CIS. Center for Internet Security®

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

NATIONWIDE
CYBERSECURITY
REVIEW

NCSR 2019 October 1 – December 31

Frequently Asked Questions

Contents

What is the Nationwide Cybersecurity Review?

Answer: The Nationwide Cybersecurity Review (NCSR) is a no-cost, anonymous, annual self-assessment, designed to measure gaps and capabilities of state, local, tribal and territorial governments' cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework (NISTCSF). The NCSR is sponsored by the Department of Homeland Security (DHS) and the Multi-State Information Sharing and Analysis Center® (MS-ISAC®).

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.

Using the results of the NCSR, DHS delivers a bi-yearly anonymous summary report to Congress, providing a broad picture of cybersecurity maturity across the SLTT communities.

When is the NCSR open?

Answer: The NCSR is open on an annual basis. For 2019, the NCSR will be open **October 1, 2019 through December 31, 2019**.

Do I need to be a member of the MS-ISAC to take the NCSR?

Answer: No. All States, State Agencies/Departments, Local Government Jurisdictions, Local Government Agencies/Departments, Tribal Organizations and Territorial Governments are encouraged to participate.

To learn more about the MS-ISAC please visit: **https://www.cisecurity.org/ms-isac**.

How much does it cost to take the NCSR? How long does it take to complete?

Answer: The NCSR is available at no cost to the user and takes approximately two to three hours to complete.

Who from my organization should participate in the NCSR?

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

- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Chief Security Officer (CSO)
- Chief Technology Officer (CTO)
- Director of Information Technology (IT)/Information Systems (IS)
- Individuals responsible for Information Technology management

What are the benefits of participating in the NCSR?

Answer: There are many benefits! Many participants have found that participating in the NCSR raises awareness and communication within their organization with both internal and external stakeholders, including executive leadership. By participating in the NCSR, you are creating a cybersecurity baseline which can be used to develop your future security roadmap AND you can compare your scores against the aggregate scores of your peers across the nation.

Upon completion of the NCSR, you will have access to custom individual reports that are specific to your organization. NCSR users can also access cybersecurity policy templates, courtesy of the SANS Institute.

Available Reports:

- **Current NCSR Results:** Provides your organization's current NCSR results across the NIST Cybersecurity Framework Functions and Categories.

- **Year-To-Year Results:** Provides your year-to-year NCSR results across the NIST Cybersecurity Framework Functions and Categories.

- **Year-To-Year Peer Profiles:** Provides your year-to-year NCSR results across the NIST Cybersecurity Framework Functions and Categories in comparison to your peers. Your peer groups are based on your Entity Type and Industry (Example: State Health & Human Services). Please note: Your results will be compared anonymously to other organizations in your peer group.

- **Year-To-Year Compliance Reports:** Provides access to your year-to-year compliance reports. Currently, we have the HIPAA Security Rule Crosswalk mapped to the NIST Cybersecurity Framework.

- **Year-To-Year Questions and Answers:** Provides a listing of all your questionnaires and submitted answers.

- **CIS Controls Mapped to NCSR:** Provides a report that maps version 7.1 of the CIS Controls to the NCSR questions, along with your submitted answers. The report provides the CIS Control, sub-control and implementation group.

- **NCSR Policy Dash:** Displays access to a repository of authoritative sources that provide a general understanding on what guides and governs your organization.

- **2019 Findings:** Provides a report that maps your organization's NCSR questions that were answered below the recommended minimum maturity of "Implementation in Process" to the NIST Cybersecurity Framework informative references (NIST 800-53, COBIT, and CIS Controls version 7.1).

How is the NCSR different than other audits, surveys, assessments, reviews, etc.?

Answer: The NCSR is different in several key ways that are beneficial to the SLTT community. It is designed to measure the gaps and capabilities of cybersecurity programs, while most other audits are designed to determine compliance or adherence to a specific set of requirements. When completed on an annual basis, the NCSR allows participants to measure changes in their cybersecurity program over time. Its year over year trending provides more than a "snapshot in time" in comparison to other audits, surveys, reviews, etc.

Can other organizations view my results?

Answer: No. All individual self-assessments and scores are kept confidential and anonymous.

Is my information shared with anyone outside of the MS-ISAC?

Answer: No, only the individuals assigned to your specific organization can view your organization's results. After the NCSR closes, the aggregated data is used in a Summary Report that is designed to measure gaps and capabilities of SLTT governments' cybersecurity programs. Every other year the Summary Report is shared with Congress to provide a broad picture of the cybersecurity maturity across the SLTT communities.

Am I required to complete the NCSR as a Homeland Security Grant Program (HSGP) grant recipient?

Answer: As outlined in the **FY 2019 Notice of Funding Opportunity (NOFO)** new requirement, State Homeland Security Program (SHSP) and Urban Area Security Initiative (UASI) recipients and sub-recipients must complete the NCSR by the end of Calendar Year 2019 to benchmark and measure their progress of improving their cybersecurity posture. The 2019 NCSR will be open from October through December 2019.

Who is responsible for completing the NCSR under the HSGP?

Answer: All recipients and sub-recipients of the SHSP and UASI grant programs are required to take the NCSR. The Chief Information Officer (CIO), Chief Information Security Officer (CISO) or equivalent for each recipient and sub-recipient should complete the NCSR. If there is no CIO/CISO, the most senior cybersecurity professional should complete the assessment. The FY 2019 HSGP NOFO is located online at: **http://www.fema.gov/grants** as well as on **http://www.grants.gov**.

For additional questions, email **NCSR@cisecurity.org**.

How do I register for the NCSR?

Answer: To register for the 2019 NCSR, please visit: **https://www.cisecurity.org/ms-isac/services/ncsr/** and complete the registration form.

Once your registration is complete, you will receive an e-mail with your credentials from **noreply@archer.rsa.com**.

For additional questions email **NCSR@cisecurity.org**.