NATIONWIDE CYBER SECURITY REVIEW

Insert Org Name

2018 NCSR Data Reporting Template

Background (possible discussion items)

- Provide background on current security program
- Include recent milestones & security program successes
- Discuss where you have been and where we are heading
- Discuss planned/milestones goals
- Discuss number of years participated in NCSR

Previous Year’s Accomplishments (possible discussion items)

- List acknowledgments/accomplishments
- New Hires
- List new implementations
- Updates
- Participated in

Assessing INSERT ORG NAME Security Posture

This past year **INSERT ORG NAME** participated in MS-ISAC’s Nationwide Cybersecurity Review (NCSR).

The Nationwide Cybersecurity Review (NCSR) is a free, confidential, annual self-assessment survey that is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). It is sponsored by the Department of Homeland Security (DHS) and the Multi-State Information Sharing & Analysis Center (MS-ISAC).

The NCSR evaluates cybersecurity maturity across the nation while providing actionable feedback and metrics directly to individual respondents in State, Local, Tribal & Territorial (SLTT) governments.

Using the results of the NCSR, DHS delivers a biennial anonymous summary report to Congress providing a broad picture of the cybersecurity maturity across the SLTT community.

The NCSR is a valuable tool, it allows us to receive metrics specific to our organizations, develop a benchmark to gauge our year-to-year progress, and anonymously measure our results against our peers. It also provides a way to map our security strategies to the controls specified by NIST 800-53, COBIT & CIS Controls.

NCSR Structure

The NCSR question set was built upon the NIST CSF with some minor alterations. The questions set consists of a collection of cybersecurity-related activities organized into five main functions: **Identify, Protect, Detect, Respond,** and **Recover**. These five main functions are broken down into 108 sub-categories which the NCSR uses as a basis for the questions in the NCSR self-assessment.

Overview of the NIST CSF Functions:

Identify Function: The activities under this functional area are key for an organization's understanding of their current internal culture, infrastructure, and risk tolerance. By incorporating sound risk management principles into cybersecurity programs, organizations will be able to continuously align their efforts towards protecting their most valuable assets against the most relevant risks.

Protect Function: The activities under the Protect Function pertain to different methods and activities that reduce the likelihood of cybersecurity events from happening and ensure that the appropriate controls are in place to deliver critical services. These controls are focused on preventing cybersecurity events from occurring.

Detect Function: The activities under the Detect Function pertain to an organization's ability to identify incidents.

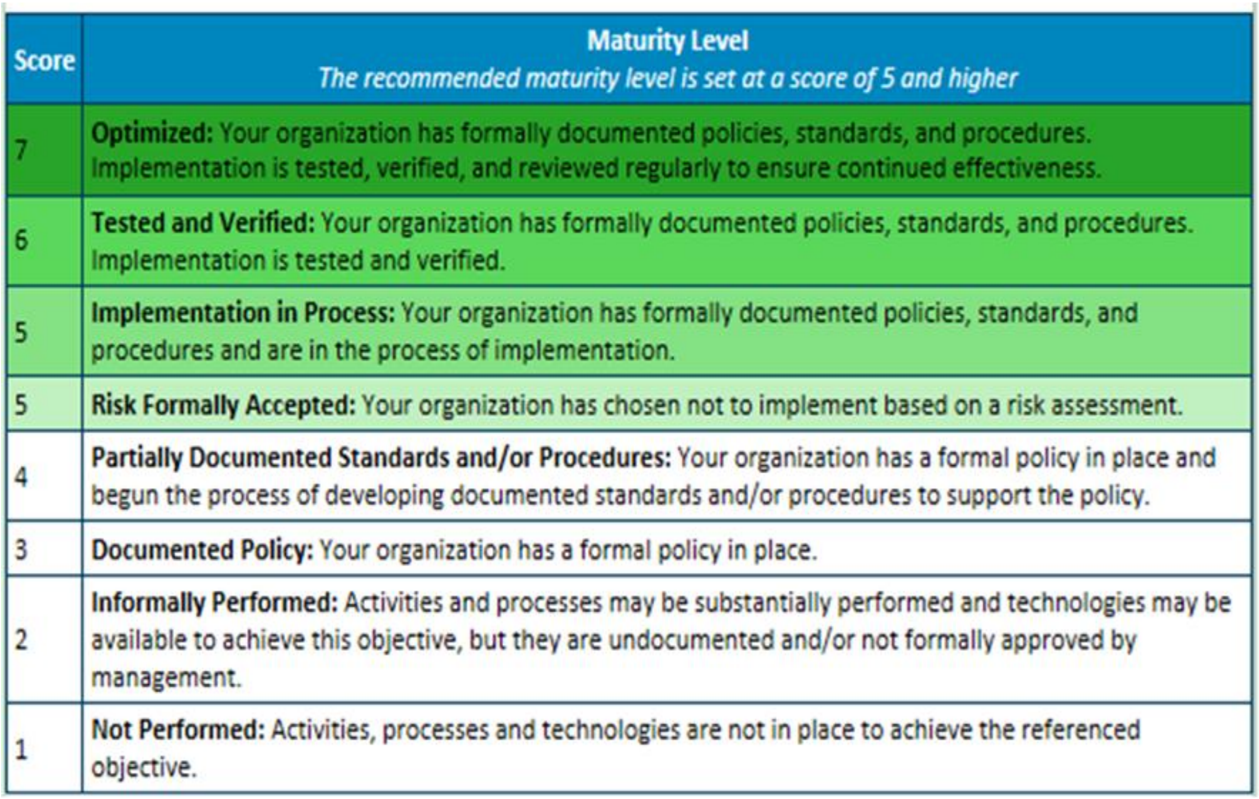
Respond Function: The activities within the Respond Function examine how an organization plans, analyzes, communicates, mitigates, and improves its response capabilities.

Recover Function: The activities within the Recover Function pertain to an organization's ability to return to its baseline after an incident has occurred. Such controls are focused not only on activities to recover from the incident, but also on many of the components dedicated to managing response plans throughout their lifecycle.

NCSR Maturity Scale

The NCSR utilizes a maturity scale that assesses how an organization is addressing the different activities within the NIST CSF. The maturity scale allows participants to indicate how formalized these cybersecurity activities are within their organization. Following risk management principles, the response framework includes allowing organizations to identify which activities they have formally acknowledged and chosen not to implement because of their own risk assessment.

In order to provide a target for the SLTT community, a team of SLTT cybersecurity professionals developed a recommended minimum maturity level as a common baseline for the NCSR. The maturity level uses ***Implementation in Process*** as the recommended minimum maturity level. The below figure provides a full breakdown of the NCSR Maturity Level response scale along with the scores associated with each maturity level.



Score	Maturity Level *The recommended 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 are 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.

Where Are We Today?

Insert report titled: **"Current NCSR Results"** Provides your organizations current years NCSR results across the NIST CSF Functions and Categories.

Possible Discussion Items:

- Call out strengths
- Call out areas for improvement
- Create a baseline/road map based on these results

Where Have We Progressed?

Insert report titled: **"Year-to-Year Results"** Provides your year-to-year NCSR results aligned to the NIST CSF Functions and Categories.

Possible Discussion Items:

- Drill down to different categories to see where you increased/decreased
- To what do you attribute your scores increasing/decreasing (what can you tie to this data to?)
- What road blocks are you seeing?

How Do We Compare Against Our Peers?

Insert report titled: **"Year-To-Year Peer Profiles"** A report that provides your NCSR scores against your peers.

Possible Discussion Items:

- Explain why above and/or below your peers
- Possibly discuss different ways maturity is being measured
- Are there relative factors that differentiate you from your peers?

HIPAA Compliance

If applicable, attach report titled: **"Year-to-Year Compliance Reports"** which is a unique report that maps the HIPAA Security Rule to the NIST CSF and ties in your NCSR responses.

Possible Discussion Items:

- The intent of this report is to use it as a tool for a self-assessment of your HIPAA Security Rule compliance. The report assists in developing a gap assessment and identifying areas of improvement
- Serves as a valuable documentation trail

Attach 2017 Nationwide Cybersecurity Review Summary Report

Click Here