# Nationwide Cybersecurity Review

- **Annual Self-Assessment**
  - No Cost
  - Anonymous
- **NIST Framework**
- **Required for some FEMA HSGP grant recipients**
  - Align use of these funds to gaps measured by the NCSR year to year
- **Cybersecurity Roadmap**
  - Identify Areas for Improvement
  - Justify Investments

| Score | Maturity Level — *The recommended minimum maturity level is set at a score of 5 and higher* |
|---|---|
| 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. |

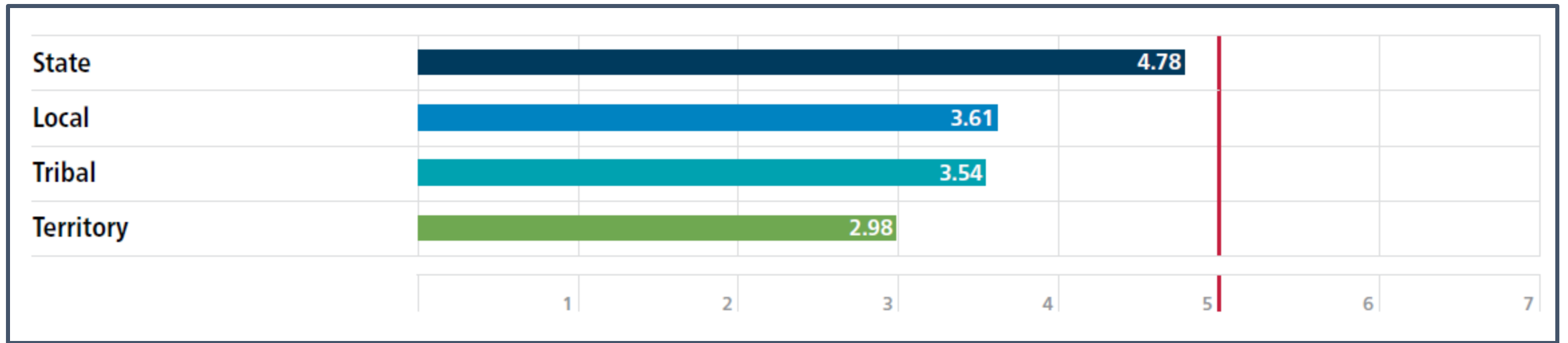**TLP: WHITE**

# Nationwide Cybersecurity Review

## 2019 Participants

- 3,135 Total Participant Organizations
  - 50 State Governments
  - 16 State Level Elections Offices
  - 2,523 Local Governments
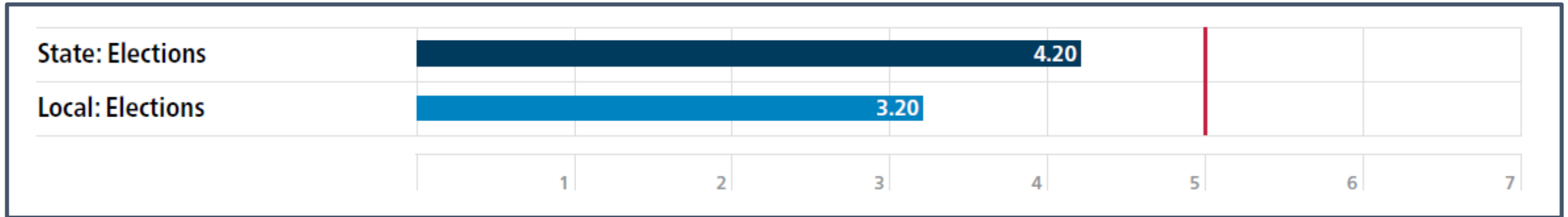  - 19 Tribal Governments
  - 6 Territorial Participants

https://www.cisecurity.org/ms-isac/services/ncsr

# 2019 NCSR Results for State, Local, Tribal, and Territorial Governments

| Category | Value |
|----------|-------|
| State | 4.78 |
| Local | 3.61 |
| Tribal | 3.54 |
| Territory | 2.98 |

# 2019 NCSR Results for State and Local Elections



| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| State: Elections | | | | 4.20 | | | |
| Local: Elections | | | 3.20 | | | | |

# 2019 NCSR Key Findings

- All peer groups of SLTT organizations continued to score below the overall minimum recommended maturity level of five (Implementation in Process).

- Adoption of a security framework has a significant impact on organizational cyber maturity.

- Continuous engagement is a key factor in the cybersecurity maturity of SLTTs.

- The lowest scoring categories measured in the NCSR are related to risk management and supply chain risk management.

# Highlighted Results by NIST CSF Category

- **Identify - Supply Chain Risk Management** was the area of lowest maturity for State Elections, Local Elections, and State, Local, Tribal, and Territorial Governments

- **Identify - Risk Management Strategy** was the area of second lowest maturity for State Elections, Local Elections, and State, Local, and Tribal Governments

- **Respond – Improvements and Recover – Improvements** were the lowest scoring categories within their functions for the State, Local, Tribal, and Territorial Governments

# Improving Maturity Moving Forward
## Some Key Recommendations for the SLTT Community and Partners

- **General Recommendation:** Use the [NIST CSF Policy Template Guide](#) to locate template policies for customization and adoption.

- **General Recommendation:** Services and resources for SLTT organizations should be delivered at no or low-cost with low impact on staffing.

- **Identify - Supply Chain Risk Management:** Leverage the [CIS Election Technology Procurement Guide](#). The MS-ISAC Metrics Working Group's new Supply Chain Subcommittee is collecting policy/procedure templates.

- **Respond – Improvements and Recover – Improvements:** Utilize the MS-ISAC Business Resiliency Working Group's guide on reviewing lessons learned and turning after-action reporting into improvements to processes.

# 2019 Top Reported Security Concerns

| | |
|---|---|
| **1** | Lack of sufficient funding |
| **2** | Increasing sophistication of threats |
| **3** | Lack of documented processes |
| **4** | Emerging technologies |
| **5** | Inadequate availability of cybersecurity professionals |
| **6** | Lack of a cybersecurity strategy (i.e., shifting priorities) |

# Nationwide Cybersecurity Review
## Tell all the SLTT about it!

- **2019 NCSR Summary Report is coming in Fall 2020**
  - Learn more about our findings and data set regarding SLTT maturity

- **2020 NCSR**
  - Currently Open for Registration
  - Officially open October 1 through December 31
  - More participation leads to better data and recommendations

- **Registration & Resources**
  - Located on NCSR Webpage
  - End-User Guidance
  - Results & Reporting Templates

**Resources**

---> **NCSR-FAQ**

---> **NCSR One Page Overview**

---> **NCSR-General User Guide**