



October 1 – February 28

# Frequently Asked Questions

## Contents

### General NCSR Questions

- What is the Nationwide Cybersecurity Review? ..... 2
- When is the NCSR open? ..... 2
- What if my organization misses the deadline to complete the NCSR? Could I request an extension? ..... 2
- Do I need to be a member of the MS-ISAC to take the NCSR? ..... 2
- How much does it cost to take the NCSR? How long does it take to complete? ..... 2
- Who from my organization should participate in the NCSR? ..... 3
- What are the benefits of participating in the NCSR? ..... 3
- How is the NCSR different than other audits, surveys, assessments, reviews, etc.? ..... 4
- Can other organizations view my results? ..... 4
- Is my information shared with anyone outside of the MS-ISAC? ..... 4
- How do I register for the NCSR? ..... 4
- If I sign up with the incorrect organization name, can I request a name change? ..... 4
- How can I add or remove contacts who have access to my organization's NCSR assessment? ..... 4

### Grant Requirement Questions

- Am I required to complete the NCSR as a Homeland Security Grant Program (HSGP) grant recipient? ..... 5
- Who is responsible for completing the NCSR under the HSGP? ..... 5
- 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? ..... 5
- I work for an IT department that services multiple agencies, all on the same IT infrastructure. Do we have to complete it twice? ..... 5
- Will we be notified when our NCSR assessment is submitted? Or when reporting is available? ..... 6
- Questions ..... 6

## General NCSR 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 from October 1 to February 28.

After the close date of February 28, the NCSR data is compiled into an anonymized Summary Report that is presented to Congress as part of a program requirement for the MS-ISAC. While the October through February timeframe applies to NCSR submission, all NCSR participants have the opportunity to access their reporting and resources in the NCSR portal at any time.

### What if my organization misses the deadline to complete the NCSR? Could I request an extension?

**Answer:** There are no extensions to complete the NCSR. The assessment officially closes on February 28 each year. If your organization misses the deadline, you will be able to complete the next offered NCSR, which will open on October 1. If you are a recipient of the Homeland Security Grant Program (HSGP) and have missed the deadline, you can select the appropriate fiscal year you are participating on behalf of in the next assessment. You will then be covered for both years.

### 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-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. Please note, the first time the NCSR is taken may take longer, as participants may need to gather information and consult other teams. Once you have completed the NCSR for the first time, a majority of your responses will be pre-populated the next year so you can update responses where applicable.

**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.
- **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. You can view your peer profiles two ways. The detail view will show all category and subcategory responses to the NCSR. The summary view is where you can view the function and category responses.
- **HIPAA Compliance Report:** Provides access to your year-to-year compliance reports. Currently, we have the HIPAA Security Rule Crosswalk mapped to the NIST Cybersecurity Framework.
- **Cybersecurity Resources Report:** Aligns your NCSR results to resources such as MS-ISAC services, open source tools, and policy templates.
- **CIS Controls v8 Report:** Displays your NCSR results aligned to the practices within the CIS Controls cybersecurity framework.

Additionally, the MS-ISAC provides resources and guidance to assist with evaluating NCSR results, as well as potential "next steps" towards cybersecurity improvements. These materials can be found under the "NCSR Resources" section of the [NCSR website](#).

**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 NCSR, please visit: <https://www.cisecurity.org/ms-isac/services/ncsr/> and complete the registration form.

Your user account will be created within 2 to 4 business days so please sign up in advance of the submission deadline. Once your account has been created, you will receive an e-mail with your credentials from [customer.support@logicmanager.com](mailto:customer.support@logicmanager.com).

For additional questions email [NCSR@cisecurity.org](mailto:NCSR@cisecurity.org).

**If I sign up with the incorrect organization name, can I request a name change?**

**Answer:** If you signed up with the incorrect organization name, the NCSR team can change the name, as long as the organization is a first time NCSR participant. For historical tracking and consistency, we cannot change an organization name within the NCSR, if the organization has participated in the past."

**How can I add or remove contacts who have access to my organization's NCSR assessment?**

**Answer:** Please email [NCSR@cisecurity.org](mailto:NCSR@cisecurity.org) with the new contact person's name and email address. To remove a contact, please notify [NCSR@cisecurity.org](mailto:NCSR@cisecurity.org) of the specific contact, and the NCSR team will complete that step.

## Grant Requirement Questions

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

**Answer:** As outlined in the [FY 2022 Notice of Funding Opportunity \(NOFO\)](#), State Homeland Security Program (SHSP) and Urban Area Security Initiative (UASI) recipients and sub-recipients must complete the NCSR by February 28, 2023, to benchmark and measure their progress of improving their cybersecurity posture.

**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 2022 HSGP NOFO is located online at: <https://www.fema.gov/media-collection/homeland-security-grant-notice-funding-opportunity> as well as on <http://www.grants.gov>.

For additional questions, email [askcsid@fema.dhs.gov](mailto:askcsid@fema.dhs.gov).

**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](mailto:NCSR@cisecurity.org).

If you are a nonprofit organization taking the NCSR on behalf of SHSP and UASI grants, please email [NCSR@cisecurity.org](mailto: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](mailto: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 the following Demographics question 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 as seen in the questions below.

Who are you answering the NCSR on behalf of? If your IT operations and infrastructure covers multiple departments/offices, please select all applicable department/office types below. For Homeland Security Grant Program (HSGP) recipients, enter all applicable entity names that your NCSR submission is covering within the next question's text box. This organizational information must reflect the "Legal Agency Name" as part of the Biannual Strategic Implementation Report (BSIR) reporting within the HSGP process. For additional details, please refer to the help text (question mark icon). \* ⓘ

Select option(s) ▼

If this NCSR submission is covering additional entities who receive HSGP funding, please enter those entity names here. Please see the help text (question mark icon) for examples. If this NCSR submission is not covering additional entities who receive HSGP funding, please enter "N/A": ⓘ

Enter text

**Will we be notified when our NCSR assessment is submitted? Or when reporting is available?**

**Answer:** You will not get a notification upon submitting the NCSR. However, upon selecting "Submit Task", your NCSR answers will be locked in. You will then have access to a Completion Certificate in the NCSR portal. All reporting is automatically available in the NCSR portal the day after you submit your assessment task. There will not be an email notification that reporting is available.

**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](mailto:ncsr@cisecurity.org).