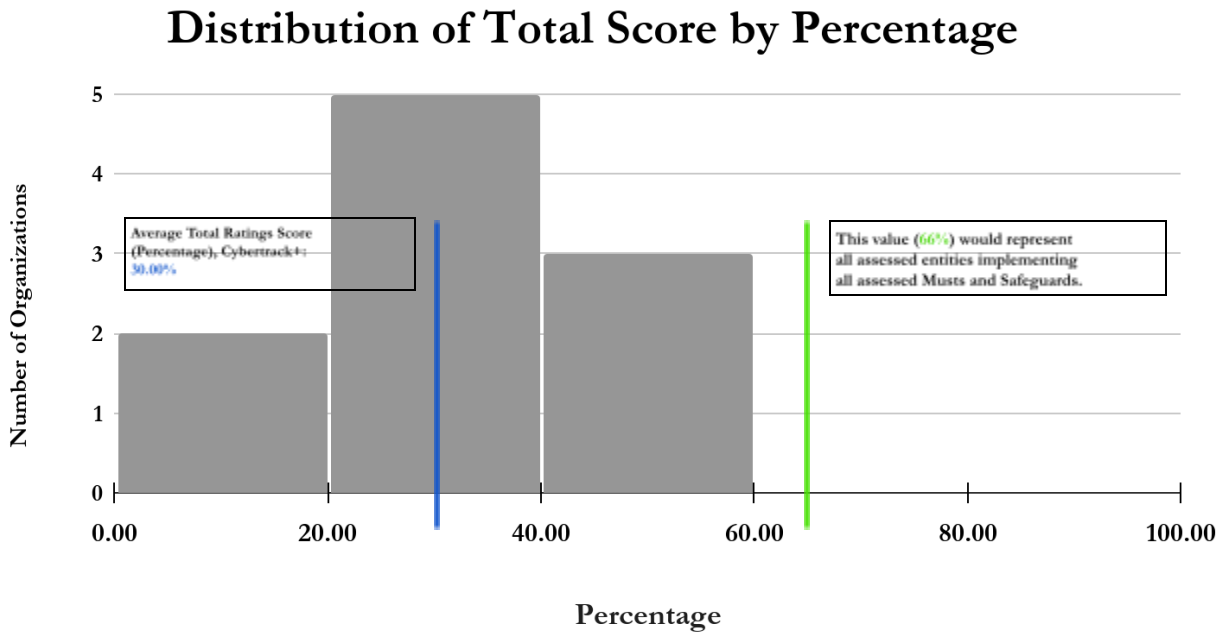
These findings serve as a key metric, providing evidence of Cybertrack's positive return on investment for the state. As of this report, there are four additional organizations scheduled, being scheduled for onboarding, or in the process of receiving a reassessment.

3.3 Results from Cybertrack+ Assessments

Cybertrack+ assessments also use the implementation ratings coding system described in Section 2.2. To tailor Cybertrack assessments to operational technology-reliant environments, Cybertrack+ assessments evaluate 40, rather than 27, CIS Safeguards while also evaluating the same six Trusted CI Musts. Table 5 below shows that Cybertrack+ assessments have 138 possible points, which represents Optimizing on all 46 assessed Musts & Safeguards. Implementing ratings on all Cybertrack+ Safeguards achieves 92 points. A Developing rating on all Musts & Safeguards achieves 46 points. Of the 10 organizations that have received Cybertrack+ assessments so far, ratings total scores ranged from 21 to 77 points.

The following results and analysis discuss general trends in the assessment data, but the results of individual assessments varied widely. These results include three organizations whose Cybertrack+ assessments functioned as first reassessments of the Musts, as well as the 27 Safeguards included in both their initial Cybertrack assessments and this Cybertrack+ assessment. The graph below shows the distribution of assessment total scores.

Figure 6: Distribution of Assessment Total Scores (Number of Organizations (Y) x Ranges of Percentage of Total Score (X), Cybertrack+ Assessments



The average total score for organizations receiving Cybertrack+ assessments (n=10) was 45.20 out of 138 possible points for each of the 46 assessed Musts & Safeguards. Overall, organizations completing Cybertrack+ assessments included in this report again averaged just under one point (0.98 points) per assessed Must & Safeguard – roughly a Developing implementation rating. For the 6 assessed Trusted CI Musts, organizations averaged 6.60 points or 1.10 points per Must. For CIS Safeguards only, organizations averaged 38.60 points, or 0.97 points per Safeguard.

While these results reflect, in aggregate, our assessments of OT-reliant environments, they also include the three organizations that previously received Cybertrack assessments. Removing these three organizations from our calculations lowers the average points achieved per assessed Must & Safeguard from 0.98 to 0.90 (n=7). Similarly, the average ratings points per assessed Must fall to 0.98 from 1.10; points per assessed Safeguard also falls to 0.89 from 0.97.

Implementation was the lowest for the following Cybertrack Safeguards assessed across all assessment types:

- CIS Safeguard 2.1: Establish and Maintain a Software Inventory
- **CIS Safeguard 3.4: Enforce Data Retention**
- **CIS Safeguard 6.5: Require MFA for Administrative Access**
- CIS Safeguard 8.1: Establish and Maintain an Audit Log Management Process
- CIS Safeguard 17.3: Enterprise Process for Reporting Incidents
- CIS Safeguard 17.7: Conduct Routine Incident Response Exercises (IG2 & IG3)

Of particular note is the fact that Safeguards 3.4 and 6.5 (**bolded above**) are members of the Transformative Twelve discussed in Section 2.1.

Because of the relatively small number of first reassessments performed, we did not compare aggregate ratings by type of organization, nor do we address in-depth organizations' performance on the 13 Safeguards that are part of the Cybertrack+ assessment but not part of a Cybertrack assessment. What we can say now about these 13 Safeguards is that our list of the seven Safeguards with the lowest levels of implementation would change to the following if we included all 40 Cybertrack+ assessed Safeguards in our analysis.

- CIS Safeguard 2.1: Establish and Maintain a Software Inventory
- **CIS Safeguard 3.4: Enforce Data Retention**
- **CIS Safeguard 7.2: Establish and Maintain a Remediation Process**
- **CIS Safeguard 7.6: Automated Vulnerability Scans of Externally-Exposed Enterprise Assets**
- **CIS Safeguard 11.5 Test Data Recovery**
- CIS Safeguard 17.3: Enterprise Process for Reporting Incidents
- CIS Safeguard 17.7: Conduct Routine Incident Response Exercises (IG2 & IG3)

In this list, the bolded Safeguards are members either of the Transformative Twelve or the OT-22 (a.k.a the Sturdy 30, which, as discussed in Section 2, resulted from similar research focused on OT-reliant environments. When we include all Cybertrack+ assessed Safeguards in our list of Safeguards with the lowest levels of implementation, we see some important similarities. Difficulties in maintaining software inventories (CIS 2.1), in developing and implementing cyber incident response (CIS 17.3 & 17.7), and in implementing strong vulnerability management (CIS 7 Control Family) are common regardless of the type of environment we assess. IT and OT-reliant environments struggle with some of the same fundamental cybersecurity challenges. Because our number of Cybertrack+ assessed organizations is still small and because these data vary widely among assessed organizations, we will continue to monitor these trends but will not address them in depth in this report.

3.4 Results from Free Response Data

Cybertrack's Written Discovery Requests (WDRs) also ask several questions of assessed organizations that seek to understand organizations themselves and further characterize their cybersecurity postures beyond the assessed Musts & Safeguards. These questions include additional descriptions of barriers to individual Must or Safeguard implementations, as well as "Wrap-up"

questions at the end of the WDR that provide space for respondents to inform the Cybertrack team of important details of their cybersecurity posture that may not be adequately described by specific Must- and Safeguard-focused responses. These questions ask for information including:

- Wrap-Up Q1: **Participants**. "Provide a listing of all people who participated or were consulted in providing your responses. Include full names and titles/roles."
- Wrap-Up Q2: **Strengths and Capabilities**. "Does your organization have any cybersecurity strengths or capabilities, whether discussed in responses to prior questions or not, that you want to highlight? If so, please describe."
- Wrap-Up Q3: **Weaknesses and Challenges**. "Does your organization have any cybersecurity weaknesses or challenges, whether discussed in responses to prior questions or not, that you want to highlight? If so, please describe."
- Wrap-Up Q4: **Incidents**. "Has your organization experienced an impactful cybersecurity incident in the last 3 years? If so, please describe."
- Wrap-Up Q5: **Population**. "What is the population of your jurisdiction?"
- Wrap-Up Q6: **Users**. "How many employee and contractor users have access to your network?"
- Wrap-Up Q7: **IT Personnel**. "How many IT personnel, including contractors, does your organization employ? Please respond in terms of full-time equivalents (FTEs)."
- Wrap-Up Q8: **Endpoints**. "How many networked systems and devices (*e.g.*, laptops, desktops, mobile devices, IP phones, servers, virtual servers, network equipment) does your organization manage?"
- Wrap-Up Q9: **Use of State Resources**. "Does your organization use any Indiana State Government services related to IT and/or cybersecurity?"
- Wrap-Up Q10: **Overall Annual Budget**. "What is the overall annual budget (not limited to IT or technology) for your entire local organization? Be specific about the fiscal year. Provide a link to supporting documentation if available."
- Wrap-Up Q11: **Anything Else?** Is there anything else you want to share with the Assessment Team? If so, please use this response to describe."

Wrap-Up questions 1, 2, 3, and 9 yielded the following results of interest.

Based on responses to Wrap-Up Q1, to which all assessed organizations responded (n=216), we noted that 165 organizations (76.4%) completed the assessment exclusively using IT employees or IT consultants. Seventy organizations (32.4%) engaged non-IT members of leadership in the assessment process. This percentage is significantly lower than the percentage of organizations (54.2%) that received a rating of Implementing or better on Must 5: Leadership during assessment. Must 5 requires that non-IT organizational leaders are involved in cybersecurity decision making.[38]

To build a more complete understanding of cybersecurity in assessed organizations, we ask participants to share what they perceive as their organization's cybersecurity strengths (Wrap-Up Q2) and weaknesses (Wrap-Up Q3).

Ninety-six organizations (49.0%) responded with strengths; one hundred twenty-six (64.2%)

[38] https://www.trustedci.org/framework/core.

provided perceived weaknesses. As shown in **Table 5**, assessed organizations' reported strengths were distributed across 17 coded responses. The distribution of these coded responses again shows perceived cybersecurity strengths are diverse, but two patterns were notable. Several organizations listed their IT staff members and contractors as a strength. Strength of personnel was the most frequently cited strength overall (33) and the most frequently cited (15) since our June 2025 report. Endpoint protection became the second most frequent cited strength, up one spot since June 2025 with 19 responses.

Table 5: Coded, Perceived Cybersecurity Strengths as Reported by Assessed Organizations

ID#	Characterization of Strengths	# of Organizations
4	Personnel (Contractor/staff knowledge)	33
10	Endpoint Protection	19
8	Network Security Infrastructure	13
1	Access Control - MFA Imp	12
7	Training	7
6	Data Resiliency - Backups	7
5	Network Monitoring	7
3	Patching	4
18	Leadership Support	4
13	Cybersecurity Program	4
11	Vulnerability Management	4
2	Access Control	3
12	Access to State Resources	3
19	Motivated IT Team	3
17	Threat Intel	1
16	Cybersecurity Community	1
15	Network Isolation	1
14	Response Plans	1
20	Limited Data Stored/Transmitted/Processed	1
21	Documentation	1

Perceived weaknesses were less diverse and the gap between the three most frequently listed weaknesses and the rest is much wider. Of the 126 organizations that responded with cybersecurity weaknesses, 71 noted a lack of adequate cybersecurity-specific staffing, 46 reported a lack of

cybersecurity-related policies and procedures, and 34 commented on the need for additional funding in their budgets for cybersecurity. The reported weaknesses are summarized in **Table 6** below.

Table 6: Coded, Perceived Cybersecurity Weaknesses as Reported by Assessed Organizations

ID#	Characterization of Weaknesses	# of Organizations
6	Lack of Staffing/knowledge	71
8	Lack of Documentation	46
12	Budget	34
11	Lack of Cybersecurity Program	12
13	Cybersecurity infrastructure	4
10	Access Control - Passwords	4
1	Backups	4
3	Lack of Logging/Monitoring	4
9	Lack of Controls Testing	3
2	Lack of Encryption	2
16	Lack of Training	2
14	Lack of MFA Imp	2
5	Lack of Isolation	2
7	No IR Exercises	2
15	Lack of DR	2
17	Vuln Management	2
4	Lack of Device Configuration Process	1

As mentioned above, we also ask organizations which cybersecurity resources offered by the State of Indiana they're using. Fifty-six percent (110 of 196 unique organizations) make use of State cybersecurity resources. Forty percent (78 of 195) reported using State-purchased licenses for the KnowBe4 security awareness product, making it the most widely used State-sponsored service among Cybertrack assessed organizations. Fifty-one (26.0%) reported using the CrowdStrike licensing program. Twenty-six (13.3%) have .gov domains hosted by the State. Other State services being used by assessed organizations include Udemy online training, website hosting, and the QPI purchasing program. The CrowdStrike and Udemy partnerships were new in June 2024 and gained significant usage since.. The number of organizations that told us they use the CrowdStrike program grew from five in June 2024 to fifty-one today. Udemy usage has grown from twelve organizations using the Udemy program to 27 over the past year.

4 Analysis

This section presents our analysis of assessment results and information from 216 Indiana local public sector organizations assessed between March 2023 and May 2026. We start our analysis with a general characterization of assessment results (Section 4.1). Next, we discuss a sampling of specific results that are noteworthy, either as reasons for optimism or concern, in terms of the assessed Trusted CI Musts (Section 4.2) and CIS Safeguards (Section 4.3). Finally, we present particularly strong correlations present in these data (Section 4.4) and correlations among the data that we're watching.

4.1 General Characterization of Assessment Results

4.1.1 Initial Cybertrack Assessments

The Cybertrack Team's analysis focuses on implementation rating data generated from assessments. As described in Section 2.1 (Assessment Methodology), this assessment is focused on the most proven, most impactful, most fundamental organizational (aka "programmatic") "Musts" and "Safeguards." On average, assessed organizations received nearly one point (0.97) per assessed Must and Safeguard out of the 3 points possible.

Notably, the results have remained largely consistent since our first Aggregate Results & Analysis Report in November of 2023. Our data continue to show that, in general, organizations averaged a Developing implementation rating. Across all organizations assessed during the Cybertrack program, none of the assessed Musts or Safeguards individually averages above Developing. More granular trends in assessment results have also remained consistent over the lifespan of the program including: most commonly implemented Musts & Safeguards, least implemented Musts & Safeguards, and most commonly cited barriers to progress. As our sample size of initial Cybertrack assessments continues to grow, we can characterize local public sector organizations with increasing confidence as struggling to implement the most fundamental cybersecurity controls.

4.1.2 First Reassessments

As with initial assessments, the Cybertrack Team's analysis of reassessments focuses on ratings data generated from assessment of the same most proven, fundamental, and impactful Musts & Safeguards. On average, the 20 organizations receiving first reassessments averaged 40.79 points out of 99 possible points. Compared against the same metric (31.89 points) for the 189 initial Cybertrack assessments, first reassessments averaged nearly 9 (8.9%) more total points per assessment. The 40.79 average points achieved by first reassessments represent 1.24 points per assessed Must and Safeguard – significantly above the threshold for a Developing rating. Across all first reassessment assessments performed, two Safeguards (CIS Safeguard 7.3: Automated Operating System Patch Management and CIS Safeguard 10.2: Configure Automatic Anti-Malware Signature Updates) averaged two points out of the possible three, an Implementing rating.

Focusing our comparison, we also evaluated changes in ratings between assessed organizations' first reassessments and their initial Cybertrack assessments performed approximately 18 months ago.

Notably, our reassessed organizations outperformed their peers on their initial assessments. On average, reassessed organizations increased their total ratings scores from their initial assessments by 8.20 points, or 8.3%. This is a smaller increase than the comparison of average total ratings score of reassessed organizations against the average total rating score of all initial assessments because the average total ratings score of *all* organizations' initial assessments is lower than initial assessments of reassessed organizations.

Additionally, we've removed a (positive) outlier from our analysis of reassessments. The average increase (and other aggregate statistics) from initial assessment to first reassessment **does not** include one reassessed organization that increased or refined its implementation of evaluated Musts & Safeguards by 40 points, tripling its ratings score in reassessment! In this case, the assessed organization 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 & Safeguards, the organization advanced two ratings levels. In this case, free response data from the organization's reassessment questionnaire combined with these ratings data illustrate the power to make exceptional progress on cybersecurity when leadership, resources, and expert guidance are aligned and brought to bear.

As discussed in the Section 3.2 "Results from Cybertrack First Reassessments", we compared differences in total Musts ratings points directly with the corresponding organizations' initial assessments, the increase is a 1.31 point increase, on average, across all assessed Musts. Turning to the CIS Safeguards, first reassessments averaged 7.47 more ratings points in total on average than on Cybertrack initial assessments. These gains tended to be expressed in a positive movement of one ratings level over seven or eight of the Safeguards we assess, although ratings movement varied on individual reassessments. **Nearly fifty-eight percent of the ratings points gained in reassessment were achieved through actions taken by these organizations in response to recommendations provided on their initial Cybertrack assessment.** Though our sample size of first reassessments is relatively small, this progress is quite encouraging.

Organizations usually scored an equal or greater number of ratings points on Musts & Safeguards when reassessed but not always. In a few cases, an organization's degree of implementation of a particular Must or Safeguard decreased. When this backward movement of ratings scores occurred, common factors included: loss of personnel who played a significant role in the organization's cybersecurity, replacement of a vendor or product with a less secure alternative within a department, or change in organizational tolerance for cybersecurity risk. Most frequently, though, backward ratings movement occurred because the assessment team always seeks to more closely align a particular rating with the organization's cybersecurity posture. In some cases, the assessors performing the reassessment simply disagreed with the rating given by the initial assessment team on a Must or Safeguard based on the information available from the initial assessment. In reassessment, the assessment team has the benefit of all of the information about the organization that was learned during the initial assessment, as well as an opportunity to refine their questions in reassessment and dig even more deeply into an organization's responses to each Must & Safeguard. The additional information learned in reassessment sometimes compels an assessment team to revise a rating lower. Despite several occasions where organizations lost ratings points on particular Musts & Safeguards in reassessment, reassessed organizations generally broadened and deepened their implementations, which is reflected in the significant ratings (and points) gains over their initial assessments.

4.1.3 Cybertrack+ Assessments

As noted in Sections 2.1.3 (Assessment Methodology) and 3.3 (Results) the Cybertrack Team analyzed ratings data for the same six Trusted CI Musts and original 27 CIS Safeguards but added 13 Safeguards to more comprehensively evaluate cybersecurity in OT-reliant environments. Again, the 13 additional Safeguards evaluated in Cybertrack+ assessments were proven to be the most powerful, most impactful, and most fundamental Safeguards in OT-reliant environments through the research methodology detailed in Section 2.1.3. As discussed in Section 3.3, when we remove these three organizations from our analysis, the seven initial Cybertrack+ assessed organizations achieved average points per assessed Must & Safeguard of 0.90 points. The average points per Must for this group is 0.97 points; the average points per Safeguard is 0.88 points. In general, Cybertrack+-assessed organizations average fell substantially short of a Developing implementation rating.[39] In sum, **Cybertrack+ assessed organizations struggle to implement these most fundamental cybersecurity protections similarly to their Cybertrack-assessed peers.** In fact, Cybertrack and Cybertrack+ assessed organizations struggle most to implement some of the same Musts & Safeguards including: maintaining software inventories (CIS 2.1), in developing and implementing cyber incident response (CIS 17.3 & 17.7), and in implementing strong vulnerability management (CIS 7 Control Family). With that said, our sample is small and may change significantly as we assess more OT-reliant organizations.

4.2 Noteworthy Results: Trusted CI Framework Musts

As noted in Section 2.1 above, the Trusted CI Framework Musts evaluate organizational **cybersecurity fundamentals, or programmatics,** driving organizations' cybersecurity efforts. Cybertrack assessments evaluate 6 of the Framework's 16 Musts, listed in Appendix A. The ranking of Musts by mean rating scores are highly consistent across all assessment types. These rankings have remained consistent with our samples of Cybertrack initial assessments between November 2023 and June 2026 reports even though our assessment of 216 organizations includes a wider range of organization types. **Table 7** below shows the similarity of the mean score ranking among Musts in all Cybertrack assessment types. In each type of assessment, organizations were most commonly implementing Must 5 (Leadership) and Must 7 (Cybersecurity Lead) and least commonly implementing Must 9 (Policy) and Must 15 (Baseline Control Set).

[39] Organizations averaged a slightly lower than the same average total score calculated after our initial 23 assessed organizations described in our first report.

Table 7: Mean Ranking of Trusted CI Musts (high to low) by Reassessment, May 2026

Control Description	Means			
	Initial Assessment	Reassessment	CT+ Assessment	Reassessment Progress
Must 5 (Leadership)	1.48	1.63	1.50	0.16
Must 7 (Cybersecurity Lead)	1.14	1.53	1.40	0.39
Must 13 (Personnel)	0.95	1.21	1.50	0.26
Must 12 (Cybersecurity Budget)	0.78	1.47	1.10	0.70
Must 9 (Policy)	0.76	1.00	0.80	0.24
Must 15 (Baseline Control Set)	0.39	0.47	0.30	0.08
Average	**0.92**	**1.22**	**1.10**	**0.30**

Table 7 also summarizes progress made by reassessed organizations on Trusted CI Musts since their initial assessments, which is most encouraging. As noted in Section 3 (Results), organizations receiving first reassessments achieved an average of 1.22 points per Must compared to an average of 0.92 points for all initial assessments – a 32.6% increase. Additionally, comparing ratings scores on Musts from first reassessments against only the initial assessments of the reassessed organizations lowers the average points per Must from the sample of initial assessments to 0.89. Though reassessed organizations outperformed their peers on initial assessments in terms of total score, they were underachievers in terms of Musts total score. Correspondingly, the percentage increase from initial assessment to first reassessment increases to 37.1%. Categorizing these averages in terms of ratings, organizations receiving initial assessments were, on average, Not Implementing most Musts, but made significant strides in Developing the Musts after their initial assessments. These results are especially encouraging because, as discussed in each of these reports, we've observed an increasingly strong and explanatory correlation between higher rates of implementation on Trusted CI Musts and higher implementation rates on the CIS Safeguards we assess.

Table 8 illustrates the longitudinal stability of the mean score ranking among the Musts in initial Cybertrack assessments despite some volatility in the means themselves.

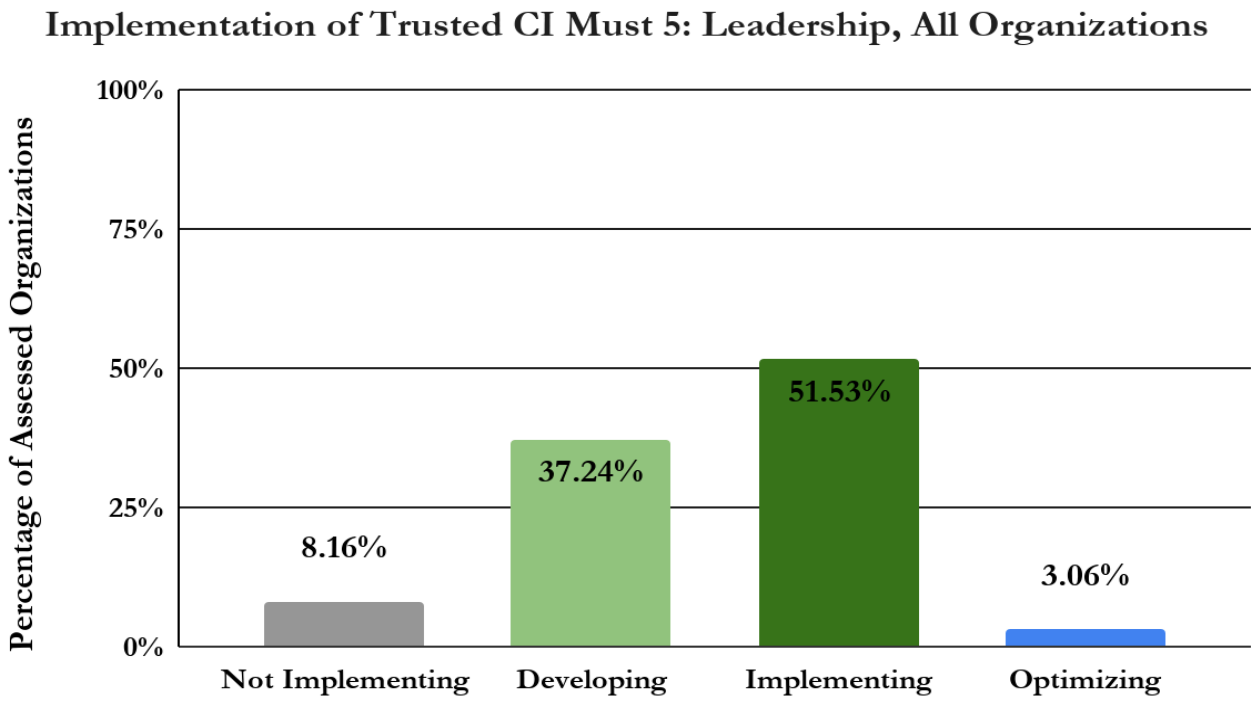
Table 8: Longitudinal Mean Ranking of Trusted CI Musts (high to low) with Percentage Change in Means, November 2023 - May 2026

Changes in Mean Ratings Score for Trusted CI Musts in Initial Assessments November 2023 - May 2026					
Must	November 2023 Mean	May 2024 Mean	May 2025 Mean	May 2026 Mean	Percentage Change Since 2023
Must 5: Leadership	1.39	1.38	1.46	1.48	5.70%
Must 7: Cybersecurity Lead	1.04	1.16	1.10	1.14	8.13%
Must 13: Personnel	0.91	1.03	0.89	0.95	3.08%
Must 12: Cybersecurity Budget	0.78	0.80	0.75	0.78	-1.60%
Must 9: Policy	0.65	0.80	0.76	0.76	17.25%
Must 15: Baseline Control Set	0.48	0.46	0.41	0.39	-18.38%

Because Musts rankings have been very similar across assessment types, our analysis of the Musts that follows speaks generally to notable trends in the Musts. When our analyses differ by assessment type, those differences are noted below in our characterization of results on individual Musts.

Another encouraging result from our evaluation of the Musts continues to be the involvement of leadership in cybersecurity decision making. More than half of assessed organizations received at least an Implementing rating on this Must (54.59%), while 37.24% received a Developing rating. Slightly more than 8% of assessed organizations received a rating of Not Implementing. **Figure 7** below illustrates the ratings distribution for Must 5. Assessed organizations averaged 1.49 points on Must 5 (Organizations must involve leadership in cybersecurity decision making.), up very slightly from 1.46 points in our last report. This average implementation rating on Must 5 continues to exceed the average rating of other Musts.

Figure 7: Implementation Rating Distribution: Must 5 (Leadership)



Senior leadership must be involved in cybersecurity decision-making to address cybersecurity competently. Organizational leaders are the primary agents of the organizations for which they work, representing the organization to the outside world. They are ultimately responsible for the organization and are best positioned to bear the burdens of tough decisions about risk taking and risk reduction. No job roles are more directly and holistically connected with the organization's mission than those of its leadership. They ultimately control the allocations of resources, budget, and personnel to support the cybersecurity program. The causes of these relatively positive results are not clear, but they may be a result of increasing awareness of the importance of cybersecurity, increasing frequency of successful cyber attacks on local governments,[40] and/or the relatively small nature of local public sector organizations where most if not all expenditures require senior leadership engagement. Regardless, we view the relatively high distribution of implementation ratings for Must 5 as a reason for optimism.

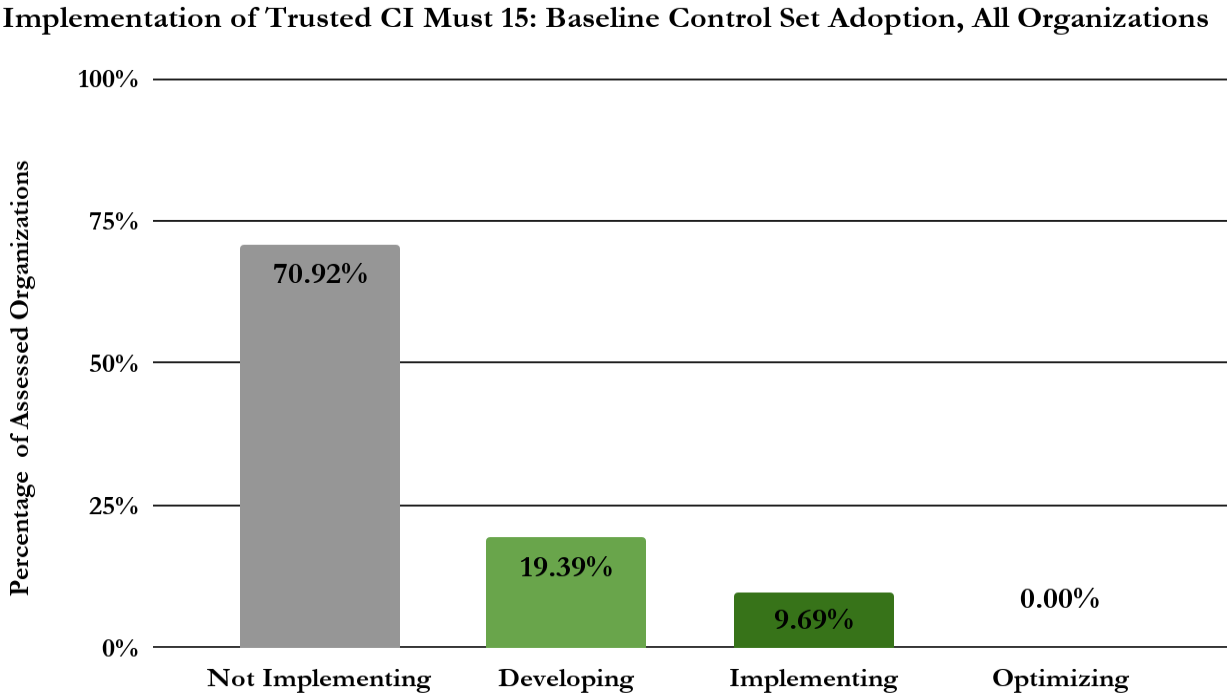
On the other end of the spectrum, few assessed organizations have adopted a baseline set of cybersecurity controls (Must 15). Assessed organizations averaged only 0.40 points on this Must on initial assessments and 0.29 points across the small number of Cybertrack+ assessments (n=10) conducted so far. While this average improved for first reassessments (0.50; n=20), it is well below a Developing rating for each type of assessment.

Across all assessment types, less than 10% (9.69%) had formally adopted a baseline set of

[40] Mahendru, P. *The State of Ransomware in State and Local Government 2023*. Sophos. https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-government.

cybersecurity controls, such as the CIS Safeguards or NIST Cybersecurity Framework. As shown in **Figure 8** below, nearly 71% of assessed organizations had made no progress on this programmatic fundamental as of their assessment. Sixty percent of reassessed organizations were still Not Implementing Must 15 at the time of their reassessments despite a corresponding recommendation on 70.0% of their initial assessment reports to do so. Organizations are struggling significantly to adopt baseline control sets even when provided templates and instructions on how adoption can be accomplished. Feedback from the Reassessment Questionnaires provided insight into organizations' struggles. Most reassessed organizations (9) that struggled to implement Must 15 cite a lack of time to invest in implementing this Must. Time pressures are caused, according to these organizations, by the time requirements of the process to adopt a corresponding policy in a public meeting and by a need for training on the adopted baseline control set.

Figure 8: Implementation of Trusted CI Must 15: Adoption of a Baseline Control Set



Control set adoption is critical to a well-functioning cybersecurity program. An adopted framework provides a common language that facilitates the organization's discussion of cybersecurity concepts and topics. Additionally, an adopted control set provides organizations with a clear yardstick against which to measure. When creating cybersecurity plans and budgets, an adopted control set helps to ensure that executive, IT, and OT leaders can translate cybersecurity risks into technical, physical, and policy solutions that mitigate those risks. A control set also facilitates the assessment of the organization's cybersecurity posture. Cybersecurity assessment provides a baseline understanding of an organization's cybersecurity posture, gaps in controls, and—when performed regularly over time—insight into an organization's progress in reducing cybersecurity risk.

Our overall evaluation of the state of cybersecurity programmatics among assessed organizations includes the average score on all assessed Musts, the mode for each Must implementation rating, and

the relationship between an organizations' total Musts scores and total Safeguards scores. Assessed organizations averaged only 5.46 points out of 18 possible across all assessed Musts on initial assessment. Reassessed organizations averaged a significantly higher 7.16 points – a difference of 31.1%. Though reassessed organizations made strong gains toward implementing these six Musts, achieving 7.16 points on average represents slightly more than half of the score needed to average an Implementing rating on all 6 Musts we assess.

Unfortunately, Must 5 is the only assessed Must where organizations most commonly achieved a rating of Implementing during their initial assessments. The Musts most frequently achieving a Developing rating are Must 7 (having an established cybersecurity lead role and Must 9 (implementation of formal cybersecurity policy. Assessed organizations most frequently received a Not Implementing rating for Must 12 (not having a cybersecurity budget), Must 13 (lacking the formal designation of personnel to cybersecurity responsibilities), and Must 15 (not adopting and using a baseline control set. These data continue to indicate that assessed organizations' leaders are aware of cybersecurity as a source of risk to their organizations but that they have a lot of work to do to build formal cybersecurity programs to address those risks.

Among reassessed organizations, Must 12 (cybersecurity budget), Must 9 (implementation of a formal cybersecurity policy), and Must 13 (the formal designation of personnel to cybersecurity responsibilities) were most commonly assessed as Implementing; however, Must 5 (leadership involvement) was most frequently Developing. As with initial assessments, Must 7 (establishment of a cybersecurity lead role) was also most frequently rated as Developing. More than 70% of reassessed organizations were making progress implementing both Musts 9 and Must 13, an increase from initial assessments from 64.6% on Must 9 and 60.9% on Must 13. Only Must 15 (adopting and using a baseline control set) most commonly (71.4%) received a Not Implementing rating among reassessed organizations.

On average among the Musts, reassessed organizations made the most progress on implementing Must 12. The progress made toward fully implementing Must 12 is especially encouraging because of the particular power of an established cybersecurity budget to drive implementation of other Musts & Safeguards. A formalized budget is an indicator of more formalized thinking about cybersecurity needs and priorities. When we consider that reassessed organizations achieved the second largest average gain toward implementing Must 9 (Policy), we see indicators that these organizations are beginning to address cybersecurity risk in a systematic way.

We know the importance of addressing cybersecurity risk systematically. As we've noted in each of these reports, organizations' total scores on the six assessed Trusted CI Musts significantly predict organizations' total Safeguard scores. With 216 organizations assessed, the **organizations that have made more progress developing cybersecurity programs have made more progress implementing technical cybersecurity Safeguards** (α=0.05, p=<0.001, r^2=0.63). **The predictive power of this correlation has continued to strengthen as we've assessed more organizations.** The next section discusses assessed organizations' implementation of technical Safeguards.

4.3 Noteworthy Results: CIS Safeguards

Organizations received, on average, a Developing rating (1.02 point per Safeguard) across all Cybertrack assessments. While still in the range of a Developing rating, reassessed organizations performed significantly better, achieving 1.24 points per Safeguard. Organizations performed somewhat better when we narrow the focus to only the Transformative Twelve Safeguards. Across all assessments, organizations averaged 1.39 points per Safeguard; reassessed organizations averaged 1.95 points per Safeguard—nearly an Implementing rating. When we rank each Safeguard by average points per Safeguard, 8 of the 10 Safeguards with the highest average points per Safeguard are the same members of the Transformative Twelve, regardless of the type of assessment. Because assessed organizations are not implementing or only developing their implementations of many of the Safeguards we've assessed, they have many cybersecurity priorities to address. With that said, the statistics above suggest that assessed organizations are focusing on the most fundamental and impactful controls but are struggling to fully implement them.

In this section, we highlight and discuss Safeguards on which organizations were rated the highest on average. Then, we discuss results from Safeguards in two CIS Control families (6 and 4); they contain several Safeguards that are members of the Transformative Twelve, and our research shows them to be particularly powerful in preventing or disrupting cyber attacks. Finally, we'll present results from our assessed Safeguards from CIS Control 2 family, with which assessed organizations particularly struggled.

4.3.1 The Most Commonly Implemented Safeguards

Implementation ratings for the two assessed CIS Control 10 "Malware Defenses" Safeguards continued to be the two highest rated by mean score among all 27 assessed CIS controls in Cybertrack initial and reassessment, as well as the 40 Safeguards evaluated in Cybertrack+ assessments.[41] Both of these are members of the "Transformative Twelve" discussed in Section 2.1. The mean score for both CIS Safeguard 10.1, "Deploy and Maintain Anti-Malware Software"[42] and CIS Safeguard 10.2, "Configure Anti-Malware Signature Updates"[43] were 1.83 and 1.84 points, respectively, across all assessments. Initial assessments averaged slightly lower scores (CIS 10.1: 1.82; CIS 10.2: 1.81) in the upper range of a Developing rating, while reassessed organizations averaged scores that were just slightly below or at an Implementing rating (CIS 10.1: 1.94; CIS 10.2: 2.00). The mode rating for both Safeguards across assessment types was Implementing, and only seven assessed organizations received a Not Implementing rating for either Safeguard, all of which occurred in initial Cybertrack assessments. **Figures 9 and 10** below provide a graphical representation of implementation ratings for these safeguards.

[41] When assessing these Safeguards in Cybertrack+ assessments, each is considered to be Implemented if anti-malware software is deployed and automatically updated on all devices that have the capability to deploy anti-malware software. Many OT devices do not have this capability.
[42] Center for Internet Security. (2021, May). *CIS Critical Security Controls Version 8*. cissecurity.org/controls. p. 31.
[43] Ibid.

Figure 9: Implementation Rating Distribution: CIS Safeguard 10.1: Deploy and Maintain Anti-Malware Software

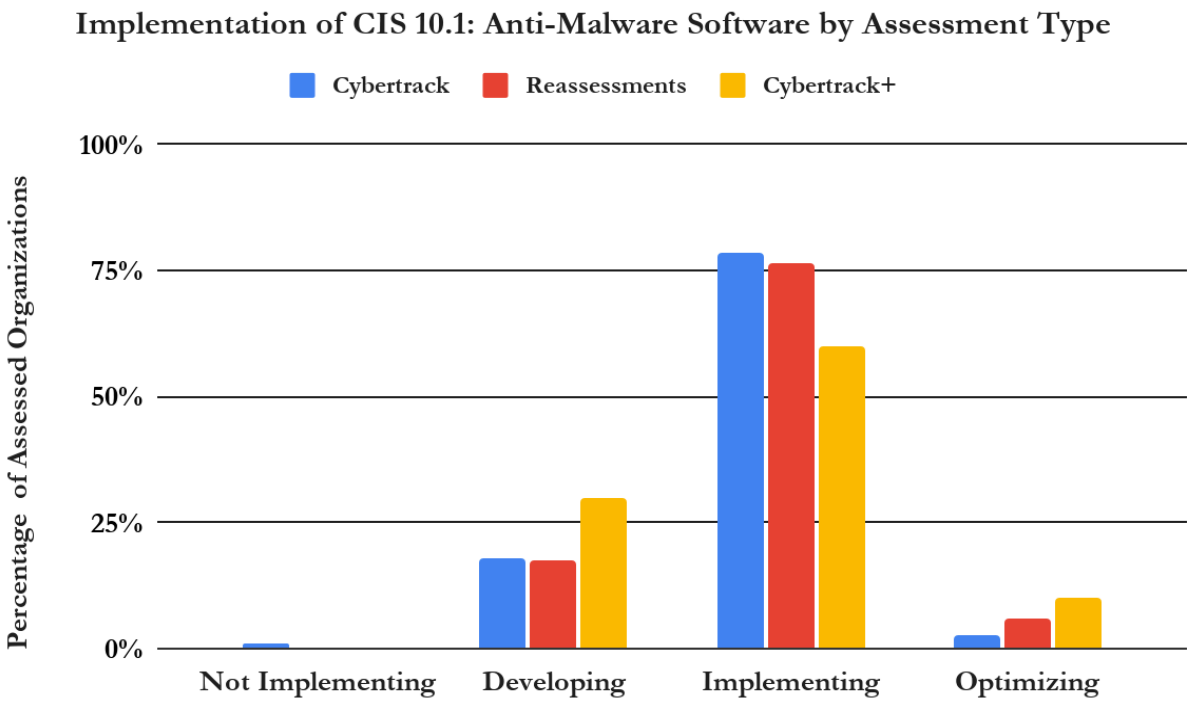
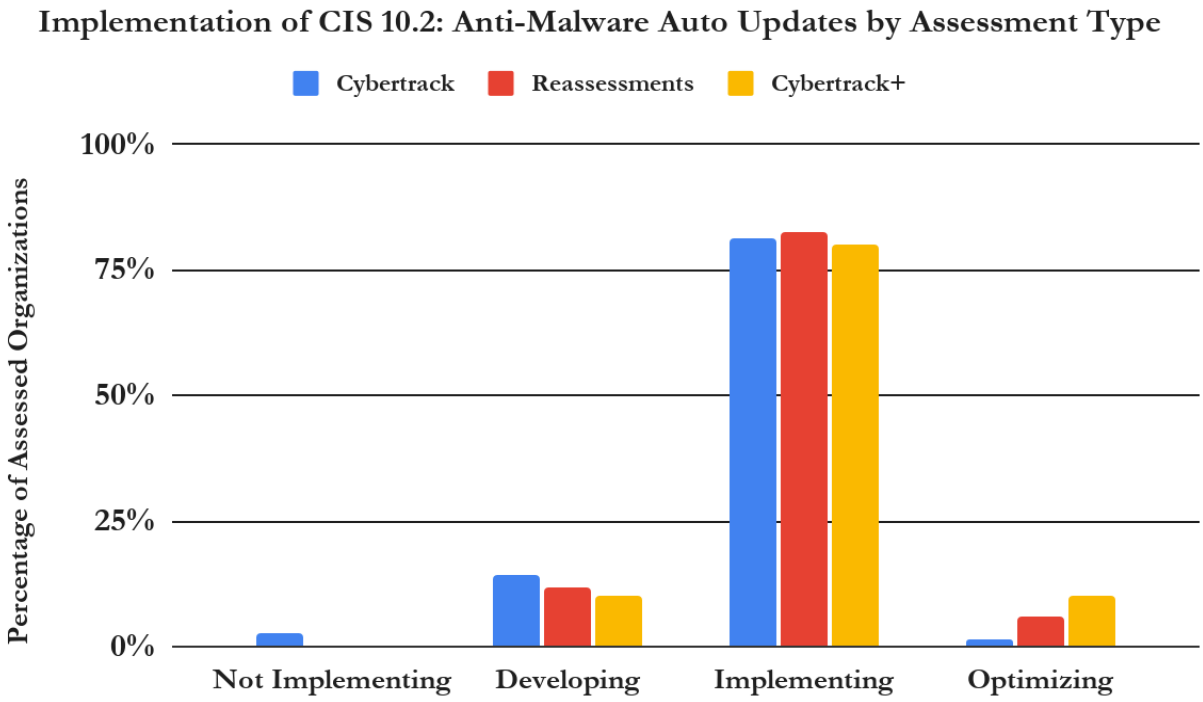


Figure 10: Implementation Rating Distribution: CIS Safeguard 10.2: Configure Anti-Malware Signature Updates



Ransomware incidents have been costly to local public sector organizations. Attacks on Atlanta, GA[44] and Baltimore, MD[45] are prominent examples, but Indiana local public sector organizations have also been extorted through ransomware.[46,47] Implementing and maintaining anti-malware software can protect devices on which they're installed from some types of ransomware infections. Relatively high ratings and the nearly total lack of Not Implementing ratings for assessed organizations on CIS Safeguards 10.1 and 10.2 represent a point of strength in Indiana local organizations' cybersecurity postures.

4.3.2 Implementation of Multi-factor Authentication (MFA) and other Evidence-Proven Safeguards

Substantial empirical research, including that resulting in the identification of the Transformative Twelve and OT-22 Safeguards, indicates multi-factor authentication is an especially powerful control in preventing successful cyberattacks. All evidence-based sources we've found indicate that MFA is one of, if not the most, effective cybersecurity controls available to defenders.[48] Moreover, under Senate Enrolled Act 150, public organizations that connect to the State's technology infrastructure will be required to implement "a secondary end user authentication mechanism"[49] by July 2027. Each of the three CIS Control 6 Safeguards that Cybertrack assesses are members of the Transformative Twelve. Assessed organizations have mixed results implementing MFA in remote access processes. Moving these Safeguards, in particular, from Not Implementing to Developing to Implementing could provide a very substantial reduction in cybersecurity risk to an organization. Cybertrack assesses organizations' implementation and use of multi-factor authentication through CIS Safeguards 6.3, "Require MFA for Externally-Exposed Applications,"[50] 6.4, "Require MFA for Remote Access,"[51] and 6.5, "Require MFA for Administrative Access."[52]

Cybertrack assessed 166 unique organizations after adding Safeguard 6.3 in January 2024 (inclusive of all assessment types). Of those, 57 (34.3%) are fully implementing multi-factor authentication for applications that are accessible externally. The low rate of implementation of MFA on externally-exposed applications continues to be quite concerning because these applications are defined by their exposure to attackers on the Internet. More than half (53.0%) of assessed organizations were Developing this Safeguard; 12.7% were Not Implementing. Organizations that are Developing or Not Implementing MFA in this context should prioritize cybersecurity resources to do so because of the high risk of attack that comes with exposing applications to the Internet. **Figure 11** below provides a graphical representation of implementation ratings for CIS Safeguard 6.3.

---

[44] https://www.justice.gov/usao-ndga/pr/atlanta-us-attorney-charges-iranian-nationals-city-atlanta-ransomware-attack.

[45] https://www.baltimoresun.com/politics/bs-md-ci-ransomware-expenses-20190828-njgznd7dsfaxbbaglnvnbkgjhe-story.html.

[46] https://cyberscoop.com/indiana-ransomware-la-porte-county/.

[47] https://www.nwitimes.com/news/local/education/crown-point-schools-victim-of-ransomware-attack/article_1ee07b98-57ff-11ee-bb41-5fe43ab302d8.html.

[48] *See, e.g.*, https://arxiv.org/abs/2305.00945.

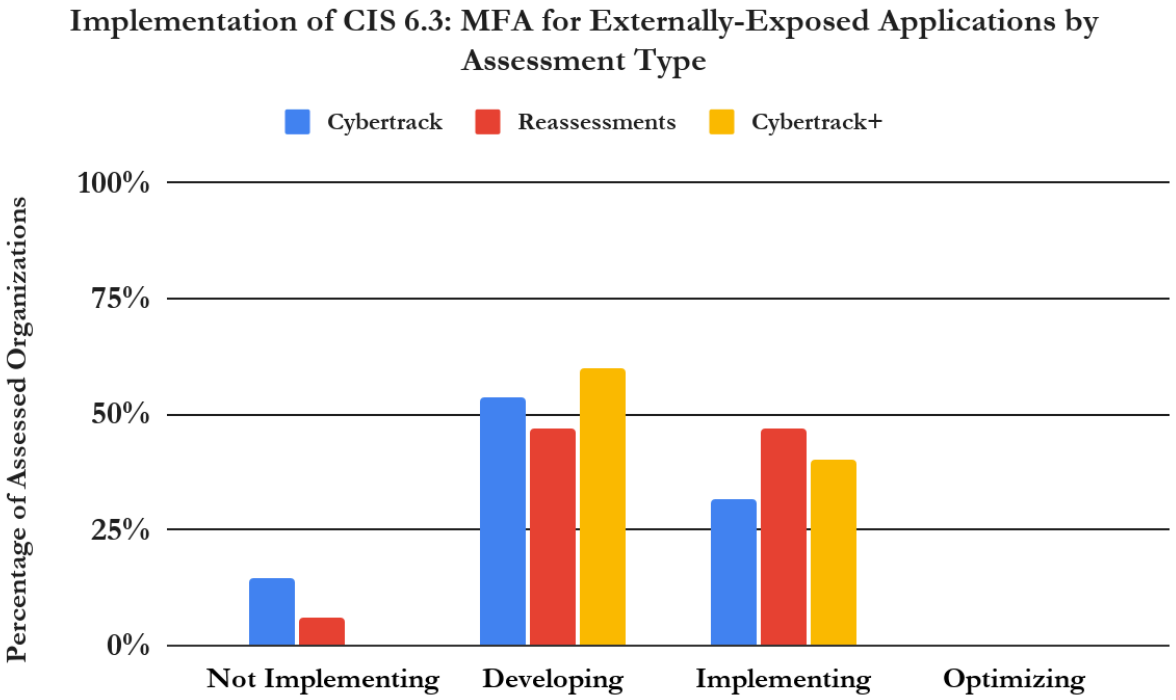
[49] https://iga.in.gov/pdf-documents/123/2024/senate/bills/SB0150/SB0150.06.ENRH.pdf, p.6.

[50] Center for Internet Security. (2021, May). *CIS Critical Security Controls Version 8*. cissecurity.org/controls. p. 22.

[51] Ibid.

[52] Ibid.

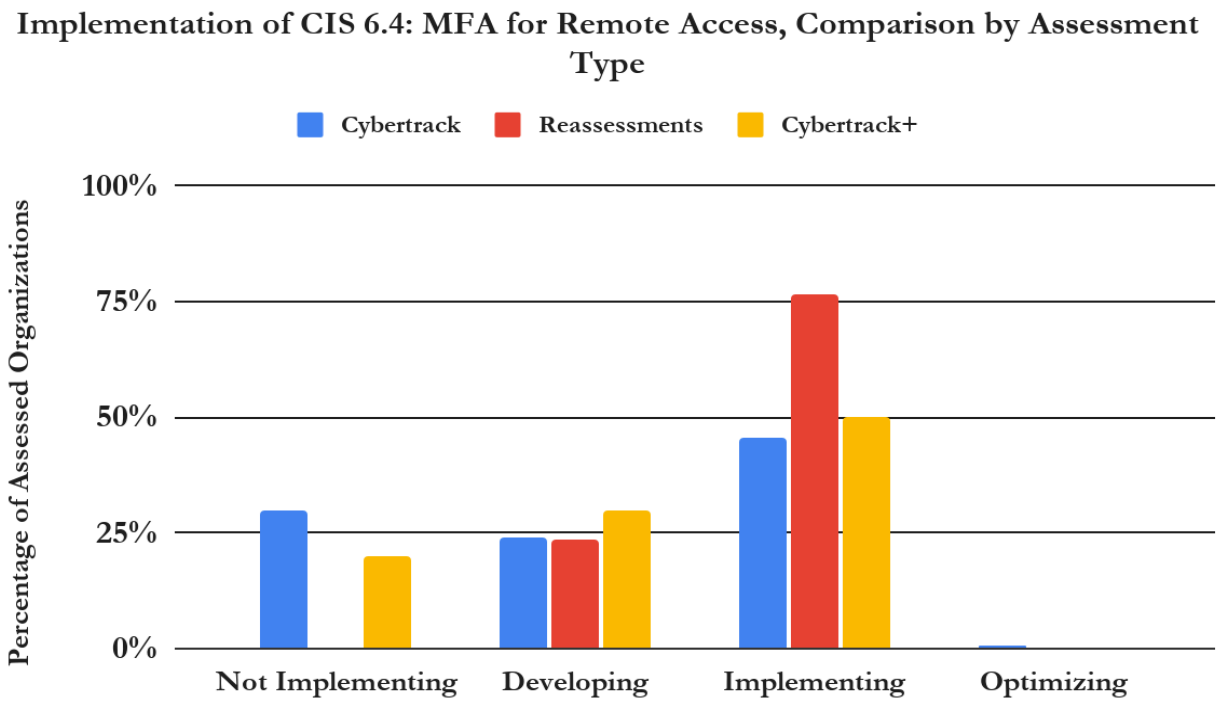
Figure 11 Distribution of Implementation Ratings for CIS Safeguard 6.3: Require MFA for Externally-Exposed Applications



We assessed Safeguard 6.4, "Require MFA for Remote Network Access," for 194 unique organizations assessed in the program so far. Close to half (47.9%) of all assessed organizations were implementing MFA for remote access. Slightly more that 24% of organizations were Developing MFA for remote access. Nearly thirty percent (27.3%) of assessed organizations were not implementing MFA for remote access. In sum, more than half (51.3%) of participating organizations were not fully implementing MFA on remote access at the time of assessment, but 72% (72.13%) of them had made at least some meaningful progress toward implementation, as shown in **Figure 12** below.

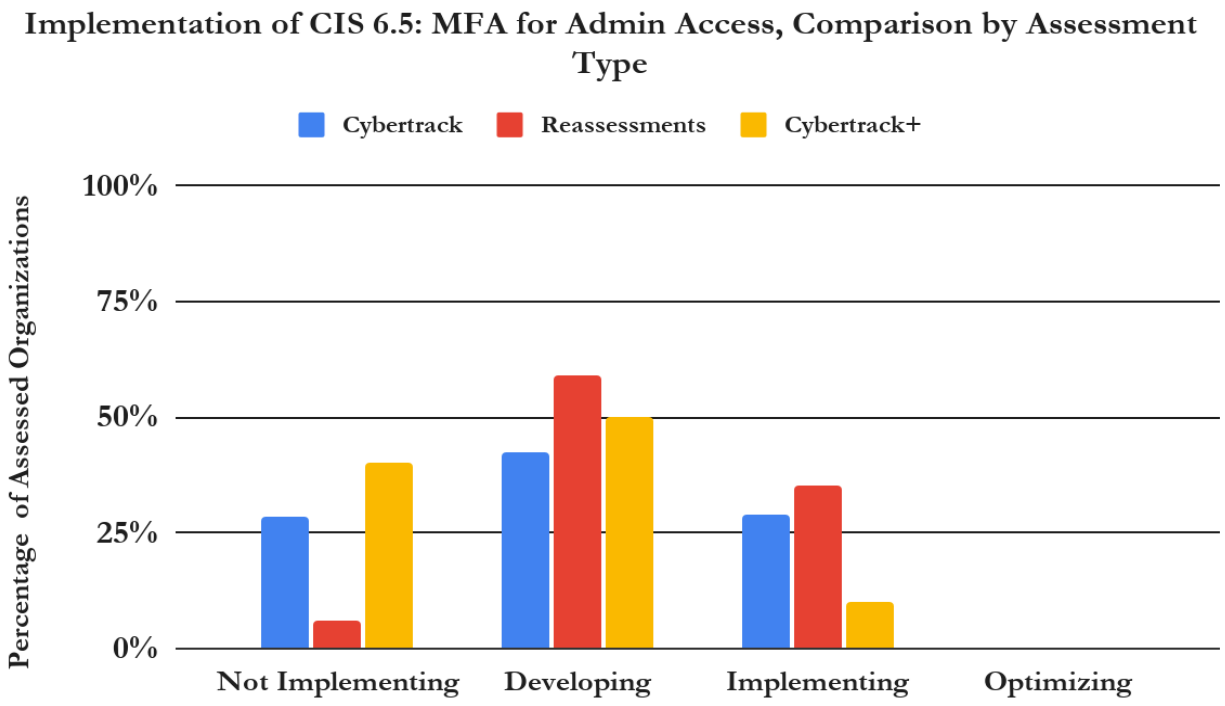
Once again, reassessed organizations were implementing MFA for remote access at a significantly higher rate, 76.5%, compared to all assessed organizations, the group of initial assessments (46.0%) and to the Cybertrack+ assessed organizations (50.0%). Most encouraging, all reassessed organizations so far have made progress toward implementing this Safeguard. Again, sample sizes for both first reassessments (n=20) and Cybertrack+ assessments (n=10) are small, but we are excited to see organizations embracing the use of MFA for remote access.

Figure 12: Distribution of Implementation Ratings for CIS Safeguard 6.4: Require MFA for Remote Network Access



Assessed organizations have been less successful in requiring MFA for administrative access to their systems. Less than thirty percent (27.6%) of unique, assessed organizations were implementing this Safeguard. Not quite 30% (28.6%) were not implementing MFA for administrative access. The percentage of reassessed organizations Implementing this Safeguard rises to 35.3%; reassessed organizations were Not Implementing this Safeguard at a significantly lower 5.9%. Relatively low implementation of MFA across all assessed organizations on accounts that have the most powerful access to organizational systems is very concerning, especially given the enormous power MFA has as a control to prevent unauthorized access and, therefore, prevent successful cybersecurity attacks. With that said, the significant progress made by reassessed organizations on Implementing this Safeguard is encouraging. **Figure 13** displays these results.

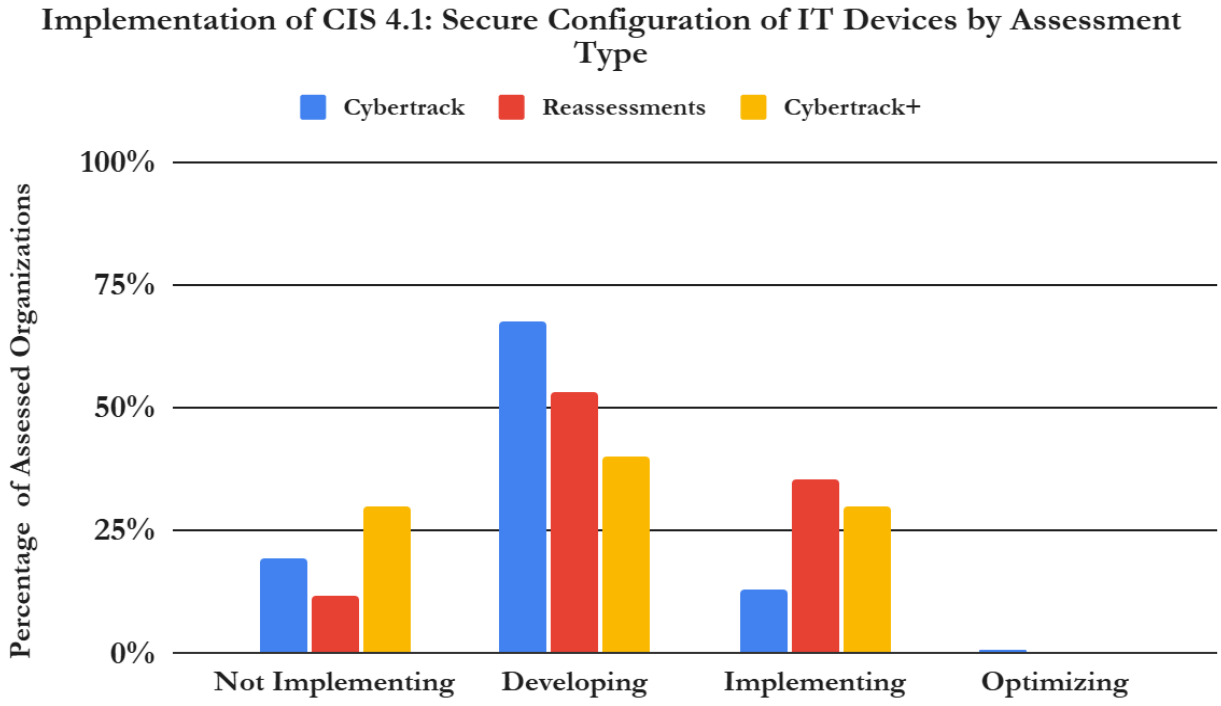
Figure 13: Distribution of Implementation Ratings for CIS Safeguard 6.5: Require MFA for Administrative Access



Like MFA, secure configuration also provides critical protections against unauthorized access. Organizations can limit unauthorized access by reducing vulnerable and unnecessary software packages and services as part of secure configuration processes for IT and OT assets as detailed in CIS Safeguard 4.1.[53] Of the five Control 4 Safeguards Cybertrack assesses, two (4.1 & 4.7) are members of the Transformative Twelve. However, three of the five, including a member of the Transformative Twelve (Safeguard 4.1), have very low levels of implementation across all assessed organizations (4.1: 16.4%, 4.2: 17.86%, 4.3: 11.2%). For each of these three Safeguards, the average number of points achieved falls below a Developing rating, which remains consistent with our June 2025 report. Again, reassessed organizations achieved a significantly greater degree of implementation on these three Safeguards (4.1: 35.29%, 4.2: 35.29%, 4.3: 29.41%) By fully implementing the five CIS Safeguards from Cybertrack assessments focused on secure configurations, organizations' devices will become far more resistant to cyber attacks. We highlight Safeguard 4.1 here because our evaluation produced very concerning results. We found this member of the Transformative Twelve was implemented in only 18.0% of unique assessed organizations. Most commonly (65.6%), assessed organizations received a Developing implementation rating on Safeguard 4.1, but 18.0% remained rated as Not Implementing. A stunning 83.6% of assessed organizations were not fully implementing Safeguard 4.1. **Figure 14** below represents assessed organizations' ratings on Safeguard 4.1 graphically.

[53] Center for Internet Security. (2021, May). *CIS Critical Security Controls Version 8*. cissecurity.org/controls. p. 16.

Figure 14: Implementation Rating Distribution for CIS Safeguard 4.1: Establish and Maintain a Secure Configuration Process.



Generally, low implementation ratings for Safeguard 4.1 are concerning because, lacking a process to ensure repeatability of strong asset configurations, organizations put substantially less secure devices into operation. These devices are unnecessarily vulnerable to cyber attacks. Weaknesses in device configuration can, for example, allow users to install vulnerable or malicious software or remove protective software, which may create additional vulnerabilities that allow devices to be compromised.

Consistently low ratings for Safeguards related to software inventory and control (CIS Control 2), log management (CIS Control 8), vulnerability management (CIS Control 7), and cybersecurity incident response (CIS Control 17) over the course of the Cybertrack program indicate that assessed organizations struggle hardest to implement them. Assessed organizations had the lowest incidence of employing controls focused on creating vulnerability management processes (Safeguard 7.1), log management (Safeguard 8.1), and incident reporting (Safeguard 17.3) programs, as well as conducting incident response exercises (Safeguard 17.7).

The Cybertrack Team assesses three CIS Safeguards in Control 2: Safeguard 2.1, "Establish and Maintain a Software Inventory,"[54] Safeguard 2.2, "Ensure Authorized Software is Currently Supported,"[55] and Safeguard 2.3, "Address Unauthorized Software,"[56] another member of the Transformative Twelve. The mean Implementation Rating scores for these three controls across all,

[54] Center for Internet Security. (2021, May). *CIS Critical Security Controls Version 8*. cissecurity.org/controls. p. 12.
[55] Ibid.
[56] Ibid.

unique assessments were 0.71 points, 0.59 points, and 0.74 points, respectively, indicating that few assessed organizations have started developing implementations related to these Safeguards. These three Safeguards are all characterized by high percentages of Not Implementing ratings among assessed organizations.

Though means increased on Control 2 Safeguards in each of our reporting periods since our November 2023 sample, results remained nearly identical since June 2024, which is concerning. For each of the 216 organizations, we assessed and rated three Control 2 Safeguards (2.1, 2.2, & 2.3, as shown in **Figures 15, 16, and 17** below). Across all organizations and each of these three Safeguards, a total of 648 ratings, only 44 Implementing were earned (6.8%). One was Optimizing. Of the assessed Safeguards, those in the Control 2 family remain the second least implemented by percentage, behind the Control 17 family (Incident Response & Management).

Reassessed organizations again were implementing the Safeguards evaluated in Control 2 to a greater degree than in organizations' initial Cybertrack assessments and Cybertrack+ assessments. Of the 44 Implementing ratings achieved across Safeguards 2.1, 2.2, and 2.3, 11 (25.0%) were achieved in the 20 reassessments. That is, one quarter of the achieved Implementing ratings were achieved by the small number of reassessed organizations. Furthermore, nine of the 11 Implementing ratings achieved on reassessment were rated Developing on the organization's initial assessment. This result is a powerful, specific case of organizations receiving Cybertrack recommendations, applying resources based on those recommendations, and taking action to make cybersecurity progress on critical Safeguards. As noted in Section 3.2: Results from First Reassessments, progress made by reassessed organizations on Safeguard 2.3 moved it out from among the seven Safeguards with the lowest average points per Safeguard. While this statistic reinforces that reassessed organizations are making substantial progress on the Safeguards we assess, the degree to which Control 2 Safeguards are being implemented remains dangerously low.

Most critically, only 17 (7.8%) of all assessed organizations we've assessed so far have implemented Safeguard 2.3, a member of the Transformative Twelve that requires organizations to ensure the removal of or documentation of exceptions for all unauthorized software.[57] Failure to implement CIS 2.3 can lead directly and quickly to serious cyber incidents. Organizations should make the implementation of this Safeguard a top technical priority in their cybersecurity programs.

[57] Ibid.

Figure 15: Implementation Rating Distribution for CIS Safeguard 2.1, Software Inventory.

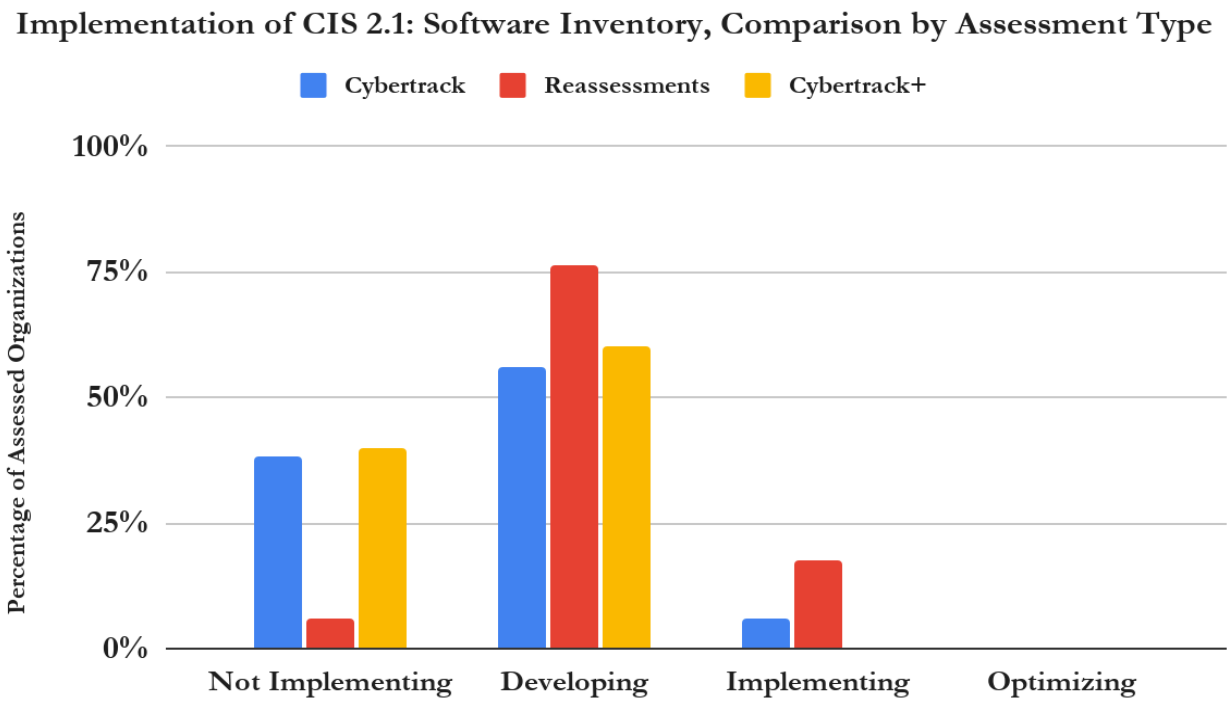


Figure 16: Implementation Rating Distribution for CIS Safeguard 2.2, Ensure Authorized Software is Supported.

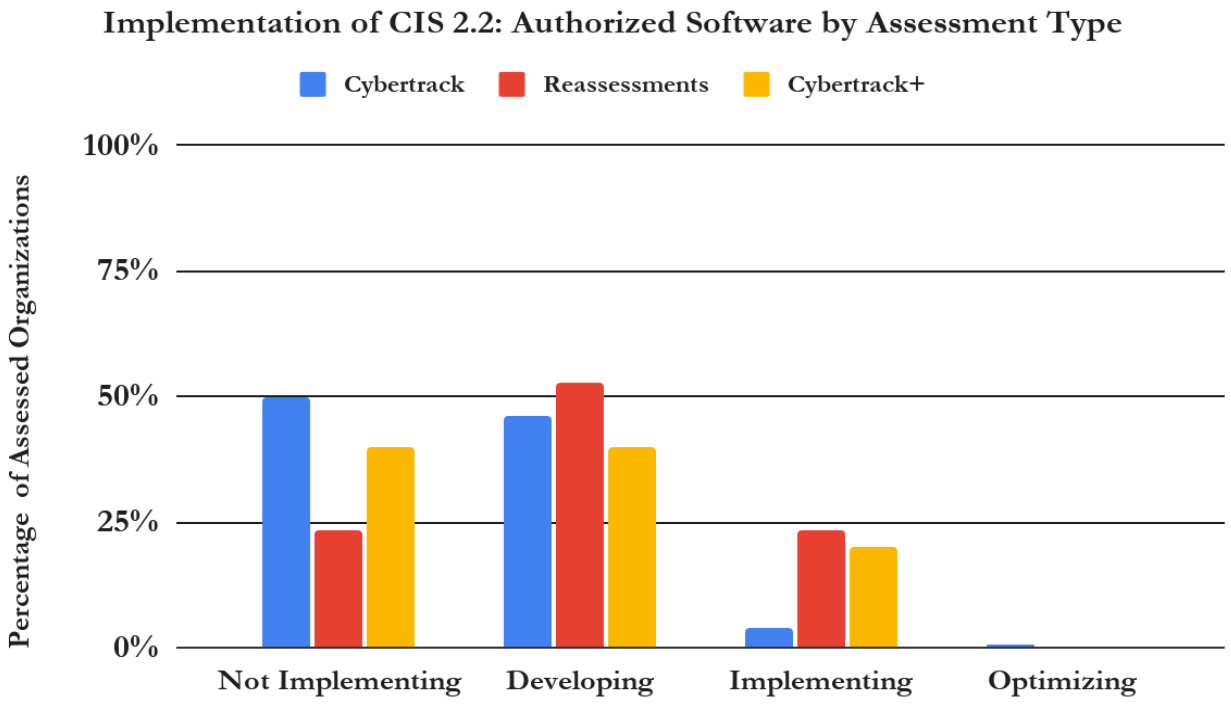
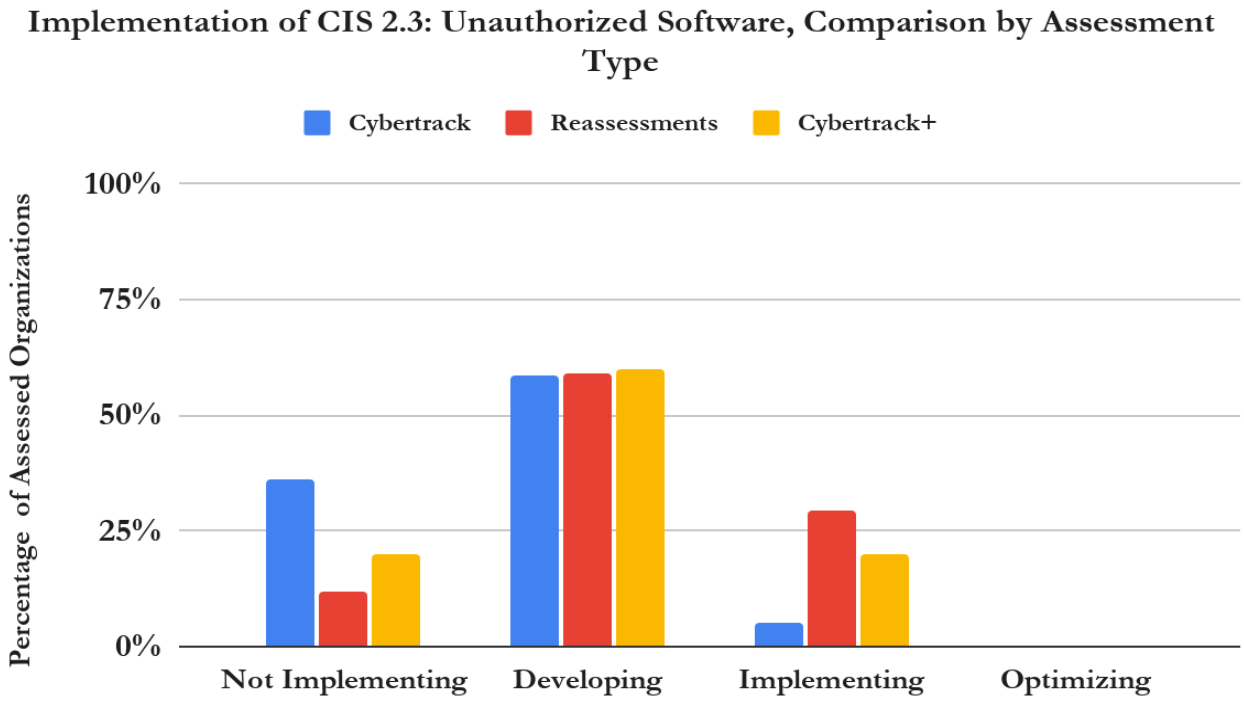


Figure 17: Implementation Rating Distribution for CIS Safeguard 2.3, Address Unauthorized Software.



Since our June 2024 report, we noted that all three of these Safeguards ranked near the bottom of the assessed Safeguards by mean score. Like the CIS Safeguards 10.1 and 10.2 discussed above, Safeguards 2.1, 2.2, and 2.3 also impact an organization's ability to prevent system compromises. When unauthorized software is installed or when authorized software is not properly maintained, software retains vulnerabilities on computers and networks that facilitate cybersecurity attacks. Though we are heartened by the progress being made among reassessed organizations, our results and analysis make clear that there is much work to be done to adequately protect Indiana's critical infrastructure from cyber attack.

4.4 Correlations

In our first Aggregate Results & Analysis Report in November 2023, we presented two correlations that stood out to us based on our first 23 assessments. First, we found the **total assessed score on Trusted CI Musts to be significantly positively correlated with total scores on CIS Safeguards**. Second, we found that **having experienced a cybersecurity incident in the past three years was significantly positively correlated with the total assessed score**. In our work since that report, those correlations continue to hold (although their characteristics have changed). Additional correlation also became evident as our sample size grew. These correlations are discussed below.

Our analysis continues to show that an organization's total score on assessed Trusted CI Musts is significantly positively correlated to its total score on assessed CIS Safeguards. That is, where

organizations received higher total scores on Trusted CI Musts, those organizations generally received correspondingly higher scores on CIS Safeguards and vice versa (α=0.05, $p<0.0001$, r^2=0.58). With data from an additional 194 assessments, this correlation remained explanatory with little change since our June 2025 report. As we assess a larger number of organizations, our confidence in this correlation continues to increase. That is, it is more likely to be describing an actual causal relationship. Among the Musts, all were significantly correlated (α=0.05, $p<.0001$) with an organization's total score on assessed CIS Safeguards. Their explanatory power (r^2) varied in a narrow range between 0.20 (Must 5 - Leadership) and 0.30 (Must 7 - Cybersecurity Lead). These statistics indicate the power (if not necessity) of these organizational fundamentals in enabling the implementation of the more tactical, more technical controls that are frequently the focus of cybersecurity standards. **Once again, this correlation supports the claim that organizations cannot successfully put the technical cart before the organizational horse, and these correlations continue to support this argument. Finally, this evidence suggests that local public sector organizations in Indiana will continue to struggle to implement even the most fundamental cybersecurity Safeguards until they address organizational and governance challenges.**

In addition to investigating individual Musts & Safeguards and groupings of Musts & Safeguards for correlations to assessment scores, we also evaluated demographic data for statistical significance of correlation to total assessment scores. We analyzed the following data for these analyses against the total score of assessment ratings.

- Total population (as reported by the United States Census Bureau)[58]
- Total annual spending (as reported in public filings)[59]
- Use of state cybersecurity resources (self-reported, WDR Wrap-Up Q9)
- Type of organization (city, town, county, etc.) (self-reported, verified through the United States Census Bureau)[60]
- Number of users (self-reported, WDR Wrap-Up Q6)
- Number of IT personnel employed (self-reported, WDR Wrap-Up Q7)
- Number of IT endpoints (self-reported, WDR Wrap-Up Q8)
- Whether the organization experienced a cybersecurity incident in the past three years (self-reported, WDR Wrap-Up Q4)
- Whether organizations partner with other organizations by sharing information technology and cybersecurity resources (*e.g.*, a city and county working together on technology)
- Cybersecurity strengths and weaknesses (self-reported, WDR Wrap-Up Q2 & 3, respectively)

In our previous reports, we noted that a prior cybersecurity incident (self-reported via WDR Wrap-Up Q4) was significantly correlated with higher assessment ratings scores. Consistent with our findings in the November 2023 and June 2024 reports, organizations that reported experiencing a cybersecurity incident in the past three years continue to implement more of the Musts & Safeguards we assess. Using an ANOVA test, prior incidents were significant predictors of the total score (α=0.05, p=0.02, r^2=0.03). Since our June 2025 report, the explanatory power of this correlation (r^2)

[58] https://www2.census.gov/programs-surveys/popest/tables/.
[59] https://gateway.ifionline.org/report_builder/.
[60] https://www2.census.gov/programs-surveys/popest/tables/.

fell from 0.06 to 0.03, continuing to fall from 0.12 in our June 2024 report. We do not have data that point to a particular reason why experiencing a cybersecurity incident in the three years preceding a Cybertrack assessment explains higher total ratings scores to a lesser degree than it did in our previous analyses. Reasons may include a general rise in awareness of cybersecurity risk among our target population or a change in state law requiring Indiana's public sector organizations to undertake cybersecurity assessment. For example, more organizations that have not experienced an incident may be driven to participate in a Cybertrack assessment because the law now requires assessment. With that said, this result continues to support an anecdotally common assertion across the cybersecurity community: many organizations find ways to invest in cybersecurity only after the organization itself experiences an incident, even in the face of evidence that similar organizations are falling victim.

In the previous year, we found that assessed organizations' use of IOT-sponsored tools (self-reported via WDR Wrap-Up Q9) correlated significantly with higher assessment ratings (α=0.05, $p<0.0001$, r^2=0.08). This is the first time this correlation has been statistically significant. We also ask organizations to list the IOT-sponsored services they use. Of the 128 assessed organizations that told us they were using these services, they listed: KnowBe4 (78), CrowdStrike (51), Udemy (27), and website hosting (26) most frequently. The significance of this correlation supports the claim that IOT-sponsored tools are making a measurable impact on cybersecurity in the organizations that implement them.

In our previous report, we observed that organizations that partnered with others by sharing cybersecurity resources tended to have higher total scores on Cybertrack assessments than individual organizations. Examples of these partnerships include counties sharing IT and cybersecurity resources with other counties or with municipalities within their borders, or municipalities sharing resources with their local K-12 school district. In these cases, organizations consolidated their IT resources to such an extent that only a single IT resource pool existed. When assessed, we were able to assess them as a single organization. Upon further investigation, we noted that half of the organizations scoring in the top 10% of total scores on Cybertrack assessments were partnered organizations. While this observation continues to be true, we have not assessed another partnered organization since. Therefore, we have not yet assessed enough partnered organizations to be confident that the correlation between partnership and total score is causal but will continue to track this trend in the data.

5 Conclusion and Impact

Since this program's beginnings in 2023, the Cybertrack team has worked to make Indiana more secure, a primary goal of this program. In April 2026, the Cybertrack program hit a milestone when we delivered our 200th Cybertrack assessment report. Today, more than 200 Indiana public sector organizations including counties, municipalities, K-12 schools, libraries, and utilities have received the most powerful, most practical, most doable cybersecurity advice from leading cybersecurity experts.

Results from first-time Cybertrack assessments have remained largely consistent since our first Aggregate Results & Analysis Report in November of 2023. Data continue to show that, in general, organizations averaged a Developing implementation rating. More granular trends in assessment

results have also remained consistent over the lifespan of the program including: most commonly implemented Musts & Safeguards, least implemented Musts & Safeguards, and most commonly cited barriers to progress. As our sample size of Cybertrack assessments continues to grow, we can characterize local public sector organizations with increasing confidence as struggling to implement the most fundamental cybersecurity controls.

Results from reassessments of the same local public sector organizations show positive trends that provide local public sector organizations with a path to improve cybersecurity. Cybersecurity gains shown in reassessments show that these organizations are making strong progress on cybersecurity, although progress varied significantly on individual reassessments. Nearly fifty-eight percent of the ratings points gained in reassessment were achieved through actions taken by these organizations in response to recommendations provided on their initial Cybertrack assessment. Notably, one reassessed organization that increased or refined its implementation of evaluated Musts & Safeguards by 40 points, tripling its ratings score in reassessment! In this case, free response data from the organization's reassessment questionnaire combined with these ratings data illustrate the power to make exceptional progress on cybersecurity when leadership, resources, and expert guidance are aligned and brought to bear. Though our sample size of first reassessments is relatively small, this progress is quite encouraging.

Since June 2025, we have implemented the Cybertrack+ assessment, which enhances our ability to evaluate cybersecurity in local public sector organizations in critical environments that are OT reliant, including water and wastewater facilities. Though the sample size of Cybertrack+ assessments does not yet support definitive analysis, our results so far exhibit trends similar to our initial Cybertrack assessments. Like other local organizations, the organizations supporting Indiana's OT-reliant, critical infrastructure also struggle to: 1) build awareness among organizational leadership of cybersecurity risk in support of implementing basic governance and risk management practices, 2) implement even the most fundamental, powerful cybersecurity controls, and 3) apply sufficient knowledge and effort to do so. These trends are especially concerning among OT-reliant environments because of the criticality of the services that they provide (*e.g.* delivering water, removing wastewater, providing electricity) and the increased likelihood of direct, real-world impacts resulting from a successful cyber attack.

Another of Cybertrack's primary goals is to inform Indiana's local government cybersecurity policy and strategy. This report, along with our quarterly reports, supports that goal. Considering Cybertrack only assesses cybersecurity practices that are known to be among the most powerful, the results of these 216 assessments continue to illustrate that Indiana's local public sector organizations have a long way to go in basic cybersecurity capability. Based on notable trends from Cybertrack+ assessments, Indiana's OT-reliant critical infrastructure organizations face very similar key challenges They most certainly continue to need help. The results highlight the following specific needs, which are quite similar to the recommendations we delivered in our previous reports. The additional data we gathered and analyzed continues to reinforce those recommendations and illustrate paths forward toward improved cybersecurity in local public sector organizations.

Our analysis continues to support our three calls to action, which have remained consistent since our November 2023 report. Data from Cybertrack+ assessments and Cybertrack reassessments since June 2025 indicate that these three actions are critical to increasing cybersecurity across the

population of local public sector organizations including OT-reliant environments. The community should act to:

A. **Increase leadership involvement in cybersecurity and implement basic governance and decision making practices.** In only about half of the assessed organizations, organizational leadership is involved in cybersecurity decision making (Must 5). Though assessed organizations implemented Must 5 at the highest rate of the Musts we assessed (a cause for optimism), much more leadership involvement is needed. Based on the 45% of assessed organizations who are Developing or Not Implementing on this Must, we are hopeful that more organizations' leaders will become involved in cybersecurity decision making and soon. As leadership becomes more involved in organizational cybersecurity, our early analysis suggests that they should focus on building a cybersecurity-specific budget (Must 12), assigning people to cybersecurity tasks (Must 7 and Must 13), and adopting a baseline cybersecurity control set to gauge cybersecurity posture, find gaps, and monitor progress (Must 15). These are actions that all local public sector organizations can and should take, regardless of their size and resourcing. Statistically significant correlations in our results validate a common sense conclusion: basic organizational practices (leadership involvement, governance, communication, documentation) provide a basis for sound, intentional prioritization of cybersecurity investment. Indiana local public sector organizations should prioritize these organizational fundamentals. They are necessary to support sound decision making and cybersecurity investment. They are particularly important when resources are scarce.

B. **Address the most glaring gaps in evidence-based control implementation.** Our results continue to show that most Indiana local public sector organizations are struggling to implement even the most fundamental, powerful cybersecurity controls. Our research narrowed the 153 CIS Safeguards down to a list of 27 (IT-focused environments) and 40 (OT-reliant environments), including 12 of the most empirically-proven as powerful in IT focused environments and 30 in OT-reliant environments like utilities. Investing in these Safeguards, certainly to include the Transformative Twelve and Sturdy 30 discussed in Section 2.1 (Assessment Methodology), will lead to significant reductions in organizations' cybersecurity risk exposure. Moreover, Cybertrack's assessment data present three CIS control families in which increased effort would likely most significantly improve local public sector organizations' cybersecurity postures:

    - Growing evidence supports the particular power of secure configurations (CIS Control 4). Of the five Control 4 Safeguards we assess, two (4.1 & 4.7) are members of the Transformative Twelve. However, three of the five, including a member of the Transformative Twelve, have very low levels of implementation (4.1: 16.4%, 4.2: 17.86%, 4.3: 11.2%). By fully implementing the five CIS Safeguards from Cybertrack assessments focused on secure configurations, organizations' devices will become far more resistant to cyber attack.
    - All evidence-based sources we've found indicate that MFA (CIS Control 6) is one of, if not the most, effective cybersecurity controls available to defenders.[61] MFA is highly effective at preventing and disrupting attacks by reducing an attacker's ability

[61] *See, e.g.*, https://arxiv.org/abs/2305.00945.

to gain unauthorized access to a user account. Safeguards 6.3, 6.4, and 6.5 are all members of the Transformative Twelve. Fully implementing these three Safeguards should be among the community's very top priorities.

- Results from "Inventory and Control of Software Assets" (CIS Control 2) Safeguards provide a particularly extreme example of organizations' struggles to implement cybersecurity controls. Only 26 of 216 (12.0%) assessed organizations received an Implementing rating on Safeguards 2.1, 2.2, or 2.3 (Safeguard 2.3 is the Control 2 member of the Transformative Twelve). Of the 26 organizations receiving an Implementing on Safeguards 2.1, 2.2, *or* 2.3, six achieved this rating only on reassessments. Respectively, 35%, 48%, and 33% of assessed organizations were Not Implementing these three Safeguards. Organizations have particularly significant opportunities to improve cybersecurity by implementing Safeguards 2.1, 2.2, and 2.3 because of the importance of properly managing software.. With that said, the rating distribution of these Safeguards is representative of several Safeguards we assessed.

C. **Address the expertise and effort gap.** Program participants most frequently cited insufficient availability of cybersecurity-knowledgeable personnel as a weakness or barrier to advancing their cybersecurity.[62] There are multiple ways to tackle this problem, including training existing staff, hiring new staff, engaging private sector firms, and further developing and engaging public sector / public interest resources available through, for example, the state's public universities, the Indiana Office of Technology, the State and Local Cybersecurity Grant Program committee, CIS, and CISA, and each other. Intentional expansion, coordination, and vetting of these approaches and resources is necessary. We noted a statistical trend in Cybertrack data that local organizations that have partnered their cybersecurity resources perform significantly better on Cybertrack assessments compared with those that do not. Though this correlation reflects the results of a small number of assessed organizations, it does support the need to address the expertise and effort gap. Based on the current state of cybersecurity postures of the local public sector organizations we've assessed as well as on the feedback we've received from Cybertrack participants, all of these approaches and resources are likely to be needed. Collaboration and coordination among, as well as vetting of, these resources is needed. The Cybertrack Team and our institutions are expanding our efforts and stand ready to provide additional support. Current federal policy means that—more than ever—Indiana needs to rally its own resources to turn the corner on cybersecurity.[63]

March 2025 marked the two year mark since Cybertrack assessed its first cohort of local public sectors. Since that time, we've been performing Cybertrack's first reassessments on our pilot and early adopting organizations. Data from first reassessments of some of our earliest adopters show the direct impacts that Cybertrack's assessments and guidance have made on cybersecurity in these organizations. Reassessed organizations have averaged a 7.5 point ratings increase, which excludes

[62] Moreover, the second most frequently cited barrier had to do with lack of documentation of the policies and processes that support a competent, resilient cybersecurity program. [This latter barrier is a result (at least in part) of the former. It takes effort and expertise to develop these programmatic tools.]

[63] *See* https://www.whitehouse.gov/presidential-actions/2025/03/achieving-efficiency-through-state-and-local-preparedness/ "Federal policy must rightly recognize that **preparedness is most effectively owned and managed at the State, local, and even individual levels**, supported by a competent, accessible, and efficient Federal Government."

one organization's 40-point ratings increase! These cybersecurity gains are impressive and demonstrate the effectiveness of Cybertrack's focus on cybersecurity governance and programmatics to drive the implementation of technical Safeguards.

The Cybertrack team will continue publishing aggregate results reports like this one regularly. We will continue to focus on clarifying, detailing, and (where necessary) correcting our analysis of trends with additional data and analysis as the number in our sample set grows. As we do here for the first time, we'll also continue to report on the feedback we've received about the Cybertrack program and its impacts on the organizations we've assessed. Each participating organization still receives an optional **Feedback Questionnaire** with the delivery of its report and **Impact Questionnaires** at 6 months following the delivery of their assessment report and at 6-month intervals thereafter. Thus far, the responses are limited but inspiring. Highlights are summarized in **Appendix C**.

We welcome feedback on this report and ideas on how to maximize the value of future Cybertrack reporting to the community.

Appendix A: Musts & Safeguards Assessed

Trusted CI Framework Musts (assessing 6 of 16)

Must 5: Leadership
Organizations must **involve leadership** in cybersecurity decision making.
Must 7: Cybersecurity Lead
Organizations must establish a **lead role** with responsibility to advise and provide services to the organization on cybersecurity matters.
Must 9: Policy
Organizations must develop, adopt, explain, follow, enforce, and revise cybersecurity **policies**.
Must 12: Budget
Organizations must establish and maintain a **cybersecurity budget**.
Must 13: Personnel
Organizations must allocate **personnel** resources to cybersecurity.
Must 15: Baseline Control Set
Organizations must adopt and use a **baseline control set**.

CIS Safeguards (assessing 27 of 153, each from Implementation Group 1 unless otherwise noted)

CIS 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
CIS 2.1: Establish and Maintain a Software Inventory
CIS 2.2: Ensure Authorized Software is Currently Supported
CIS 2.3: Address Unauthorized Software ‡
CIS 3.3: Configure Data Access Control Lists ‡
CIS 3.4: Enforce Data Retention ‡
CIS 3.10: Encrypt Sensitive Data in Transit (IG2 & IG3)
CIS 3.11: Encrypt Sensitive Data at Rest (IG2 & IG3)
CIS 4.1: Establish and Maintain a Secure Configuration Process ‡
CIS 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure
CIS 4.3: Configure Automatic Session Locking on Enterprise Assets
CIS 4.6: Securely Manage Enterprise Assets and Software
CIS 4.7: Manage Default Accounts on Enterprise Assets and Software ‡
CIS 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts ‡
CIS 6.3: Require MFA for Externally-Exposed Applications ‡
CIS 6.4: Require MFA for Remote Network Access ‡
CIS 6.5: Require MFA for Administrative Access ‡
CIS 7.1: Establish and Maintain a Vulnerability Management Process
CIS 7.3: Automated Operating System Patch Management
CIS 8.1: Establish and Maintain an Audit Log Management Process
CIS 10.1: Deploy and Maintain Anti-Malware Software ‡
CIS 10.2: Configure Automatic Anti-Malware Signature Updates ‡
CIS 11.1: Establish and Maintain a Data Recovery Process
CIS 11.4: Establish and Maintain an Isolated Instance of Recovery Data ‡
CIS 13.3: Deploy a Network Intrusion Detection Solution (IG2 & IG3)
CIS 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents
CIS 17.7: Conduct Routine Incident Response Exercises (IG2 & IG3)

‡ In the Transformative Twelve. *See* Section 2.1 for a discussion.

Appendix B: Musts & Safeguards Assessed - Cybertrack+

Trusted CI Framework Musts (assessing 6 of 16)

Must 5: Leadership
Organizations must **involve leadership** in cybersecurity decision making.
Must 7: Cybersecurity Lead
Organizations must establish a **lead role** with responsibility to advise and provide services to the organization on cybersecurity matters.
Must 9: Policy
Organizations must develop, adopt, explain, follow, enforce, and revise cybersecurity **policies**.
Must 12: Budget
Organizations must establish and maintain a **cybersecurity budget**.
Must 13: Personnel
Organizations must allocate **personnel** resources to cybersecurity.
Must 15: Baseline Control Set
Organizations must adopt and use a **baseline control set**.

CIS Safeguards (assessing 40 of 153)

CIS 1.1: Establish and Maintain Detailed Enterprise Asset Inventory
CIS 2.1: Establish and Maintain a Software Inventory
CIS 2.2: Ensure Authorized Software is Currently Supported
CIS 2.3: Address Unauthorized Software ‡
CIS 3.3: Configure Data Access Control Lists ‡
CIS 3.4: Enforce Data Retention ‡
CIS 3.10: Encrypt Sensitive Data in Transit (IG2 & IG3)
CIS 3.11: Encrypt Sensitive Data at Rest (IG2 & IG3)
CIS 4.1: Establish and Maintain a Secure Configuration Process ‡
CIS 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure
CIS 4.3: Configure Automatic Session Locking on Enterprise Assets
CIS 4.6: Securely Manage Enterprise Assets and Software
CIS 4.7: Manage Default Accounts on Enterprise Assets and Software ‡
CIS 5.2: Use Unique Passwords ‡
CIS 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts ‡
CIS 6.3: Require MFA for Externally-Exposed Applications ‡
CIS 6.4: Require MFA for Remote Network Access ‡
CIS 6.5: Require MFA for Administrative Access ‡
CIS 6.8: Define and Maintain Role-Based Access Control ‡
CIS 7.1: Establish and Maintain a Vulnerability Management Process
CIS 7.2: Establish and Maintain a Remediation Process ‡
CIS 7.3: Automated Operating System Patch Management
CIS 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets ‡
CIS 7.7 Remediate Detected Vulnerabilities ‡
CIS 8.1: Establish and Maintain an Audit Log Management Process
CIS 10.1: Deploy and Maintain Anti-Malware Software ‡
CIS 10.2: Configure Automatic Anti-Malware Signature Updates ‡
CIS 11.1: Establish and Maintain a Data Recovery Process
CIS 11.4: Establish and Maintain an Isolated Instance of Recovery Data ‡
CIS 11.5: Test Data Recovery ‡
CIS 12.2: Establish and Maintain a Secure Network Architecture ‡
CIS 13.3: Deploy a Network Intrusion Detection Solution (IG2 & IG3)

CIS 13.4: Perform Traffic Filtering Between Network Segments ‡
CIS 13.5: Manage Access Control for Remote Assets ‡
CIS 13.6: Collect Network Traffic Flow Logs ‡
CIS 17.1: Designate Personnel to Manage Incident Handling ‡
CIS 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents
CIS 17.4: Establish and Maintain an Incident Response Process ‡
CIS 17.5 Assign Key Roles and Responsibilities (IN IR PLAN) ‡
CIS 17.7: Conduct Routine Incident Response Exercises (IG2 & IG3)

‡ In the Sturdy Thirty. *See* Section 2.1.3 for a discussion.

Appendix C: 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 organizations. 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.)	79 of 94 respondents selected "Yes." 15 respondents selected "No"
Senior Leadership Review. Has your organization's most senior leadership reviewed or been briefed on the Cybertrack assessment report?	74 of 94 selected "Yes." 20 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?	129 of 190 respondents selected "5 - Extremely Likely," 50 selected "4 - Likely," 9 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."	115 of 190 respondents selected "5 - Strongly Agree," 64 selected " 4 - Agree," 8 selected "3 - Undecided", 2 selected "2 - Disagree."[64], 1 selected "1 "Strongly Disagree"[65]

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

> "The process was easy, the discovery meeting was informative for both sides. The staff was nice and knowledgeable." - *Heartland Career Center, Wabash, IN*
>
> "I really appreciated the understanding from the team doing the questioning. They understood the constraints that we face as a school district." - *Dustin Shadbolt, Director of Technology*
>
> "At a time when money, time, and resources are increasingly difficult to come by for school corporations, the time spent on the CyberTrack assessment was well worth it. The report provides clear, actionable recommendations and serves as an effective tool for communicating cybersecurity needs to decision-makers. It helps raise awareness of where resources are needed to keep the school corporation secure in a rapidly changing threat landscape." *Byron Gerber Norwell Community Schools*
>
> "The Cybertrack assessment was valuable in terms of distilling our immediate cybersecurity needs. Additionally, it gave our internal team an outsider's recommendation of resources that should be allocated to provide a baseline of security for our organization." - *Joe Vought, Colby Koppelmann, Delphi Community School Corporation*
>
> "'Pleasure in the job puts perfection in the work.' - Aristotle It is quite obvious that the Cybertrack Team is passionate about what they do; they have been an absolute pleasure to work alongside during this whole process. The Team is not only very personable, but the knowledge they possess and support for their clients is unmatched. They are not only supportive but very professional in their work. I greatly recommend this Organization! Thank you Indiana Cybertrack!" - *Alexandrea Eckstein, Wastewater Superintendent*
>
> "In an era of tightening government budgets, it's very hard to beat the price of free; the Cybertrack program bringing free professional cybersecurity advice to our small town library is a game changer!" - *Robert Rensberger/Library Technician*

The following are selected quotes from previous quarters' responses:

[64] 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.
[65] The respondent felt the effort was not worth it because the value of the report was "downplayed" by leadership.

Previous Quarters' Responses
"Cybertrack enabled us to identify and address key vulnerabilities with measurable outcomes. The assessment provided targeted insights into high-priority areas and outlined actionable steps for improvement. These findings served as a compelling basis to justify additional funding, equipment, and personnel, further supported by recommendations from industry experts in our state. During the reassessment phase, we validated our progress and demonstrated substantial improvement from our original baseline. When approached with transparency and a commitment to follow through, this assessment will significantly elevate your cybersecurity posture." - *James Gerald, IT Director, City of Elkhart*
"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 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 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 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."

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."
"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."
"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*

Previous Quarters' Responses
"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."
"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."
"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."

Previous Quarters' Responses
"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)."
"The Cybertrack experience is well worth the time and effort! Thank you for providing the service to Indiana communities!"
"Well worth the effort (WDP, etc.) for the results."
"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. Great experience, specifically enjoyed the review process."
"A great experience and I learned a lot from the program."
"EACS values the input and the Cybertrack process, and Cybertrack has affirmed that we have made some strides, but also affirmed that we have some work to do."
"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."
"We've been happy to partner with Cybertrack to allow us to gain further traction with our constituents to show how the things we're doing are moving in a concise and intentional direction that is backed by industry standards."
"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."

Previous Quarters' Responses
"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."
"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."
"As a local emergency manager, this is one of the things that keeps me up at night. Our local hospital was hacked; a local high school was attacked, and we lose internet connection often. After working through the CyberTrack assessment process and the face-to-face conversation, I'm encouraged that CyberTrack is guiding us in the right direction to become as secure as we can. Thank you, CyberTrack, for making a very complex emergency seem more manageable."