Center for Internet Security®

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

NATIONWIDE CYBERSECURITY REVIEW

NCSR 2020

Frequently Asked Questions

Contents

General NCSR Questions:

Grant Requirement Questions:

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 (NIST CSF). 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 2020, the NCSR will be open through December 31, 2020.

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.

However, the MS-ISAC is free to join, and provides many cybersecurity resources and services at no cost. SLTT governments are always encouraged to join the MS-ISAC.

To learn more about the MS-IASC 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. Please note, the first time the NCSR is taken may take longer, as participants may need to gather information and consult other teams.

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.

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

Additionally, the MS-ISAC provides the following resources and guidance to assist with evaluating NCSR results, as well as potential "next steps" towards cybersecurity improvements:

Available Resources and Guidance

- NCSR One Page Overview
- NCSR General User Guide
- NCSR Data Reporting Template
- NIST CSF Policy Template Guide
- CIS Controls Version 7.1 – NCSR Results Mapping Template
- Cybersecurity Resources Guide
- Cybersecurity Resources Guide – NCSR Results Mapping Template
- The NCSR & Your HIPAA Security Rule Assessment Requirement
- NIST CSF Overview

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. The 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.

The NCSR is hosted on a password-protected GRC platform that does not allow an organization to access the records of other organizations.

Further, the NCSR assessment does not identify any specific internal technology or data points utilized by an organization. The answers are based on a custom response scale, based on policy usage and level of formalized activity along the NIST Cybersecurity Framework. This high-level data helps our MS-ISAC team and DHS assess how to best assist public organizations at the state and local level through funded initiatives.

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 an anonymized 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.

How do I register for the NCSR?

Answer: To register for the 2020 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. Your user account will be created within 2 to 4 business days so please sign up in advance of the submission deadline.

For additional questions email NCSR@cisecurity.org.

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

Answer: As outlined in the FY 2020 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 2020 to benchmark and measure their progress of improving their cybersecurity posture. The 2020 NCSR will be open from through December 31, 2020.

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 2020 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.

My small agency is a Homeland Security Grant Program grant sub-recipient, but our IT services are managed by another agency (i.e., consolidated IT department). Which entity is responsible for completing the NCSR?

Answer: Given the technical nature of the NCSR, it should be completed by the CIO, CISO or equivalent responsible at the agency that provides IT services to the recipient and/or sub-recipient. Outside vendors can assist agencies complete the NCSR, but each recipient and sub-recipient is responsible for ensuring that the response to the assessment accurately reflects their agency's capabilities. If an agency is unable to complete the NCSR because the state or local entity uses a privately contracted outside party, the state or local entity must have a specific person within that group register for a user account.

If an organization does not have an IT employee or contractor, then the organization should select the employee who can best answer technology-related questions.

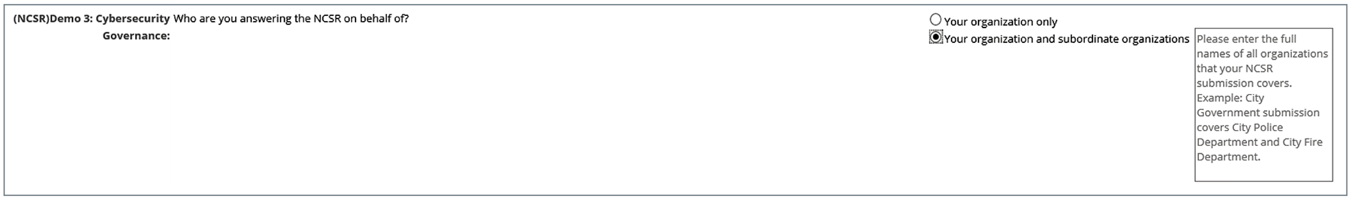
All registrants of the NCSR must utilize a government email address. Gmail, Yahoo, Hotmail etc. will not be used to create an NCSR user account, unless it is verified as an official work email. If you are a private contractor hired by a state, local, tribal, or territorial government, you will need to create a government email address. If you do not have a government email address but need to take the NCSR on behalf of a government, please reach out to NCSR@cisecurity.org.

If you are a nonprofit organization taking the NCSR on behalf of SHSP and UASI grants, please email NCSR@cisecurity.org confirming your State Administrative Agency (SAA): https://www.fema.gov/media-library/assets/documents/28689.

If you have any questions regarding these requirements, please email NCSR@cisecurity.org.

I work for an IT department that services multiple agencies, all on the same IT infrastructure. Do we have to complete it twice?

Answer: No. The NCSR is a network-level assessment. It only needs to be completed once when multiple recipients and/or sub-recipients share a network. For the entity completing the NCSR, please make sure to identify all recipients and/or sub-recipients within Demographics Question #3 of the NCSR so that each are reflected in the compliance reporting. This may mean multiple departments or agencies within your organization, so please identify all that apply. Demographics Question #3 states, “Who are you answering the NCSR on behalf of?” The screenshot below shows how that question appears, with a text box for the user to list the applicable recipients:



(NCSR)Demo 3: Cybersecurity Who are you answering the NCSR on behalf of?
Governance:

○ Your organization only
● Your organization and subordinate organizations

Please enter the full names of all organizations that your NCSR submission covers. Example: City Government submission covers City Police Department and City Fire Department.

Questions

For administrative and technical questions about the NCSR, please contact the Multi-State Information Sharing and Analysis Center® (MS-ISAC®) at ncsr@cisecurity.org.