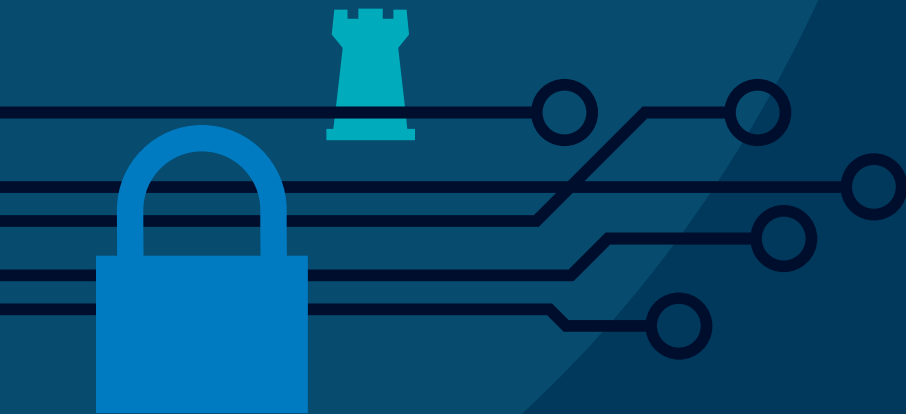


Nationwide Cybersecurity Review: Summary Report

2018



MS-ISAC[®]

Multi-State Information
Sharing & Analysis Center[®]

Nationwide Cybersecurity Review:

Summary Report

2018

Acknowledgments

The Multi-State Information Sharing & Analysis Center® (MS-ISAC®) would like to thank everyone who has previously participated and continues to participate in the Nationwide Cybersecurity Review (NCSR). Your continued support in the NCSR helps us work towards our mission of improving the overall cybersecurity posture of the nation's state, local, tribal, and territorial governments.

We would also like to acknowledge and thank the members of the MS-ISAC Metrics Workgroup for their continued support. Their knowledge, expertise, and dedication assist in the continued success of the NCSR. A special "thank you" to these individuals who contributed to this report: Gary Coverdale, Jim Cusson, Amelia Gifford, Tyler Scarlotta, Greg Bown, Dustin Stark, Kim LaCroix, and Joe Frohlich.





This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number, 2010-PD-123-000001.

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

Table of Contents

Executive Summary	1
2018 NCSR Key Findings	2
Methodology	3
Question Set	3
Targeted Participants	3
NCSR Individual Reports	3
Participation by Entity Type	3
Peer Groups Defined	3
NCSR Participation	4
NCSR Participation Highlights	4
NCSR Demographic Analysis	5
NCSR Maturity Scale	8
Analysis by Function	9
Identify Function	11
Protect Function	12
Detect Function	13
Respond Function	15
Recover Function	16
Partners	18
U.S. Department of Homeland Security	18
Multi-State Information Sharing & Analysis Center	18
National Association of State Chief Information Officers	18
National Association of Counties	18
GMIS International	18
Appendix I: Acronyms	19
Appendix II: Peer Group Detailed Data Analysis for Function Categories	19
Identify Function	20
Protect Function	23
Detect Function	26
Respond Function	28
Recover Function	31
Appendix III: Sub-Sector Peer Groups	33
2018 NCSR Participation by Sub-Sector	33
2018 Sub-Sector Average of All Functions	34
2018 Sub-Sector Identify Function	35
2018 Sub-Sector Protect Function	36
2018 Sub-Sector Detect Function	37
2018 Sub-Sector Respond Function	38
2018 Sub-Sector Recover Function	39



Preface

In June of 2009, the U.S. Department of Homeland Security (DHS) was directed by the United States Congress to develop a cyber-network security assessment that would measure gaps and capabilities of state, local, tribal, and territorial (SLTT) governments' cybersecurity programs. The first Nationwide Cybersecurity Review (NCSR) was conducted in 2011 by DHS. In 2013, DHS partnered with the Multi-State Information Sharing & Analysis Center (MS-ISAC), the National Association of State Chief Information Officers (NASCIO), and the National Association of Counties (NACo) to develop and conduct the second NCSR. Since 2013, the NCSR has been conducted on an annual basis, and 2018 marks the seventh year the self-assessment has been conducted.

Executive Summary

The 2018 Nationwide Cybersecurity Review (NCSR) provides insight on the level of maturity and risk awareness of the state, local, tribal, and territorial (SLTT) information security programs from year to year. Using the results of this Summary Report, DHS and the MS-ISAC continue to work with SLTT partners on improving their cybersecurity maturity. The 2018 NCSR results are based on participation from 669 SLTT entities consisting of 43 states, 277 local governments (from 43 states), 6 tribes, and 343 state agencies (from 24 states). This reflected a 41% increase in participation from 2017.

In 2018, NCSR participants identified a lack of sufficient funding for personnel and security tools as their top security concern. Resource limitations has been a consistent issue for SLTT organizations.

While there were a very large number of first-time survey respondents, especially local government organizations, there was little change in the overall security maturity scores. However, organizations who participate in multiple surveys and take advantage of the products and services offered by the MS-ISAC did show steady improvement in their security posture year over year, with MS-ISAC member organizations reporting maturity scores 34% higher than organizations who do not participate in the MS-ISAC. A continuing priority for DHS and the MS-ISAC then is to increase active participation of SLTT organizations.

In addition, a persistent finding is that local, tribal, and territorial government organizations have much less mature cybersecurity postures, as evidenced by their lower NCSR scores, than state level organizations. For example, the average local government scores are 27% lower than the average state government scores. Analysis of the limitations of these organizations suggests that DHS and the MS-ISAC consider a tailored set of products and services that relieve a burden on technical staff and budgets. This will be a priority for the MS-ISAC in 2019 and 2020.

2018 NCSR Key Findings

In 2018, both the state and local peer groups reported a decrease in overall maturity (-1% for the state peer group and -4% for the local peer group).



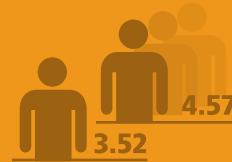
1

Changes in the NCSR question set negatively affected average scores for state, local and tribal peer groups (-1.5%).



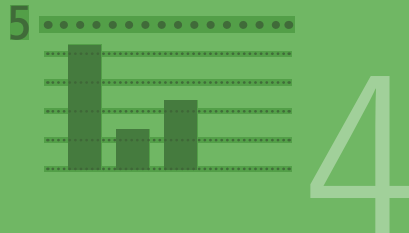
2

New survey participants (+115% for locals) report lower scores (3.52 average) than repeat participants (4.57 average) due to the fact that newer NCSR participants tend to have less mature cybersecurity programs.



3

State, local and tribal peer groups continue to report overall scores that fall below the recommended minimum maturity level (5).



4

On average, entities that have been members of the MS-ISAC for 2 or more years report higher maturity scores (+34%) than entities who have been members for less than 1 year.



5

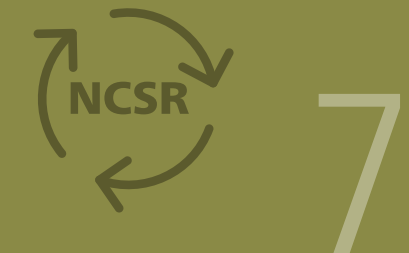
Entities that participate in the NCSR and utilize MS-ISAC Monitoring Services report higher maturity scores (+48%) than those who do not.



Albert
CIS Network Monitoring

6

Organizations who continuously participate in the NCSR report a 6% increase in their year-to-year scores.



7

All peer groups have identified the same top five security concerns for four consecutive years. **"Lack of sufficient funding"** became the top concern in 2018.



8

State governments with centralized cybersecurity governance structures typically report higher overall maturity scores (62%) than state governments with decentralized governance.



9



Key Finding 2

Changes in the question set negatively affected average scores

Methodology

In 2015, the NCSR was redesigned to align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) <https://www.nist.gov/cyberframework>. The Framework uses existing standards, guidelines, and best practices as guidance for organizations to manage and reduce cybersecurity risk. In April of 2018, NIST Version 1.1 was released. In total, 10 additional sub-categories were added (for a total of 108 sub-categories) and Supply Chain Risk Management was added as a category within the Identify Function. The 2018 NCSR was updated to align to version 1.1 of the NIST Cybersecurity Framework. Through the alignment of the NCSR to the NIST Cybersecurity Framework, MS-ISAC and DHS continue to develop a common understanding of the current cybersecurity management practices across SLTT governments.

Question Set

The NCSR question set was built upon the NIST CSF Core, with some minor alterations. The Core consists of a collection of cybersecurity-related activities organized into five main functions: **Identify**, **Protect**, **Detect**, **Respond**, and **Recover**. Each of the five functions is subdivided into a total of 23 categories and then further into 108 sub-categories.

The NCSR leverages the 108 sub-categories as the questions for the assessment. For assessment purposes, the sub-categories provide enough details for organizations to identify actionable steps to improve their cybersecurity maturity and the ability to utilize pre-existing cross-references to best practices, standards, and requirements.

Targeted Participants

The target audience for the NCSR are personnel within the SLTT community who are responsible for cybersecurity management within their organization.

NCSR Individual Reports

Upon completion of the NCSR, the participant who completed the self-assessment has access to custom individual reports that are specific to their organization. All individual self-assessments and scores are kept confidential and anonymous. The reports allow participants to develop a benchmark to gauge year-to-year progress and continuously compare themselves against their peers.

Participation by Entity Type

For the purposes of continuous data analysis and trending, respondents are grouped into three main peer groups: state, local, and tribal. (**Figure 1**)

Peer Groups Defined

The state peer group involves participation from among the 50 state governments.

The local peer group consists of any local government entity. This includes cities, counties, parishes, boroughs, K-12 public school districts, public libraries, associations, and authorities.

The tribal peer group includes participation by any federally recognized tribe. Note: Historical data for the 2015 tribal peer group is not present as 2016 marks the first year there was enough participation from tribal governments to create a separate peer group.

In 2018, the MS-ISAC was able to capture and create an additional 33 sub-sector peer groups, which are discussed in further detail in **Appendix III**. Peer groups are based on participation from a minimum of five organizations per group.

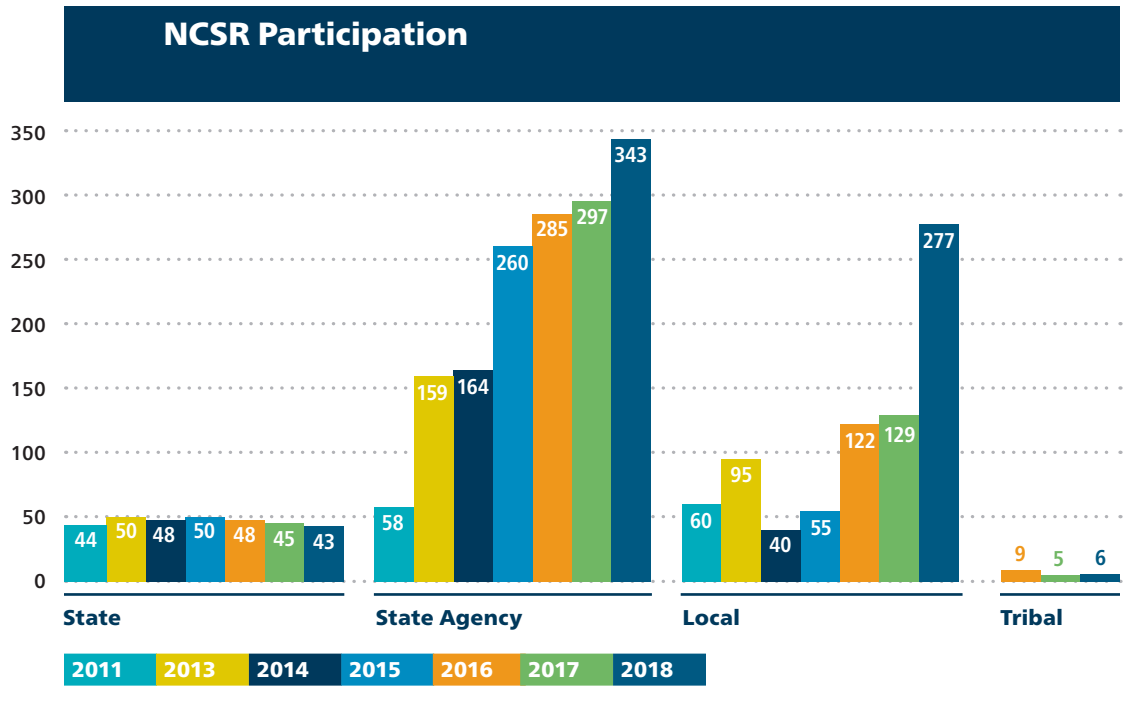


Figure 1 represents SLTT participation in the NCSR over the years.

NCSR Participation Highlights

- In 2018 there was a 41% increase in participation
- 38% of organizations participated the NCSR for the first time in 2018
- Of the 669 organizations that participated in 2018, 37% of those organizations participated in the 2015, 2016, 2017, and 2018 NCSR

41%

Participation increase

38%

First time participation

37%

Of the 669 organizations that participated in 2018, 37% have participated since 2015

3

Key Finding 3
New participants score lower than repeat participants

3.52 (New participants)
4.57 (Repeat participants)

2+ years

Key Finding 5
MS-ISAC members have higher maturity scores

7

Key Finding 7
Continuous participation boosts scores



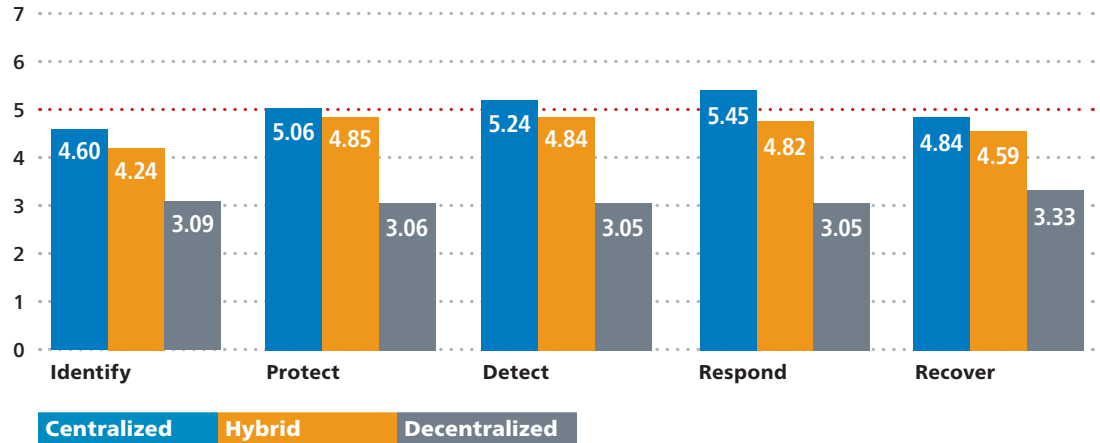
Key Finding 9

Centralized cybersecurity governance structures report higher overall maturity scores

NCSR Demographic Analysis

The following information was collected in doing an analysis on the 43 states that participated in the 2018 NCSR.

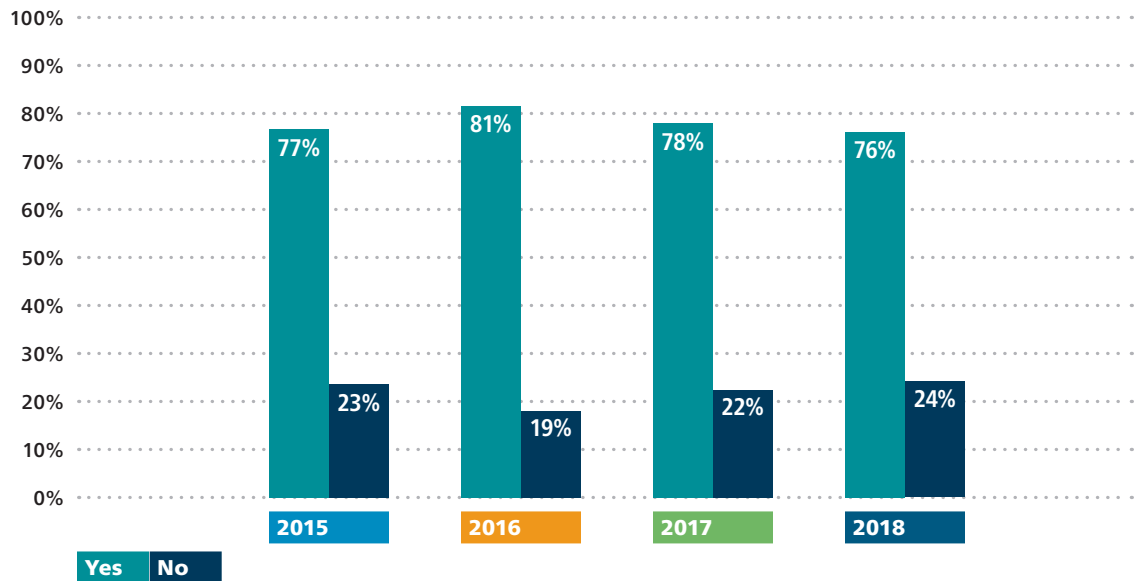
How would you categorize your cybersecurity governance structure?



According to **Figure 2**, state governments with a centralized cybersecurity governance structure report higher overall maturity scores.

The following information was collected in doing an analysis on the demographic and post-survey responses from the 2015, 2016, 2017, and 2018 NCSRs.

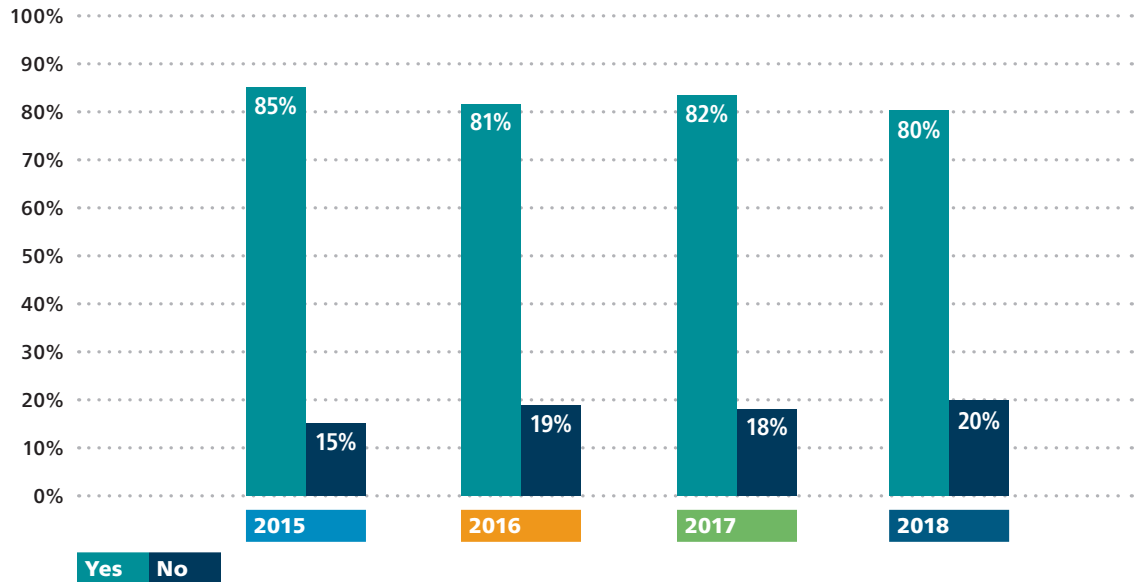
Do your top-level decision-makers receive periodic (at least annual) reports on the status of information risks, controls and/or security from the departments, divisions and/or agencies within your organization?



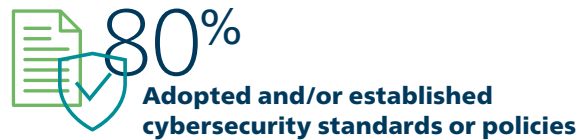
76%
Top-level decision-makers are receiving periodic reports

According to **Figure 3**, on average, 76 percent of top-level decision-makers are receiving period reports.

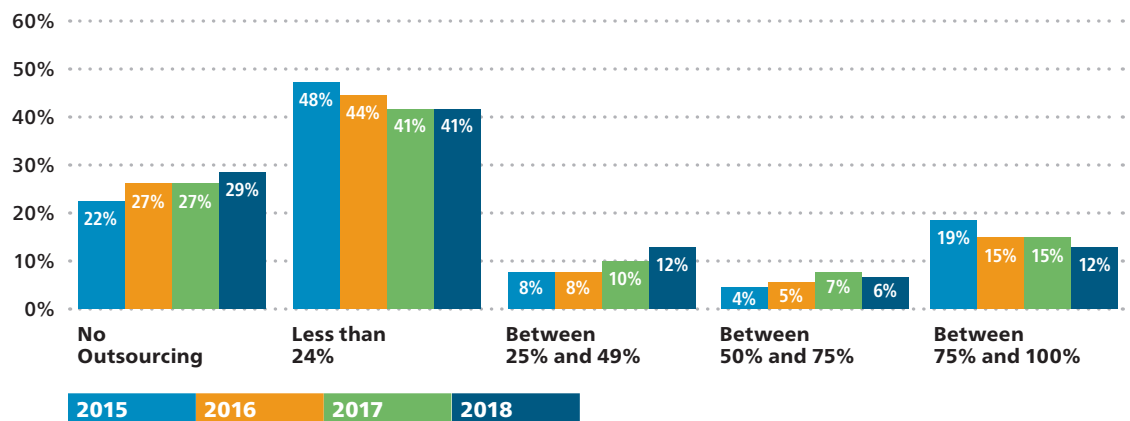
Has your organization adopted or established a set of cybersecurity executive mandates, laws, statutes, approved legislation, policies, or standards to help guide the implementation of information security controls across your organization?



According to **Figure 4**, 80 percent of respondents have adopted and/or established cybersecurity standards or policies within their organizations.

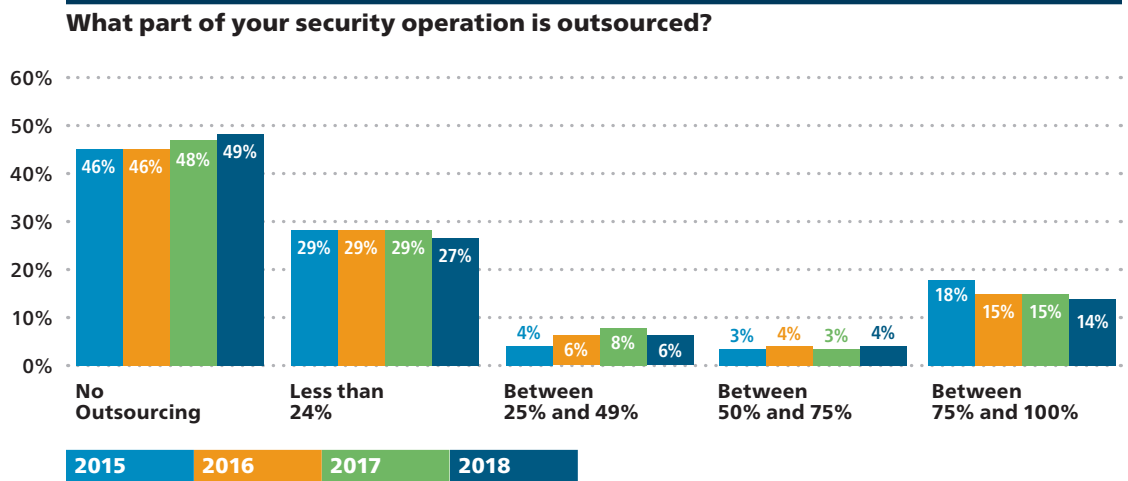


What part of your IT operation is outsourced?



According to **Figure 5**, the majority of respondents outsource less than 24 percent of their IT operations.





According to **Figure 6**, the majority of respondents are not outsourcing their security operations.

Top Five Security Concerns:

Participants have continually identified the same top five security concerns over the past four years. Their concerns below are presented in rank order from highest to lowest as identified in 2018.

- 

1 Lack of sufficient funding
- 

2 Increasing sophistication of threats
- 

3 Lack of documented processes
- 

4 Emerging technologies
- 

5 Inadequate availability of cybersecurity professionals

NCSR Maturity Scale

The NCSR utilizes a maturity scale that assesses how an organization is addressing the different activities within the NIST CSF. The maturity scale allows participants to indicate how formalized these cybersecurity activities are within their organization. Following risk management principles, the response framework allows organizations to identify which activities they have chosen not to implement because of their own risk assessment.

In order to provide a target for the SLTT community, a team of SLTT cybersecurity professionals developed a **recommended minimum maturity level** as a common baseline for the NCSR. The maturity level uses **Implementation in Process** and **Risk Formally Accepted** as the recommended minimum maturity level.

Figure 7 below provides a full breakdown of the NCSR Maturity Level response scale along with the scores associated with each maturity level.

Maturity Level		
Score	<i>The recommended minimum maturity level is set at a score of 5 and higher</i>	
7	Optimized:	Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	Tested and Verified:	Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	Implementation in Process:	Your organization has formally documented policies, standards, and procedures and is in the process of implementation.
5	Risk Formally Accepted:	Your organization has chosen not to implement based on a risk assessment.
4	Partially Documented Standards and/or Procedures:	Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy.
3	Documented Policy:	Your organization has a formal policy in place.
2	Informally Performed:	Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.
1	Not Performed:	Activities, processes and technologies are not in place to achieve the referenced objective.

Analysis by Function

This section provides a high-level analysis at the function level of the 2015, 2016, 2017, and 2018 cybersecurity maturity of the state, local, and tribal peer groups, which are displayed in the below figures.

The function scores are calculated by taking the averages within each function’s categories of the NIST CSF. For more information regarding an analysis of the categories, please see **Appendix II**.

The definition of each function is provided below, followed by an analysis of the data in three different formats:

- **Year-to-Year Function Averages:** The graphs display the year-to-year scores (averages) within each peer group across the functions, and provide an approximation to the overall maturity.
- **Year-to-Year Percentage Increase/Decrease:** The charts display the percentage increase or decrease captured from year to year within each peer group across the functions.
- **Function Analysis:** This section lists any trends and/or significant findings.

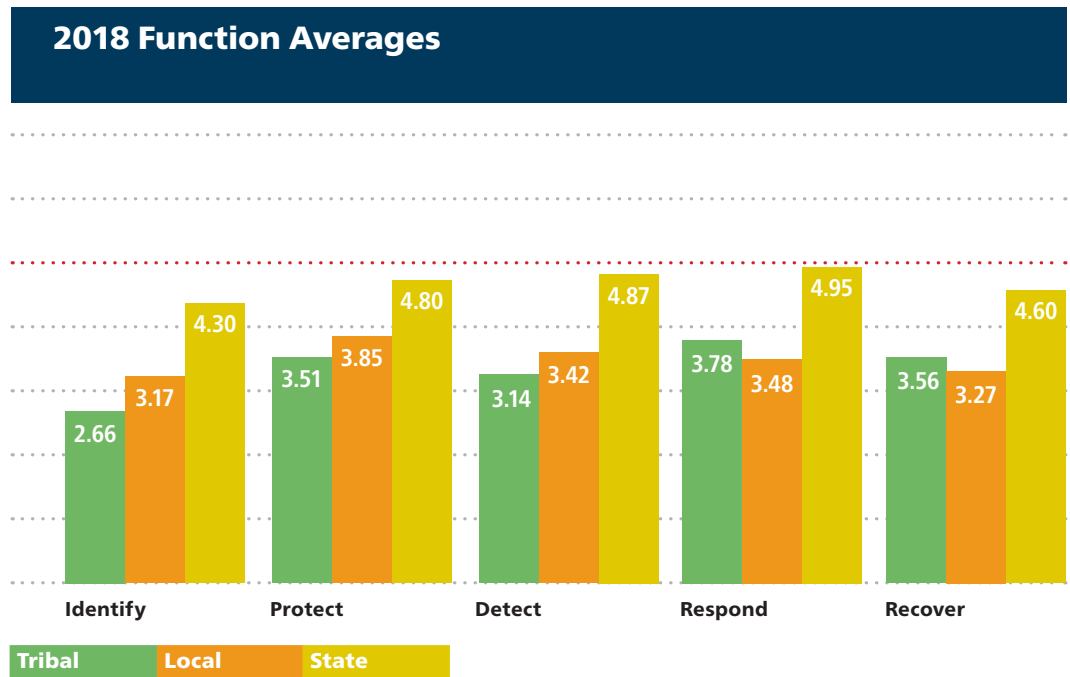


Figure 8 above displays the current 2018 cybersecurity maturity of the state, local, and tribal peer groups. The horizontal red rule on this graph and the other graphs in this report represent the recommended minimum maturity level of **Implementation in Process**, which represents the average score of 5.

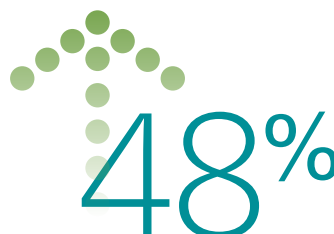
Year-to-Year Percentage Increase/Decrease Across Functions

Year	Identify	Protect	Detect	Respond	Recover	AVG
Tribal Peer Profile						
2017	-21%	2%	-10%	0%	-30%	-12%
2018	46%	7%	20%	74%	95%	48%
Local Peer Profile						
2016	15%	11%	15%	5%	8%	11%
2017	10%	8%	13%	11%	6%	10%
2018	-9%	-5%	-3%	-1%	0%	-4%
State Peer Profile						
2016	2%	2%	4%	3%	3%	3%
2017	3%	4%	2%	4%	3%	3%
2018	0%	-2%	-1%	-1%	0%	-1%

Figure 9 above represents the Year-to-Year Percentage Increase/Decrease identified within each peer group across the functions.

Overall Function Analysis

- In both 2016 and 2017, the local peer group average increase across the functions was higher than the state average *increase*. The local average increase across the functions was **11%** in 2016 and **10%** in 2017.
- In both 2016 and 2017, the average *increase* for the state peer group across the functions was **3%**.
- In 2018, the local and state peer groups reported an average *decrease* across the functions.
 - The state peer group average *decrease* across the functions in 2018 was **1%**
 - The local peer group average *decrease* across the functions in 2018 was **4%**
- In 2018 the tribal peer group reported a percentage *increase* in each of the functions.
- In 2017 the tribal peer group reported a **12% average decrease** across the functions, whereas in 2018, the tribal peer group saw an average *increase* of **48%** across the functions.
- The local and tribal peer groups continue to lag behind the state peer group in terms of overall cybersecurity maturity.



48% Tribal peer group saw an average increase of **48%** across the functions



Identify Function

The activities under this functional area are key for an organization’s understanding of their current internal culture, infrastructure, and risk tolerance. This functional area tends to be one of the lowest-rated functions for many organizations. Immature capabilities in the Identify Function may hinder an organization’s ability to effectively apply risk management principles for cybersecurity. By incorporating sound risk management principles into cybersecurity programs, organizations will be able to continuously align their efforts towards protecting their most valuable assets against the most relevant risks.



Supply Chain Risk Management was added as a category in the Identify function which resulted in 5 additional questions.

Year-to-Year Identify Function Averages

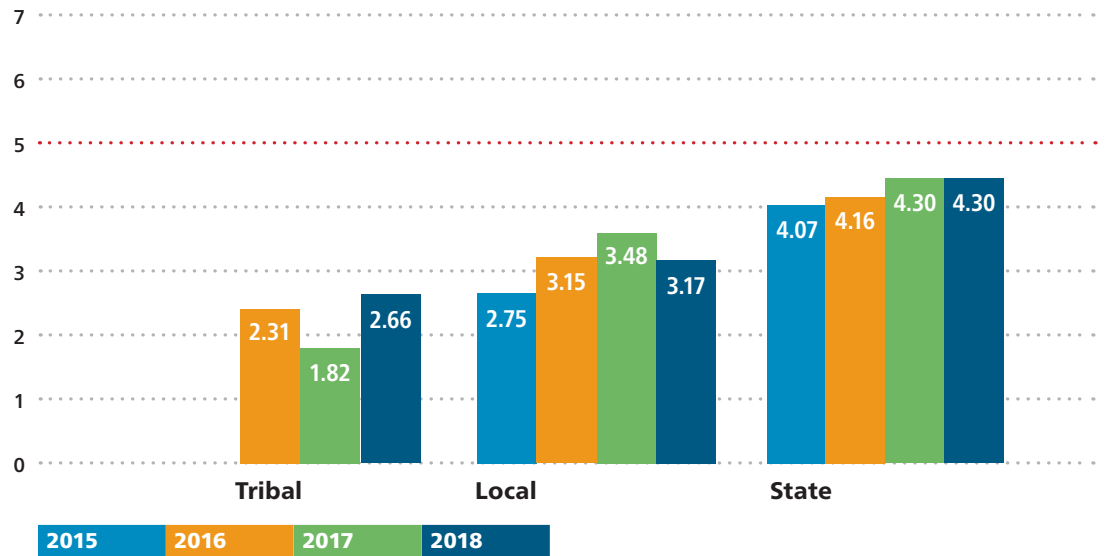


Figure 10 above represents the year-to-year average for the Identify Function across the peer profiles.

Year-to-Year Identify Function Percentage Increase/Decrease

Year	Tribal Peer Group	Local Peer Group	State Peer Group
2016	—	15%	2%
2017	-21%	10%	3%
2018	46%	-9%	0%

Figure 11 above displays the percentage increase or decrease identified in 2016, 2017, and 2018 within each peer group across the Identify Function.

Since 2015, the identify function is consistently the lowest



Identify Function Analysis

- Identify was the least mature function for each of the State, Local, and Tribal peer groups. Supply Chain Risk Management (ID.SC) was included as a new category within the Identify Function in 2018. This was recorded as the least mature category within the Identify function for the State, Local, and Tribal peer groups. This contributed to the Identify function overall being the least mature function for State, Local, and Tribal peer groups. This may be indicative of a need for national strategy and resources to assist State, Local, Tribal, and Territorial governments in assessing and mitigating supply chain risk.
- Outside of the Supply Chain Risk Management category, "Risk Management Strategy" was one of the least mature categories within the Identify function for State, Local, and Tribal organizations. This may indicate that resources to assist with formal risk assessments could be beneficial for the SLTT community.
- In 2015, 2016, 2017, and 2018 the state peer group scored lowest in the Identify Function.
- In 2018, the state peer group score remained unchanged in the Identify Function.
- In 2017 and 2018, the tribal peer group scored lowest in the Identify Function.
- A **46% increase** was reported in the Identify Function for the tribal peer group between 2017 and 2018. In 2018, the local peer group scored lowest in the Identify Function.
- In 2018, the local peer group reported the most significant percentage *decrease* (9%) in the Identify Function when comparing 2017 and 2018 data.
- Since 2015, the Identify Function is where the SLTT community has consistently reported the lowest scores amongst the functions.



Protect Function

The activities under the Protect Function pertain to different methods and activities that reduce the likelihood of cybersecurity events from happening and ensure that the appropriate controls are in place to deliver critical services. These controls are focused on preventing cybersecurity events from occurring through common attack vectors, including attacks targeting users and attacks leveraging inherent weakness in applications and network communication.

Year-to-Year Protect Function Averages

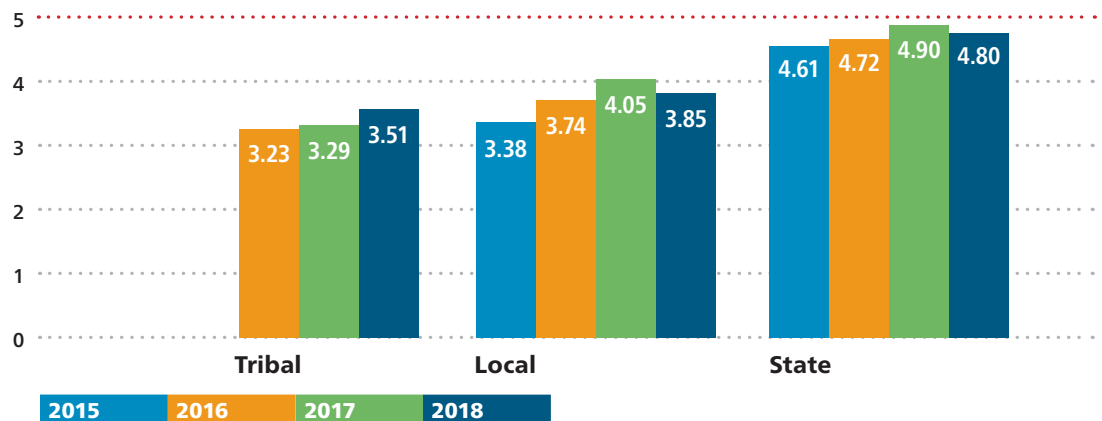


Figure 12 above represents the year-to-year average for the Protect Function across the peer groups.

Year-to-Year Protect Function Percentage Increase/Decrease


Year	Tribal Peer Group	Local Peer Group	State Peer Group
2016	—	11%	2%
2017	2%	8%	4%
2018	7%	-5%	-2%

Figure 13 above displays the percentage increase or decrease identified in 2016, 2017, and 2018 within each peer group across the Protect Function.

Protect Function Analysis

- Within the Protect function, the State peer group is above the minimum recommended maturity level of “Implementation in Process” (numerical value of 5) for the categories of “Identity Management, Authentication, & Access Control” and “Awareness Training”. This indicates that attention has been focused on policy and procedure development for protecting access assets, as well as providing security training to both technical and non-technical employees.
- In 2015, 2016, 2017, and 2018 the local peer group scored highest in the Protect Function.
- In 2018, the state peer group saw the most significant percentage decrease (2%) within the Protect Function when comparing 2017 and 2018 data.
- In 2016 and 2017 the tribal peer group scored highest in the Protect Function.
- In 2018, the tribal peer group saw the least significant percentage increase (7%) within the Protect Function when comparing 2017 and 2018 data.

 **Local peer group scored highest for 4 years straight**

 **State peer group recorded the most significant decrease from 2017 to 2018**



Detect Function

The quicker an organization is able to detect a cybersecurity incident, the better positioned it is to be able to remediate the problem and reduce the consequences of the event. Activities found within the Detect Function pertain to an organization’s ability to identify incidents. These controls are becoming more important as the quantity of logs and events occurring within an environment can be overwhelming to handle and can make it difficult to identify the key concerns. This function continues to represent the largest maturity gap between state and local governments.



Albert
CIS Network Monitoring

Key Finding 6

Participants utilizing monitoring services report higher maturity

Year-to-Year Detect Function Averages

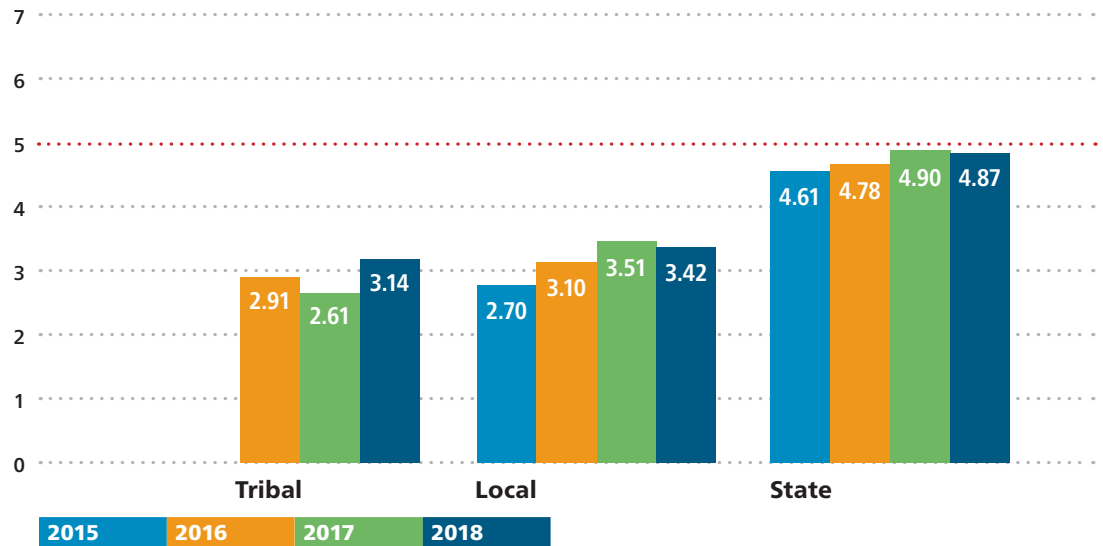


Figure 14 above represents the year-to-year average for the Detect Function across the peer groups.

Year-to-Year Detect Function Percentage Increase/Decrease

Year	Tribal Peer Group	Local Peer Group	State Peer Group
2016	—	15%	4%
2017	-10%	13%	2%
2018	20%	-3%	-1%

Figure 15 above displays the percentage increase or decrease identified in 2016, 2017, and 2018 within each peer group across the Detect Function.

Detect Function Analysis

- Within the Detect function, Local entities scored lowest in Anomalies & Events, which measures capabilities related to detecting anomalous activity and understanding the potential impact of events that are detected. We believe this could indicate that Local entities need more resources to establish and understand a baseline of normal activity on their networks, in order to be able to identify anomalies. They should map internal and external data flows to understand data movement and establish a data life cycle with policies regarding management and protection of data.
- In 2018, the tribal peer group reported a 20% increase in the Detect Function.
- In 2018, the state peer group reported a 1% decrease and the local peer group reported a 3% decrease in the Detect Function.



Tribal peer group reported a 20% increase



Respond Function

An organization’s ability to quickly and appropriately respond to an incident plays a large role in reducing the incident’s consequences. As such, the activities within the Respond Function examine how an organization plans, analyzes, communicates, mitigates, and improves its response capabilities. For many organizations, integration and cooperation with other entities is key. Many organizations do not have the internal resources to handle all components of incident response. One example is the ability to conduct forensics after an incident, which helps organizations identify and remediate the original attack vector. This gap can be addressed through resource sharing within the SLTT community and leveraging organizations such as MS-ISAC and DHS’s National Cybersecurity and Communications Integration Center (NCCIC), which have dedicated resources to provide incident response at no cost to the victim.

Year-to-Year Respond Function Averages

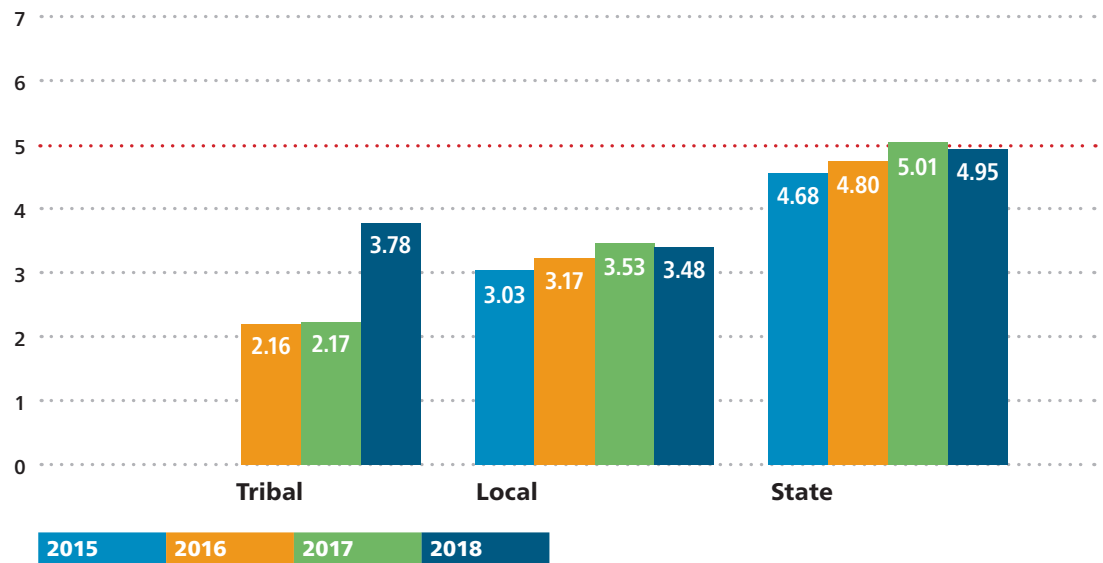


Figure 16 above represents the year-to-year average for the Respond Function across the peer groups.

Year-to-Year Respond Function Percentage Increase/Decrease

Year	Tribal Peer Group	Local Peer Group	State Peer Group
2016	—	5%	3%
2017	0%	11%	4%
2018	74%	-1%	-1%

Figure 17 above displays the percentage increase or decrease identified in 2016, 2017, and 2018 within each peer group across the Respond Function.

Respond Function Analysis

- Within the Respond function, the Improvements category is lowest for the State and Local peer groups. State and Local governments could allocate more time and develop policy to properly document and analyze lessons learned following incident response and exercises. Additionally, response strategies should be updated, if necessary, following incidents and exercises.
- Within the Communications category of the Respond function, the least mature response is specific to voluntary information sharing with external stakeholders to achieve broader cybersecurity situational awareness. The Local average score for this specific subcategory is 3.25. Local organizations could become more mature by sharing information with regional and Federal organizations or resources.
- In 2015, 2016, 2017, and 2018, the state peer group scored highest in the Respond Function.
- In 2018, the tribal peer group scored highest in the Respond Function.



State peer group scored highest for 4 years straight



Recover Function

Activities within the Recover Function pertain to an organization’s ability to return to its baseline after an incident has occurred. Such controls are focused not only on activities to recover from the incident, but also on many of the components dedicated to managing response plans throughout their lifecycle.

Year-to-Year Recover Function Averages

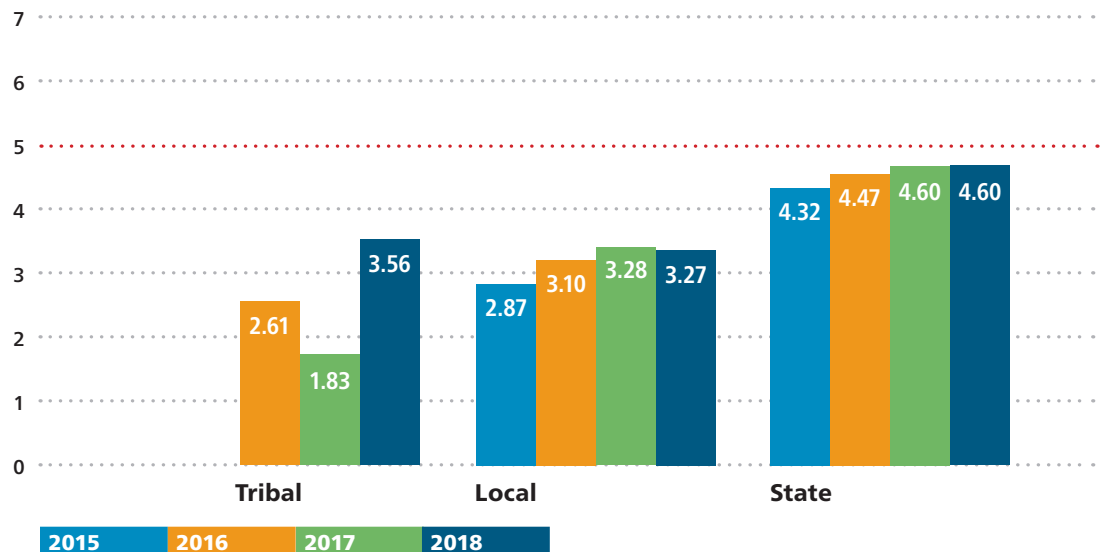


Figure 18 above represents the year-to-year average for the Recover Function across the peer groups.


Year-to-Year Recover Function Percentage Increase/Decrease

Year	Tribal Peer Group	Local Peer Group	State Peer Group
2016	—	8%	3%
2017	-30%	6%	3%
2018	95%	0%	0%

Figure 19 above displays the percentage increase or decrease identified in 2016, 2017, and 2018 within each peer group across the Recover Function.

Recover Function Analysis

- State and Local Organizations maintained the same scores in the Recover function for the past two years. We recognize that organizations need assistance to develop and implement policies and procedures for regularly exercising and enhancing incident response and business resiliency plans. This would result in an increase of maturity in the Recover function.
- In 2017 the local peer group scored lowest in the Recover Function.
- In 2018, the local peer group did not report a percentage increase/decrease within the Recover Function.
- In 2018, the state peer group did not report a percentage increase/decrease within the Recover Function.
- In 2018, the tribal peer group reported the most significant percentage increase (95%) in the Recover Function.

 **95%** Tribal peer group reported a 95% increase

0%
Both state & local peer groups reported no percentage change

Partners

The U.S. Department of Homeland Security (DHS) has partnered with the Multi-State Information Sharing & Analysis Center (MS-ISAC), the National Association of State Chief Information Officers (NASCIO), and the National Association of Counties (NACo) to develop the Nationwide Cybersecurity Review.

U.S. Department of Homeland Security

DHS is responsible for safeguarding our nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. The National Protection and Programs Directorate leads DHS' efforts to secure cyberspace and cyber infrastructure. For additional information, please visit www.dhs.gov/cyber.

Multi-State Information Sharing & Analysis Center

Grant-funded by DHS, MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. The MS-ISAC 24/7 Security Operations Center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation, and incident response. For more information about the MS-ISAC, please visit <https://www.cisecurity.org/ms-isac/>.

National Association of State Chief Information Officers

NASCIO's mission is to foster government excellence through quality business practices, information management, and technology policy.

Founded in 1969, NASCIO is a nonprofit, 501(c)(3) association representing state chief information officers and information technology executives and managers from the states, territories, and the District of Columbia. The primary state members are senior officials from state government who have executive-level and statewide responsibility for information technology leadership. State officials who are involved in agency level information technology management may participate as associate members. Representatives from federal, municipal, international government, and nonprofit organizations may also participate as members. Private-sector firms join as corporate members and participate in the Corporate Leadership Council. For more information about NASCIO, please visit <https://www.nascio.org/>.

National Association of Counties

The National Association of Counties (NACo) is the only national organization that represents county governments in the United States.

Founded in 1935, NACo provides essential services to the nation's 3,069 counties. NACo advances issues with a unified voice before the federal government, improves the public's understanding of county government, assists counties in finding and sharing innovative solutions through education and research, and provides value-added services to save counties and taxpayers money. For more information about NACo, please visit <http://www.naco.org/>.

GMIS International

GMIS International is a professional IT association of worldwide government IT leaders dedicated to providing best practice solutions for initiatives by providing its members with enhanced professional development, training, conferences, awards, and networking while offering leadership through advocacy, research, and shared experiences. GMIS International's primary mission is to leverage the collective knowledge of its members.

In 1971, a group of IT professionals, realizing the need to foster the sharing of experiences among all levels of government involved in providing IT services, organized GMIS International. Today, there are members in 36 states, plus 15 state chapter affiliates and six international affiliates.

Membership in GMIS is open to public sector agencies at any level of government (federal, state, county, city, etc.) including schools (K-12, community college and university) and special districts. Corporate memberships are also available.



Appendix I: Acronyms

DHS	U.S. Department of Homeland Security
MS-ISAC	Multi-State Information Sharing & Analysis Center
NACo	National Association of Counties
NASCIO	National Association of State Chief Information Officers
NCCIC	National Cybersecurity and Communications Integration Center
NCSR	Nationwide Cybersecurity Review
NIST	National Institute of Standards and Technology
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
SLTT	State, Local, Tribal, and Territorial

Appendix II: Peer Group Detailed Data Analysis for Function Categories

This appendix provides a detailed year-to-year analysis of the categories within the functions of the NIST CSF for the state, local, and tribal peer groups.

The definition of the function and categories within each function are provided and accompanied by an analysis of the data in three different ways:

- **Year-to-Year Category Averages:** The graphs display the year-to-year scores within each peer group across the categories within each function and provide an approximation as to the overall maturity.
- **Year-to-Year Category Percentage Increase/Decrease:** The charts display the percentage increase/decrease captured from year to year within each peer group across the categories of the functions.
- **Category Percentage Increase/Decrease Highlights:** These sections provide highlights that are displayed in two different formats:
 - **Moderate:** Lists any percentage increases and/or decreases between 5 percent and 9 percent in each of the function categories across the peer groups in 2016, 2017, and 2018.
 - **Significant:** Lists any percentage increases and/or decreases of 10 percent or more in each of the function categories across the peer groups in 2016, 2017, and 2018.

The categories' scores are calculated by averaging the sub-categories within each category of the NIST CSF.

Identify Function

The activities found within this functional area are key for an organization's understanding of their current internal culture, infrastructure, and risk tolerance. This functional area tends to be one of the lowest functions rated for many organizations. Immature capabilities in the Identify Function may hinder an organization's ability to effectively apply risk management principles for cybersecurity. By incorporating sound risk management principles into cybersecurity programs, organizations will be able to continuously align their efforts towards protecting their most valuable assets against the most relevant and pertinent risks.

Identify Categories

- **Asset Management:** The data, personnel, devices, system, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
- **Business Environment:** The organization's missions, objectives, stakeholders, and activities are understood and prioritized. This information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
- **Governance:** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
- **Risk Assessment:** The organization understands the cybersecurity risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
- **Risk Management Strategy:** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
- **Supply Chain Risk Management:** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.



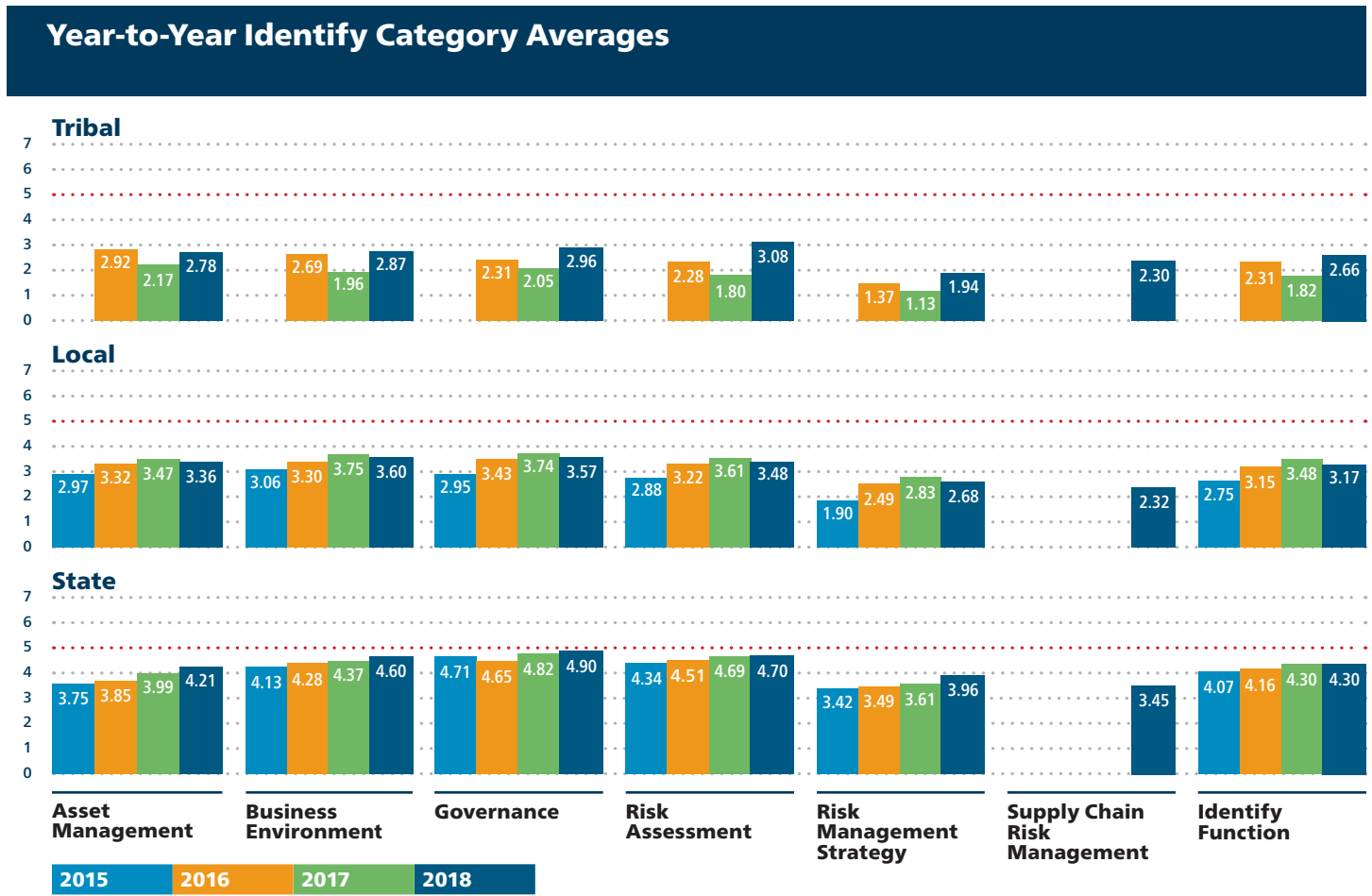


Figure 20 above represents the year-to-year averages for the Identify categories across the peer groups.

Year-to-Year Identify Categories Percentage Increase/Decrease

Year	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy	Supply Chain Risk Management	Identify Function
Tribal Peer Profile							
2017	-26%	-27%	-11%	-21%	-18%	—	-21%
2018	28%	46%	44%	71%	71%	—	46%
Local Peer Profile							
2016	12%	8%	16%	12%	31%	—	15%
2017	5%	14%	9%	12%	14%	—	10%
2018	-3%	-4%	-5%	-4%	-5%	—	-9%
State Peer Profile							
2016	3%	4%	-1%	4%	2%	—	2%
2017	4%	2%	4%	4%	4%	—	3%
2018	6%	5%	2%	0%	10%	—	0%

Figure 21 above displays the percentage increase or decrease identified in 2016, 2017, and 2018 within each peer group across the Identify categories.

Identify Categories Percentage Increase/Decrease Highlights

Moderate: The below image lists any percentage increase and/or decrease between 5 percent and 9 percent that was identified in the Identify categories across the peer groups in 2016, 2017, and 2018.

Increase/Decrease of 5% to 9%	
2016 Local	<ul style="list-style-type: none"> • 8% increase identified in Business Environment
2017 Local	<ul style="list-style-type: none"> • 5% increase identified in Asset Management • 9% increase identified in Governance
2018 State	<ul style="list-style-type: none"> • 6% increase identified in Asset Management • 5% increase identified in Business Environment
2018 Local	<ul style="list-style-type: none"> • 5% decrease identified in Governance • 5% decrease identified in Risk Management Strategy

Significant: The below image lists any percentage increase and/or decrease of 10 percent or more that was identified in the Identify categories across the peer groups in 2016, 2017, and 2018.

Increase/Decrease of 10% or More	
2016 Local	<ul style="list-style-type: none"> • 12% increase identified in Asset Management • 16% increase identified in Governance • 12% increase identified in Risk Assessment • 31% increase identified in Risk Management Strategy
2017 Local	<ul style="list-style-type: none"> • 14% increase identified in Business Environment • 12% increase identified in Risk Assessment • 14% increase identified in Risk Management Strategy
2017 Tribal	<ul style="list-style-type: none"> • 26% decrease identified in Asset Management • 27% decrease identified in Business Environment • 11% decrease identified in Governance • 21% decrease identified in Risk Assessment • 18% decrease identified in Risk Management Strategy
2018 State	<ul style="list-style-type: none"> • 10% increase identified in Risk Management Strategy
2018 Tribal	<ul style="list-style-type: none"> • 28% increase identified in Asset Management • 46% increase identified in Business Environment • 44% increase identified in Governance • 71% increase identified in Risk Assessment • 71% increase identified in Risk Management Strategy

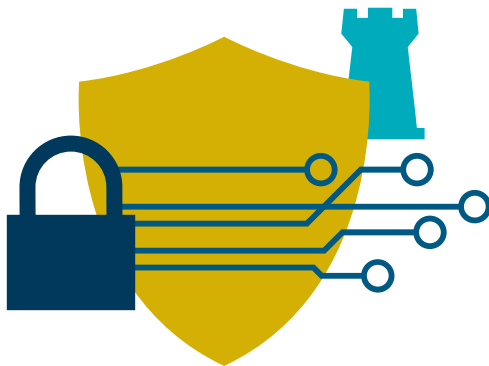


Protect Function

The activities under the Protect Function pertain to different methods and activities that reduce the likelihood of cybersecurity events from happening and ensure that the appropriate controls are in place to deliver critical services. These controls are focused on preventing cybersecurity events from occurring through common attack vectors, including attacks targeting users and attacks leveraging inherent weakness in applications and network communications.

Protect Categories

- **Access Control:** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
- **Awareness and Training:** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
- **Data Security:** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- **Information Protection Processes & Procedures:** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
- **Maintenance:** Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
- **Protective Technology:** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.



Year-to-Year Protect Category Averages

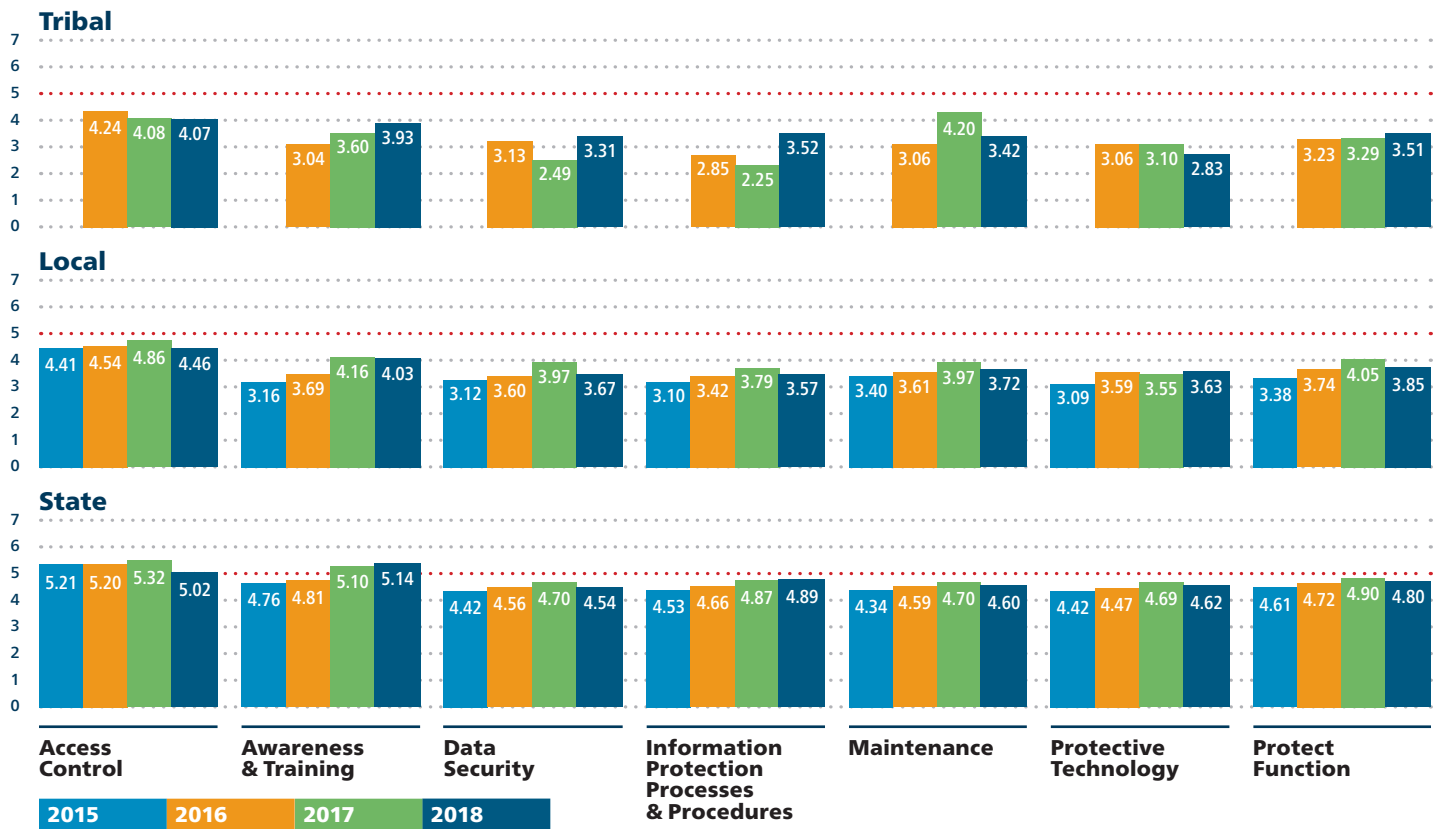


Figure 22 above represents the year-to-year averages for the Protect categories across the peer groups.

Year-to-Year Protect Categories Percentage Increase/Decrease

Year	Access Control	Awareness & Training	Data Security	Information Protection Processes & Procedures	Maintenance	Protective Technology	Protect Function
Tribal Peer Profile							
2017	-4%	18%	-20%	-21%	37%	1%	2%
2018	0%	9%	33%	56%	-19%	-9%	7%
Local Peer Profile							
2016	3%	17%	15%	10%	6%	16%	11%
2017	7%	13%	10%	11%	10%	-1%	8%
2018	-8%	-3%	-7%	-6%	-6%	2%	-5%
State Peer Profile							
2016	0%	1%	3%	3%	6%	1%	2%
2017	2%	6%	3%	5%	2%	5%	4%
2018	-6%	1%	-3%	0%	-2%	-1%	-2%

Figure 23 above displays the percentage increase or decrease identified in 2016, 2017, and 2018 within each peer group across the Protect categories.

Protect Categories Percentage Increase/Decrease Highlights

Moderate: The below image lists any percentage increase and/or decrease between 5 percent and 9 percent that was identified in the Protect categories across the peer groups in 2016, 2017, and 2018.

Increase/Decrease of 5% to 9%	
2016 State	• 6% increase identified in Maintenance
2016 Local	• 6% increase identified in Maintenance
2017 State	<ul style="list-style-type: none"> • 6% increase identified in Awareness & Training • 5% increase identified in Information Protection Processes & Procedures • 5% increase identified in Protective Technology
2017 Local	• 7% increase identified in Access Control
2018 State	• 6% decrease identified in Access Control
2018 Local	<ul style="list-style-type: none"> • 8% decrease identified in Access Control • 7% decrease identified in Data Security • 6% decrease identified in Information Protection Processes & Procedures • 6% decrease identified in Maintenance
2018 Tribal	<ul style="list-style-type: none"> • 9% increase identified in Awareness and Training • 9% decrease identified in Protective Technology



Significant: The below image lists any percentage increase and/or decrease of 10 percent or more that was identified in the Protect categories across the peer groups in 2016, 2017, and 2018.

Increase/Decrease of 10% or More	
2016 Local	<ul style="list-style-type: none"> • 17% increase identified in Awareness & Training • 15% increase identified in Data Security • 10% increase identified in Information Protection Processes & Procedures • 16% increase identified in Protective Technology
2017 Local	<ul style="list-style-type: none"> • 13% increase identified in Awareness & Training • 10% increase identified in Data Security • 11% increase identified in Information Protection Processes & Procedures • 10% increase identified in Maintenance
2017 Tribal	<ul style="list-style-type: none"> • 18% increase identified in Awareness & Training • 20% decrease identified in Data Security • 21% decrease identified in Information Protection Processes & Procedures • 37% increase identified in Maintenance
2018 Tribal	<ul style="list-style-type: none"> • 33% increase identified in Data Security • 56% increase identified in Information Protection Processes & Procedures • 19% decrease identified in Maintenance



Detect Function

The quicker an organization is able to detect a cybersecurity incident, the better postured it is to be able to remediate the problem and reduce the consequences of the event. Activities found within the Detect Function pertain to an organization’s ability to identify incidents. These controls are becoming more important as the quantity of logs and events occurring within an environment can be overwhelming to handle and can make it difficult to identify the key concerns. This function represented the largest maturity gap between local and state governments.

Detect Categories

- **Anomalies and Events:** Anomalous activity is detected in a timely manner and the potential impact of events is understood.
- **Security Continuous Monitoring:** The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
- **Detection Processes:** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

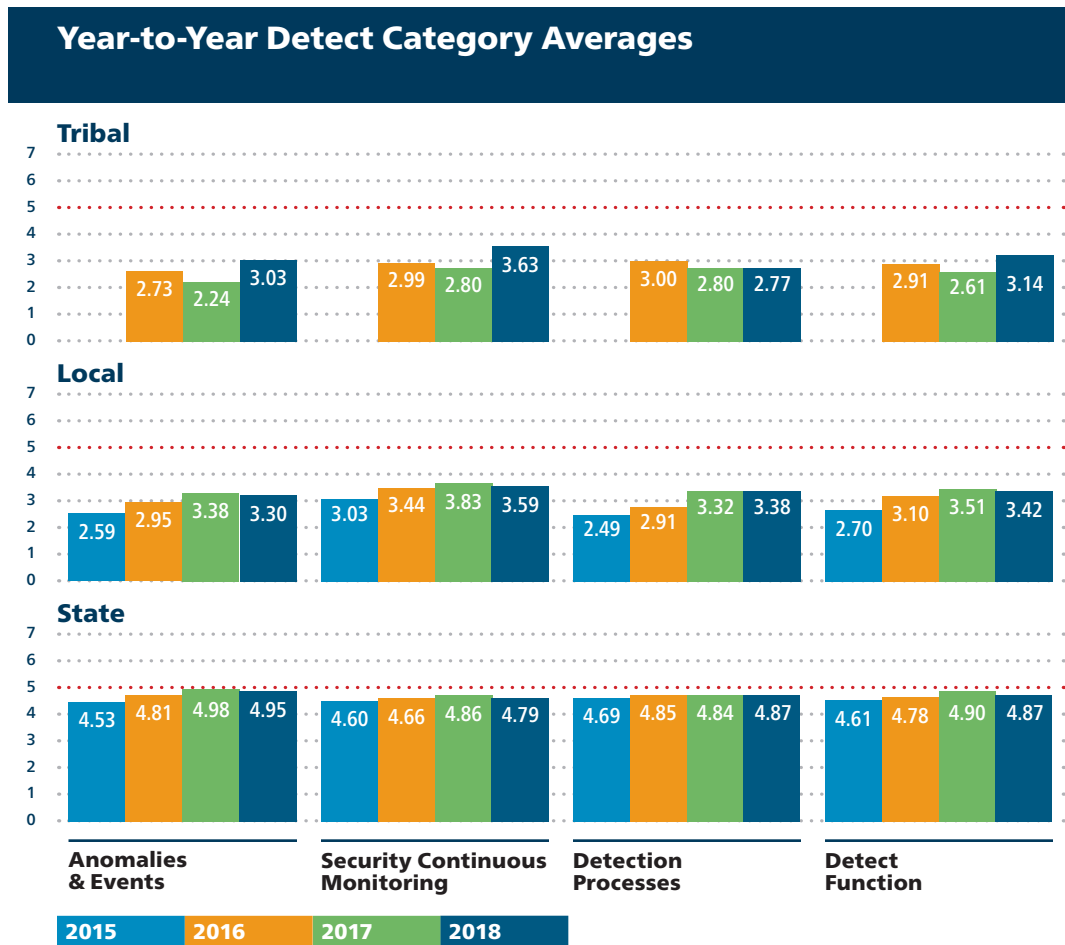


Figure 24 above represents the year-to-year averages for the Detect categories across the peer groups.

Year-to-Year Detect Categories Percentage Increase/Decrease				
Year	Anomalies & Events	Security Continuous Monitoring	Detection Processes	Detect Function
Tribal Peer Profile				
2017	-18%	-6%	-7%	-10%
2018	35%	30%	-1%	20%
Local Peer Profile				
2016	14%	14%	17%	15%
2017	14%	11%	14%	13%
2018	-2%	-6%	2%	-3%
State Peer Profile				
2016	6%	1%	3%	4%
2017	4%	4%	0%	2%
2018	-1%	-1%	1%	-1%

Figure 25 above displays the percentage increase or decrease identified in 2016, 2017, and 2018 within each peer group across the Detect categories.

Detect Categories Percentage Increase/Decrease Highlights

Moderate: The below image lists any percentage increase and/or decrease between 5 percent and 9 percent that was identified in the Detect categories across the peer groups in 2016, 2017, and 2018.

Increase/Decrease of 5% to 9%	
2016 State	• 6% increase identified in Anomalies & Events
2017 Tribal	• 6% decrease identified in Security Continuous Monitoring • 7% decrease identified in Detection Processes
2018 Local	• 6% decrease identified in Security Continuous Monitoring

Significant: The below image lists any percentage increase and/or decrease of 10 percent or more that was identified in the Detect categories across the peer groups in 2016, 2017, and 2018.

Increase/Decrease of 10% or More	
2016 Local	• 14% increase identified in Anomalies & Events • 14% increase identified in Security Continuous Monitoring • 17% increase identified in Detection Processes
2017 Local	• 14% increase identified in Anomalies & Events • 11% increase identified in Security Continuous Monitoring • 14% increase identified in Detection Processes
2017 Tribal	• 18% decrease identified in Anomalies & Events
2018 Tribal	• 35% increase identified in Anomalies & Events • 30% increase identified in Security Continuous Monitoring

35%
Tribal Anomalies & Events

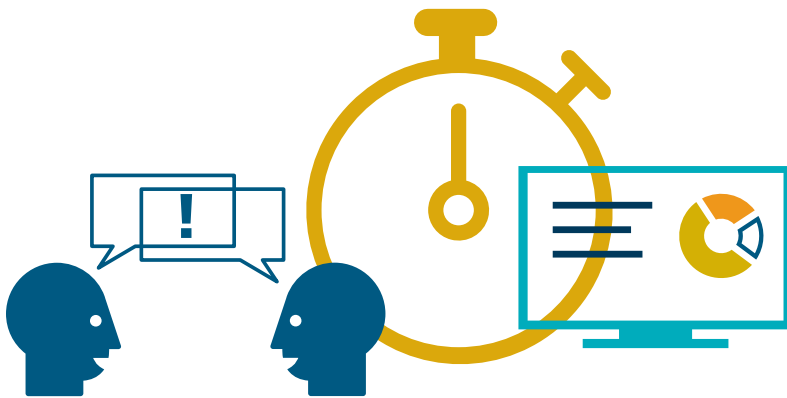
30%
Tribal Security Continuous Monitoring

➤ Respond Function

An organization's ability to quickly and appropriately respond to an incident plays a large role in reducing the incident's consequences. As such, the activities within the Respond Function examine how an organization plans, analyzes, communicates, mitigates, and improves its response capabilities. For many organizations, integration and cooperation with other entities is key. Many organizations do not have the internal resources to handle all components of incident response. One example is the ability to conduct forensics after an incident, which helps organizations identify and remediate the original attack vector. This gap can be addressed through resource sharing within the SLTT community and leveraging organizations such as MS-ISAC and DHS's National Cybersecurity and Communications Integration Center (NCCIC), which have dedicated resources to provide incident response at no cost to the victim.

Respond Categories

- **Response Planning:** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
- **Communications:** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
- **Analysis:** Analysis is conducted to ensure adequate response and support recovery activities.
- **Mitigation:** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
- **Improvements:** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.



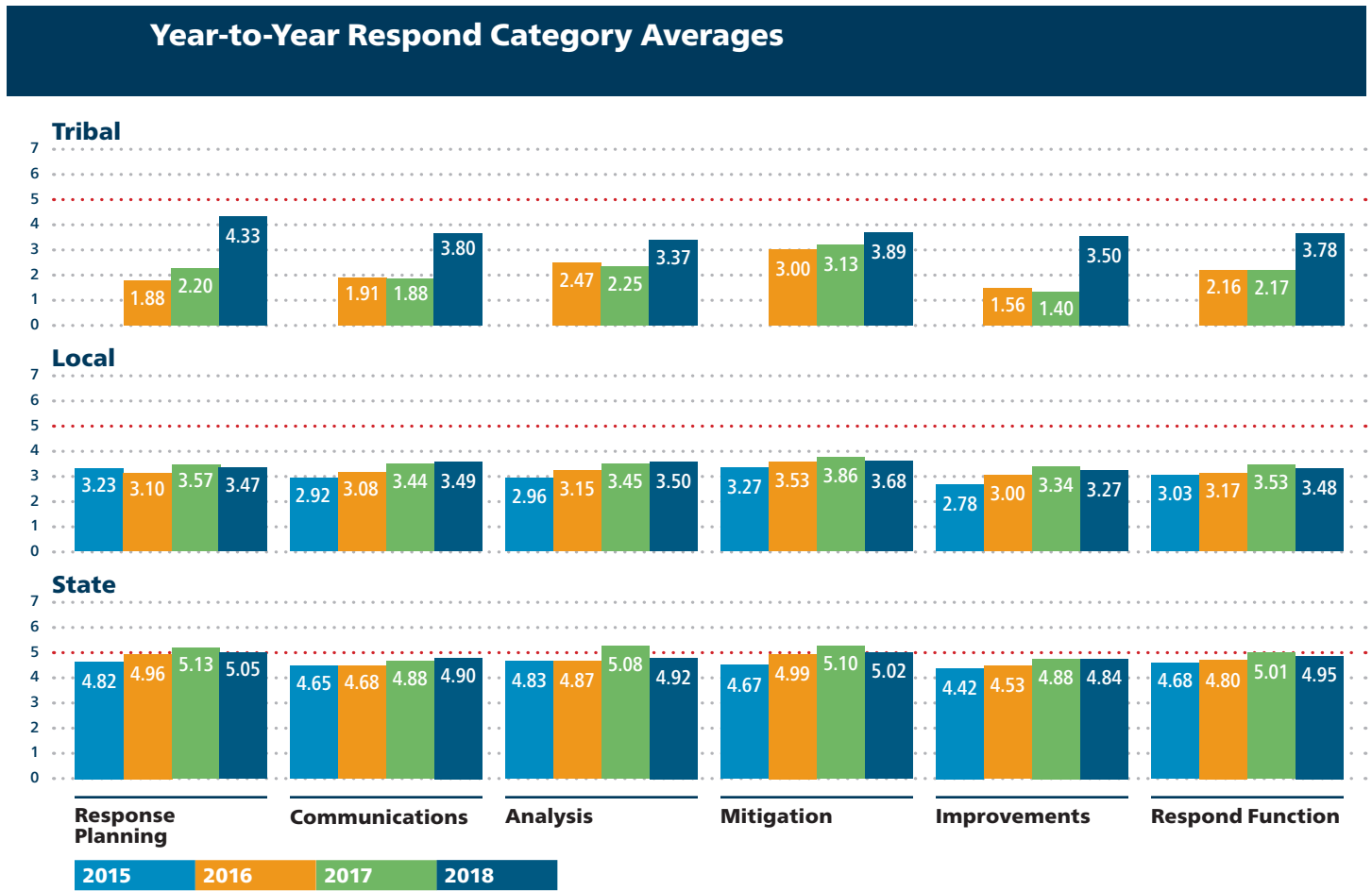


Figure 26 above represents the year-to-year averages for the Respond categories across the peer groups.

Year-to-Year Respond Categories Percentage Increase/Decrease

Year	Response Planning	Communications	Analysis	Mitigation	Improvements	Respond Function
Tribal Peer Profile						
2017	17%	-2%	-9%	4%	-10%	0%
2018	97%	102%	50%	24%	150%	74%
Local Peer Profile						
2016	-4%	5%	6%	8%	8%	5%
2017	15%	12%	10%	9%	11%	11%
2018	-3%	2%	1%	-5%	-2%	-1%
State Peer Profile						
2016	3%	1%	1%	7%	2%	3%
2017	3%	4%	4%	2%	8%	4%
2018	-2%	0%	-3%	-2%	-1%	-1%

Figure 27 above displays the percentage increase or decrease identified in 2016, 2017, and 2018 within each peer group across the Respond categories.

Respond Categories Percentage Increase/Decrease Highlights

Moderate: The below image lists any percentage increase and/or decrease between 5 percent and 9 percent that was identified in the Respond categories across the peer groups in 2016, 2017, and 2018.

Increase/Decrease of 5% to 9%	
2016 State	• 7% increase identified in Mitigation
2016 Local	<ul style="list-style-type: none"> • 5% increase identified in Communications • 6% increase identified in Analysis • 8% increase identified in Mitigation • 8% increase identified in Improvements
2017 State	• 8% increase identified in Improvements
2017 Local	• 9% increase identified in Mitigation
2017 Tribal	• 9% decrease identified in Analysis
2018 Local	• 5% decrease identified in Mitigation

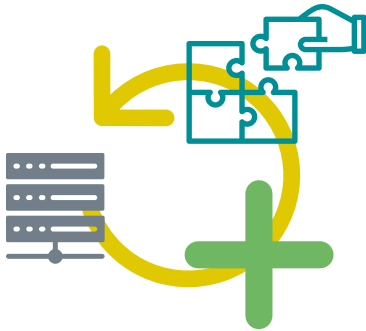
Significant: The below image lists any percentage increase and/or decrease of 10 percent or more that was identified in the Respond categories across the peer groups in 2016, 2017, and 2018.

Increase/Decrease of 10% or More	
2017 Local	<ul style="list-style-type: none"> • 15% increase identified in Response Planning • 12% increase identified in Communications • 10% increase identified in Analysis • 11% increase identified in Improvements
2017 Tribal	<ul style="list-style-type: none"> • 17% increase identified in Response Planning • 10% decrease identified in Improvements
2018 Tribal	<ul style="list-style-type: none"> • 97% increase identified in Response Planning • 102% increase identified in Communications • 50% Increase identified in Analysis • 24% Increase identified in Mitigation • 150% increase identified in Improvements



Recover Function

Activities within the Recover Function pertain to an organization’s ability to return to its baseline after an incident has occurred. Such controls are focused not only on activities to recover from the incident, but also on many of the components dedicated to managing response plans throughout their lifecycle.



Recover Categories

- **Recovery Planning:** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
- **Improvements:** Recovery planning and processes are improved by incorporating lessons learned into future activities.
- **Communications:** Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other Computer Security Incident Response Teams, and vendors.

Year-to-Year Recover Category Averages

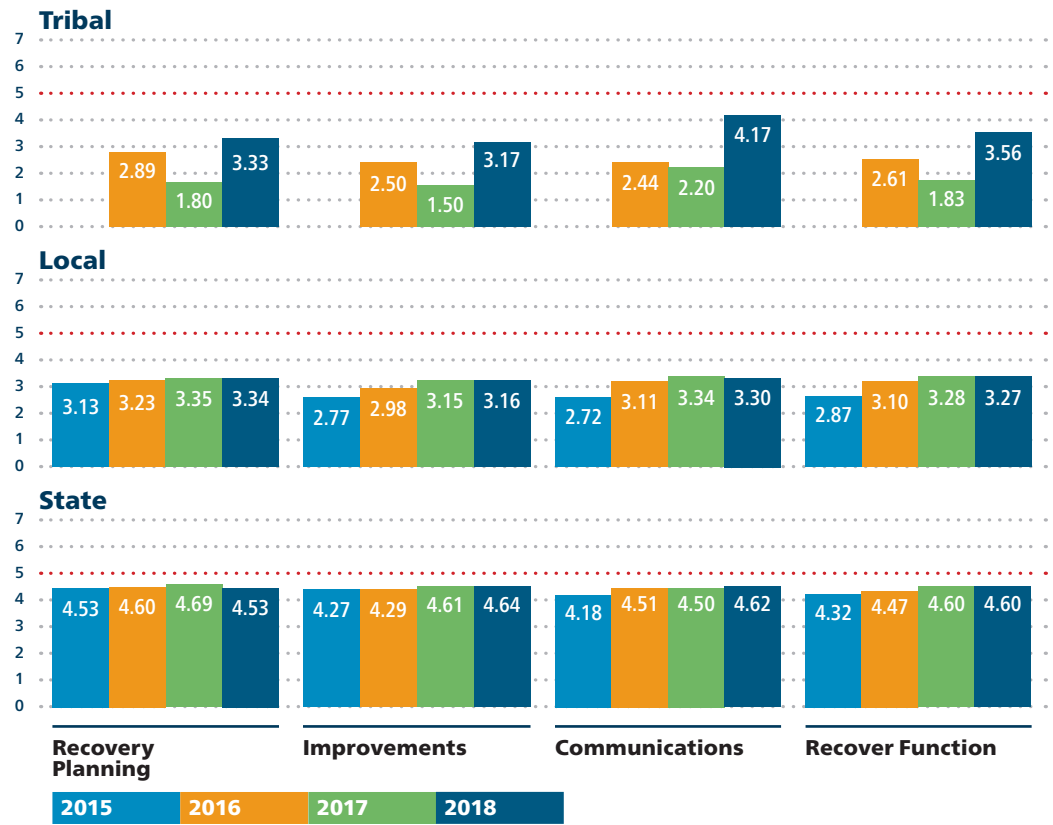


Figure 28 above represents the year-to-year averages for the Recover categories across the peer groups.

Year-to-Year Recover Categories Percentage Increase/Decrease

Year	Recovery Planning	Improvements	Communications	Recover Function
Tribal Peer Group				
2017	-38%	-40%	-10%	-30%
2018	85%	111%	90%	95%
Local Peer Group				
2016	3%	8%	14%	8%
2017	4%	6%	8%	6%
2018	0%	0%	-1%	0%
State Peer Group				
2016	2%	0%	8%	3%
2017	2%	7%	0%	3%
2018	-3%	1%	3%	0%

Figure 29 above displays the percentage increase or decrease identified in 2016, 2017, and 2018 within each peer group across the Recover categories.

Recover Categories Percentage Increase/Decrease Highlights

Moderate: The below image lists any percentage increase and/or decrease between 5 percent and 9 percent that was identified in the Recover categories across the peer groups in 2016, 2017, and 2018.

Increase/Decrease of 5% to 9%	
2016 State	• 8% increase identified in Communications
2016 Local	• 8% increase identified in Improvements
2017 State	• 7% increase identified in Improvements
2017 Local	• 6% increase identified in Improvements • 8% increase identified in Communications

Significant: The below image lists any percentage increase or decrease of 10 percent or more that was identified in the Recover categories across the peer groups in 2016, 2017, and 2018.

Increase/Decrease of 10% or More	
2016 Local	• 14% increase identified in Communications
2017 Tribal	• 38% decrease identified in Recovery Planning • 40% decrease identified in Improvements • 10% decrease identified in Communications
2018 Tribal	• 85% increase identified in Recovery Planning • 111% increase identified in Improvements • 90% increase identified in Communications



Appendix III: Sub-Sector Peer Groups

In 2018, the NCSR captured **33** additional peer groups based on sub-sectors. The sub-sector peer groups were created for any sub-sector that had a minimum of five organizations complete the NCSR.

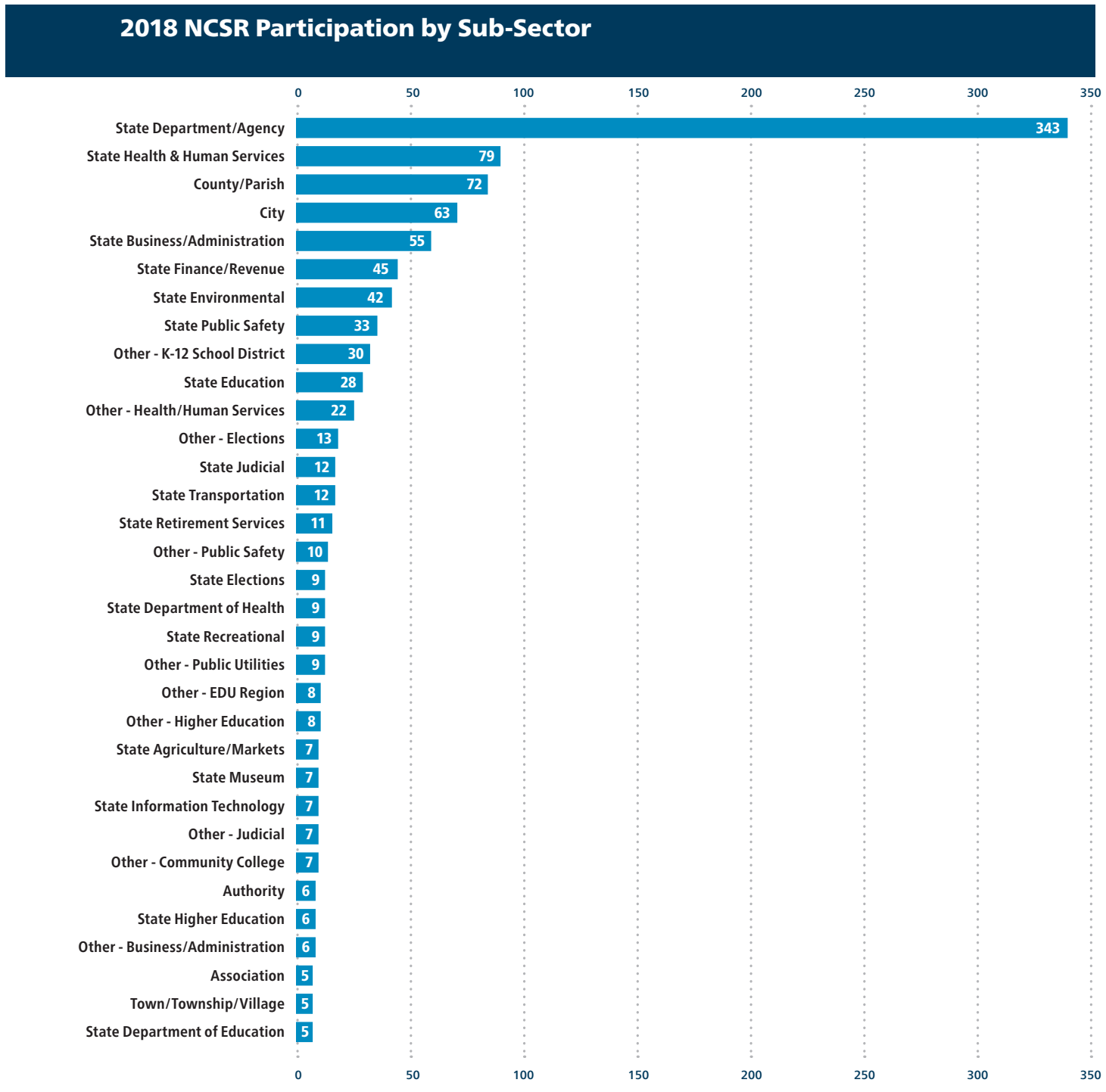


Figure 30 above lists the sub-sector name and the total number of organizations that are applicable to that specific sub-sector.

2018 Sub-Sector Average of All Functions

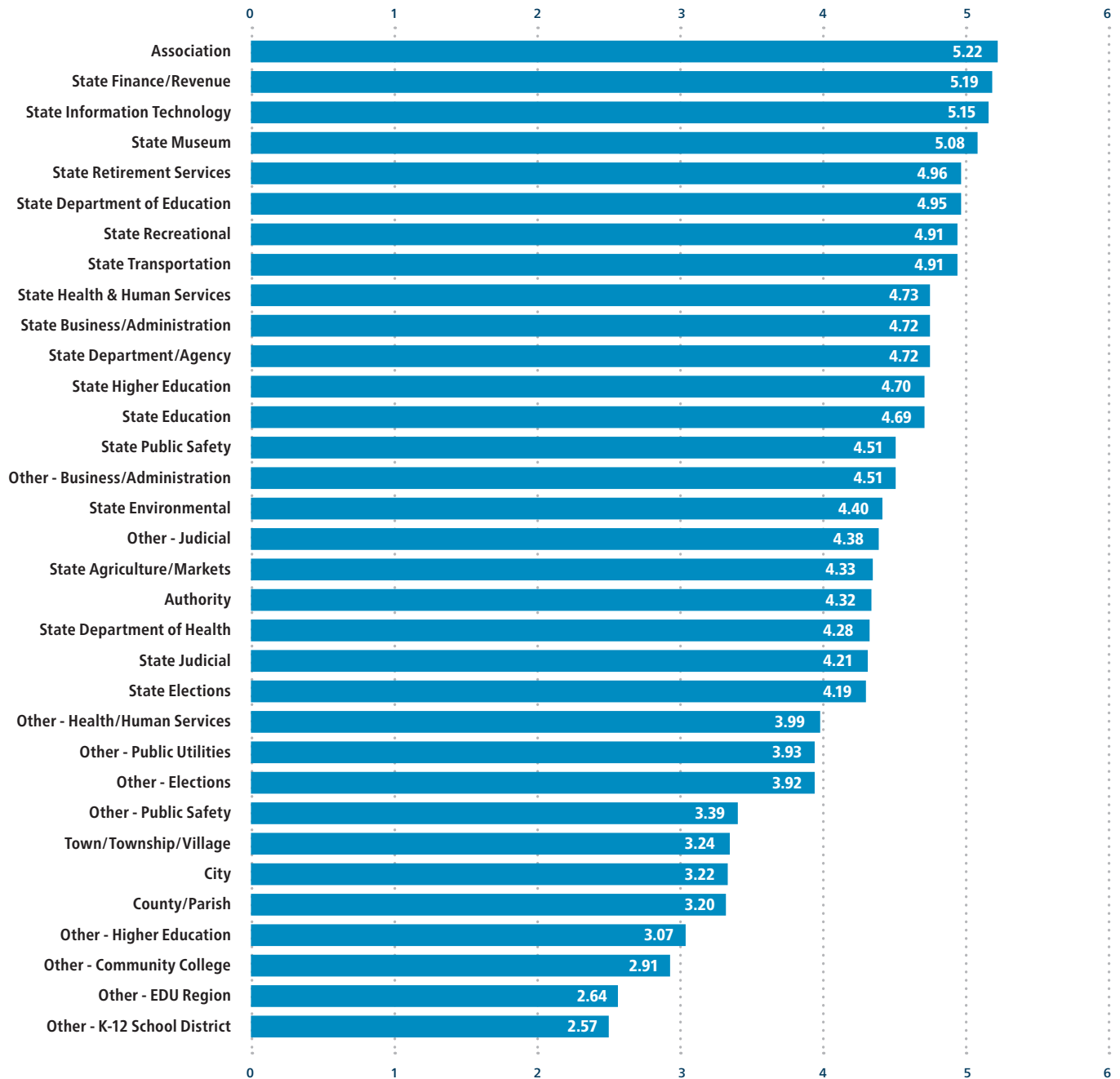


Figure 31 above represents the 2018 average of all functions across the sub-sector peer groups. The graph is sorted from highest to lowest.

2018 Sub-Sector Identify Function

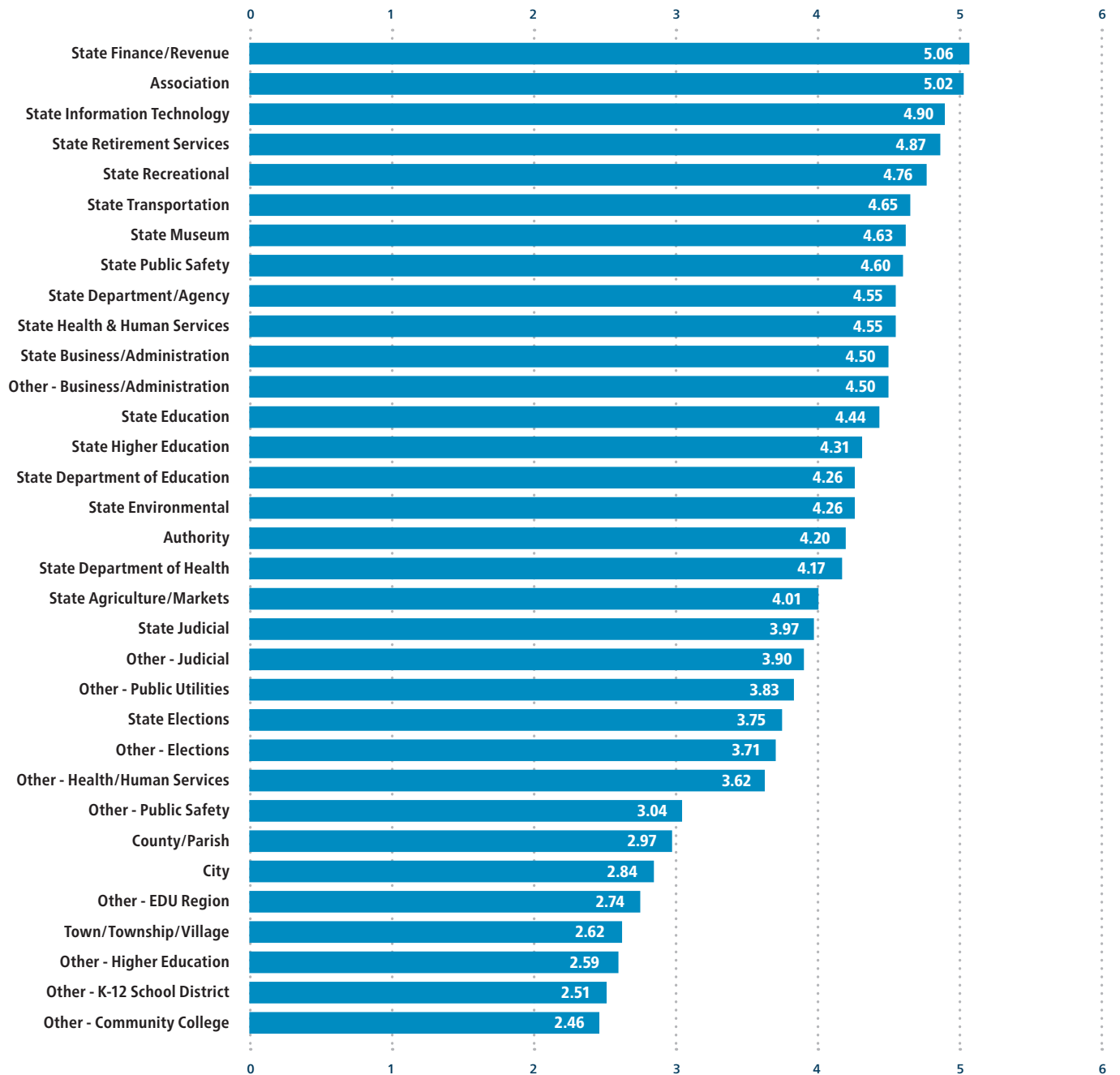


Figure 32 above represents the 2018 average for the Identify Function across the sub-sector peer groups. The graph is sorted from highest to lowest.

2018 Sub-Sector Protect Function

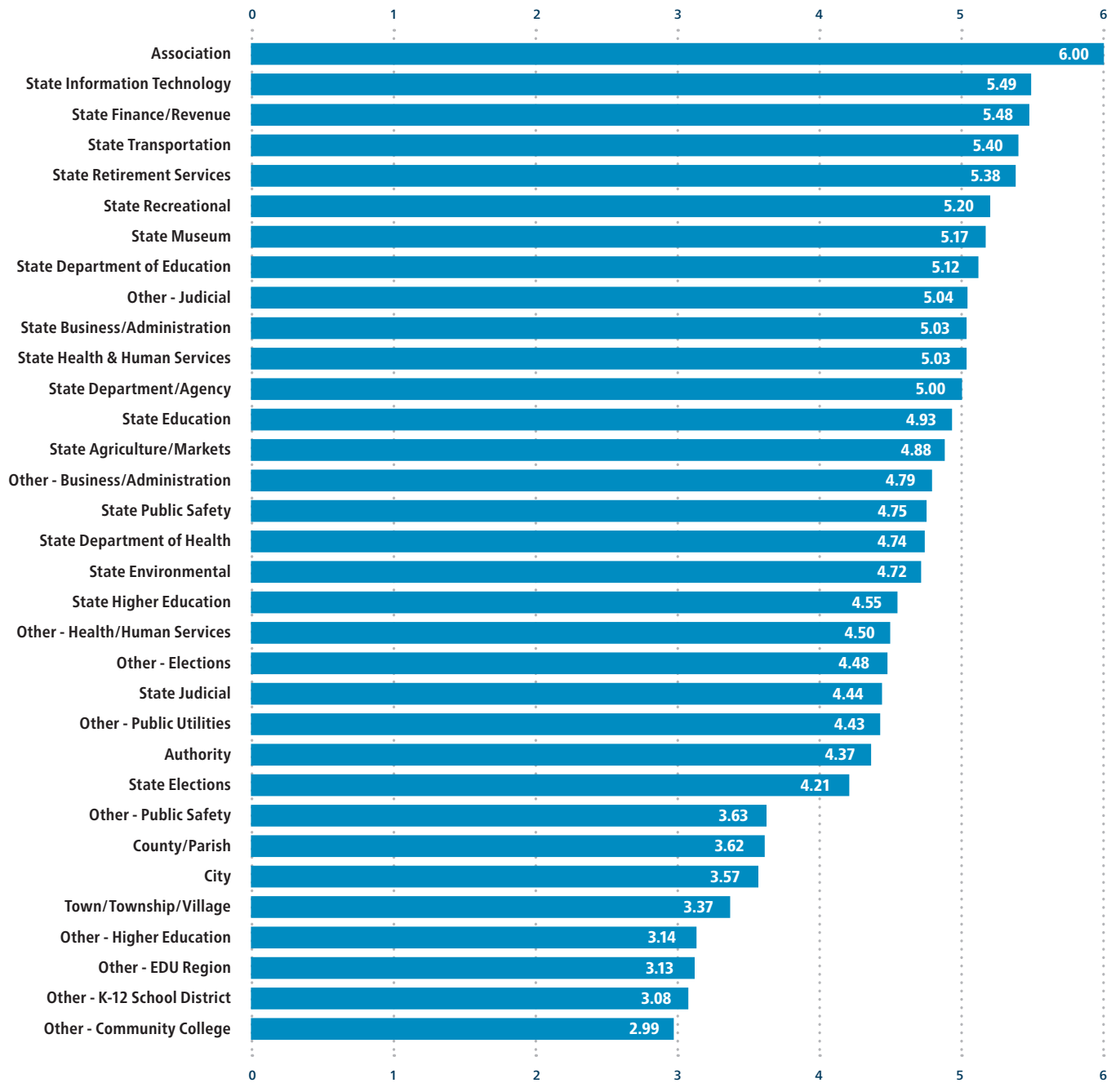


Figure 33 above represents the 2018 average for the Protect Function across the sub-sector peer groups. The graph is sorted from highest to lowest.

2018 Sub-Sector Detect Function

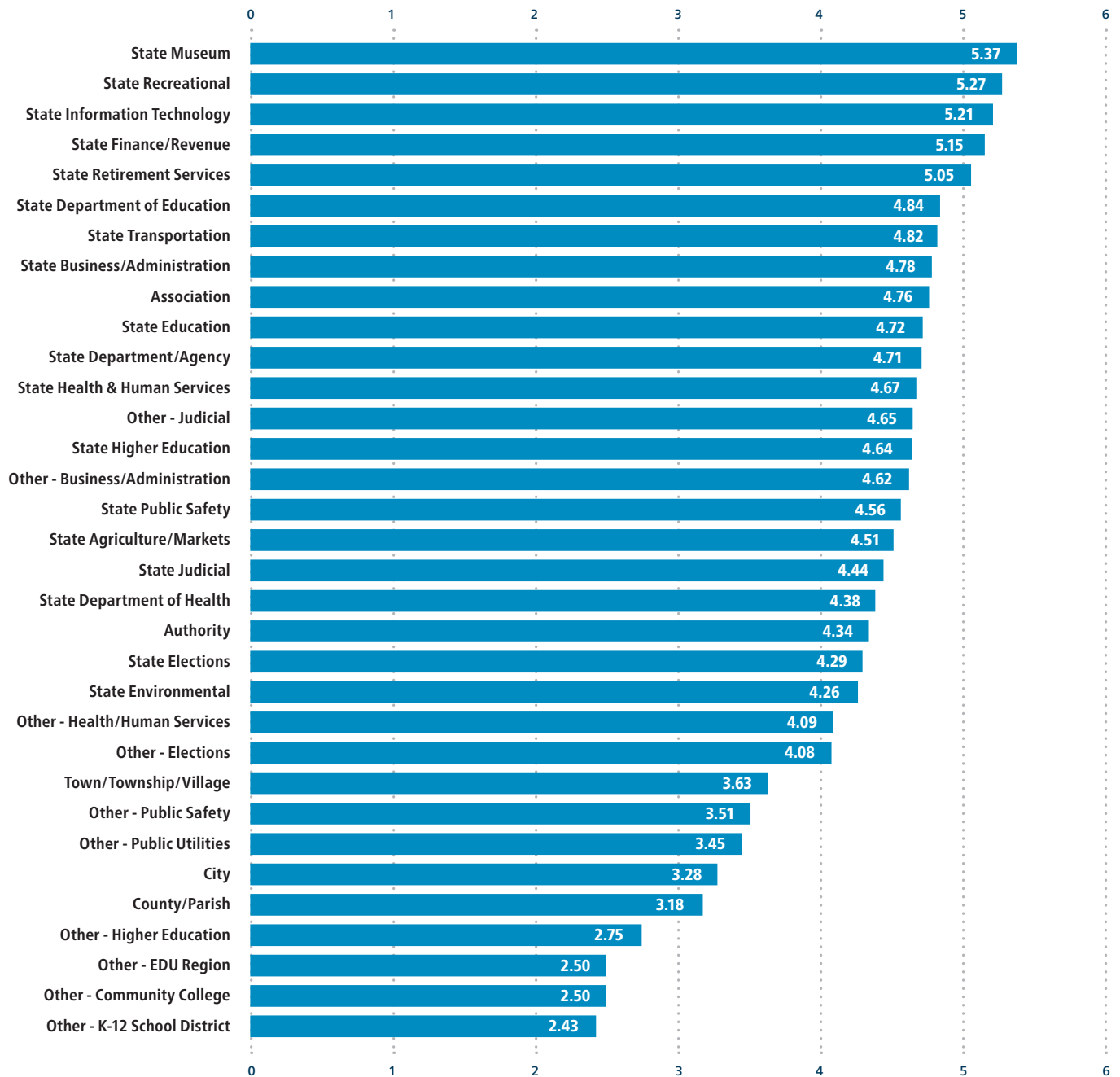


Figure 34 above represents the 2018 average for the Detect Function across the sub-sector peer groups. The graph is sorted from highest to lowest.

2018 Sub-Sector Respond Function

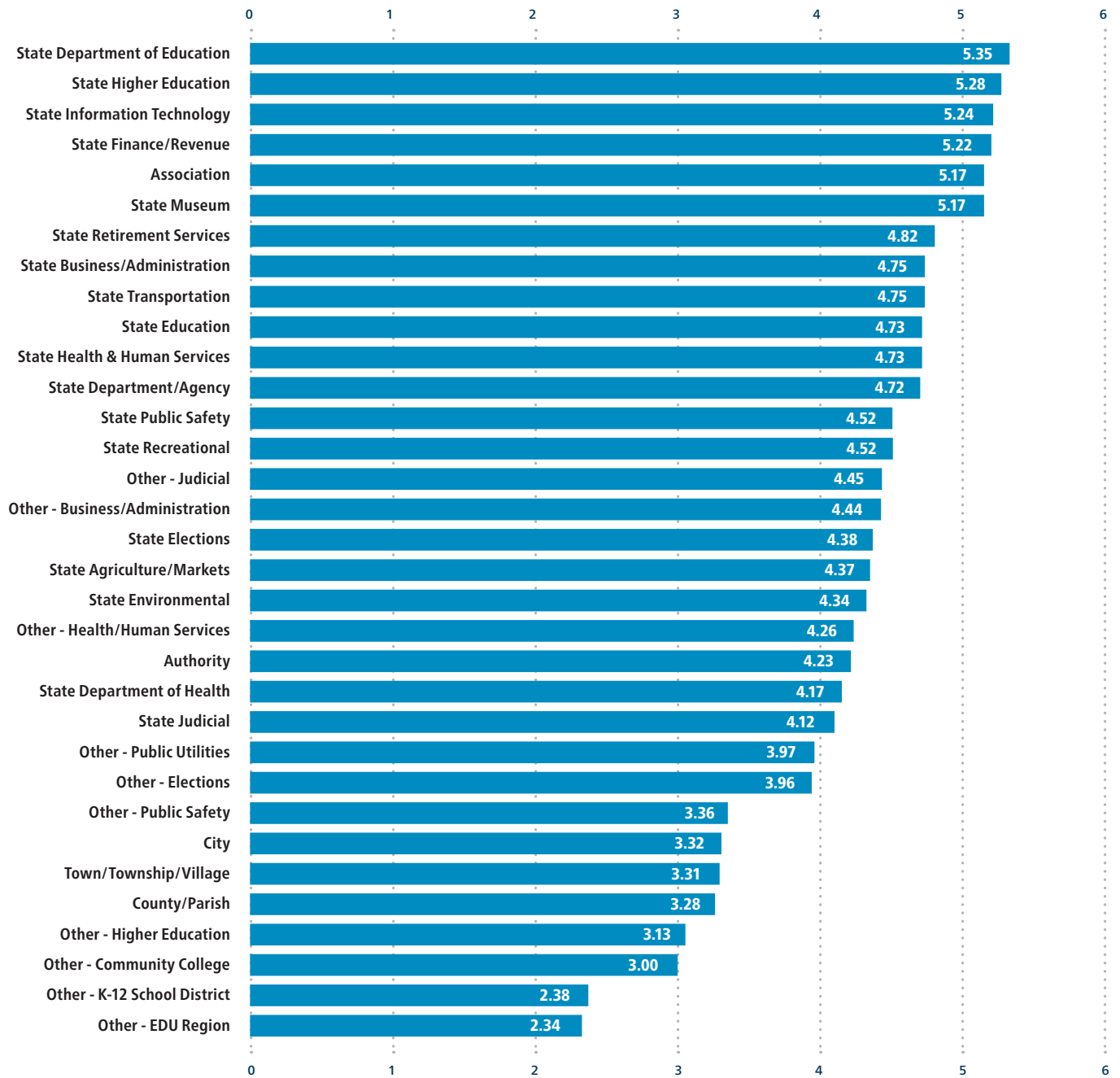


Figure 35 above represents the 2018 average for the Respond Function across the sub-sector peer groups. The graph is sorted from highest to lowest.

2018 Sub-Sector Recover Function

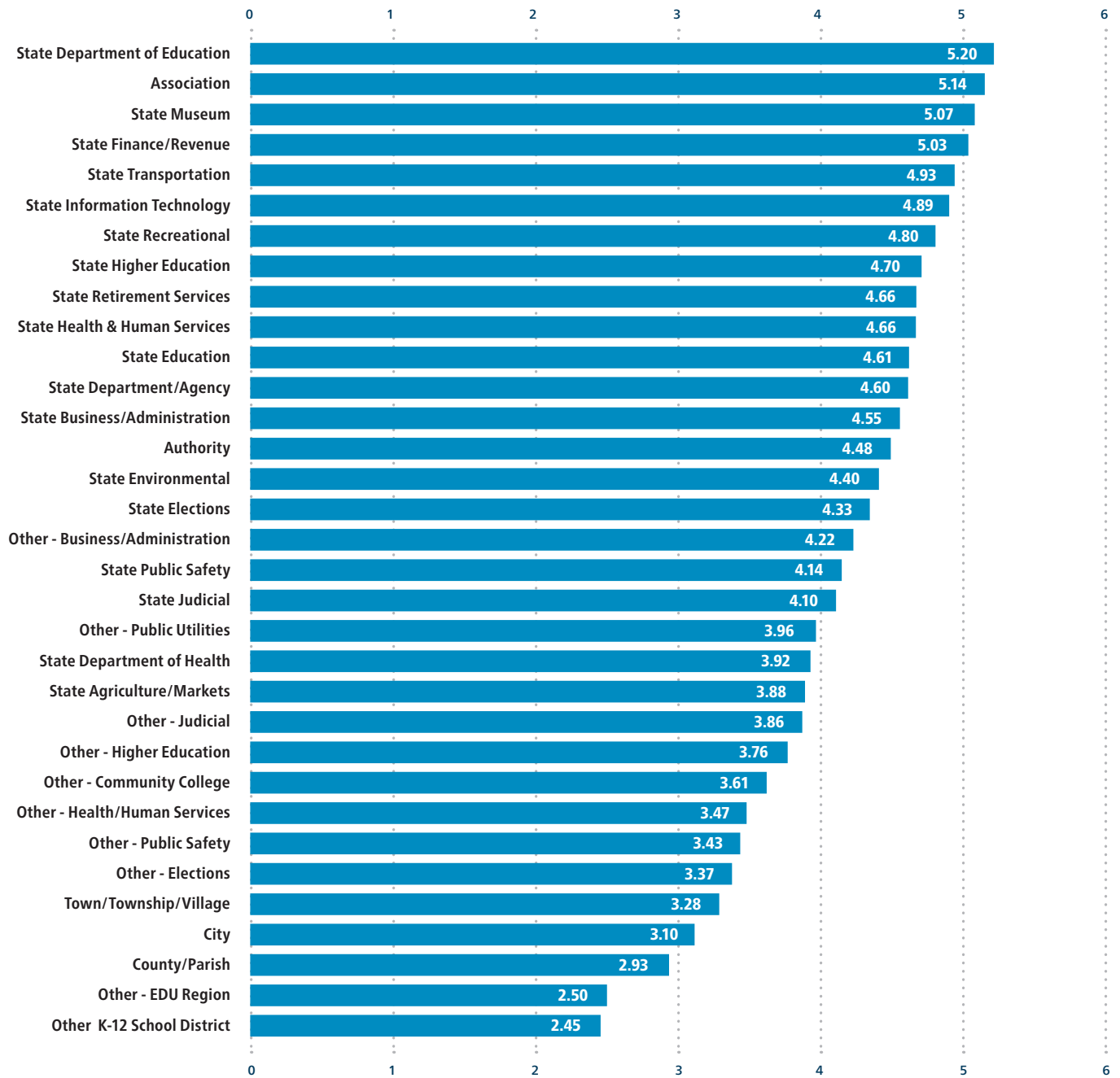


Figure 36 above represents the 2018 average for the Recover Function across the sub-sector peer groups. The graph is sorted from highest to lowest.

