CIS Center for Internet Security®

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

NCSR Overview

The Nationwide Cybersecurity Review (NCSR) is a no-cost, anonymous, annual self-assessment that is designed to measure gaps and capabilities of U.S. State, Local, Tribal, and Territorial (SLTT) governments' cybersecurity programs. The NCSR is open annually from October 1 to February 28.

The NCSR is aligned to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The CSF provides a common language for understanding, managing, and expressing cybersecurity risk. It can be used to help identify and prioritize actions for reducing cybersecurity risk as well as align policy, business, and technological approaches for managing risk.

Register for the NCSR

To register for the NCSR, please visit www.cisecurity.org/ms-isac/services/ncsr/

Benefits

- Receive metrics specific to your organization to identify gaps and develop a benchmark to gauge year-to-year progress.
- Have the option of anonymously measuring your results against your peers.
- Attain reporting in order to prioritize the "next steps" towards cybersecurity improvement based on area(s) of deficiency.
- Obtain resources and services that can help you fulfill the desired steps towards cybersecurity improvement.
- Translate your NCSR scores to the HIPAA Security Rule scores using an automatic self-assessment tool.
- Utilize data summaries to justify resource and funding opportunities within your organization.
- Fulfill the NCSR assessment requirement for the Homeland Security Grant Program (HSGP).

For administrative and technical questions about the NCSR, please contact the NCSR team at ncsr@cisecurity.org.

NCSR Maturity Scale

Responses to the NCSR correspond to scale below. The lowest score is a "1," which indicates a maturity level of "Not Performed." Meanwhile, "7" is the highest score at a maturity level of "Optimized."

7	**Optimized**	Your organization is executing the activity or process and has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	**Tested and Verified**	Your organization is executing the activity or process and has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	**Implementation in Process**	Your organization has an activity or process defined within documented policies, standards, and/or procedures. Your organization is in the process of implementing and aligning the documentation to a formal security framework and/or methodology.
4	**Partially Documented Standards and/or Procedures**	Your organization has a formal policy in place and has 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 that has been approved by senior management.
2	**Informally Done**	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 senior management.
1	**Not Performed**	Activities, processes, and technologies are not in place to achieve the referenced objective.