# Cybertrack Report:
## Aggregate Results & Analysis from 76 Assessments (May 2023 - May 2024)

Indiana's Local Government Cybersecurity Assessment Program

June 2024

Joe Beckman, Purdue University cyberTAP
Craig Jackson, Indiana University Center for Applied Cybersecurity Research
Ranson Ricks, 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 government cybersecurity assessment program. Cybertrack is designed to put local governments in contact with top tier cybersecurity experts and provide them with **practical, prioritized advice about doable, powerful cybersecurity fundamentals.** Our goal is to make Indiana more secure in the short term and shape our collective cybersecurity strategy and policy for the long term. Cybertrack cybersecurity assessments are available for no fee to Indiana local government entities.

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 individual local government's 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 Craig Jackson, scjackso@iu.edu.

# Acknowledgements

The Cybertrack Team thanks the Indiana local governments 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 members Emily Adams, Mark Krenz, and Bob Cowles.

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 the IOT or any other organization.

# 1 Executive Summary

This report is the second report of aggregate assessment results and analysis from Cybertrack, Indiana's Local Government Cybersecurity Assessment Program. The program serves a diverse set of Indiana's local entities, including counties, cities, towns, K-12 school districts, and more. This report covers aggregated results from Cybertrack's first 76 of 342 planned assessments. The Cybertrack Program is ongoing, but these results offer some clear views into the current state of cybersecurity for Indiana's local government entities, and 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.

Considering Cybertrack only assesses cybersecurity practices known to be among the most powerful, these results are sobering and show that Indiana's local government entities have a long way to go in basic cybersecurity capability.[1] They most certainly need help. The results of 76 assessments highlight that these organizations and the supporting community need to:

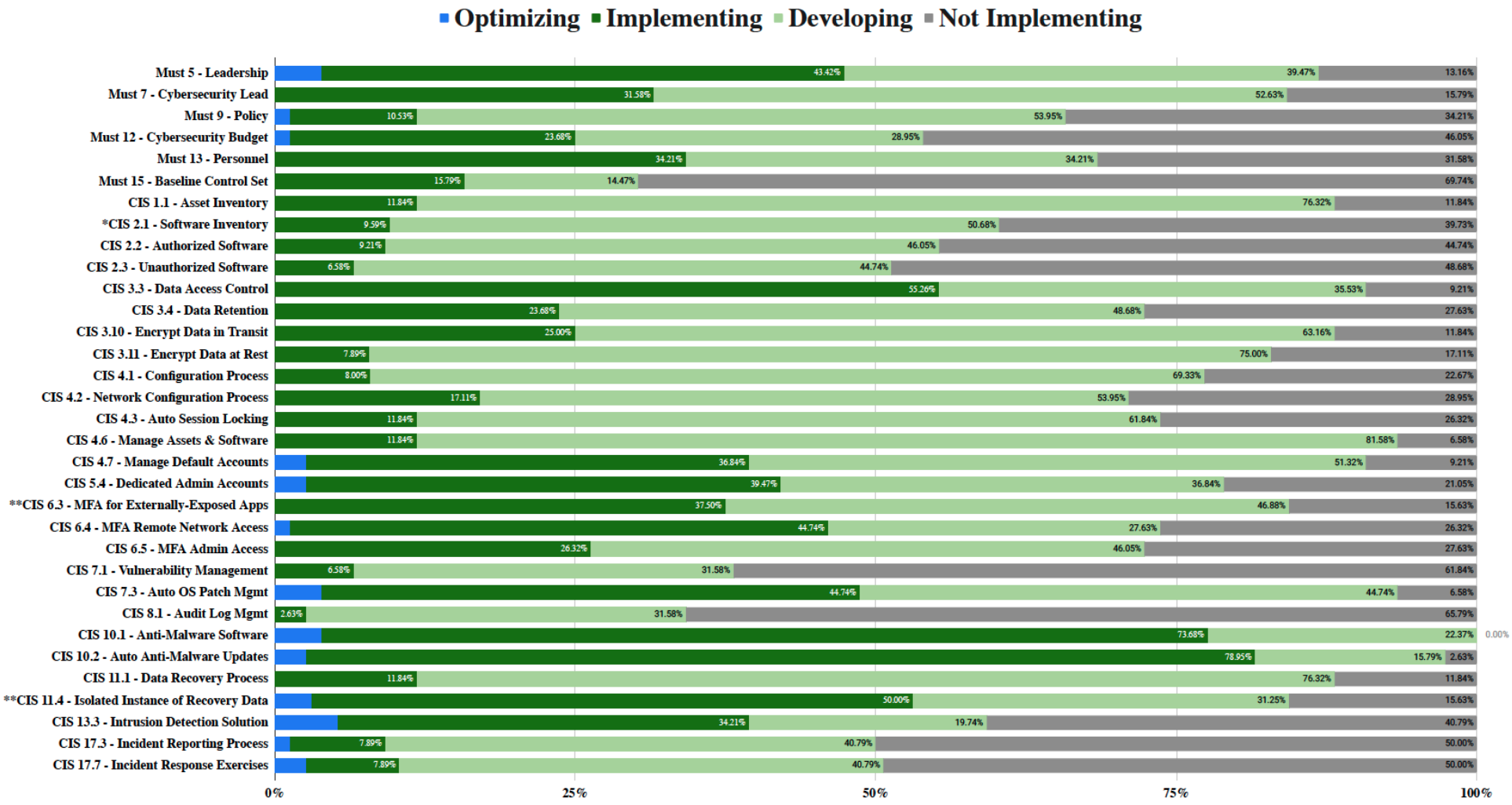
A. **Increase leadership involvement and implement basic governance and decision making practices.** Our results show that entities with more functional cybersecurity programs, as assessed by Trusted CI Musts, are more successfully addressing the CIS Safeguards we assessed. Aggregate results on many 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 entities 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 entities 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 entities 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). Intentional expansion, coordination, and vetting of these approaches and resources is necessary.

We also see reason for optimism. We've 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 stand ready to expand our efforts.

**Roadmap for the report.** Section 2 (Methodology) describes the Cybertrack assessment methodology, including what we assess, why we assess it, and how we assess it, as well as 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] see Figures 1 & 2 below, as well as Figure 4 on p. 14

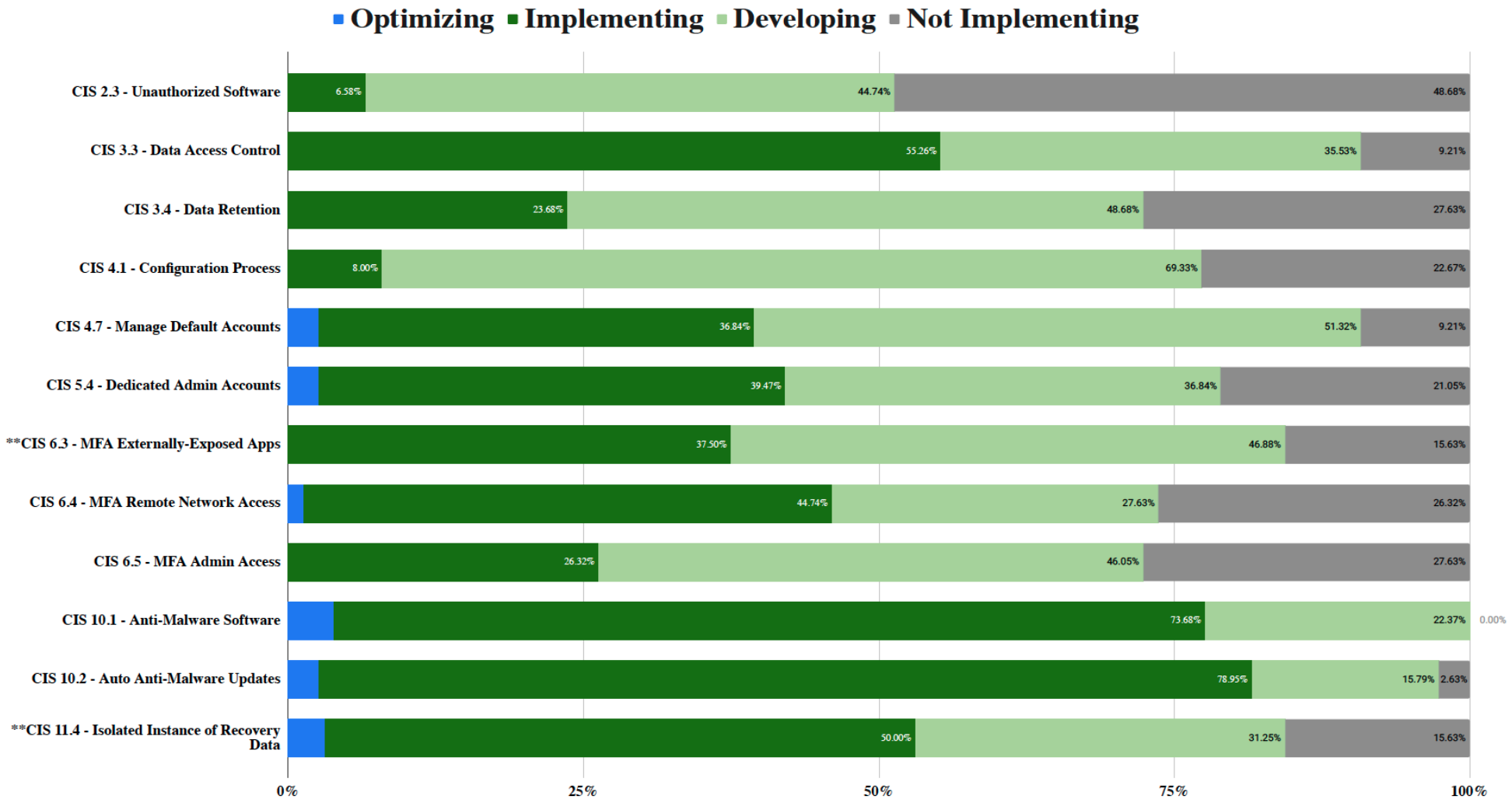
**Figure 1.** Distribution of Implementation Ratings




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

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

**Figure 2.** Distribution of Implementation Ratings for Cybertrack Assessments (Transformative Twelve)




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

# 2 Methodology

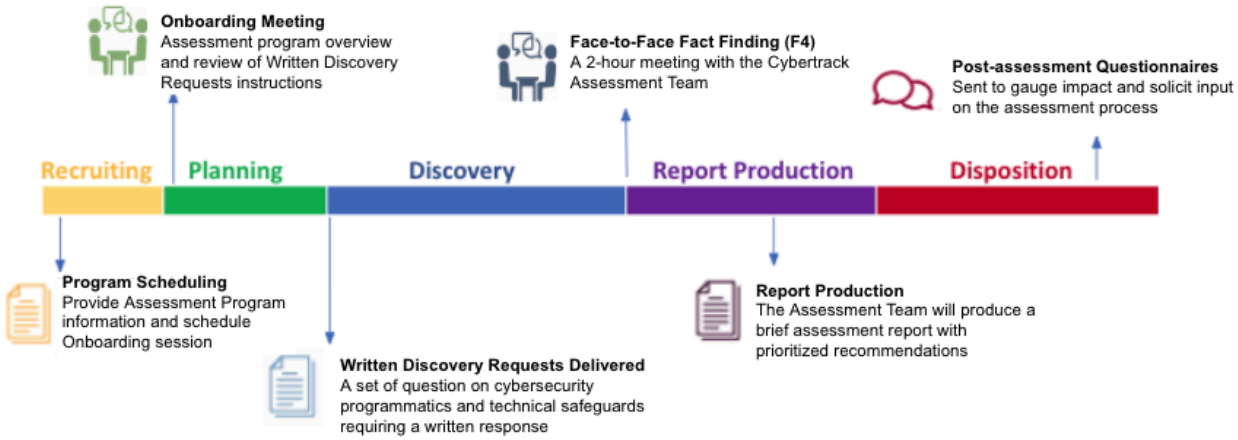
This section describes the Cybertrack assessment methodology, including what we assess, why and how we assess it, and how we aggregated and analyzed the data from those assessments.

## 2.1 Assessment Methodology

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 local government entities. The 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 local government entities prioritize the most doable, impactful actions and 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 local government entities attend an Onboarding Meeting where Cybertrack Team members explain the assessment process and where local government personnel can ask questions. After the Onboarding Meeting, the local government identifies the local government 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 local government entity (*e.g.*, type, population, number of endpoints).

**Figure 3.** Cybertrack Assessment Phases




[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 (including Jackson), and is based heavily on more than dozen prior assessments for the NSF Cybersecurity Center of Excellence and the US Navy, and has been successfully used in a wide range of environments. For more about PACT, *see* https://cacr.iu.edu/pact/index.html.

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 government invitees). The F4 is a 2-hour meeting designed to clarify relevant facts and help the Assessment Team identify and tailor the recommendations that 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 emphasize individual local government's cybersecurity strategies, with a particular focus on short-term priorities.

After the report is delivered and time is allowed for the local government to review and consider the report, the Cybertrack Team follows up with post-assessment questionnaires 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 local government's 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 alignment to federal grant programs, mapped to, and ultimately selected primarily from Implementation Group 1 of the CIS Controls v8.[6] The Musts and Safeguards covered in this assessment are listed in **Appendix A**.

The **Trusted CI Framework** is a minimum standard for cybersecurity programs, developed by IU CACR personnel for Trusted CI, the NSF Cybersecurity Center of Excellence. The Trusted CI Framework matches 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 basic 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

[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.
[6] https://www.cisecurity.org/controls.

'must-do, do-first' starting point for every enterprise seeking to improve their cyber defense."[7] 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 government entities. 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)**[8] is a set of 56 Safeguards that "represents a minimum standard of information security for all enterprises"[9] 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. We found three studies that qualified: (a) the CIS Community Defense Model v2.0[10]; (b) the Microsoft Digital Defense Report[11]; and (c) the Australian Signals Directorate's Essential Eight.[12] 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.

This research resulted in a top-scoring group of 12 IG1 Safeguards. We validated this **"Transformative Twelve"** via independent IU and Purdue subject matter expert analysis and confirmed the very high presence of these Safeguards in other standards (*e.g.*, NIST's), compared to the results of a recent NC State University study[13] that followed a similar methodology to the CIS Community Defense Model v2.0 and ultimately conducted a detailed reanalysis[14].

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.[15]

---

[7] https://www.cisecurity.org/controls/cis-controls-faq.
[8] https://www.cisecurity.org/controls/implementation-groups/ig1.
[9] https://www.cisecurity.org/insights/white-papers/establishing-essential-cyber-hygiene.
[10] https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0.
[11] 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.
[12] https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight.
[13] * "An investigation of security controls and MITRE ATT&CK techniques," Md Rayhanur Rahman & Laurie Williams, 1 Nov 2022, arXiv:2211.06500v1, available at https://arxiv.org/pdf/2211.06500.pdf.
[14] This reanalysis resulted in two Safeguards (6.3 and 11.4) joining the top-scoring group.
[15] For more discussion of the Transformative Twelve and Trusted CI Framework, *see* https://www.lawfaremedia.org/article/the-difficulties-of-defining-secure-by-design

**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 governments, 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 an additional handful of Safeguards that map to "cybersecurity best practices" emphasized in the federal State and Local Cybersecurity Grant Program,[16] but not already included via our research. All said, Cybertrack is assessing 27 of CIS's 153 Safeguards, including 23 of IG1's 56.

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

> **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.

[16] https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program.

**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.

## 2.2 Approach to Data Analysis

Data collected for analysis are taken from completed WDRs, final implementation ratings for each Must and Safeguard for each assessed entity, 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, entity type, municipal spending information) were used directly in the analysis. Most of the data used, including those from WDRs and assessment ratings, were coded to facilitate our analysis. Our analysis relied heavily on assessment teams' assessment ratings, which were coded as shown in the table below.

**Table 2**: 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.[17] These metrics included intermediary aggregate scores for both the assessed Trusted CI Musts and the assessed CIS Safeguards and, ultimately, an overall assessment rating score for each entity for both the Musts and the Safeguards.

We began our analysis by generating basic descriptive statistics (mean and variance) for each implementation rating across all entities. The team also generated a bar graph for each Must and Safeguard that showed the percentage of entities that achieved each implementation rating. We performed basic statistical comparisons. The team validated calculations and results by having a second team member validate the formulae used in calculations. We performed more advanced statistical comparisons, such as regression and analysis of variance (ANOVA) analyses, using SAS version 9.4.

To derive results and analyze the local government 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 were checked by the analyst entering the data, then re-checked by another member of the team before the analysis began. The Cybertrack analysis team broke various statements into the individual elements related to the question being answered, and then grouped into categories with similar responses. We then analyzed these categorized data. The results of those analyses are shown in this report.

# 3 Results

This section provides an overview of the aggregated assessment results of the first 76 local government entities to participate in the Cybertrack program. We begin by refining the basic characteristics of the local government population and sample-to-date [Table 3] discussed in our first report[18]released in November 2023 and again summarize the aggregated results of the implementation ratings across the Musts and Safeguards we assess [Figures 1 & 2] in the context of our larger sample size of assessed entities.

According to the 2022 United States Public Sector Annual Survey and Census of Governments,[19] 2,649 local government entities exist in the State of Indiana. These entities include: "counties, cities, townships, special districts (such as water districts, fire districts, library districts, mosquito abatement districts, and so on), and school districts."[20] Of these, 1,662 are general purpose governments (eg. counties, cities, and other municipalities)[21] that served as the primary governing entity. The remaining 987 local governmental entities include K-12 school districts and special service

[17] We do not provide numerical scores to assessed entities 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 and 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.
[18] https://incybertrack.org/media/cfkas1cv/cybertrack-aggregate-results-report-november2023.pdf
[19] https://data.census.gov/table/GOVSTIMESERIES.CG00ORG01?q=local+governments+in+Indiana.
[20] https://www.census.gov/programs-surveys/gus/about.html.
[21] https://www2.census.gov/programs-surveys/gus/datasets/2017/2017_gov_org_meth_tech_doc.pdf.

governing bodies, among others. The 2022 United States Census estimates Indiana's population to be 6,833,037 people.

Data collected as part of this assessment include descriptions of assessed entities based on the type of local governmental entity and population. Table 3 below classifies assessed entities by the type of local entity. Nearly all (22 of 23) of the entities we assessed between the March 2023 start of this program and November 2023 were county or municipal governments. Since November 2023, the Cybertrack team has assessed a more diverse sample of entity types. Most notably, we have assessed 15 K-12 school districts in the previous six months ending June 1, 2024. The county, municipal, and township governments assessed by the Cybertrack program to date represent 2.9% of Indiana's general purpose governments, but these entities serve 44.57% of Indiana's total population. Populations served by assessed entities ranged from 560 to 970,000 people.[22] Fifty-two assessed entities were "rural" as defined by The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2022 Homeland Security Grant Program[23] (*i.e.*, they serve a population of 50,000 or fewer people). Average yearly spending among assessed entities ranged from approximately $6.1 million dollars to nearly $3 billion dollars.[24]

**Table 3**: Cumulative Number of Assessed Entities by Type of Entity

| Type of Entity | Number of Entity Type As of November 2023 | Number of Entity Type As of May 2024 |
|---|---|---|
| County Government | 12 | 22 |
| Municipal (City/Town) Government | 10 | 27 |
| Township Government | 0 | 2 |
| K-12 School District | 0 | 20 |
| Library | 1 | 2 |
| Other | 0 | 3 |
| **Total** | **23** | **76** |

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

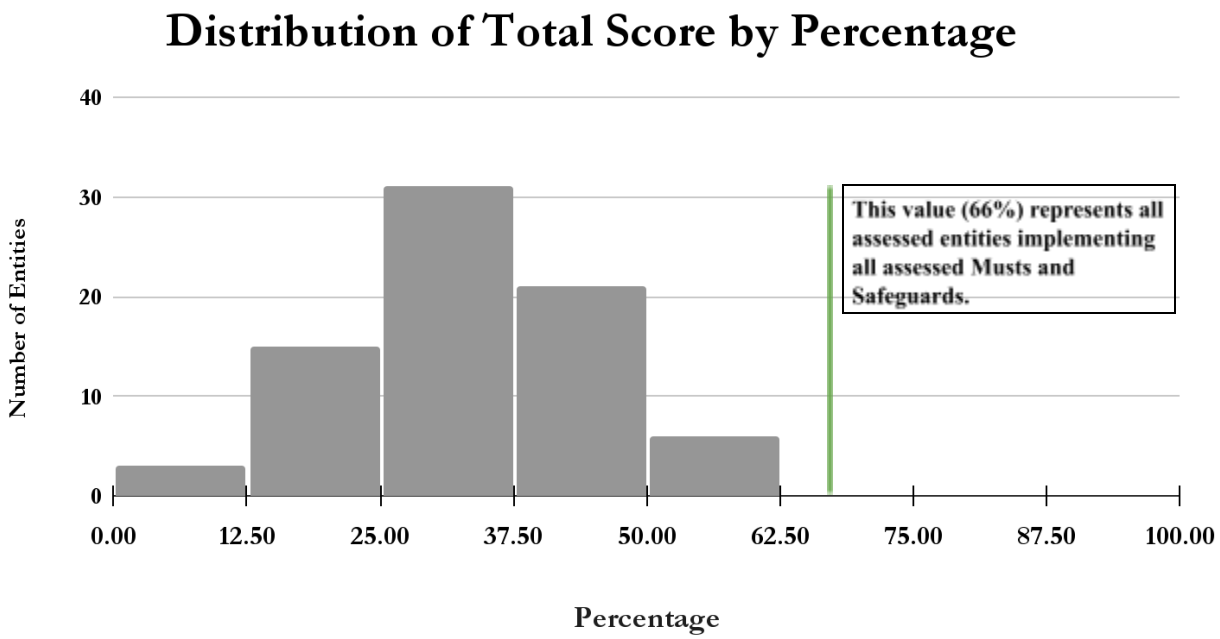
Using the implementation ratings coding system described in Section 2.2, total scores for assessed entities ranged from 2 to 56 points. Due to the January 2024 addition to our assessment of CIS Safeguards 6.3 "Require MFA for Externally-Exposed Applications"[25] and 11.4 "Establish and Maintain an Isolated Instance of Recovery Data,"[26] entities assessed after December 2023 can be

[22] https://data.census.gov.
[23] https://www.fema.gov/grants/preparedness/homeland-security/fy-22-nofo
[24] https://gateway.ifionline.org/report_builder/
[25] Center for Internet Security. (2021, May). *CIS Critical Security Controls Version 8*. cissecurity.org/controls. p. 22.
[26] Center for Internet Security. (2021, May). *CIS Critical Security Controls Version 8*. cissecurity.org/controls. p.33

assessed up to six points more than those entities assessed prior. For example, an entity that was implementing all Musts and Safeguards would score 62 points through December 2023 and 66 since. An entity that was assessed to be developing all Musts and Safeguards would score 31 points through December 2023 but 33 points since. The maximum possible assessment rating score, which represents an "Optimizing" rating on all assessed Musts and 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 2 points differs greatly from an organization scoring 56 points, organizations with similar scores may well have very different postures. This is due in part to the fact that not all Musts and Safeguards are equally powerful. That said, the graph below shows the distribution of assessment total scores.

**Figure 4:** Distribution of Assessment Total Scores (Number of Entities (Y) x Ranges of Percentage of Total Score (X)




The average total score for entities assessed **before** the addition of Safeguards 6.3 and 11.4 to the assessment (n=44) was 27.68 out of 93 possible points.[27] points for each of the 31 assessed Musts and Safeguards. The average total score for entities all assessed **after** the addition of Safeguards 6.3 and 11.4 to the assessment (n=32) was 36.40 out of 99 possible points. Overall, the 76 assessed included in this report averaged 0.99 points per assessed Must & Safeguard – slightly below a Developing implementation rating. For the 6 assessed Trusted CI Musts, entities averaged 5.88 points or 0.98 points per Must. For CIS Safeguards only, entities averaged 1.00 points per Safeguard. In both cases, entities reached nearly one point per Safeguard, or a Developing rating, in general. Additionally, implementation was the lowest for the following Safeguards:

[27] Three assessed entities received no rating for CIS Safeguard 2.1. One assessed entity received no rating for CIS Safeguard 4.1.

- 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 4.1: Establish and Maintain a Secure Configuration Process**
- CIS 7.1: Establish and Maintain a Vulnerability Management Program
- CIS 8.1: Establish and Maintain an Audit Log Management Program
- CIS 17.7: Conduct Routine Incident Response Exercises

Six of these seven same Safeguards were noted in our November 2023 report as not being implemented by any assessed entities. Though these Safeguards are no longer notable for the absence of Implementing ratings among all assessed entities, these results continue to serve as a key characteristic of our following analysis of the cybersecurity posture of Indiana's local entities that have thus far participated in the Cybertrack program. Of particular note is the fact that two of these six (**bolded above**, 2.3 and 4.1) are members of the Transformative Twelve discussed in Section 2.1.

During this phase of work, Cybertrack assessed more types of entities than in the time period we reported on in the November 2023 report. The broader sample of entities facilitated a comparison of total assessment rating score by type of entity. Though we found no statistically significant differences in total score by type of entity, we did note that K-12 school districts scored highest, on average. The mean total rating score for assessed K-12 entities was 35.17 points. All other entities combined averaged 29.65 points. Also of interest, K-12 entities' scores varied less (a range of 8.44 points) versus a range of 12.22 points for all others. Though these differences are not statistically significant, the difference in scores by entity type could be an important data set; so we continue to watch this metric.

Cybertrack's Written Discovery Requests (WDRs) also ask several questions of assessed entities that seek to describe entities themselves and further characterize their cybersecurity postures beyond the assessed Musts and 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 government entity? 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 entities responded (n=76), we noted that 38 entities completed the assessment exclusively using IT employees or IT consultants. Thirty-two entities (45.7%) engaged non-IT members of leadership in the assessment process. This percentage is largely consistent with the percentage of entities (48.6%) 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.[28]

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

Thirty-six entities (51.4%) responded with strengths; forty-five (64.2%) provided perceived weaknesses. As shown in Table 4, assessed entities' reported strengths were distributed across 17 coded responses. The distribution of these coded responses does not provide generalizable insight into local government cybersecurity postures, other than that their perceived cybersecurity strengths are diverse.

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

**Table 4**: Coded, Perceived Cybersecurity Strengths as Reported by Assessed Entities

| Characterization of Strengths | # of Entities |
|---|---|
| Network Security Infrastructure (overall collection of cybersecurity tools in use) | 9 |
| Personnel (Contractor/staff knowledge | 7 |
| User Training | 6 |
| Network Monitoring Tools/Processes | 6 |
| Endpoint Protection | 5 |
| Data Resiliency - Backups | 5 |
| Access Control - MFA Imp | 5 |
| Patching (Regularity) | 3 |
| Access Control - Role-based Access | 3 |
| Cybersecurity Program | 2 |
| Vulnerability Management | 2 |
| Threat Intel | 1 |
| Cybersecurity Community | 1 |
| Network Isolation/Segmentation | 1 |
| Response Plans | 1 |
| Access to State Resources | 1 |

The perceived weaknesses provided were less diverse. Of the 45 entities that responded with cybersecurity weaknesses, 19 noted a lack of adequate cybersecurity-specific staffing, and 18 reported a lack of sufficient cybersecurity-related policies and procedures. The reported weaknesses are summarized in the Table 5 below. Of the 18 entities that reported a lack of documentation as a cybersecurity weakness, only four were classified as urban. Conversely, of those reporting a lack of adequate cybersecurity-specific staffing, 11 of 19 were urban.

**Table 5**: Coded, Perceived Cybersecurity Weaknesses as Reported by Assessed Entities

| **Characterization of Weaknesses** | **# of Entities** |
|---|---|
| Lack of Staffing/Knowledge | 19 |
| Lack of Documentation | 18 |
| Budget Adequacy | 9 |
| Lack of Cybersecurity Program | 6 |
| Network Security Infrastructure (overall collection of cybersecurity tools in use in an entity) | 4 |
| Lack of Logging/Monitoring | 3 |
| Lack of Controls Testing | 3 |
| Access Control - Passwords | 3 |
| Lack of Adequate Backups | 2 |
| Lack of Encryption | 2 |
| Lack of Training | 2 |
| Lack of Device Configuration Process | 1 |
| Lack of Network Isolation/Segmentation | 1 |
| No Incident Response Exercises | 1 |
| Lack of MFA Imp | 1 |
| Lack of Disaster Recovery Plans | 1 |
| Vulnerability Management | 1 |

As mentioned above, we also asked entities which cybersecurity resources offered by the State of Indiana they're using. Slightly less than half (35 of 76) make use of State cybersecurity resources. Twenty-three (32.8%) reported using State-purchased licenses for the KnowBe4 security awareness product. Nine (12.8%) have .gov domains hosted by the State. Other State services being used among assessed entities include Crowdstrike, Trellix[29], website hosting, and the QPI purchasing program.

[29] Trellix services are available through the Indiana Secretary of State's office, and only to county governments .

# 4 Analysis

This section presents our analysis of assessment results and information from 76 Indiana local governments assessed between March 2023 and May 2024. 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

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 entities received nearly one point (0.98) per assessed Must and Safeguard out of the 3 points possible. This means that, **in general, entities averaged slightly below a Developing implementation rating**.[30] Across all entities assessed during the Cybertrack program, **none of the assessed Musts or Safeguards individually averages a score of 2 or greater, which would represent an average status of "Implementing" or better.**

## 4.2 Noteworthy Results: Trusted CI Framework Musts

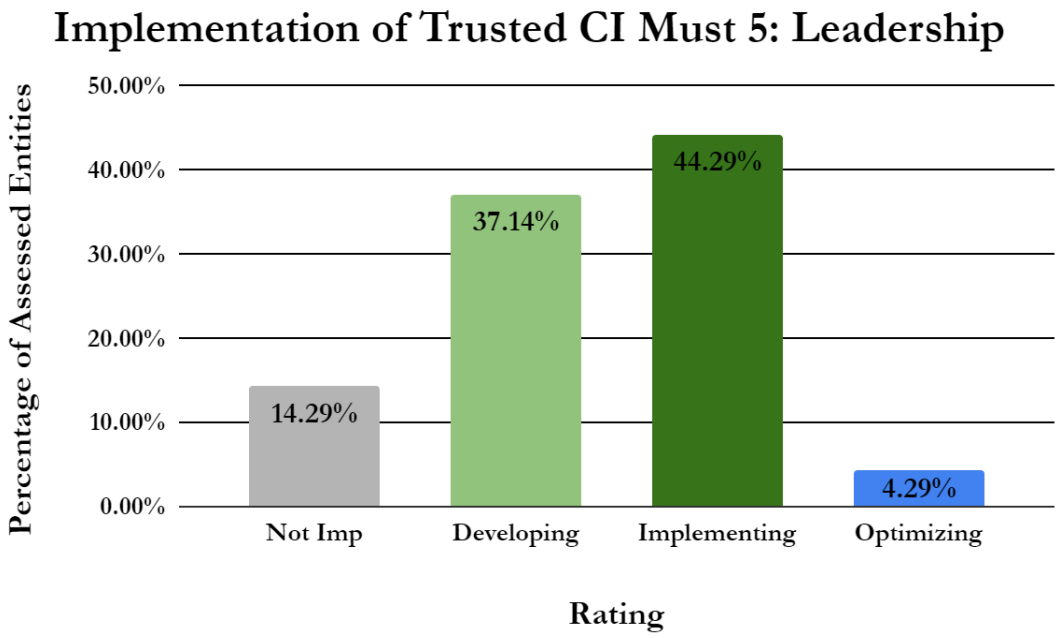
As noted in Section 2.1 above, the Trusted CI Framework Musts evaluate organizational **cybersecurity fundamentals, or programmatics,** driving entities' cybersecurity efforts. Cybertrack assessments evaluate 6 of the Framework's 16 Musts, listed in Appendix A. The ranking of Musts by mean rating scores remained consistent with our November 2023 sample despite our assessment of an additional 50+ entities that included a wider range of organization types. Table 6 below illustrates the stability of the mean score ranking among the Musts despite some volatility in the means themselves. The most encouraging result from our evaluation of the Musts remained the involvement of leadership in cybersecurity decision making. Assessed entities averaged 1.39 points on Must 5 (Organizations must involve leadership in cybersecurity decision making.). This average implementation rating on Must 5 continues to exceed the average rating of other Musts, as well as 21 of 27 assessed Safeguards. More than half of the assessed entities (44.29%) received an "Implementing" rating on this Must, while 37.14% received a "Developing" rating. Ten assessed entities received a rating of "Not Implementing." Figure 5 below illustrates the rating distribution from Must 5.

[30] Entities averaged a slightly lower than the same average total score calculated after our initial 23 assessed entities described in our first report.

**Table 6**: Mean Ranking of Trusted CI Musts (high to low) With Percentage Change in Means November 2023 - May 2024

| Changes in Mean Rating Score for Trusted CI Musts November 2023 - May 2024 | | | |
|---|---|---|---|
| Must | November 2023 Mean | May 2024 Mean | Percentage Change |
| Must 5: Leadership | 1.39 | 1.39 | -0.40% |
| Must 7: Cybersecurity Lead | 1.04 | 1.14 | 9.52% |
| Must 13: Personnel | 0.91 | 1.01 | 11.09% |
| Must 12: Cybersecurity Budget | 0.78 | 0.83 | 5.87% |
| Must 9: Policy | 0.65 | 0.79 | 21.76% |
| Must 15: Baseline Control Set | 0.48 | 0.47 | -1.43% |

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



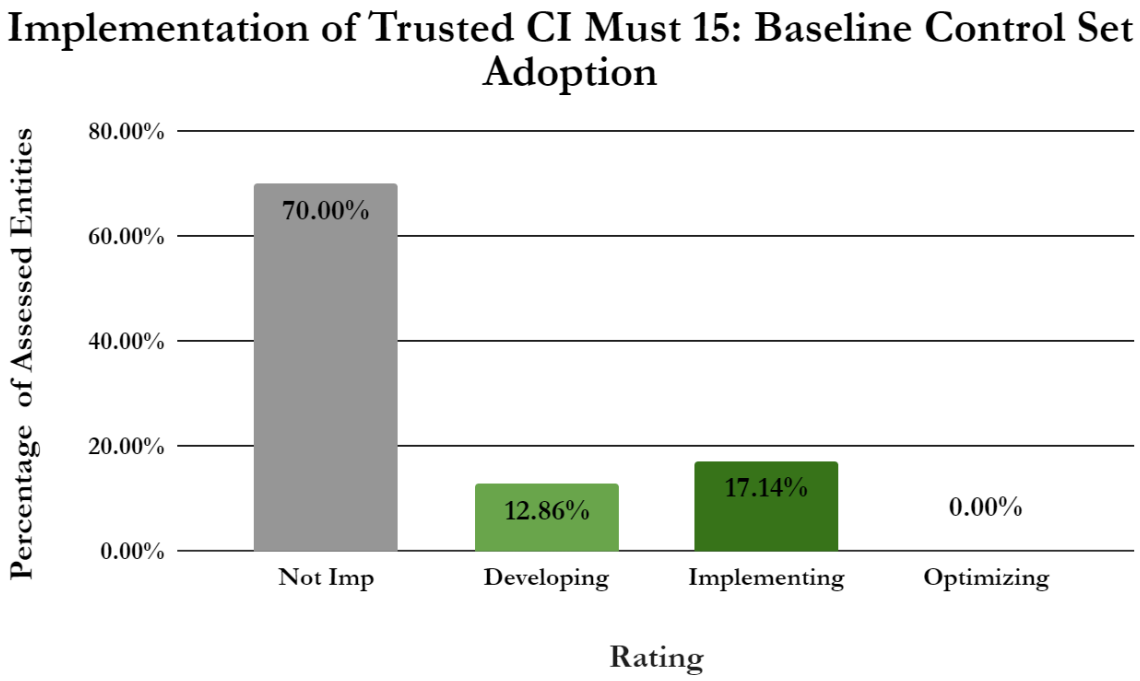

Senior leadership must be involved in cybersecurity decision-making to address cybersecurity competently. Organizational leaders are the primary agents of the organizations for which they work, representing the organization to the outside world. They are ultimately responsible for the organization and 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[31], and/or the relatively small

[31] Mahendru, P. *The State of Ransomware in State and Local Government 2023*. Sophos.

nature of local government entities 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 entities had adopted a baseline set of cybersecurity controls (Must 15). Assessed entities averaged only 0.47 points on this Must. As shown in Figure 6 below, less than 20% had formally adopted a baseline set of cybersecurity controls, such as the CIS Safeguards or NIST Cybersecurity Framework. Fully 70% of assessed entities had made no progress on this programmatic fundamental as of their assessment.

**Figure 6:** 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. When creating cybersecurity plans and budgets, an adopted control set helps to ensure that executive and IT 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 entities considered the results from Musts 5 and 15 presented above, as well as the average score on all assessed Musts, the mode for each Must implementation rating, and the relationship between an entities' total Musts scores and total Safeguards scores. Assessed entities averaged only 5.91 points

https://www.sophos.com/en-us/whitepaper/state-of-ransomware-in-government.

out of 18 possible across all assessed Musts. Unfortunately, Must 5 is the only assessed Must where the most commonly achieved rating of "Implementing." We most frequently evaluated Musts requiring an established cybersecurity lead role (Must 7), implementation of a formal cybersecurity policy (Must 9), and the formal designation of personnel to cybersecurity responsibilities (Must 13) as "Developing." Assessed entities most frequently received a "Not Implementing" rating for not having a cybersecurity budget (Must 12) and for not adopting and using a baseline control set (Must 15). **These data continue to indicate that assessed entities' 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.**

Entities' total scores on the six assessed Trusted CI Musts significantly predict entities' total Safeguard scores. With 76 entities assessed, the entities that have made more progress developing formal cybersecurity programs have made more progress implementing technical cybersecurity Safeguards ($\alpha$=0.05, p=0.01, $r^2$=0.26). The next section discusses assessed entities' implementation of technical Safeguards.

## 4.3 Noteworthy Results: CIS Safeguards

Entities received, on average, one point (1.00) per Safeguard in Cybertrack assessments. The same is true when we narrow the focus to only Safeguards that are members of the Transformative Twelve (1.07 points per Safeguard). Because assessed entities are not implementing or only developing implementations of the Safeguards we've assessed, they have many cybersecurity priorities to address. In this section, we highlight and discuss Safeguards on which entities 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 family 2, with which assessed entities particularly struggled.

Implementation ratings for the two assessed CIS Control 10 "Malware Defenses" Safeguards continued to be the two highest rated by mean score among all 76 assessed CIS controls. Both of these are members of the "Transformative Twelve" discussed in Section 2.1. The mean score for CIS Safeguard 10.1, "Deploy and Maintain Anti-Malware Software,"[32] was 1.82 points. The mean score for CIS Safeguard 10.2, "Configure Anti-Malware Signature Updates"[33] was also 1.82. The mode rating for both Safeguards was "Implementing," and none of the assessed entities received a "Not Implementing" rating for either Safeguard. Figures 7 and 8 below provide a graphical representation of implementation ratings for these safeguards.

[32] Center for Internet Security. (2021, May). *CIS Critical Security Controls Version 8*. cissecurity.org/controls. p. 31.
[33] Ibid.

**Figure 7**: Implementation Rating Distribution: CIS Safeguard 10.1: Deploy and Maintain Anti-Malware Software

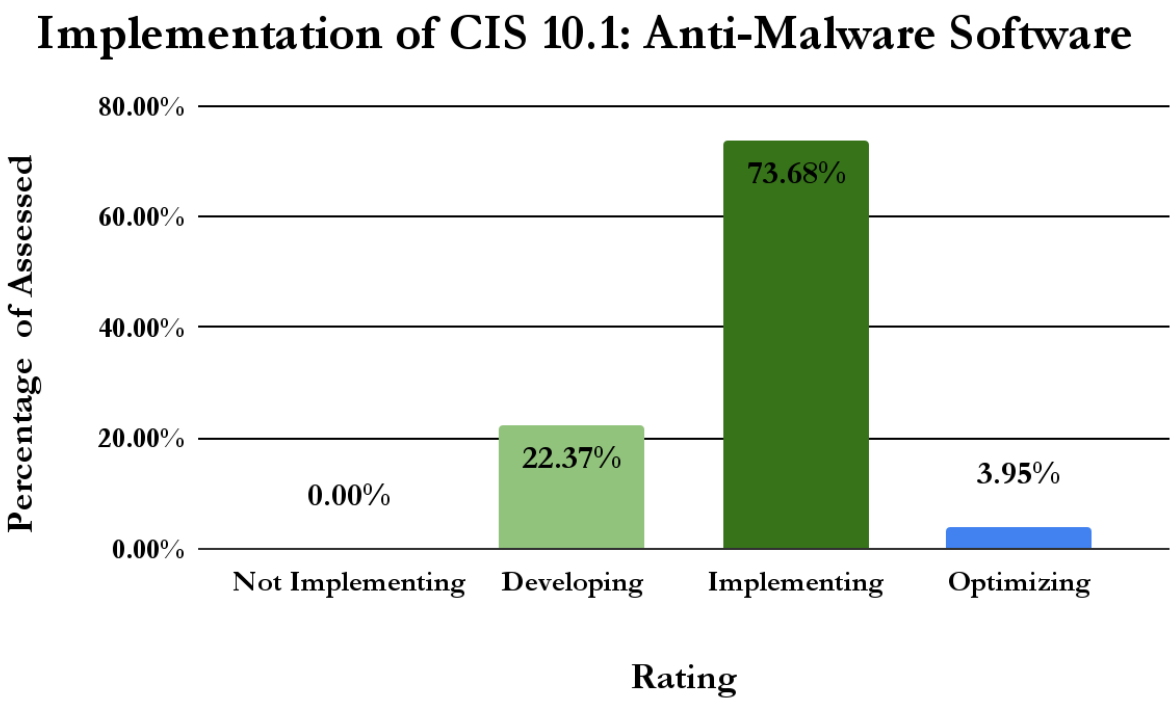
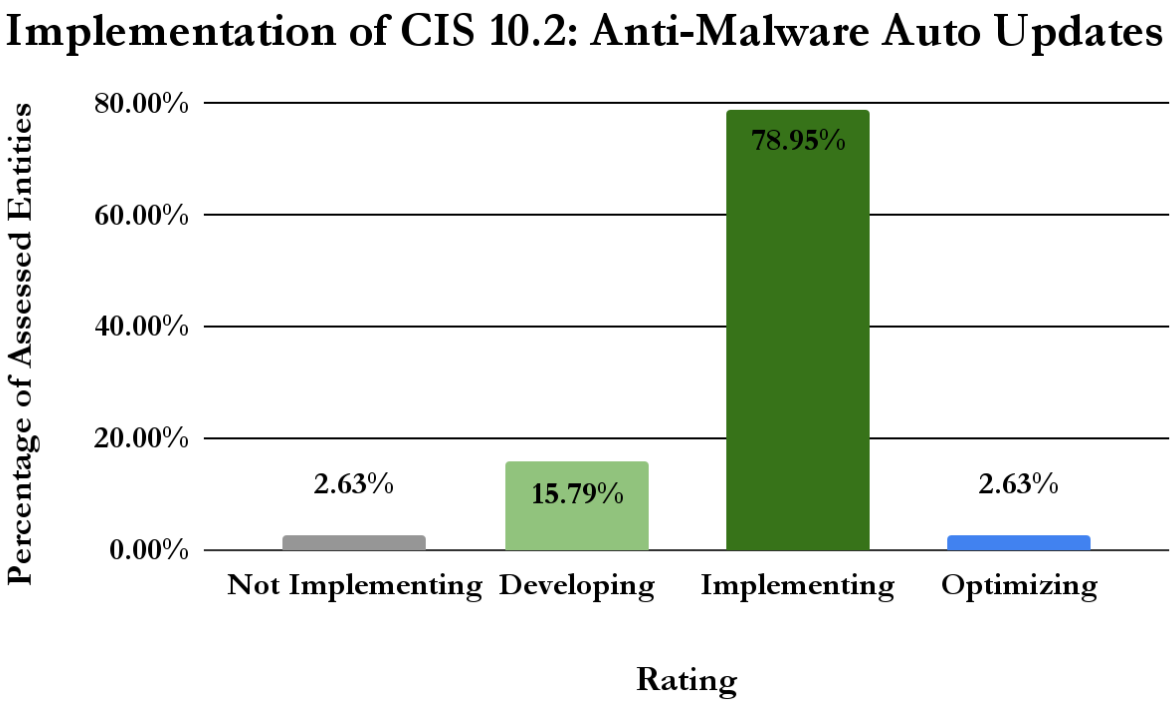


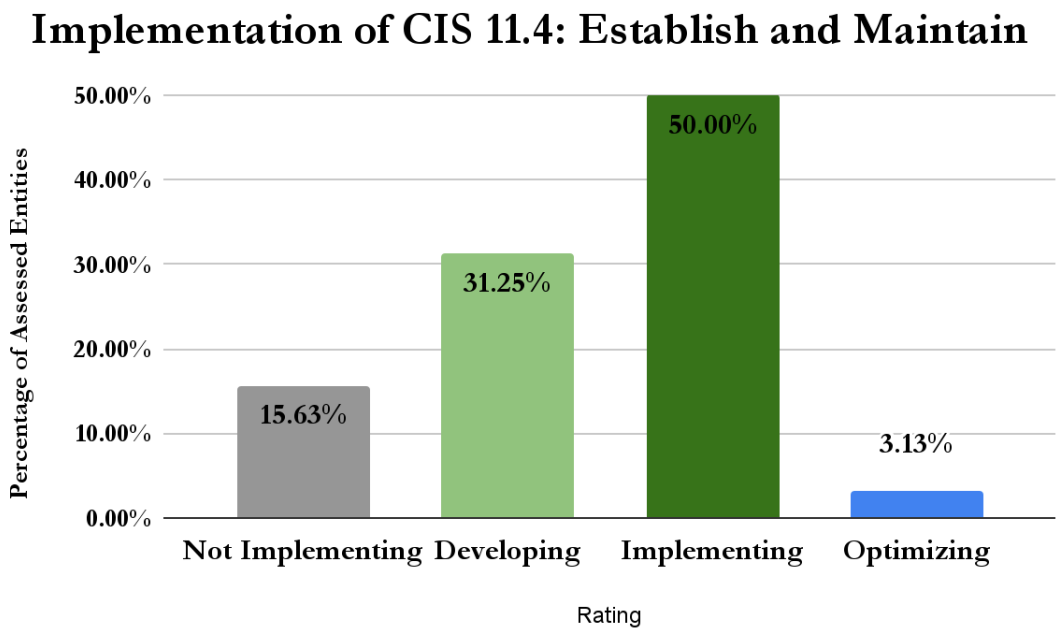

**Figure 8**: Implementation Rating Distribution: CIS Safeguard 10.2: Configure Anti-Malware Signature Updates



Ransomware incidents have been costly to local governments. Attacks on Atlanta, GA[34] and Baltimore, MD[35] are prominent examples, but Indiana local government entities and K-12 school districts have also been extorted through ransomware.[36] [37] Implementing and maintaining anti-malware software can protect devices on which they're installed from some types of ransomware infections. Relatively high ratings and lack of "Not Implementing" ratings for assessed entities on CIS Safeguards 10.1 and 10.2 represent a point of strength in Indiana local entities' cybersecurity postures.

Our addition of CIS Safeguard 11.4, "Establish and Maintain an Isolated Instance of Recovery Data" to the Transformative Twelve and to Cybertrack assessments highlighted another area of relative strength among assessed entities. The mean score across the 32 entities assessed since its addition was 1.41 points out of a possible three. By mean score, Safeguard 11.4 ranked third behind Safeguards 10.1 and 10.2 discussed above. Five (15.63%) of the 32 assessed entities were not implementing isolated instances of recovery data. More than half (53.13%) of assessed entities were implementing or optimizing implementations of the Safeguard. The figure below visually shows entities' level of implementation of this Safeguard. Keeping an isolated, up-to-date copy of data is necessary for successful recovery from a cybersecurity incident, but it is not sufficient.

**Figure 9:** Implementation Rating Distribution: CIS Safeguard 11.4: Establish and Maintain an Isolated Instance of Recovery Data




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

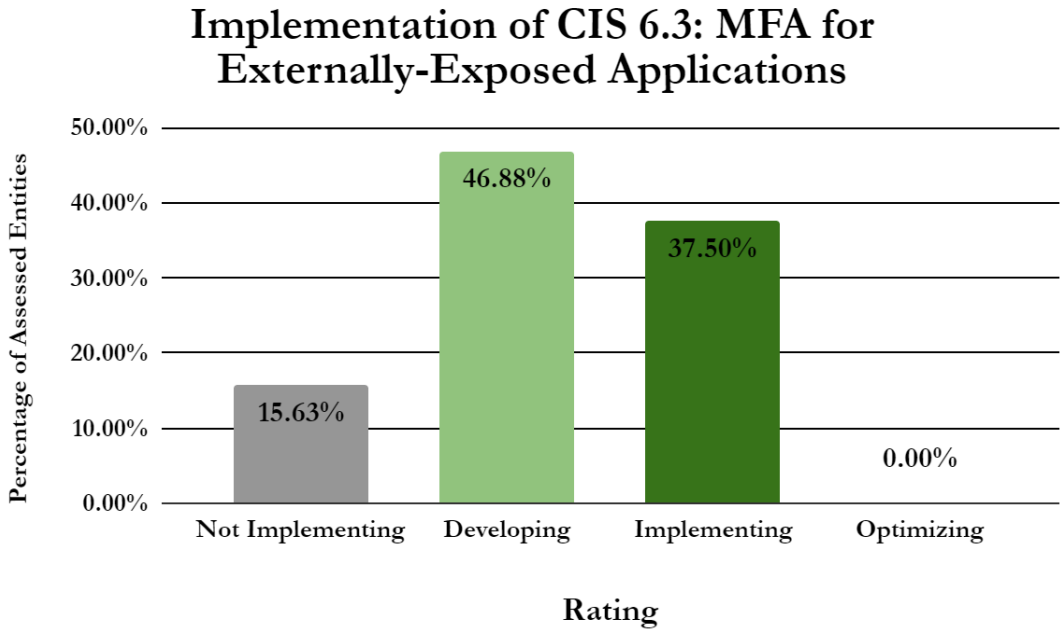
[35] https://www.baltimoresun.com/politics/bs-md-ci-ransomware-expenses-20190828-njgznd7dsfaxbbaglnvnbkgjhe-story.html

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

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

Substantial empirical research, including that resulting in the identification of the Transformative Twelve 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.[38] Moreover, under Senate Enrolled Act 150, public entities that connect to the State's technology infrastructure will be required to implement "a secondary end user authentication mechanism,"[39] by July 2027. Each of the three CIS Control 6 Safeguards that Cybertrack assesses are members of the Transformative Twelve. Assessed entities 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 entities' implementation and use of multi-factor authentication through CIS Safeguards 6.3, "Require MFA for Externally-Exposed Applications, 6.4, "Require MFA for Remote Access"[40] and 6.5, "Require MFA for Administrative Access,"[41]. Cybertrack assessed 32 entities after adding Safeguard 6.3 in January 2024. Of those, 37.50% are fully implementing multi-factor authentication for applications that are accessible externally. The low rate of implementation of MFA on externally-exposed applications is quite concerning because these applications are defined by their exposure to attackers on the Internet. 46.88% of assessed entities were Developing this Safeguard; 15.63% were Not Implementing. Entities 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.

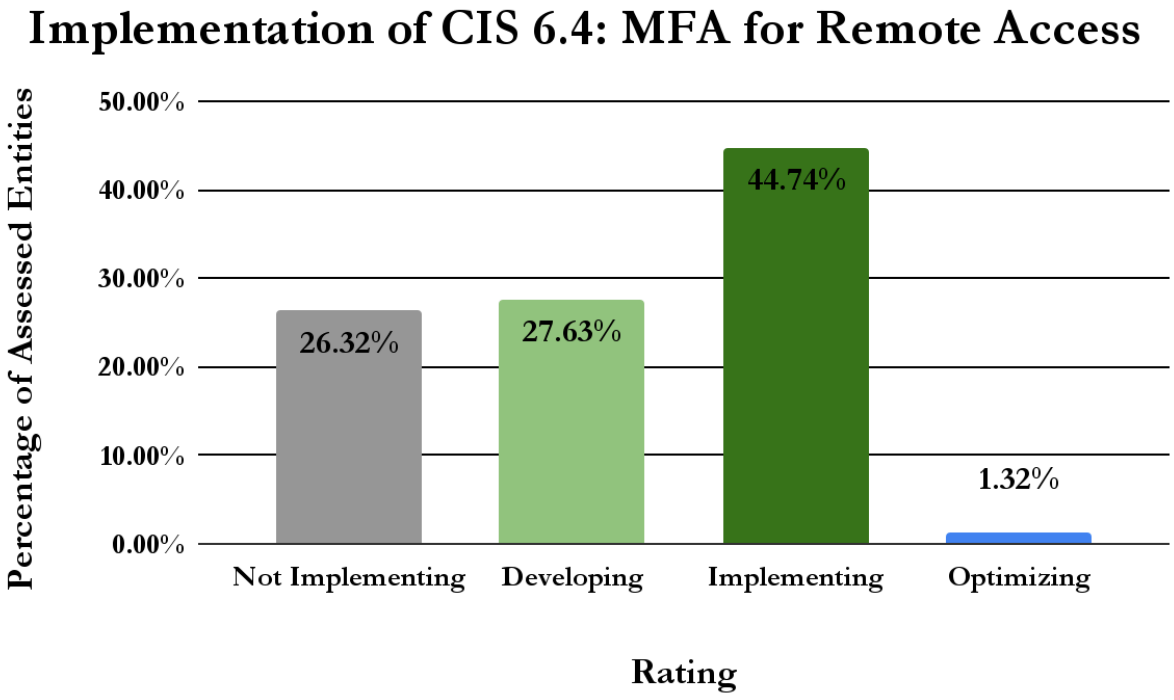
**Figure 10**: Distribution of Implementation Ratings for CIS Safeguard 6.3: Require MFA for Externally-Exposed Applications




[38] *See, e.g.*, https://arxiv.org/abs/2305.00945.
[39] https://iga.in.gov/pdf-documents/123/2024/senate/bills/SB0150/SB0150.06.ENRH.pdf, p.6.
[40] Center for Internet Security. (2021, May). *CIS Critical Security Controls Version 8*. cissecurity.org/controls. p. 22.
[41] Ibid.

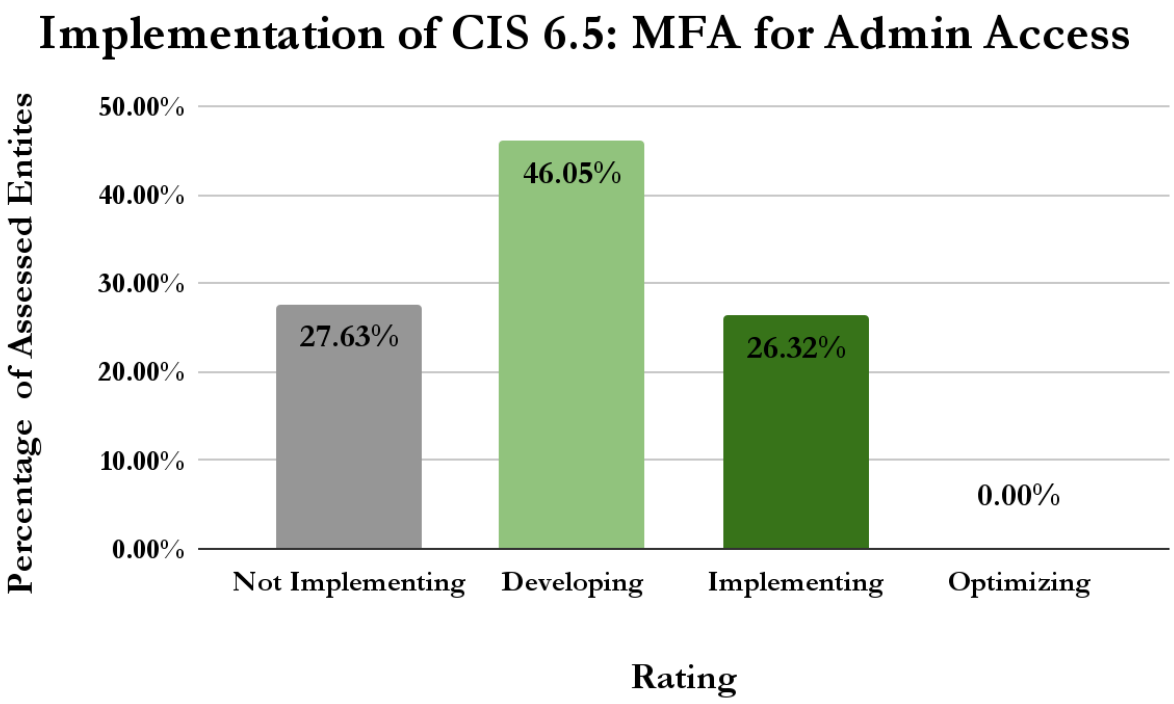
We assessed Safeguard 6.4, "Require MFA for Remote Network Access," for all 76 of the entities assessed in the program so far. More than 44.74% of assessed entities were implementing MFA for remote access. 27.63% of entities were "Developing" MFA for remote access. 26.32% of assessed entities were not implementing MFA for remote access. In sum, well more than half (53.95%) of participating organizations were not fully implementing MFA on remote access at the time of assessment, but 72.37% of them had made at least some meaningful progress toward implementation, as shown in the figure below.

**Figure 11**: Distribution of Implementation Ratings for CIS Safeguard 6.4: Require MFA for Remote Network Access




The assessed entities have been even less successful in requiring MFA for administrative access to their systems. Though slightly less than half (46.05%) of assessed entities were developing implementations of this Safeguard, 27.63% were not implementing MFA for administrative access. Relatively low implementation of MFA 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. Figure 12 displays these results.

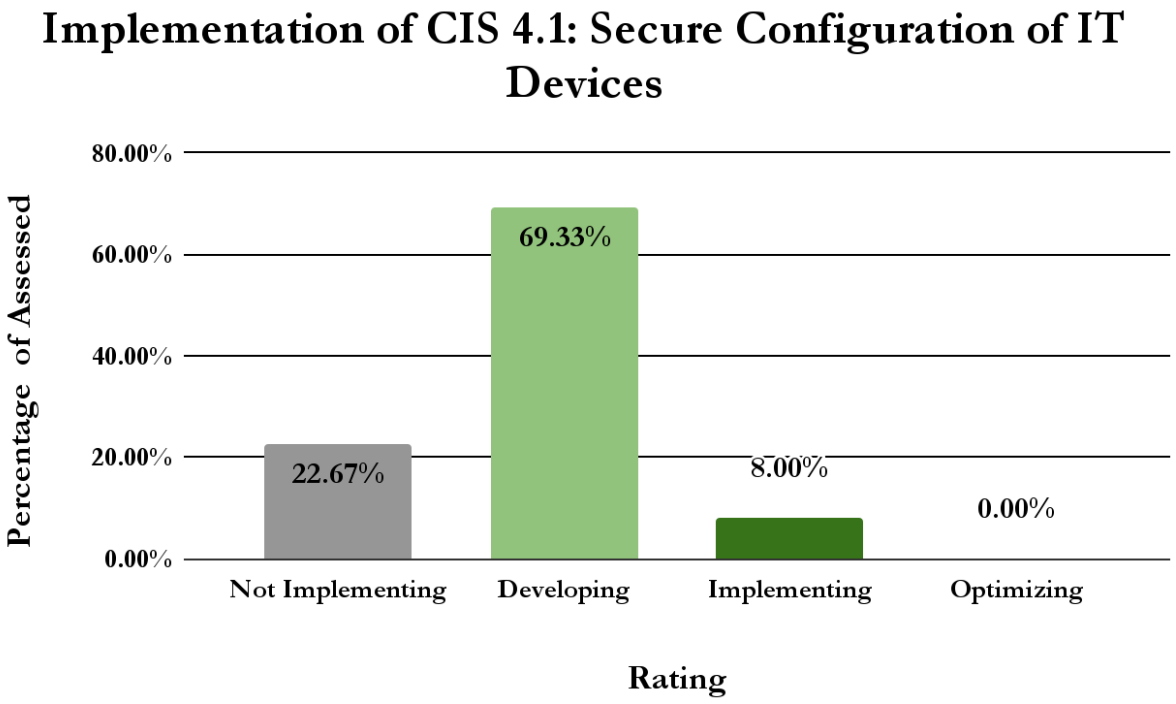
**Figure 12**: Distribution of Implementation Ratings for CIS Safeguard 6.5: Require MFA for Administrative Access




Organizations can manage software vulnerabilities, in part, by ensuring strong configuration processes for IT assets as detailed in CIS Safeguard 4.1.[42] 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 (4.1: 8%, 4.2: 17%, 4.3: 12%). By fully implementing the five CIS Safeguards from Cybertrack assessments focused on secure configurations, entities' 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 8.7% of assessed entities. Most commonly (66.67%), assessed entities received a "Developing" implementation rating on Safeguard 4.1, but 24.64% were rated as "Not Implementing." A stunning 91.31% of assessed entities were not implementing Safeguard 4.1 The figure below represents assessed entities' ratings on Safeguard 4.1 graphically.

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

**Figure 13**: 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.

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) indicate that assessed entities struggle hardest to implement them. Assessed entities had the lowest incidence of employing controls related to building software inventories and controlling software assets. The Cybertrack Team assesses three CIS Safeguards on this topic: Safeguard 2.1, "Establish and Maintain a Software Inventory," [43] Safeguard 2.2, "Ensure Authorized Software is Currently Supported," [44] and Safeguard 2.3, "Address Unauthorized Software," [45] another member of the Transformative Twelve. The mean Implementation Rating scores for these three controls were 0.69 points, 0.54 points, and 0.6 points, respectively, indicating that few assessed entities were even developing implementations related to these Safeguards. These three Safeguards are all characterized by high percentages of "Not Implementing" ratings among assessed entities.

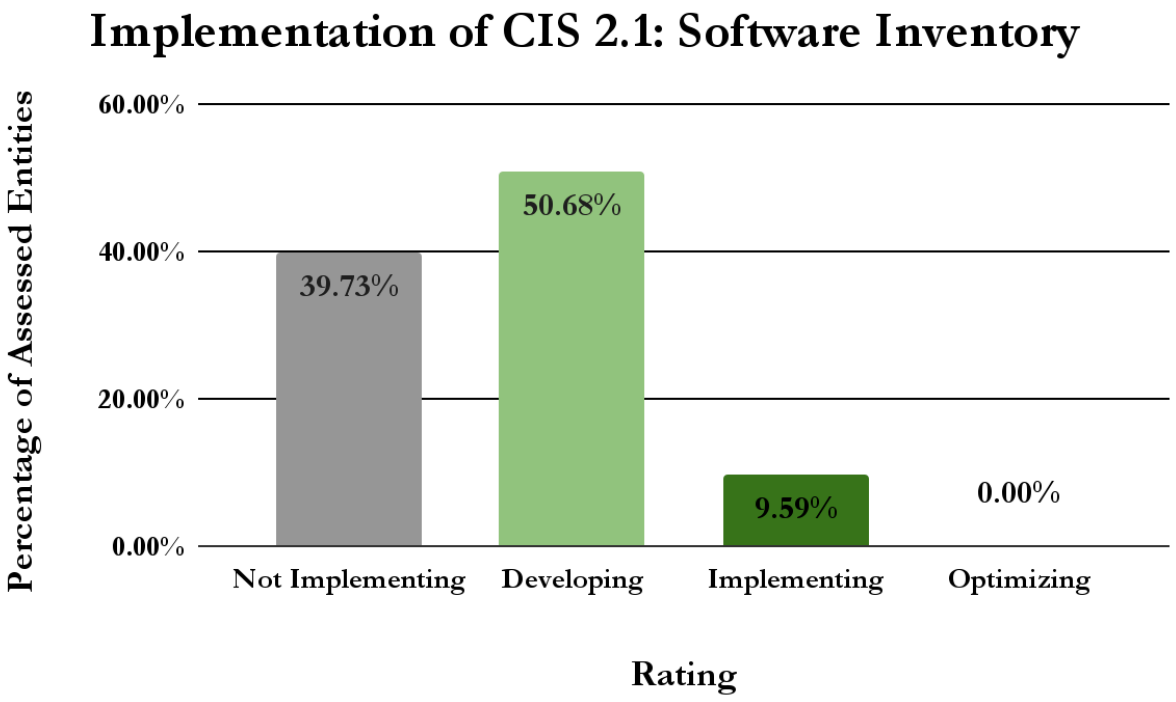
Though means increased on Control 2 Safeguards since our November 2023 sample, results remain

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

concerning. For each of the 76 entities, we assessed and rated three Control 2 Safeguards (2.1, 2.2, & 2.3, as shown in the graphs below) for a total of 210 individual ratings across all assessed entities. Of these 210 ratings, only 17 were "Implementing" (8.1%). None were "Optimizing." Of the assessed Safeguards, those in the Control 2 family remain the least implemented.

Most critically, less than 10% of the entities we've assessed so far have implemented Safeguard 2.3, a member of the Transformative Twelve that requires entities to ensure the removal or documentation of exceptions for all unauthorized software.[46] Failure to implement CIS 2.3 can lead directly and quickly to serious cyber incidents. Entities should make the implementation of this Safeguard a top technical priority in their cybersecurity programs.

**Figure 14**: Implementation Rating Distribution for CIS Safeguard 2.1, Software Inventory




[46] Ibid.

**Figure 15**: Implementation Rating Distribution for CIS Safeguard 2.2, Ensure Authorized Software is Supported

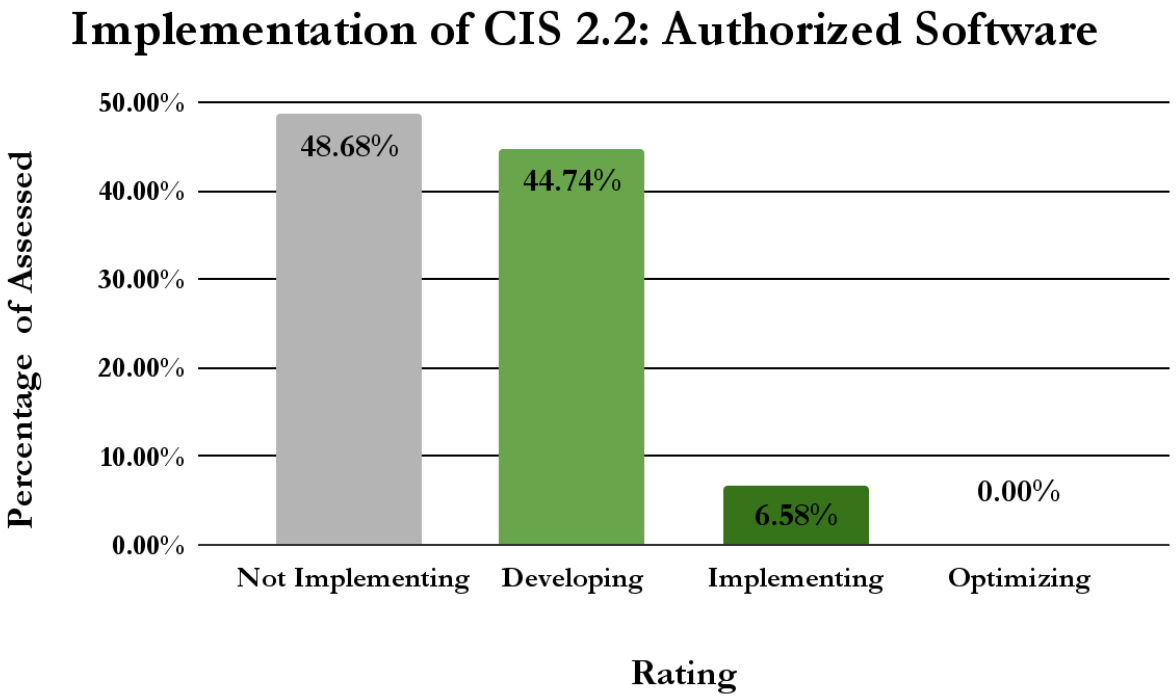
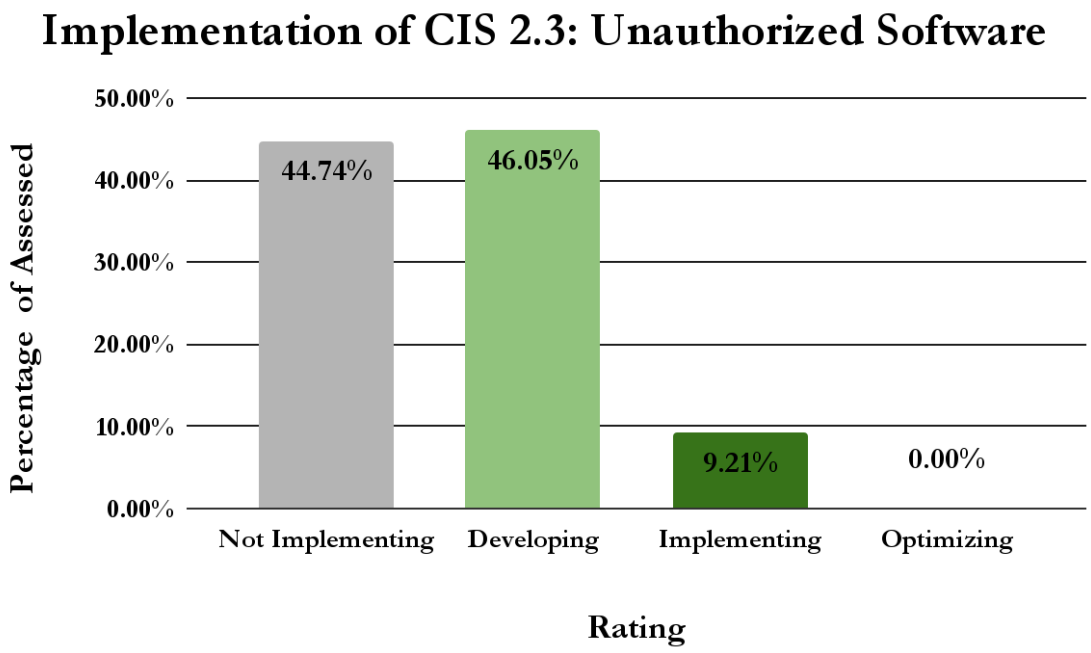



**Figure 16**: Implementation Rating Distribution for CIS Safeguard 2.3, Address Unauthorized Software




All three of these Safeguards ranked among the bottom five 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.

## 4.4 Correlations

In our November 2023 report, 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 have held (although their characteristics have changed) and gained power. Additional correlations also became evident as our sample size grew. These correlations are discussed below.

Our analysis continues to show that an entity's total score on assessed Trusted CI Musts is significantly positively correlated to its total score on assessed CIS Safeguards. That is, where entities received higher total scores on Trusted CI Musts, those entities generally received correspondingly higher scores on CIS Safeguards, and vice versa ($\alpha$=0.05, $p<0.0001$, $r^2$=0.39). With data from an additional 53 assessments, this correlation became statistically more significant and more explanatory of the difference in Safeguards total score. Because we have assessed a (much) larger number of entities since November 2023, this correlation is also more powerful. That is, it is more likely to be describing an actual causal relationship. Among the Musts, Must 12 (Cybersecurity Budget)($\alpha$=0.05, $p<.0001$, $r^2$=0.32), Must 13 (Personnel) ($\alpha$=0.05, $p<0.0001$, $r^2$=0.33), and Must 15 (Baseline Control Set) ($\alpha$=0.05, $p<0.0001$, $r^2$=0.33) were significantly correlated with an entity's total score on assessed CIS Safeguards. 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. We argue that organizations cannot successfully put the technical cart before the organizational horse, and these correlations continue to support this argument.

In addition to investigating individual Musts and Safeguards and groupings of Musts and 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[47])
- Total annual spending (as reported in public filings[48])
- 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[49])
- 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)

[47] https://www2.census.gov/programs-surveys/popest/tables/
[48] https://gateway.ifionline.org/report_builder /
[49] https://www2.census.gov/programs-surveys/popest/tables/

- Whether the entity experienced a cybersecurity incident in the past three years (self-reported, WDR Wrap-Up Q4)
- Cybersecurity strengths and weaknesses (self-reported, WDR Wrap-Up Q2 & 3, respectively)

Only previous experience of a cybersecurity incident, WDR Wrap-Up Q4, was significantly correlated with assessment ratings scores. Consistent with our findings in the November 2023 report, entities that reported experiencing a cybersecurity incident in the past three years are implementing more of the Musts and Safeguards we assess. Using an ANOVA test, prior incidents were significant predictors of the total score ($\alpha$=0.05, p=0.004, $r^2$=0.12). This result supports 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.

# 5 Conclusion

One of Cybertrack's primary goals is to inform Indiana's local government cybersecurity policy and strategy. This report supports that goal. Considering Cybertrack only assesses cybersecurity practices that are known to be among the most powerful, the results of these 76 assessments are sobering and show that Indiana's local government entities have a long way to go in basic cybersecurity capability. They most certainly need help. The results highlight the following specific needs.

The community should act to:

A. **Increase leadership involvement 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). Based on the 40% of assessed entities who are Developing 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 government 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 government entities 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 government entities 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, certainly to include the Transformative Twelve 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 add most significantly to local government cybersecurity postures:

- Growing evidence supports the particular power of secure configurations (CIS Control 4) and multi-factor authentication (CIS Control 6). 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: 8%, 4.2: 17%, 4.3: 12%). By fully implementing the five CIS Safeguards from Cybertrack assessments focused on secure configurations, entities' devices will become far more resistant to cyber attack.
- All evidence-based sources we've found indicate that MFA is one of, if not the most, effective cybersecurity controls available to defenders.[50] MFA is highly effective at preventing and disrupting attacks by reducing an attacker's ability 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 entities' struggles to implement cybersecurity controls. Only ten of 76 assessed entities received an "Implementing" rating on Safeguards 2.1, 2.2, or 2.3 (the Control 2 member of the Transformative Twelve). Respectively, 40%, 49%, and 45% of assessed entities were "Not Implementing" these three Safeguards. This control provides particularly significant opportunities for improving cybersecurity postures through developing cybersecurity controls, but its rating distribution 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.[51] 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. Based on the current state of cybersecurity postures of the local government entities 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 stand ready to expand our efforts.

The Cybertrack team will continue publishing aggregate results reports like this one regularly. As we've done in developing this second Cybertrack report, we will focus on clarifying, detailing, and (where necessary) correcting our analysis of trends as the number in our sample set grows. As we do

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

[51] 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.)

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 entities we've assessed. Each participating entity 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 B**.

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

# Appendix A: Musts and 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: Early 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 is to-be-determined, with a likely rhythm of no more frequent than every two years, we are using this instrument to determine whether and how our assessments impact the participating entities. We solicit responses from all participating organizations at 6 months following the delivery of their assessment report and at 6-month intervals thereafter. As of this report, we have 9 total responses to the Impact Questionnaire.

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 to organizations receiving their assessment reports between October 2023 and January 2024.) As of this report, we have 10 total responses. 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.) | 8 of 9 respondents selected "Yes."<br><br>1 respondent selected "No." |
| Senior Leadership Review**.** Has your organization's most senior leadership reviewed or been briefed on the Cybertrack assessment report? | 7 of 9 selected "Yes."<br><br>2 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? | 18 of 19 selected "5 - Extremely Likely," and 1 respondent selected "4 - Likely." |
| 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." | 16 of 19 selected "5 - Strongly Agree," and 3 selected " 4 - Agree." |

The following are quotes from recent responses:

> "The assessment removed the fear of the unknown from leadership and gave them a position to begin planning for the future."
>
> "You don't know what you don't know....and even if you do know, it never hurts to have another set of eyes."
>
> "Very thorough insight into your cyber environment, extremely helpful identifying your cyber strengths and weaknesses."
>
> "I had an idea where our strengths and weaknesses were, and in some instances, those were what our data supported, but this process helped us understand some of the things we weren't thinking about, and gave us a good list of work to do to be more protected."
>
> "The assessment was overall a really easy experience especially being a K12 with limited time and resources. They made the process straightforward and efficient. No need for improvement that we can see."
>
> "Well worth the time and effort. Great learning tool and roadmap to implementation of the (Trusted CI Framework "Musts") and (CIS Safeguards)."