

2019 Nationwide Cybersecurity Review



MS-ISAC[®]
Multi-State Information
Sharing & Analysis Center[®]



**Elections
Infrastructure
ISAC**[®]

Contents

Acknowledgments **ii**

Acronyms **iii**

Preface **iv**

Executive Summary 1

2019 Summary Report 4

High Score Highlights **5**

Low Score Areas of Interest and Key Deficiencies **6**

General Resources and Recommendations **8**

Current SLTT Cybersecurity Maturity at a Glance **9**

NCSR Participation **12**

2019 Function Averages **19**

Identify Function **21**

Protect Function **26**

Detect Function **32**

Respond Function **36**

Recover Function **41**

Subsector Peer Groups **45**

APPENDIX Partners A1

Acknowledgments

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

The MS-ISAC and EI-ISAC would also like to strongly thank all of our partners. With partner support and increased participation, we can continue to improve cybersecurity maturity across the nation.

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, Dustin Stark, Greg Bown, Joe Frohlich, Kim LaCroix, Catherine Wild, Eugene Kipniss, Tyler Scarlotta, and Emily Sochia.



This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number, 19PDMSI00002-01-00.

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.

Acronyms

CISA	Cybersecurity & Infrastructure Security Agency
DHS	U.S. Department of Homeland Security
EI-ISAC	Elections Infrastructure Information Sharing and Analysis Center
MS-ISAC	Multi-State Information Sharing & Analysis Center
NACo	National Association of Counties
NASCIO	National Association of State Chief Information Officers
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 Territory

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 2019 marks the eighth year the self-assessment has been conducted. A major change occurred on April 12, 2019, when DHS made the NCSR a requirement for recipients and sub-recipients funded through the State Homeland Security (SHSP) and Urban Area Security Initiative (UASI) grant programs.

The NCSR measures maturity according to the National Institute of Standards and Technology (NIST) Cybersecurity Framework's (CSF) Function areas and Categories (Version 1.1), in order to provide insight on the level of maturity and risk awareness of SLTT governments' information security programs. This allows decision makers to understand how their risk tolerance and maturity compares to similar organizations and facilitates self-comparison from year-to-year. The NCSR is scored on a seven point scale, with seven being the highest possible score and one being the lowest. The minimum recommended maturity level for SLTT governments is a score of five on the NCSR scale.

1	2	3	4	5	5	6	7
Not Performed	Informally Performed	Documented Policy	Partially Documented Standards or Procedures	Risk Formally Accepted	Implementation in Process	Tested and Verified	Optimized

Executive Summary

The background of the slide is a deep blue color. It features several glowing, curved lines that sweep across the frame from the bottom left towards the top right. These lines have a soft, ethereal glow, giving the impression of light trails or energy waves. The overall aesthetic is modern and dynamic.

In 2019, the NCSR continued to grow in significance for the SLTT community. The DHS requirement for SHSP and UASI grant recipients to take the NCSR, as well as the continued growth of the MS-ISAC membership (over 8,000 SLTT government members), caused NCSR participation to grow by more than 300% as compared to last year. NCSR results now represent 3,135 organizations from across the entire SLTT community. This level of participation provides a unique insight into the overall SLTT cybersecurity maturity, allowing some significant observations and findings to be made. Figures 2 and 3 below depict the State, Local, Tribal, Territory, State: Elections, and Local: Elections peer groups' overall maturity averages across all NIST CSF functions.

FIGURE 2 2019 SLTT Overall Maturity average across all NIST CSF Functions for the State, Local, Tribal, and Territory peer groups. The vertical red rule on this graph and the other graphs in this report represent the recommended minimum maturity level of "Implementation in Process." That is represented by an average score of "5."

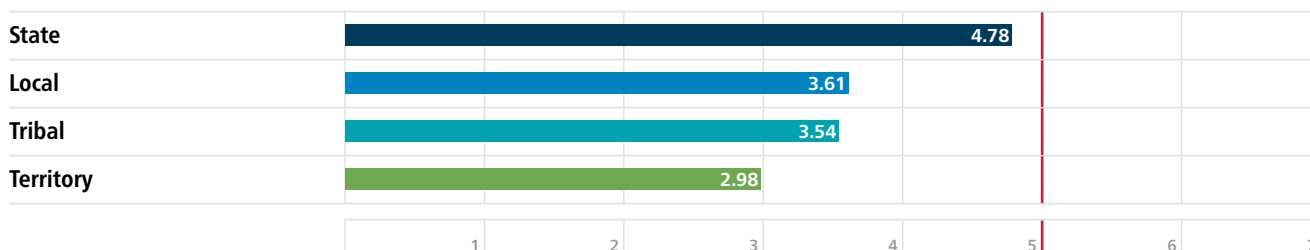
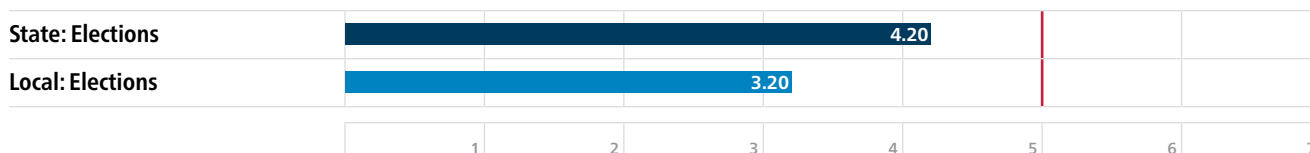


FIGURE 3 2019 Overall Maturity average across all NIST CSF Functions for the State: Elections and Local: Elections peer groups.



- **All peer groups of SLTT organizations continued to score below the overall minimum recommended maturity level of five (Implementation in Process) on the NCSR's seven-point scale.**
 - States are approaching the recommended minimum maturity level as a group, with a current score of four.
 - The Local and Tribal groups lag behind the States, and both score at a maturity level of three.
 - The Territory group scored lowest in 2019 with a maturity level of two, but were on the cusp of moving up to a maturity of three.
 - The State Elections and Local Elections sub-sectors scored significantly lower than their non-elections State and Local government counterparts.
- **State, Local, and Tribal peer group scores improved over the past four years, on average.**
 - Though no peer group has reached the recommended maturity level, progress toward higher maturity has continued.
- **The top five security concerns remained the same for the fifth consecutive year.**
 - The respondents indicated that a "Lack of Sufficient Funding" is their top concern, with personnel being another key area of concern.
 - It is recommended that cybersecurity resources and services be delivered to the SLTT community at no or low-cost, and with low impact on staffing.

- No-cost services, such as the MS-ISAC’s Malicious Domain Blocking and Reporting (MDBR), as well as DHS’ Cyber Hygiene: Vulnerability Scanning Program offer tremendous value and capability to organizations at all maturity levels with minimal impact to organizational resources.
- **Adoption of a security framework has a significant impact on organizational cyber maturity.**
 - Entities that currently employ a security framework, such as the NIST CSF, ISO 27000 series, or the CIS Controls, scored 50% higher than those organizations that do not. Adopting a framework enables organizations to assess themselves regularly against an accepted standard, plan a strategy to address their weaknesses, and continually improve their maturity.
 - A priority recommendation for SLTT organizations is that they select and use a security framework to guide their security maturation efforts.
- **Continuous engagement is a key factor in the cybersecurity maturity of SLTTs.**
 - Organizations who have taken the NCSR three or more times since 2015 scored 27% higher than those organizations who took the NCSR two or less times in the same period.
 - First time participants motivated to complete the NCSR by the grant requirement scored significantly lower than returning participants.
 - Membership in organizations such as the MS-ISAC also directly correlates to improved organizational engagement and higher maturity scores. Longer term members exhibited 9% higher scores, on average, than newer members. Such organizations provide access to resources, services, and best-practice guidance.
 - All SLTTs are encouraged to join cyber organizations and to assess themselves regularly using the NCSR and other available tools.
 - Additionally, continued support and funding for cybersecurity organizations, like ISACs, is recommended based on the services and resources they deliver to the SLTT community.
 - Adoption of MS-ISAC services was associated with increased maturity in the relevant NIST CSF Function or Category.
- **Two of the highest scoring categories in the NCSR are related to identity management and continuous monitoring activities.**
- **The lowest scoring categories measured in the NCSR are related to risk management and supply chain risk management.**
 - Cybersecurity organizations, such as CISA and MS-ISAC, should increase efforts to create additional resources and educational materials for SLTTs on cyber risk management and supply chain risk management.

Overall, the NCSR provides critical cyber maturity information about the SLTT community as a whole, as well as specific information about each of the SLTT subsectors. While this survey provides significant areas of recommendation for each subsector, future iterations of this survey will include an increased emphasis on individualized feedback for each organization based on their specific answers and maturity levels. The relative importance and accuracy of the NCSR has been enhanced by the dramatic increase in participation of SLTT organizations, therefore, the organizations can expect increasing levels of relevant feedback from year to year.

2019 Summary Report

The background of the page is a deep blue color. It features several large, overlapping, curved lines that flow from the bottom left towards the top right. These lines are a lighter shade of blue and have a soft, glowing appearance, creating a sense of movement and depth. The overall aesthetic is clean and modern.

High Score Highlights

State Year-to-Year Improvement

The 2019 state peer group increased slightly across the NIST CSF functions and are either at the minimum recommended maturity level of “Implementation in Process” (5), or are very close. This indicates the state peer group has been focused on policy and procedure development to formalize cybersecurity activity.

Local Year-to-Year Improvement

The 2019 local peer group experienced a year-over-year increase in all functions, indicating cybersecurity maturity is increasing. The local peer group represented 80% of all 2019 NCSR respondents.

Tribal Year-to-Year Improvement

The 2019 tribal peer group had a significant year-over-year increase in the Detect function, scoring 20% higher. Within the “Detection – Processes” category, the tribal peer group experienced a 36% increase, indicating they have started documenting and maintaining processes and procedures around detecting anomalous events within their environment.

Repeated Participation in the NCSR Correlates with Higher Scores

Out of all 2019 participants, entities that have participated more than one time dating back to 2015, score 21% higher than first time participants.

Identity Management and Access Control Category

“Protect – Identity Management and Access Control” was the highest scoring category in the Protect function for the state, local, tribal, and territory peer groups, as well as the “State – Elections” and “Local – Elections” subsectors. Each peer group or subsector reached “Implementation in Process” or “Partially Documented Standards and/or Procedures.” This indicates these entities understand the importance of authenticating users and managing access to sensitive information.

Security Continuous Monitoring Category

“Detect – Security Continuous Monitoring” was the highest scoring category within the Detect function for the local, tribal, and territory peer groups, as well as the “State – Elections” and “Local – Elections” subsectors. This indicates these entities are actively monitoring for cybersecurity events and remaining vigilant to threats.

Low Score Areas of Interest and Key Deficiencies

Risk Management and Supply Chain Risk Management Categories (ID.RM, ID.SC)

“Identify – Risk Management” and “Identify – Supply Chain Risk Management” continue to be the lowest scoring categories within the Identify function. The supply chain category was first introduced in the 2018 NCSR, which contributed to a decrease in the Identify function for all peer groups. This is a relatively new topic, and the lack of guidelines for implementation and resources to assist with these functions may contribute to lower scores. Entities expressed they do not have the resources to begin implementing formalized supply chain security practices in their organization. Guidance regarding language to be included in contracts or processes may be helpful and contribute to increased maturity within this category.

The MS- and EI-ISACs provide no-cost IP and Domain monitoring, which acts as a form of threat intelligence sharing and can be implemented and formalized to increase maturity in the “Risk Assessment” category within the Identify function. Respondents to the 2019 NCSR who utilize these services scored on average 6% higher in the “Identify – Risk Assessment” category than those who did not. In addition, longer term members of the MS-ISAC exhibit 9% higher scores, on average, than newer members. By becoming a member and utilizing these services, participants see higher scores in maturity.

The MS- and EI-ISAC’s Vulnerability Management Program, a component of the IP and Domain monitoring service, can be leveraged by SLTT organizations to increase maturity in the “Risk Assessment” category within the Identify function, as well as in the Detect function’s “Security Continuous Monitoring” category. This service’s Web Profiler reports monthly on out-of-date software, while the Port Profiler reports quarterly on open ports on SLTT governments’ internet facing devices so that they can mitigate these risks. Likewise, the DHS CISA Cyber Hygiene Scanning Program is a no-cost external vulnerability scanning service that can also bolster capability within this category. SLTT organizations who begin using these services and formalize their use with policy and procedures can improve their maturity and NCSR scores. The MS-ISAC observed that organizations leveraging the Web Profiler scored on average 6% higher in maturity in the “Identify – Risk Assessment” category, and 1% higher in the “Detect – Security Continuous Monitoring” category.

Improvements Categories (RS.IM, RC.IM)

“Respond–Improvements” and “Recover–Improvements” were the lowest scoring categories within the Respond and Recover functions, respectively, for the state, local, tribal, and territory peer groups. This indicates there is a common weakness within all peer groups where policies/procedures have not been implemented consistently. These important categories cover how an organization assesses lessons learned and after-action reporting following an incident, as well as how they update strategies, policies, or procedures accordingly.

Publicly available no-cost resources, such as the MS-ISAC Business Resiliency workgroup's guide to reviewing lessons learned following an incident could assist with formalizing activity, policy creation, and documentation.

Anomalies and Events Category (DE.AE)

The local, tribal, and territory peer groups scored lowest in the "Detect – Anomalies and Events" category within the Detect function. This indicates that more resources are needed to establish and understand a baseline of normal activity on their networks, in order to be able to identify anomalies.

One recommendation is to provide resources and guidance to SLTT governments to assist them in mapping internal and external data flows to understand their data movement. A data life cycle can then be established that includes policies regarding management and protection of data.

Respond – Analysis (RS.AN)

The local, tribal, and territory peer groups all scored below the recommended minimum maturity level of five in the Respond – Analysis category. This category covers analysis conducted to ensure adequate cybersecurity response which supports recovery activities, as well.

The MS-ISAC offers the Malicious Code Analysis Platform (MCAP), which allows SLTT organizations to analyze suspicious files, URLs, and emails in a sandboxed environment. They can use this service and build out policies and procedures on how to perform this analysis to increase maturity in the Respond – Analysis category. 2019 NCSR respondents who have an active MCAP account scored 5% higher within the Respond function, on average, than those who did not have an active MCAP account. Further, the respondents who have an active MCAP account scored 6% higher within the "Respond – Analysis" category specifically.

Conflicting Recommendations

Many participants also reported a conflict in the recommendations, which assume the organization is fully networked and online, as is the case with many larger SLTT governments. For example, if an entity has only a few computers, with the majority of their data being filed on paper, enterprise-level cybersecurity strategies and practices may not be a relevant or appropriate option. Many cybersecurity resources are set up as one size fits all, however, smaller organizations can struggle with the amount of attention a robust cybersecurity program needs.

Lack of Security Staffing

A majority of participants reported their organization has fewer than five full-time security employees. With a lack in security staffing, it is difficult to begin assessing and implementing an appropriate cybersecurity program.

The Federal Virtual Training Environment (FedVTE), can assist entities in increasing their scores within many functions, including Protect – Awareness and Training (PR. AT), through staff training and professional development. This is a no-cost repository of online, on-demand cybersecurity coursework for professionals. An organization can utilize FedVTE to expand their existing staff's capabilities and knowledge base by reviewing cybersecurity labs and training courses.

General Resources and Recommendations

All Functions

No-cost open source resources and software can be utilized for the activities described within the CSF. A publicly-available guide, courtesy of the MS-ISAC, provides alignment of open source resources to the CSF. By utilizing the resources mapped to the CSF activities, an organization can outline its yearly strategic plan and identify areas for improvement.

All Functions

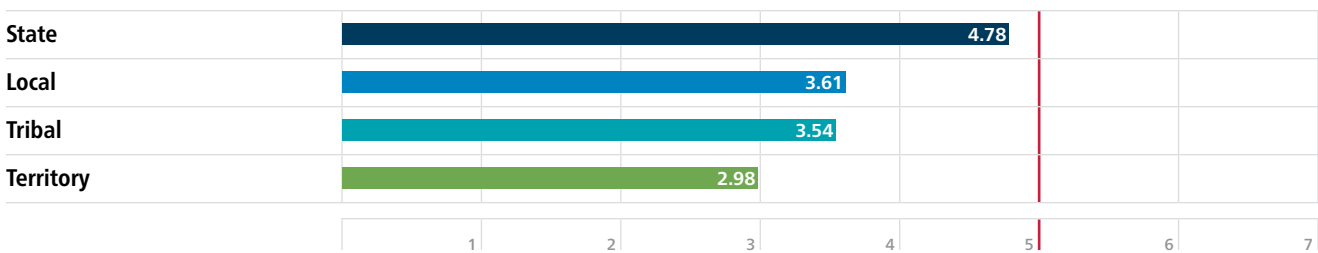
The MS-ISAC published a policy template guide that aligns publicly available SANS policy templates to 35 CSF subcategories. These policies can be modified or adopted by organizations to formalize their cybersecurity processes for every NCSR question and all NIST CSF subcategories. This can be leveraged to improve maturity in the applicable areas and achieve at least a score of “3” (Documented Policy), and in some cases a “5” (Implementation in Process), which is the recommended minimum maturity level.

General Recommendation: Regular Assessment Against Cybersecurity Frameworks

A general practice that can assist organizations in increasing maturity scores is to take a cybersecurity assessment, like the NCSR, and to adopt a cybersecurity framework as a guiding set of practices or standards. With these two pieces in place, an organization can plan out which improvements to target for funding and effort, and then repeatedly assess themselves to compare maturity over time. It was found that participants who adopted a cybersecurity framework scored higher on average than organizations who did not. In the 2019 NCSR, respondents reported that a “Lack of Cybersecurity Strategy” was a key pain point, and those who reported utilizing a cybersecurity framework scored 50% higher than those who do not.

Current SLTT Cybersecurity Maturity at a Glance

FIGURE 2 2019 SLTT Overall Maturity average across all NIST CSF Functions for the State, Local, Tribal, and Territory peer groups. The vertical red rule on this graph and the other graphs in this report represent the recommended minimum maturity level of “Implementation in Process.” That is represented by an average score of “5.”



State: Partially Documented Standards and/or Procedures (4)

The state peer group exhibited an average maturity level that corresponds to a value of “4” on the NCSR scale. This maturity level is described as “Partially Documented Standards and/or Procedures.” This reflects that on the whole, states have already developed formal policy to guide cybersecurity activity, yet are in the process of developing standards and procedures that would allow for consistent implementation of practices. This level of maturity has been seen from the state peer group every year since the 2015 NCSR, though there has been an increase from the past year, and the group is edging much closer to the recommended minimum score of 5.

Local and Tribal: Documented Policy (3)

The local and tribal peer groups each exhibited average maturity levels that correspond to a “3” on the NCSR scale. This maturity level is described as “Documented Policy.” These entities have formal cybersecurity policies in place, but are informally performing cybersecurity functions without documented standard operating procedures. Based on responses to the NCSR, these organizations provided responses that stated they do not have dedicated cybersecurity staff or established strategies to guide implementation and formalization of activity.

Territory: Informally Performed (2)

The territory peer group exhibited an average score of “2” on the NCSR scale, though were on the cusp of reaching the next level within the maturity scale. This current level of “2” is defined as activities being “Informally Performed.” These entities are performing cybersecurity functions, and may have key technologies in place, yet formal documented policies and procedures are not present or not adopted by management. This was the first year in which all 6 territories participated, so there are no prior year data sets available for comparison.

FIGURE 3 Current Elections Cybersecurity at a Glance with Figure 2: 2019 SLTT Overall Maturity average from page 9.

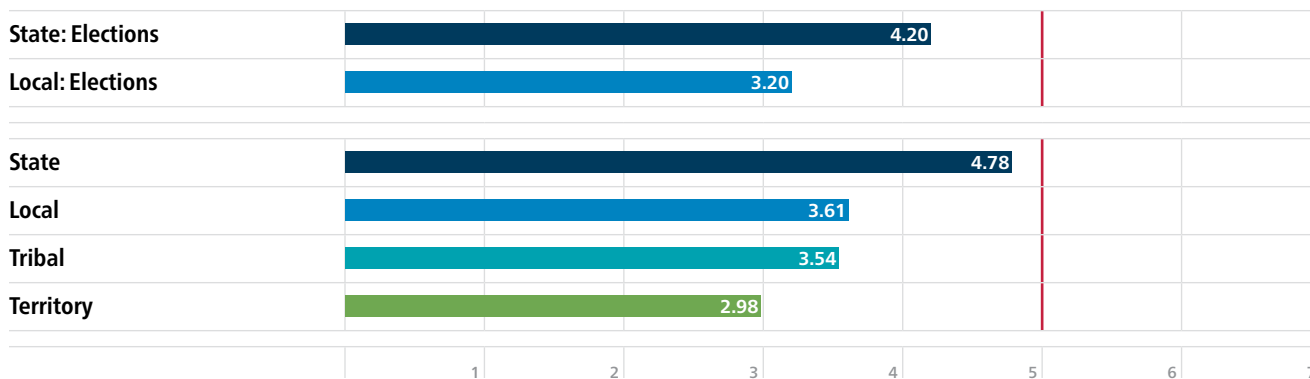


Figure 3 displays the average across all NIST CSF functions for the “State–Elections” and “Local–Elections” peer group subsectors. The “State–Elections” subsector includes entities such as State Board of Elections Offices and Secretary of State Offices. The “Local–Elections” subsector includes entities such as local Board of Elections Offices and local Registrar Offices. Figure 2 is inserted below the Elections peer group subsectors for comparison against the State, Local, Tribal, and Territory non-elections peer groups.

State Elections: Partially Documented Standards and/or Procedures (4)

State elections organizations, such as State Boards of Elections or Offices of the Secretary of State, exhibited an average maturity level that corresponds to a value of “4” on the NCSR scale. They lagged behind their non-elections state government counterparts, who scored a 4.78 compared to the state elections’ 4.2 average. This score level reflects that overall, state elections organizations have already developed formal policy to guide cybersecurity activity, yet are in the process of developing standards and procedures that would allow for consistent implementation of cybersecurity practices. Membership in the MS-ISAC and EI-ISAC provides access to federally funded services, such as cybersecurity assessments that evaluate their current resiliency, in addition to a portal to connect with other elections entities and partners to collaborate and share information. The availability of these services has heightened awareness about the need for secure elections cybersecurity practices, and led to adoption of best practices. Due to the recent availability of these resources, the community may require another year of participation to see meaningful growth in cybersecurity maturity.

Local Elections: Documented Policy (3)

Local elections organizations, such as local Boards of Elections and local Registrar Offices, exhibited an average maturity level that corresponds to a value of “3” on the NCSR scale, “Documented Policy.” Local elections organizations scored lower than non-elections local organizations with a 3.2 compared to 3.61, respectively. These entities have formal cybersecurity policies in place, but are informally performing cybersecurity functions without documented standard operating procedures. Local entities who became EI-ISAC members prior to the start of 2019 scored 10% higher than those who became members after. The EI-ISAC is relatively new, and the elections community is still in the process of adopting resources from the EI-ISAC and DHS. First time NCSR participants who became EI-ISAC members are beginning to utilize more resources, and formalize their cybersecurity policies and procedures to increase their maturity.

FIGURE 4

2019 Highlights: Progress and Deficiencies. Within each NIST CSF function below, the absolute coloring is based on the 7 point maturity scale mirroring the figure in the Preface.

	State	Local	Tribal	Territory	State: Elections	Local: Elections
Organization Total	50	2,523	19	6	16	61
Identify	4.32	3.38	2.91	2.94	3.93	2.97
Asset Management	4.26	3.66	2.91	2.44	4.01	3.25
Business Environment	4.56	3.69	3.28	4.57	4.28	3.51
Governance	4.98	3.56	2.92	2.67	4.56	3.09
Risk Assessment	4.82	3.59	3.56	3.33	4.70	3.01
Risk Management Strategy	3.77	3.02	2.58	2.44	3.29	2.53
Supply Chain Risk Management	3.56	2.78	2.23	2.17	2.75	2.41
Protect	4.90	3.98	3.91	3.39	4.44	3.54
Identity Mgmt. and Access Control	5.15	4.66	4.75	4.50	5.12	4.08
Awareness and Training	5.19	4.06	3.64	3.53	4.89	3.92
Data Security	4.66	3.89	3.89	2.98	4.44	3.34
Info. Protection Proc. and Procedures	4.95	3.65	3.54	2.82	4.38	3.29
Maintenance	4.78	3.85	4.18	3.25	3.50	3.26
Protective Technology	4.64	3.76	3.46	3.27	4.28	3.35
Detect	4.97	3.64	3.76	2.96	4.19	3.13
Anomalies and Events	5.06	3.49	3.65	2.67	4.15	2.80
Security Continuous Monitoring	4.93	3.92	3.88	3.29	4.38	3.54
Detection Processes	4.92	3.52	3.76	2.93	4.05	3.06
Respond	5.09	3.59	3.77	2.87	4.42	3.20
Response Planning	5.08	3.53	3.79	3.00	4.00	3.16
Communications	5.04	3.54	3.97	3.03	4.68	3.46
Analysis	5.18	3.58	3.97	2.83	4.66	2.84
Mitigation	5.33	3.89	3.88	2.83	4.77	3.49
Improvements	4.81	3.41	3.24	2.67	4.00	3.03
Recover	4.62	3.46	3.36	2.75	4.04	3.16
Recovery Planning	4.64	3.59	3.53	3.33	4.19	3.16
Improvements	4.58	3.40	3.26	2.25	3.81	3.16
Communications	4.65	3.40	3.28	2.67	4.12	3.17
All Function Average	4.78	3.61	3.54	2.98	4.20	3.20

NCSR Participation

Targeted Participants The target audience for the NCSR are personnel within the SLTT community who are responsible for cybersecurity management within their organization. The target participants expanded in 2019 to include all grant recipients and sub-recipients of funding through the State Homeland Security Program (SHSP) and Urban Area Security Initiative (UASI).

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.

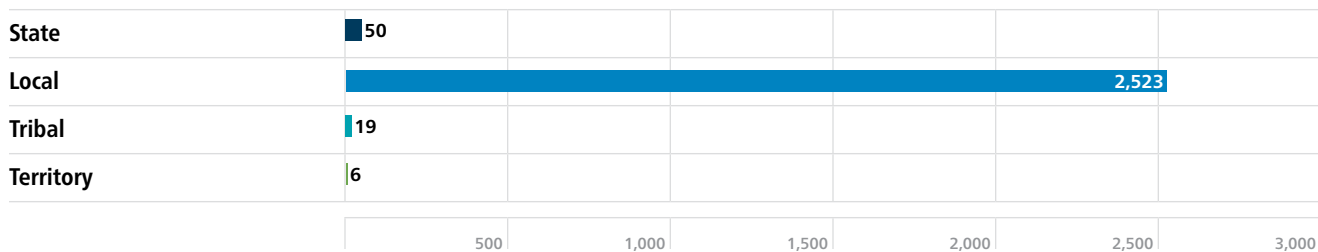
Peer Groups Defined For the purposes of continuous data analysis and trending, respondents are grouped into one of four main peer groups: state, local, tribal, and territory. The state peer group involves participation among the 50 state governments. The local peer group consists of any local government entity. This includes cities, counties, parishes, boroughs, K-12 public school districts, Fire/EMS/911, associations, authorities, and many more entity types at the local level. The tribal peer group includes participation by any federally recognized tribe. The territory peer group includes participation among the 6 territorial governments.

The MS-ISAC was able to break the state, local, tribal, and territory peer groups down into subsets represented by 39 additional sub-sector peer groups. These sub-sectors are discussed in further detail on [page 45](#). To maintain anonymity, each sub-sector peer group must include participation from a minimum of five organizations per group. An organization can be a part of multiple sub-sectors, if applicable.

2019 Homeland Security Grant Program As outlined in the FY 2019 Notice of Funding Opportunity (NOFO), State Homeland Security Program (SHSP) and Urban Area Security Initiative (UASI) recipients and sub-recipients were required to complete the NCSR by the end of Calendar Year 2019. Of the total 3,135 NCSR participants, 71% of participants identified their organization as taking the NCSR as part of the grant requirement.

In addition, first-time participants in 2019 scored significantly lower, on average, compared to all other participants. This had a large impact on the overall function scores of the NCSR as many new participants were lacking an IT or security department to assist in answering the assessment. Figure 5 below represents SLTT participation in the 2019 NCSR.

FIGURE 5 2019 SLTT Participation



Participation Highlights

Overall Highlights

Percent Increase

The 2019 NCSR saw a year-over-year participation increase of more than 300%.

Repeat Assessments

Entities that have participated 3 to 5 times since 2015, score 27% higher than entities that participated 1 or 2 times within the same timeframe.

State Highlights

State Peer Group Increase

Seven additional state governments completed the NCSR in 2019 compared to 2018. The 2019 NCSR had full representation from all 50 states.

State Aggregate Roll Up

Of the 50 state participants, 6 states aggregate their scores. This means all participating state agencies complete the NCSR and their scores are averaged to compile the overall state score. A total of 524 state agencies participated in the 2019 NCSR as part of a roll-up, or independently.

Local Highlights

Local Peer Group Increase

The local peer group saw an overall increase of 2,246 participant entities compared to 2018, with 81% of local participants identifying their entity as completing the assessment as part of the HSGP requirement.

Local Fire/EMS/911 Increase

The Fire/EMS/911 peer group subsector experienced an unprecedented increase in participation this year, growing from four participants in 2018, to 418 participants in 2019.

Tribal Highlights

Tribal Peer Group Increase

Tribal participation saw its highest volume ever in 2019, with 19 organizations completing the NCSR. In 2018, 6 tribal organizations participated.

Tribal Participation

The total number of tribal participants has continuously increased each year since 2016, when there first were enough participants to create a separate peer group.

Territory Highlights

Territory Peer Group

The 2019 NCSR saw full representation of all 6 territories. This is the first time since the NCSR began that territory participation was high enough to create a separate peer group.

FIGURE 6

The five peer group subsectors with the highest volume of organizational participation

Subsector	Total Participants
Local: County/Parish	759
Local: City	540
State Department/Agency	524
Local: Fire/EMS/911 Combined	418
Local: Public Safety	348

NCSR Demographic Analysis

The following information was collected in from an analysis of the demographic and post-survey responses from the 2019 NCSR.

FIGURE 7

Participation volume of centralized, decentralized, or hybrid governance structures within the State peer group. Data collected in analyzing the 50 states that participated in the 2019 NCSR.

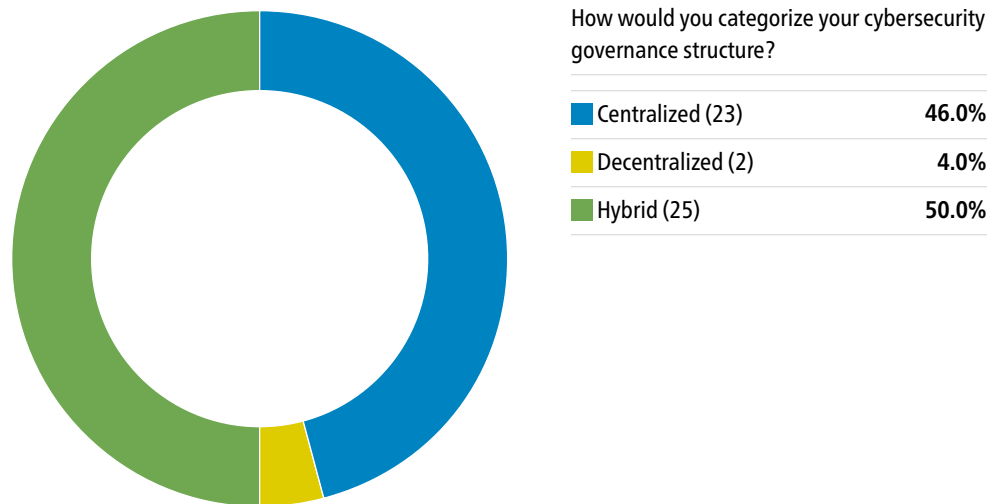
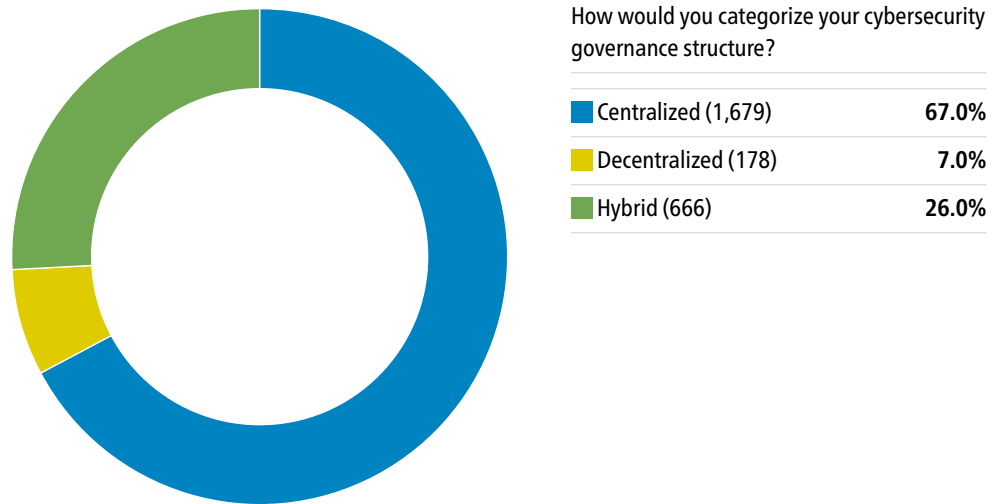


FIGURE 8

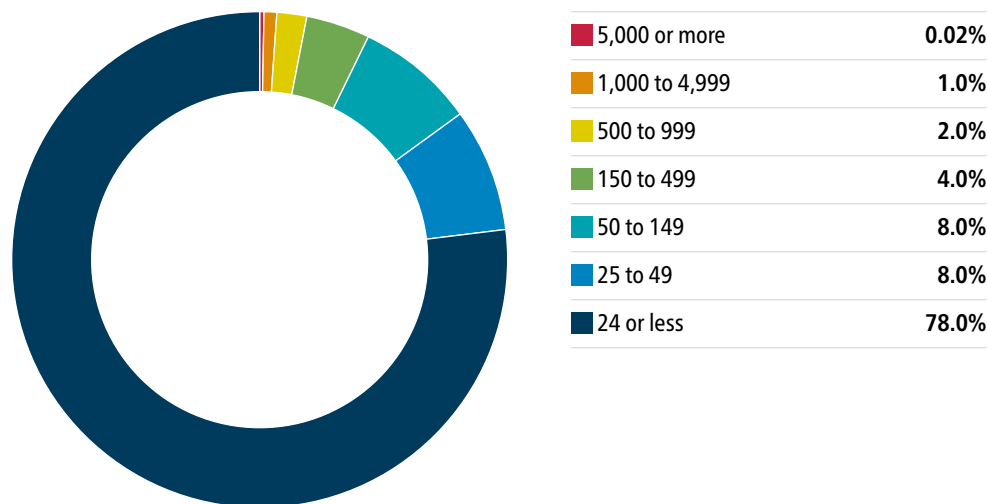
Participation volume of centralized, decentralized, or hybrid governance structures within the Local peer group. Data collected in analyzing the 2,523 local organizations that participated in the 2019 NCSR.



Both state and local participants with a centralized governance structure scored higher across all NIST CSF functions compared to state or local counterparts with a decentralized or hybrid governance structure. Centralized governance structures are typically characterized by consistently shared information, more standardized practices, as well as collective decision making within an organization. It is the MS-ISAC’s recommendation that SLTT organizations adopt a centralized government.

FIGURE 9

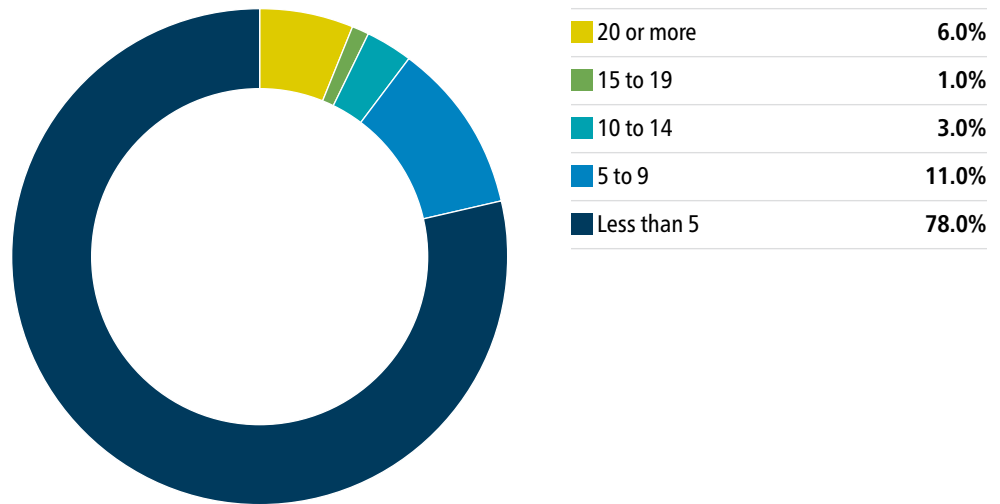
Summary of IT full-time employee staffing for NCSR participating organizations. Data collected in analyzing the number of IT staff within an organization. This data reflects all 3,135 participants of the 2019 NCSR.



- Organizations with 25 or more IT employees score 19% higher than organizations with less than 25 IT employees.

FIGURE 10

Summary of security full-time employee staffing for NCSR participating organizations. Data collected in analyzing the number of Security staff within an organization. This data reflects all 3,135 participants of the 2019 NCSR.



- Organizations with 5 or more security employees score 17% higher than organizations with less than 5 security focused employees.

Staffing Totals Key Takeaways

- Organizations with 100 or more total employees score 8% higher on average, than organizations with less than 100 total employees.
- Organizations with lower staffing totals should utilize no-cost resources from MS-ISAC, EI-ISAC, DHS, and open sources to assist with IT and cybersecurity activities.

Outsourcing Analysis

- A majority of respondents are conducting minimal outsourcing of both IT or Security operations.

Top Security Concerns

Participants have continually identified the same top five security concerns over the past five years. Their concerns below are presented in rank order from highest to lowest as identified in 2019. While traditionally only the Top 5 are reported, the sixth ranking concern: “Lack of a cybersecurity strategy (i.e., shifting priorities),” should be mentioned as it was selected by over 1,000 participants.

FIGURE 11

Top Security Concerns



ANALYSIS BY FUNCTION

2019 Function Averages

Figure 12 below displays the current 2019 cybersecurity maturity of the state, local, tribal, and territory peer groups. The vertical red rule on this graph and the other graphs in this report represent the recommended minimum maturity level of "Implementation in Process." That is represented by an average score of "5."

FIGURE 12

2019 Function Averages

■ State ■ Local ■ Tribal ■ Territory

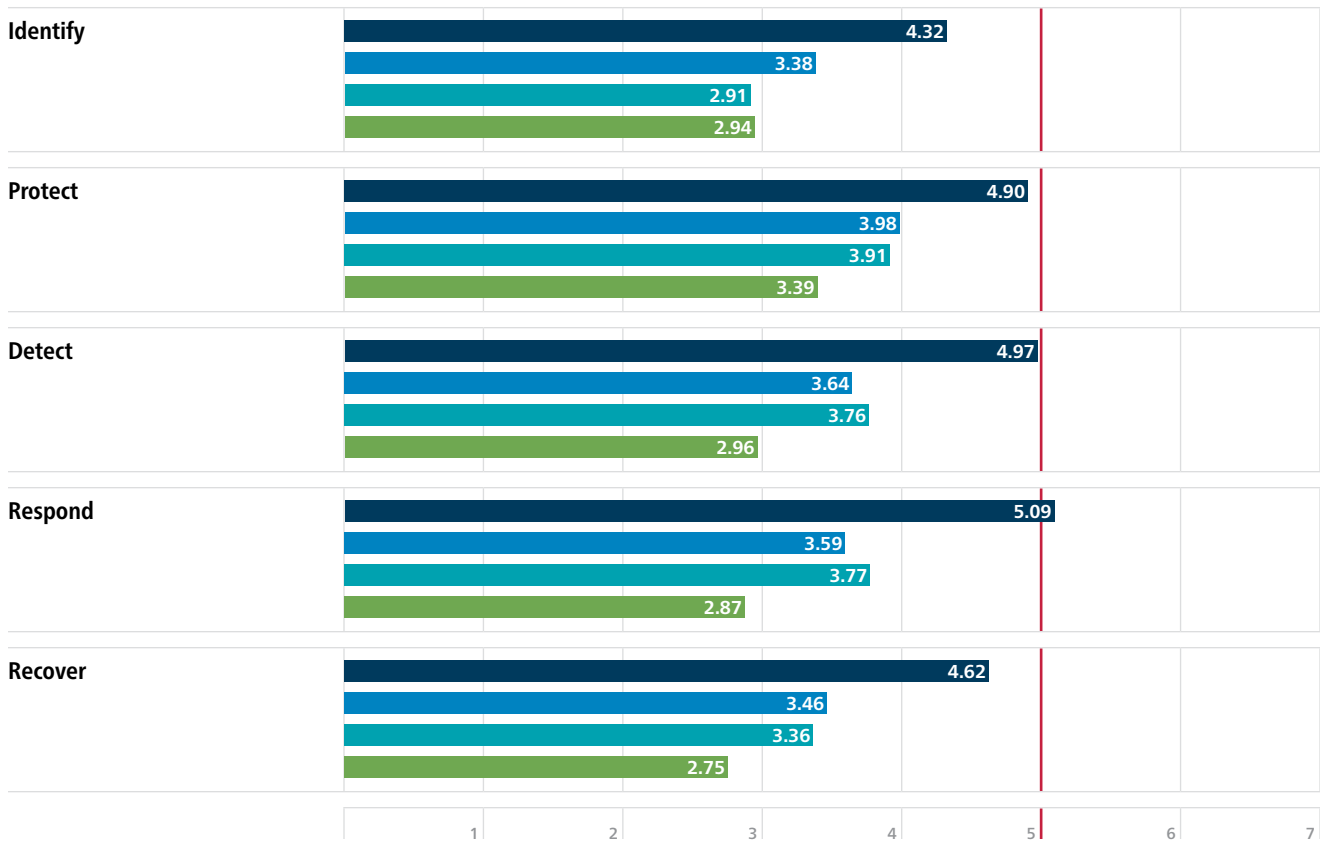
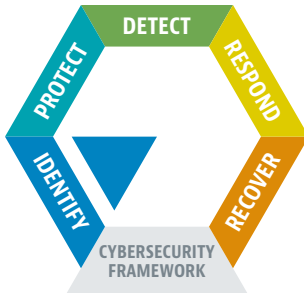


FIGURE 13

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

	Year	Identify	Protect	Detect	Respond	Recover	Average
State Peer Profile	2016	2%	2%	4%	3%	3%	3%
	2017	3%	4%	2%	4%	3%	3%
	2018	0%	-2%	-1%	-1%	0%	-1%
	2019	0%	2%	2%	3%	0%	1%
Local Peer Profile	2016	15%	11%	15%	5%	8%	11%
	2017	10%	8%	13%	11%	6%	10%
	2018	-9%	-5%	-3%	-1%	0%	-4%
	2019	7%	3%	6%	3%	6%	5%
Tribal Peer Profile	2017	-21%	2%	-10%	0%	-30%	-12%
	2018	46%	7%	20%	74%	95%	48%
	2019	9%	11%	20%	0%	-6%	7%



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.

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

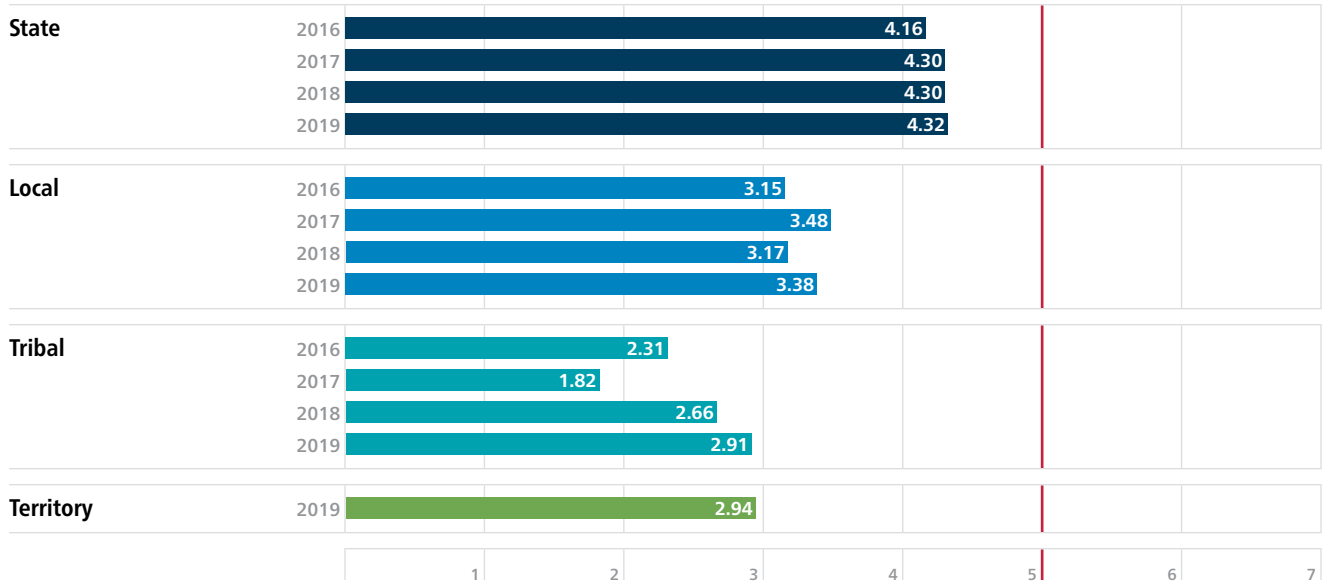
The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support supply chain decisions.

Identify Function Analysis

Figure 14 below represents the year-to-year average for the Identify Function across the peer groups.

FIGURE 14

Year-to-year Identify Function Averages



Overall

Identify continues to be the lowest scoring function for the state, local, and tribal peer groups. This is a consistent trend since 2015. This may be indicative of a need for policy and procedure guidance, in addition to supply chain resources.

Tribal

The 2019 tribal peer group increased their scores by 9%, compared to 2018, within the Identify function. Tribal entities scored lowest within the Supply Chain Risk Management subcategory of Identify. This suggests these risks are acknowledged, but entities have not implemented improvements.

FIGURE 15

Percentage increase or decrease identified in 2016, 2017, 2018, and 2019 within each peer group across the Identify Function.

Year	State	Local	Tribal
2016	2%	15%	
2017	3%	10%	-21%
2018	0%	-9%	46%
2019	0%	7%	9%

SLTT

The categories within the Identify function saw mostly positive or consistent scores in 2019. The tribal peer group continues to increase, while the local peer group bounced back from their decrease in 2018. The state peer group remained at the same Identify scores for the past two years, which is a possible indication that their improvements have plateaued.

FIGURE 16

Year-to-year averages for the Identify Categories across the peer groups

	Year	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy	Supply Chain Risk Management	Identify Function
State Peer Group	2016	3.85	4.28	4.65	4.51	3.49		4.16
	2017	3.99	4.37	4.82	4.69	3.61		4.30
	2018	4.21	4.60	4.90	4.70	3.96	3.45	4.30
	2019	4.26	4.56	4.98	4.82	3.77	3.56	4.32
Local Peer Group	2016	3.32	3.30	3.43	3.22	2.49		3.15
	2017	3.47	3.75	3.74	3.61	2.83		3.48
	2018	3.36	3.60	3.57	3.48	2.68	2.32	3.17
	2019	3.66	3.69	3.56	3.59	3.02	2.78	3.38
Tribal Peer Group	2016	2.92	2.69	2.31	2.28	1.37		2.31
	2017	2.17	1.96	2.05	1.80	1.13		1.82
	2018	2.78	2.87	2.96	3.08	1.94	2.30	2.66
	2019	2.91	3.28	2.92	3.56	2.58	2.23	2.91
Territory Peer Group	2019	2.44	4.57	2.67	3.33	2.44	2.17	2.94

FIGURE 17

Percentage increase or decrease identified in 2016, 2017, 2018, and 2019 within each peer group across the Identify categories.

	Year	Asset Mgmt.	Business Environment	Governance	Risk Assessment	Risk Mgmt. Strategy	Supply Chain Risk Mgmt.	Identify Function
State Peer Group	2016	3%	4%	-1%	4%	2%		2%
	2017	4%	2%	4%	4%	4%		3%
	2018	6%	5%	2%	0%	10%		0%
	2019	1%	-1%	2%	3%	-5%	3%	0%
Local Peer Group	2016	12%	8%	16%	12%	31%		15%
	2017	5%	14%	9%	12%	14%		10%
	2018	-3%	-4%	-5%	-4%	-5%		-9%
	2019	9%	2%	0%	3%	13%	20%	7%
Tribal Peer Group	2017	-26%	-27%	-11%	-21%	-18%		-21%
	2018	28%	46%	44%	71%	71%		46%
	2019	5%	14%	-1%	16%	33%	-3%	9%

Supply Chain

Average scores increased by 3% for states and 20% for local governments in the “Supply Chain Risk Management” category.

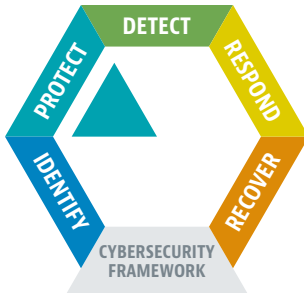
While the supply chain category scoring increased compared to 2018, it was the lowest scoring category overall for the state, local, tribal, and territory peer groups in 2019. This suggests organizations are now aware of their role in assessing and mitigating supply chain risk, but are still learning about how to approach this topic. This category was new to the NIST CSF in 2018.

The tribal peer group scored lower in the “Supply Chain Risk Management” category in 2019, compared to 2018. This may be due to the additional 13 tribal organizations that participated and are not as mature in this activity.

Tribal: Scores increased significantly for the tribal peer group in 2019 again in the “Risk Management Strategy” category. In two years, tribal organizations have increased over 100%, indicating they are on track to documenting policies in this function area.

2019 Identify Subcategory Highlights

- The lowest scoring subcategory for the 2019 state peer group (3.32) was **ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.**
- The lowest scoring subcategory for the 2019 local (2.51) and tribal (1.53) peer groups was **ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.**
- The subcategory **ID.AM-4: External information systems are catalogued** was relatively low for the state (3.62) and local (3.32) peer groups. This activity may tie in with supply chain cybersecurity issues, as the activity deals with external assets and data.



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.

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 and 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

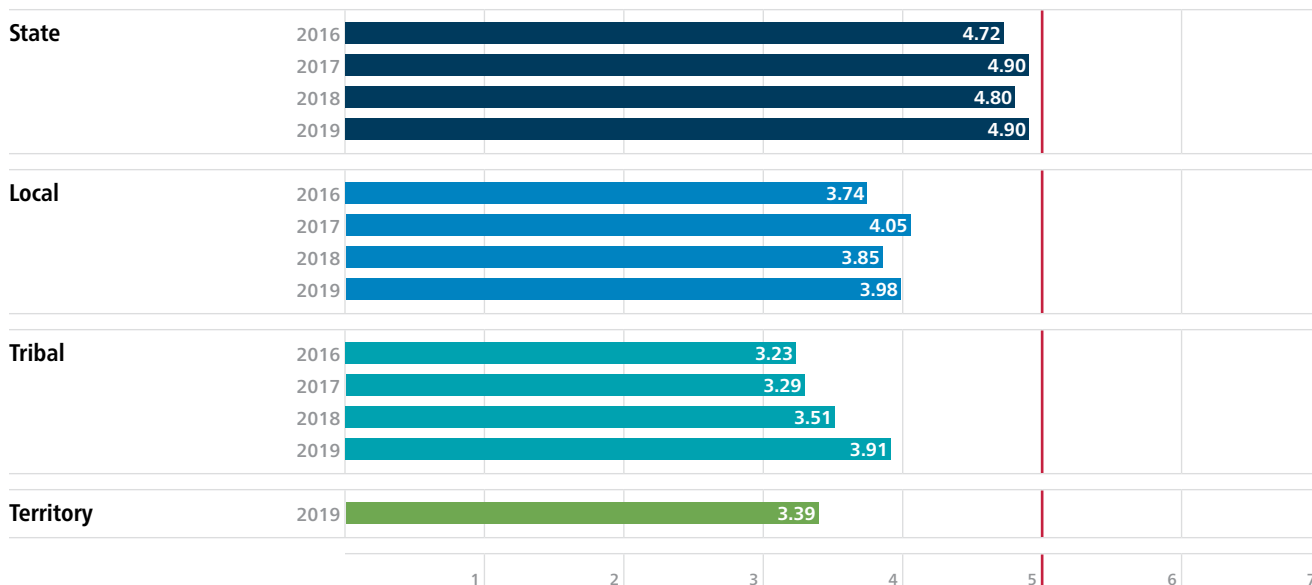
Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

Protective Technology

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

FIGURE 18

Year-to-year average for the Protect Function across the peer groups.



Local and Tribal

The 2019 local, tribal, and territory peer groups scored highest within the Protect function, indicating they have documented policies around this function and are beginning to develop additional procedures to support the policies.

Territory

The 2019 territory peer group scored highest within the Protect function, indicating they have documented policies around protecting the critical services they handle.

FIGURE 19**Percentage increase or decrease identified in 2016, 2017, 2018, and 2019 within each peer group across the Protect Function.**

Year	State	Local	Tribal
2016	2%	11%	
2017	4%	8%	2%
2018	-2%	-5%	7%
2019	2%	3%	11%

SLTT

There was an increase in all categories within the Protect function. This is a significant improvement for the state and local peer groups, who both experienced a decrease in 2018. Meanwhile, the tribal peer group saw an 11% increase in scores within the Protect function, compared to 2018. These increases suggest they have further formalized activity surrounding the categories in the Protect Function, and implemented changes on documenting their policies and procedures.

Tribal

In 2019, the tribal peer group saw an 11% increase in scores within the Protect function, compared to 2018. This suggests they have implemented changes on documenting their policies and procedures.

Category Highlights

FIGURE 20 Year-to-year averages for the Protect categories across the peer groups

	Year	Access Control	Awareness and Training	Data Security	Info. Protection Processes and Procedures	Maintenance	Protective Technologies	Protect Function
State Peer Group	2016	5.20	4.81	4.56	4.66	4.59	4.47	4.72
	2017	5.32	5.10	4.70	4.87	4.70	4.69	4.90
	2018	5.02	5.14	4.54	4.89	4.60	4.62	4.80
	2019	5.15	5.19	4.66	4.95	4.78	4.64	4.90
Local Peer Group	2016	4.54	3.69	3.60	3.42	3.61	3.59	3.74
	2017	4.86	4.16	3.97	3.79	3.97	3.55	4.05
	2018	4.46	4.03	3.67	3.57	3.72	3.63	3.85
	2019	4.66	4.06	3.89	3.65	3.85	3.76	3.98
Tribal Peer Group	2016	4.24	3.04	3.13	2.85	3.06	3.06	3.23
	2017	4.08	3.60	2.49	2.25	4.20	3.10	3.29
	2018	4.07	3.93	3.31	3.52	3.42	2.83	3.51
	2019	4.75	3.64	3.89	3.54	4.18	3.46	3.91
Territory Peer Group	2019	4.50	3.53	2.98	2.82	3.25	3.27	3.39

FIGURE 21

Percentage increase or decrease identified in 2016, 2017, 2018, and 2019 within each peer group across the Protect categories

	Year	Access Control	Awareness and Training	Data Security	Info. Protection Processes and Procedures	Maintenance	Protective Technologies	Protect Function
State Peer Group	2016	0%	1%	3%	3%	6%	1%	2%
	2017	2%	6%	3%	5%	2%	5%	4%
	2018	-6%	1%	-3%	0%	-2%	-1%	-2%
	2019	3%	1%	3%	1%	4%	0%	2%
Local Peer Group	2016	3%	17%	15%	10%	6%	16%	11%
	2017	7%	13%	10%	11%	10%	-1%	8%
	2018	-8%	-3%	-7%	-6%	-6%	2%	-5%
	2019	4%	1%	6%	2%	3%	4%	3%
Tribal Peer Group	2017	-4%	18%	-20%	-21%	37%	1%	2%
	2018	0%	9%	33%	56%	-19%	-9%	7%
	2019	17%	-7%	18%	1%	22%	22%	11%

State

The 2019 state peer group saw a 4% year-over-year increase within the “Maintenance” category, suggesting they have partially documented standards and/or procedures and are consistently updating their systems for the most secure functionality.

Local

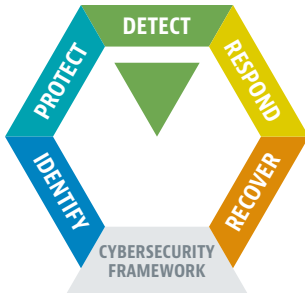
The 2019 local peer group experienced a 6% year-over-year increase within the “Data Security” category.

Tribal

The 2019 tribal peer group saw a 7% year-over-year decrease within the “Awareness and Training” category. It is possible more resources are needed to outline an awareness and training program.

2019 Protect Subcategory Highlights

- ❖ **PR.AT-3: *Third party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities*** is one of the lower scoring subcategories for the 2019 state (4.74), local (3.69), and tribal (2.89) peer groups. This may signal a similar trend as the risk management and supply chain category details: Organizations are not currently able to dedicate resources towards managing relationships with external entities and external systems/data.
- ❖ **PR.DS-8: *Integrity checking mechanisms are used to verify hardware integrity*** subcategory has improved since 2018, but is still relatively low for the 2019 state (3.36), local (3.08), and tribal (2.95) peer groups.
- ❖ **PR.IP-12: *A vulnerability management plan is developed and implemented*** subcategory is relatively low for the 2019 local (3.07) and the 2019 tribal (3.05) peer groups.



Detect Function

The quicker an organization can 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.

Detect Categories

Anomalies and Events

Anomalous activity is detected in a timely manner and the potential impact of events is understood.

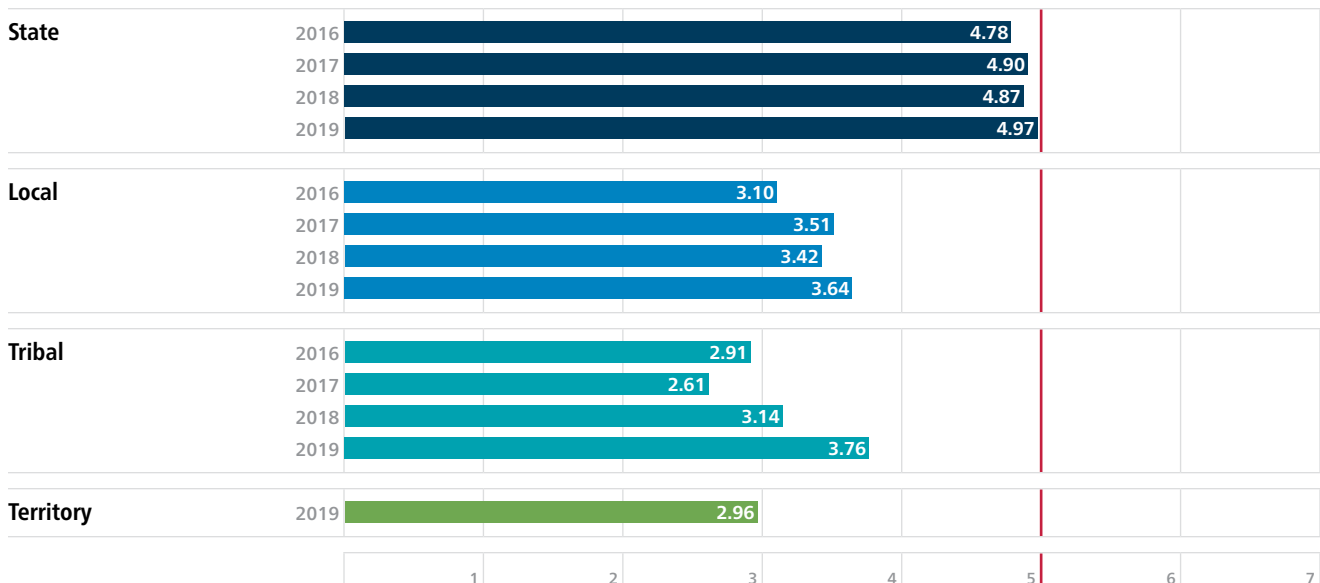
Security Continuous Monitoring

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 22 Year-to-year average for the Detect Function across the peer groups



State

The state peer group is 1% away from reaching the recommended minimum maturity level of “Implementation in Process” (5) within the Detect function. By implementing the policies and procedures they have outlined, they will reach this milestone.

FIGURE 23

Increase or decrease identified in 2016, 2017, 2018, and 2019 within each peer group across the Detect Function

Year	State	Local	Tribal
2016	4%	15%	
2017	2%	13%	-10%
2018	-1%	-3%	20%
2019	2%	6%	20%

All SLTT Peer Groups

All 2019 peer groups experienced a year-over-year increase within the Detect function. The state and local peer groups previously decreased in 2018, which may have been due to additional questions within this function.

Tribal

For the second consecutive year, the tribal peer group exhibited a 20% year-over-year increase within the Detect function. This indicates they have been successful in documenting their policies and procedures over the past two years and are working toward “Implementation in Process.”

Category Highlights

FIGURE 24 Year-to-year averages for the Detect categories across the peer groups

	Year	Anomalies and Events	Security Continuous Monitoring	Detection Processes	Detect Function
State Peer Group	2016	4.81	4.66	4.85	4.78
	2017	4.98	4.86	4.84	4.90
	2018	4.95	4.79	4.87	4.87
	2019	5.06	4.93	4.92	4.97
Local Peer Group	2016	2.95	3.44	2.91	3.10
	2017	3.38	3.83	3.32	3.51
	2018	3.30	3.59	3.38	3.42
	2019	3.49	3.92	3.52	3.64
Tribal Peer Group	2016	2.73	2.99	3.00	2.91
	2017	2.24	2.80	2.80	2.61
	2018	3.03	3.63	2.77	3.14
	2019	3.65	3.88	3.76	3.76
Territory Peer Group	2019	2.67	3.29	2.93	2.96

FIGURE 25

Increase or decrease identified in 2016, 2017, 2018, and 2019 within each peer group across the Detect categories

	Year	Anomalies and Events	Security Continuous Monitoring	Detection Processes	Detect Function
State Peer Group	2016	6%	1%	3%	4%
	2017	4%	4%	0%	2%
	2018	-1%	-1%	1%	-1%
	2019	2%	3%	1%	2%
Local Peer Group	2016	14%	14%	17%	15%
	2017	14%	11%	14%	13%
	2018	-2%	-6%	2%	-3%
	2019	6%	9%	4%	6%
Tribal Peer Group	2017	-18%	-6%	-7%	-10%
	2018	35%	30%	-1%	20%
	2019	20%	7%	36%	20%

State

The 2019 state peer group increased only 1% within the “Detection Processes” category, compared to 2018. This was their lowest scoring category within the Detect function.




Local

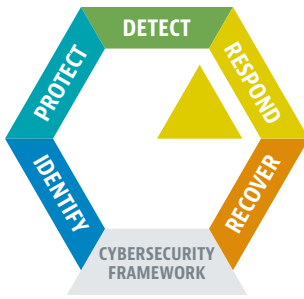
The 2019 local peer group had the most significant year-over-year increase in the “Security Continuous Monitoring” category (9%). This indicates they are 2% away from reaching a score level of “4”, which corresponds to “Partially Documented Standards and/or Procedures.” This indicates the organizations are continuously improving their security procedure documentation.

Tribal

The 2019 tribal peer group saw a significant year-over-year increase in the “Detection Processes” category (36%).

2019 Detect Subcategory Highlights

-  The following subcategory is one of the lower scoring subcategories within the 2019 state (3.70), local (3.30), and tribal (3.42) peer groups: **DE.CM-5: Unauthorized mobile code is detected.**
-  The following subcategory is relatively low within the 2019 state peer group (4.34): **DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.**
-  The following subcategory is relatively low within the 2019 local peer group (3.39): **DE.AE-5: Incident alert thresholds are established.**



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 CISA, 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.

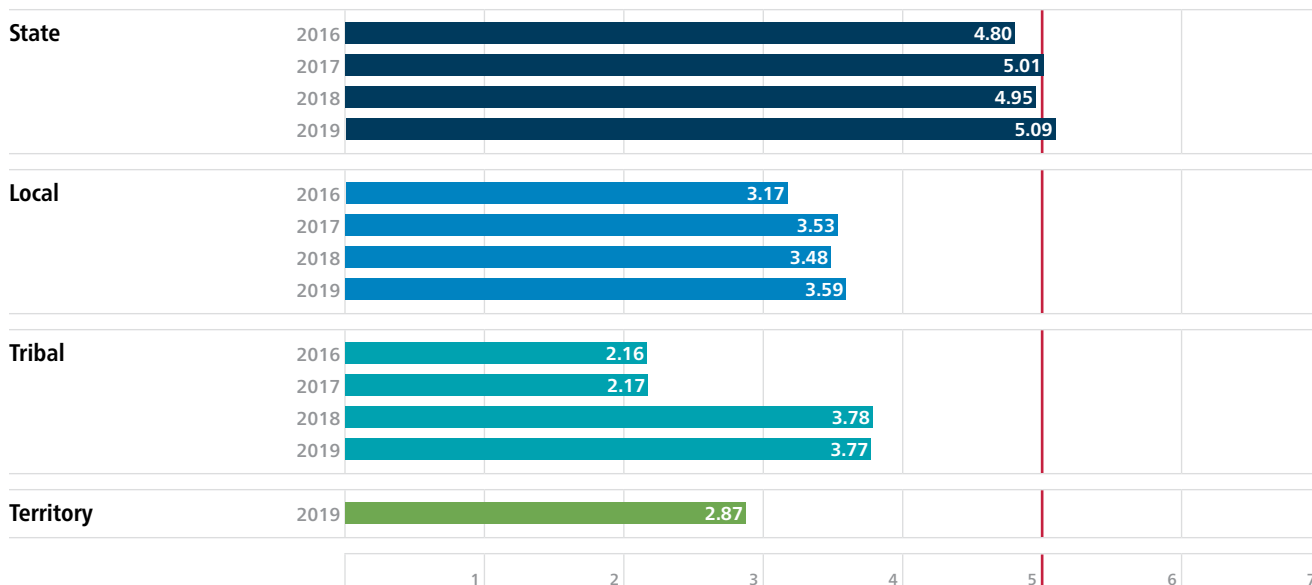
Mitigation

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 Year-to-year average for the Respond Function across the peer groups



State

The state peer group has scored above the recommended maturity level of “Implementation in Process” (score of 5). This suggests they are using tools and resources available and working to increase their scores to the maturity level of “Tested and Verified” (score of 6).

FIGURE 27 Increase or decrease identified in 2016, 2017, 2018, and 2019 within each peer group across the Respond Function

Year	State	Local	Tribal
2016	3%	5%	
2017	4%	11%	0%
2018	-1%	-1%	74%
2019	3%	3%	0%

State and Local

The 2019 state and local peer groups both experienced a year-over-year increase within the Respond function. This is an improvement from 2018, where both peer groups saw a year-over-year decrease. To continue increasing within Respond, these entities should allocate additional time to develop and understand actions following an incident to ensure they reach a maturity level of “Implementation in Process” (5).

State

For the fifth year, the state peer group have scored highest within the Respond function, indicating they have successfully implemented policies. This trend indicates that states have consistently documented their lessons learned after an incident, in addition to performing mitigation activities which allows an increase in maturity.

Category Highlights

FIGURE 28 Year-to-year averages for the Respond categories across the peer groups

	Year	Response Planning	Communications	Analysis	Mitigation	Improvements	Respond Function
State Peer Group	2016	4.96	4.68	4.87	4.99	4.53	4.80
	2017	5.13	4.88	5.08	5.10	4.88	5.01
	2018	5.05	4.90	4.92	5.02	4.84	4.95
	2019	5.08	5.04	5.18	5.33	4.81	5.09
Local Peer Group	2016	3.10	3.08	3.15	3.53	3.00	3.17
	2017	3.57	3.44	3.45	3.86	3.34	3.53
	2018	3.47	3.49	3.50	3.68	3.27	3.48
	2019	3.53	3.54	3.58	3.89	3.41	3.59
Tribal Peer Group	2016	1.88	1.91	2.47	3.00	1.56	2.16
	2017	2.20	1.88	2.25	3.13	1.40	2.17
	2018	4.33	3.80	3.37	3.89	3.50	3.78
	2019	3.79	3.97	3.97	3.88	3.24	3.77
Territory Peer Group	2019	3.00	3.03	2.83	2.83	2.67	2.87

FIGURE 29

Increase or decrease identified in 2016, 2017, 2018, and 2019 within each peer group across the Respond categories

	Year	Response Planning	Communications	Analysis	Mitigation	Improvements	Respond Function
State Peer Group	2016	3%	1%	1%	7%	2%	3%
	2017	3%	4%	4%	2%	8%	4%
	2018	-2%	0%	-3%	-2%	-1%	-1%
	2019	1%	3%	5%	6%	-1%	3%
Local Peer Group	2016	-4%	5%	6%	8%	8%	5%
	2017	15%	12%	10%	9%	11%	11%
	2018	-3%	2%	1%	-5%	-2%	-1%
	2019	2%	1%	2%	6%	4%	3%
Tribal Peer Group	2017	17%	-2%	-9%	4%	-10%	0%
	2018	97%	102%	50%	24%	150%	74%
	2019	-12%	4%	18%	0%	-7%	0%

All SLTT Peer Groups

2019 state, local, tribal, and territory participants all scored the lowest within the “Improvements” category in both Respond and Recover. Each peer group is in a different phase of the maturity scale, but are all struggling to meet the recommended maturity scoring level of “5” or “Implementation in Process.”

Local

The 2019 local peer group scored highest within the “Mitigation” category, increasing their year-over-year average scores by 6%. Continuous improvements within this category will allow incidents to be efficiently contained and help resolve an incident.

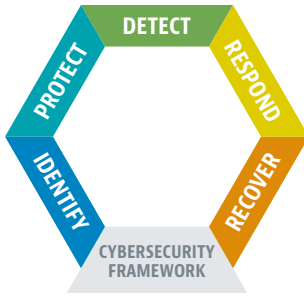
Tribal

The 2019 tribal peer group exhibited a 12% year-over-year decrease in the “Response Planning” category. This indicates more time should be spent properly documenting and updating response strategies following incidents that have occurred.

The 2019 tribal peer group had a significant year-over-year increase in the “Analysis” category (18%) indicating they are actively updating and improving their analysis processes around incident response. This will allow them to efficiently support response activities necessary in the future.

**2019 Respond
Subcategory Highlights**

- The following subcategory is one of the lower scoring subcategories within the 2019 local peer group (3.23): **RS.AN-4: *Incidents are categorized consistent with response plans.***
- The following subcategory is also relatively low for the 2019 local peer group (3.26): **RS.AN-3: *Forensics are performed.*** No cost forensic resources, such as MS-ISAC forensic analysis services, could be incorporated as part of their response plans and included in policy to increase maturity.



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.

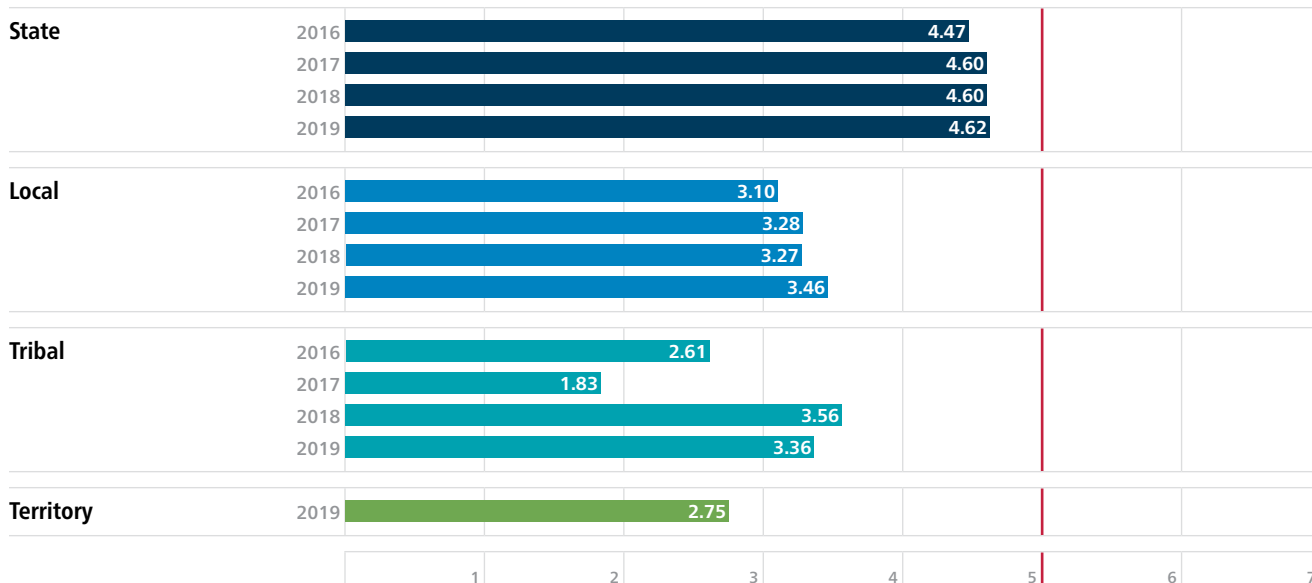
Improvements

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.

FIGURE 30 Year-to-year average for the Recover Function across the peer groups



Territory

The territory peer group scored lowest in the Recover function. This indicates that activities and processes are informally performed, however they are not documented. To assist with increasing maturity within Recover, there are free resources such as SANS policy templates and FedVTE training these entities can take advantage of.

FIGURE 31 Percentage increase or decrease identified in 2016, 2017, 2018, and 2019 within each peer group across the Recover Function

Year	State	Local	Tribal
2016	3%	8%	
2017	3%	6%	-30%
2018	0%	0%	95%
2019	0%	6%	-6%

State

The 2019 state peer group has plateaued within the Recover function, based on their scores since 2016. They are 8% away from reaching the maturity level of “Implementation in Process” (5).

Local

The 2019 local peer group exhibited a 6% year-over-year increase, which indicates work has been completed by documenting policies and procedures.

Tribal

The 2019 tribal peer group exhibited a year-over-year decrease within the Recover function. This decrease could be attributed to the additional tribal organizations that participated in 2019. Tribal organizations are currently at a maturity level of “Documented Policy” (3), indicating they need to develop standards and procedures to enhance the policy and increase their maturity.

Territory

The 2019 territory peer group scored lowest in the Recover function, suggesting they do not have formally documented policies and procedures. Procedures are needed in order for them to consistently recover from any incidents that affect their system.

Category Highlights

FIGURE 32 Year-to-year averages for the Recover categories across the peer groups.

	Year	Recovery Planning	Improvements	Communications	Recover Function
State Peer Group	2016	4.60	4.29	4.51	4.47
	2017	4.69	4.61	4.50	4.60
	2018	4.53	4.64	4.62	4.60
	2019	4.64	4.58	4.65	4.62
Local Peer Group	2016	3.23	2.98	3.11	3.10
	2017	3.35	3.15	3.34	3.28
	2018	3.34	3.16	3.30	3.27
	2019	3.59	3.40	3.40	3.46
Tribal Peer Group	2016	2.89	2.50	2.44	2.61
	2017	1.80	1.50	2.20	1.83
	2018	3.33	3.17	4.17	3.56
	2019	3.53	3.26	3.28	3.36
Territory Peer Group	2019	3.33	2.25	2.67	2.75

FIGURE 33

Percentage increase or decrease identified in 2016, 2017, 2018, and 2019 within each peer group across the Recover categories

	Year	Recovery Planning	Improvements	Communications	Recover Function
State Peer Group	2016	2%	0%	8%	3%
	2017	2%	7%	0%	3%
	2018	-3%	1%	3%	0%
	2019	2%	-1%	1%	0%
Local Peer Group	2016	3%	8%	14%	8%
	2017	4%	6%	8%	6%
	2018	0%	0%	-1%	0%
	2019	7%	8%	3%	6%
Tribal Peer Group	2017	-38%	-40%	-10%	-30%
	2018	85%	111%	90%	95%
	2019	6%	3%	-21%	-6%

State

The 2019 state peer group scored lowest in the “Improvements” category and also decreased by 1% compared to 2018. This could be an indication of a shift in cybersecurity priorities. States are 9% away from reaching the maturity level of “Implementation in Process” within this category, which would outline a specific process for updating and improving recovery activities based on lessons learned after an incident.

Tribal

The 2019 tribal peer group displayed a year-over-year decrease of 6% overall in the Recover function. Within the “Communications” category, the 2019 tribal peer group decreased by 21%. This indicates that additional communication plans and procedures should be documented and implemented.

2019 Recover Subcategory Highlights

✦ The following subcategory is one of the lower scoring subcategories for the 2019 state (4.34), local (3.23), and tribal (2.84) peer groups: **RC.CO-2: Reputation after an event is repaired.**

Subsector Peer Groups

FIGURE 34 Average scores across the NIST CSF functions for State level peer group subsectors, as well as the “Fusion Center” peer group subsector. The 2019 State: Elections group was referenced previously Figure 3 on page 10. Within each NIST CSF function below, the coloring is based on the 7 point maturity scale mirroring the figure in the Preface.

Peer Group Name	Organization Quantity	Identify	Protect	Detect	Respond	Recover	All Function Average
2019 State: Information Tech.	7	5.37	5.89	5.76	5.79	5.22	5.61
2019 State: Finance/Revenue	64	4.92	5.45	5.23	5.25	4.96	5.16
2019 State: Recreational	11	4.73	5.08	4.86	4.77	5.01	4.89
2019 State: Judicial	20	4.60	4.93	5.33	5.09	4.48	4.89
2019 State: Business/Admin.	74	4.69	5.14	4.87	4.93	4.67	4.86
2019 State: Fire/EMS/911	19	4.49	5.32	5.00	4.75	4.60	4.83
2019 State: Transportation	17	4.71	4.84	5.04	4.79	4.65	4.81
2019 State: Overall (50 States)	50	4.32	4.90	4.97	5.09	4.62	4.78
2019 State: Education	34	4.64	5.09	4.69	4.77	4.68	4.77
2019 State: Public Safety	59	4.54	4.95	4.84	4.79	4.54	4.73
2019 State: Higher Education	32	4.30	4.68	4.66	5.03	4.86	4.71
2019 State Agency: All	524	4.50	4.92	4.69	4.78	4.56	4.69
2019 State: Health and Human Svcs.	119	4.23	4.56	4.20	4.49	4.31	4.36
2019 Fusion Center	13	4.47	4.79	4.42	4.27	3.80	4.35
2019 State: Environmental	52	4.16	4.67	4.21	4.37	4.26	4.33
2019 State: Elections	16	3.93	4.44	4.19	4.42	4.04	4.20

FIGURE 35

Average scores across the NIST CSF functions for Local level peer group subsectors.
 The 2019 Local: Elections group was referenced previously in Figure 3 on page 10.
 Within each NIST CSF function below, the coloring is based on the 7-point maturity scale mirroring the figure in the Preface.

Peer Group Name	Organization Quantity	Identify	Protect	Detect	Respond	Recover	All Function Average
2019 Local: Health and Human Svcs.	44	4.49	4.89	4.80	4.62	4.53	4.67
2019 Local: Environmental	5	4.37	4.92	4.61	4.52	4.38	4.56
2019 Local: Business/Admin.	8	4.33	5.02	4.62	4.35	4.46	4.56
2019 Authority	31	4.08	4.48	4.03	3.89	3.97	4.09
2019 Local: Public Safety	348	3.81	4.39	4.13	3.99	3.91	4.05
2019 Local: Recreational	7	4.05	4.67	4.04	3.90	3.54	4.04
2019 Local: Port/Airport	15	3.73	4.26	4.26	4.06	3.80	4.02
2019 Local: Mass Transit	10	3.80	4.11	3.51	3.63	3.73	3.76
2019 Association	17	3.72	4.18	3.70	3.46	3.67	3.75
2019 Local: Public Utilities	30	3.76	3.95	3.61	3.77	3.64	3.75
2019 Local: City	540	3.44	4.11	3.75	3.67	3.47	3.69
2019 Local: Finance/Revenue	5	3.38	4.44	2.85	3.85	3.83	3.67
2019 Local: All	2,523	3.38	3.98	3.64	3.59	3.46	3.61
2019 Local: County/Parish	759	3.32	3.95	3.63	3.63	3.46	3.60
2019 Local: All Special Function	1,077	3.40	3.94	3.61	3.54	3.47	3.59
2019 Local: Emerg. Mgmt. Svc./911	279	3.22	3.76	3.45	3.39	3.24	3.41
2019 Local: Consolidated Govt.	10	3.29	3.90	3.43	3.14	3.09	3.37
2019 Local: Town/Township/Vill.	47	3.17	3.64	3.42	3.37	3.21	3.36
2019 Local: Fire/EMS/911 Comb.	418	3.14	3.68	3.40	3.30	3.21	3.35
2019 Commission	42	3.20	3.65	3.33	3.26	3.24	3.34
2019 Local: Fire Dept. and Svcs.	139	3.02	3.55	3.32	3.12	3.19	3.24
2019 Local: Elections	61	2.97	3.54	3.13	3.20	3.16	3.20
2019 Local: K-12 School District	118	2.83	3.33	2.73	2.84	2.94	2.93
2019 Local: Judicial	17	2.86	3.36	2.87	2.70	2.53	2.86
2019 Local: Community College	15	2.76	3.27	2.53	2.66	2.20	2.68

Noteworthy Subsector Findings

Education Subsectors

- The Education sector overall exhibited a year-to-year increase in participation. This indicates cybersecurity awareness is increasing in the education industry.
- The “Local–K-12 School District” subsector had an almost 300% year-to-year increase in participation, which indicates cybersecurity awareness is increasing for K-12 school districts.
- The “Local–K-12 School District” subsector saw a 14% year-to-year increase in scoring across all NIST CSF functions.
- The “State–Education” subsector experienced a 21% year-to-year increase in participation.
- The “State–Higher Education” subsector had over 5 times greater participation in 2019, compared to 2018.

State Department/Agency

- There was a 53% year-to-year increase in participation within the “State Department/Agency–All” subsector.

Public Safety and Fire/EMS/911 Subsectors

- There was a 79% increase in year-to-year participation within the “State–Public Safety” subsector, in addition to an increase of 414 participants within the “Local–Fire/EMS/911 Combined” subsector. Public Safety and Fire/EMS/911 participants on the state and local levels represent 27% of overall participation in the 2019 NCSR, which displays the change in landscape of respondents to the NCSR.

APPENDIX

Partners

The MS-ISAC and EI-ISAC are thankful for its partners in developing and conducting the NCSR: the U.S. Department of Homeland Security (DHS), the National Association of State Chief Information Officers (NASCIO), National Association of Counties (NACo), and GMIS International.



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 Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

For additional information, please visit <https://www.cisa.gov/>.



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.

For more information about GMIS International, please visit <https://www.gmis.org>.

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>.

Elections Infrastructure Information Sharing & Analysis Center

Grant-funded by DHS, the Elections Infrastructure Information Sharing and Analysis Center™ (EI-ISAC®) was established by the EIS-GCC to support the cybersecurity needs of the elections subsector. Through the EI-ISAC, election agencies will gain access to an elections-focused cyber defense suite, including sector-specific threat intelligence products, incident response and remediation, threat and vulnerability monitoring, cybersecurity awareness and training products, and tools for implementing security best practices.

For more information about the EI-ISAC, please visit <https://www.cisecurity.org/ei-isac>.



MS-ISAC[®]
Multi-State Information
Sharing & Analysis Center[®]



**Elections
Infrastructure
ISAC**[®]