EI-ISAC®

MS-ISAC®

Nationwide Cybersecurity Review Overview

Presenter & Panel Information

MS-ISAC Presenter: Tyler Scarlotta

MS-ISAC Members & Metrics Workgroup:

- Gary Coverdale
- Jim Cusson
- Joe Frohlich
- Kim LaCroix

DHS & FEMA:

- Tom Filippone
- Madelyn Weingast
- Margaret Wilson

NATIONWIDE CYBERSECURITY REVIEW

NCSR 2019 October 1–December 31

Nationwide Cybersecurity Review (NCSR)

- No-Cost, Anonymous, Annual Self-Assessment
- Measures the gaps and capabilities of State, Local, Tribal, and Territorial governments’ cybersecurity programs
  - The 2019 NCSR can be completed by organizations outside of the SLTT category, if the organization is required, as noted in the HSGP NOFO (Example: A nonprofit organization)
- Based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Sponsored by the Department of Homeland Security (DHS) and the Multi-State Information Sharing and Analysis Center® (MS-ISAC®)

Nationwide Cybersecurity Review (NCSR)

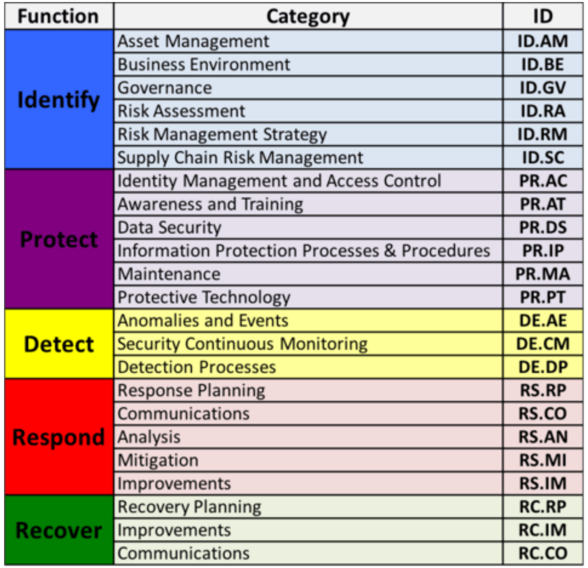
- 2019 assessment is open to complete October 1, through December 31
  - You can access your data throughout the year
- The NCSR provides metrics to help your organization
- An end-user associated with an organization in the NCSR portal is the only person viewing the specific organization's results
- The NCSR is a service offered within the Multi-State ISAC
  - MS-ISAC provides no-cost services to SLTT organizations, to help improve cybersecurity
  - You do not have to be a MS-ISAC member to take the NCSR
  - Link to MS-ISAC Page: https://www.cisecurity.org/ms-isac/
  - Contact Information: info@msisac.org

Benefits

- Receive metrics specific to your organization to identify gaps and develop a benchmark to gauge year-to-year progress, as well as anonymously measure your results against your peers
- For HIPAA compliant agencies, translate your NCSR scores to the HIPAA Security Rule scores of an automatic self-assessment tool
- Access to informative references such as NIST 800-53, COBIT, and the CIS Controls that can assist in managing cybersecurity risk
- Nationally, aggregate NCSR data provides a baseline, foundational understanding of SLTT cybersecurity posture to help drive policy, governance and resource allocation
- Results enable Federal partners to better understand the status quo and engage in more strategic, cyber-specific planning and preparedness to help manage national risk and improve SLTT core capabilities

Question Set

The NCSR question set was built upon the NIST CSF Core, with 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 includes several demographic questions, as well as automation related questions. The overall total is 141 questions.



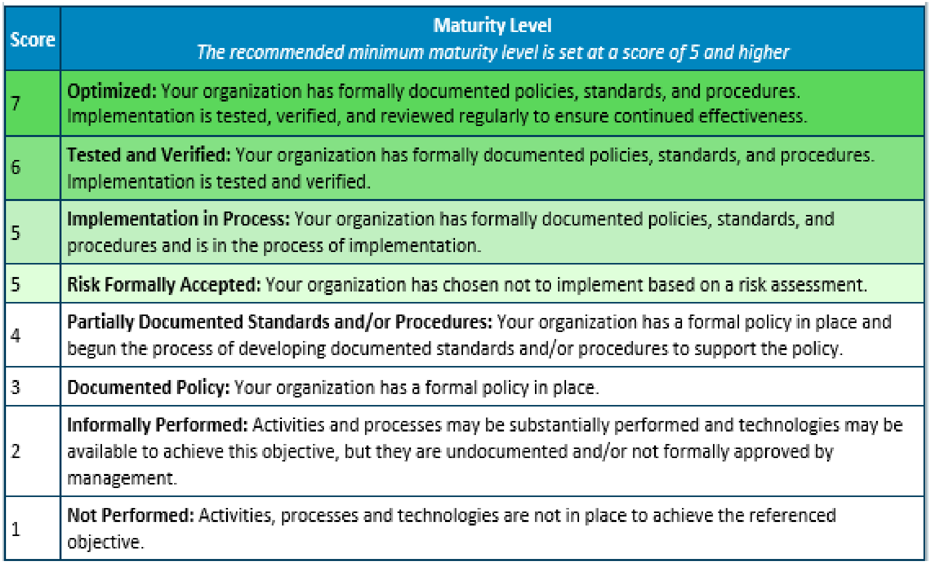
Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

NIST Cybersecurity Framework

https://www.nist.gov/cyberframework/framework

Response Scale

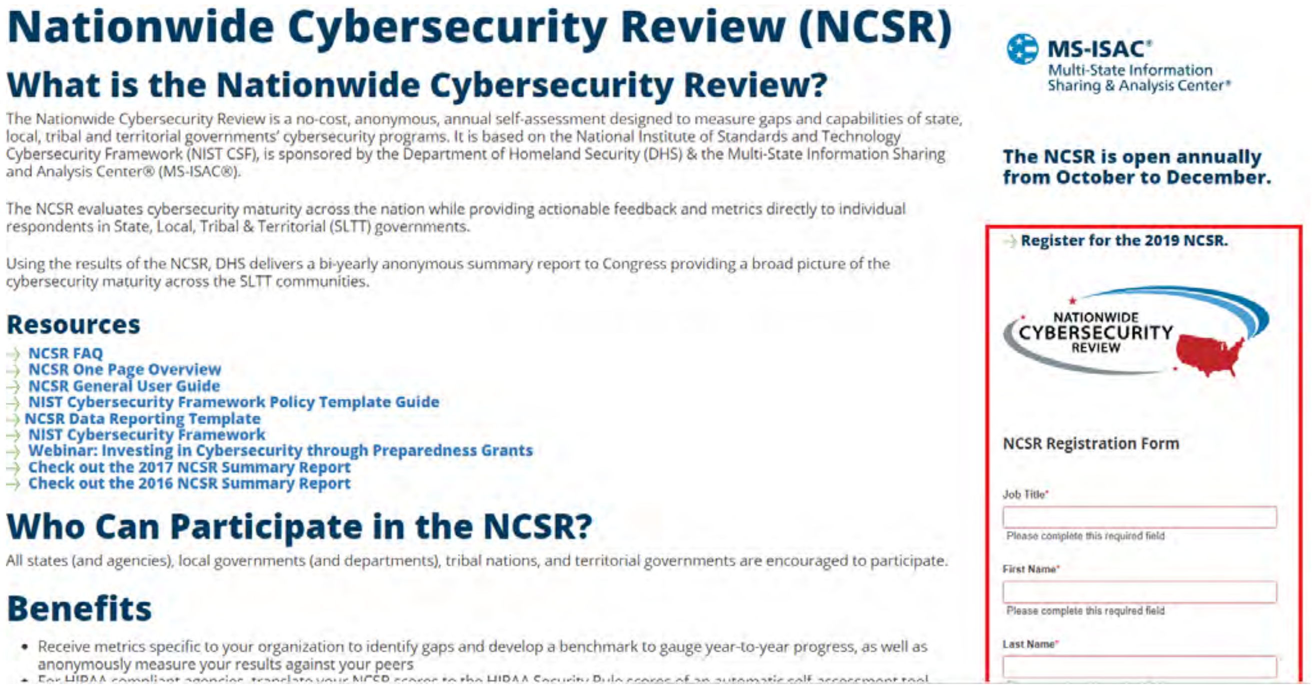
The NCSR utilizes a maturity scale that assesses how an organization is addressing the different activities within the NIST CSF. The maturity scale allows participants to indicate how formalized these cybersecurity activities are within their organization. Following risk management principles, the response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



Score	Maturity Level *The recommended minimum 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 is 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.

How to Register?

Registration Link: https://www.cisecurity.org/ms-isac/services/ncsr/



Nationwide Cybersecurity Review (NCSR)

What is the Nationwide Cybersecurity Review?

The Nationwide Cybersecurity Review 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), is sponsored by the Department of Homeland Security (DHS) & the Multi-State Information Sharing and 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 bi-yearly anonymous summary report to Congress providing a broad picture of the cybersecurity maturity across the SLTT communities.

Resources

- NCSR FAQ
- NCSR One Page Overview
- NCSR General User Guide
- NIST Cybersecurity Framework Policy Template Guide
- NCSR Data Reporting Template
- NIST Cybersecurity Framework
- Webinar: Investing in Cybersecurity through Preparedness Grants
- Check out the 2017 NCSR Summary Report
- Check out the 2016 NCSR Summary Report

Who Can Participate in the NCSR?

All states (and agencies), local governments (and departments), tribal nations, and territorial governments are encouraged to participate.

Benefits

- Receive metrics specific to your organization to identify gaps and develop a benchmark to gauge year-to-year progress, as well as anonymously measure your results against your peers
- For HIPAA compliant agencies, translate your NCSR scores to the HIPAA Security Rule scores of an automatic self-assessment tool

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

The NCSR is open annually from October to December.

→ **Register for the 2019 NCSR.**

NCSR Registration Form

Job Title*

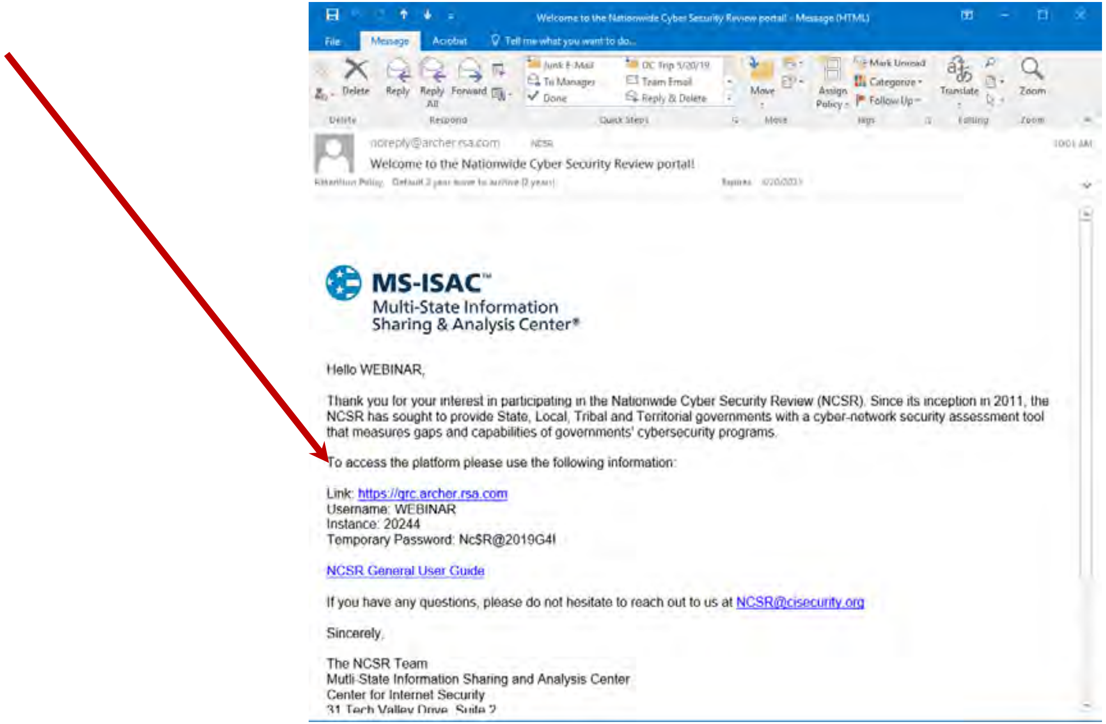
Please complete this required field

First Name*

Please complete this required field

Last Name*

NCSR Credentials



noreply@archer.rsa.com NCSR 10:01 AM

Welcome to the Nationwide Cyber Security Review portal!

Retention Policy Default 2 year move to archive (2 years) Expires 4/20/2021

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

Hello WEBINAR,

Thank you for your interest in participating in the Nationwide Cyber Security Review (NCSR). Since its inception in 2011, the NCSR has sought to provide State, Local, Tribal and Territorial governments with a cyber-network security assessment tool that measures gaps and capabilities of governments' cybersecurity programs.

To access the platform please use the following information:

Link: https://grc.archer.rsa.com
Username: WEBINAR
Instance: 20244
Temporary Password: NcSR@2019G4!

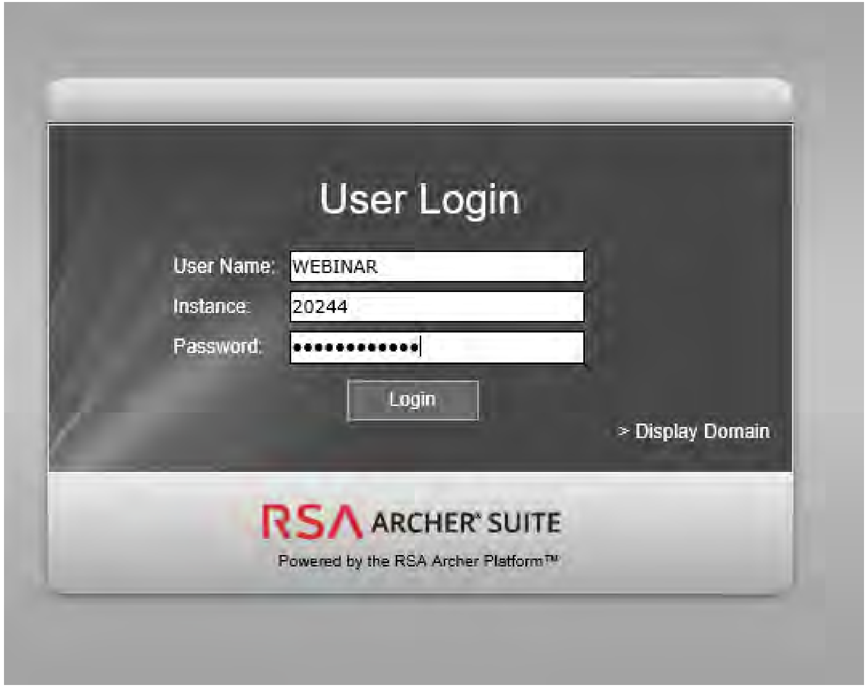
NCSR General User Guide

If you have any questions, please do not hesitate to reach out to us at NCSR@cisecurity.org

Sincerely,

The NCSR Team
Mutli-State Information Sharing and Analysis Center
Center for Internet Security
31 Tech Valley Drive, Suite 2

User Login



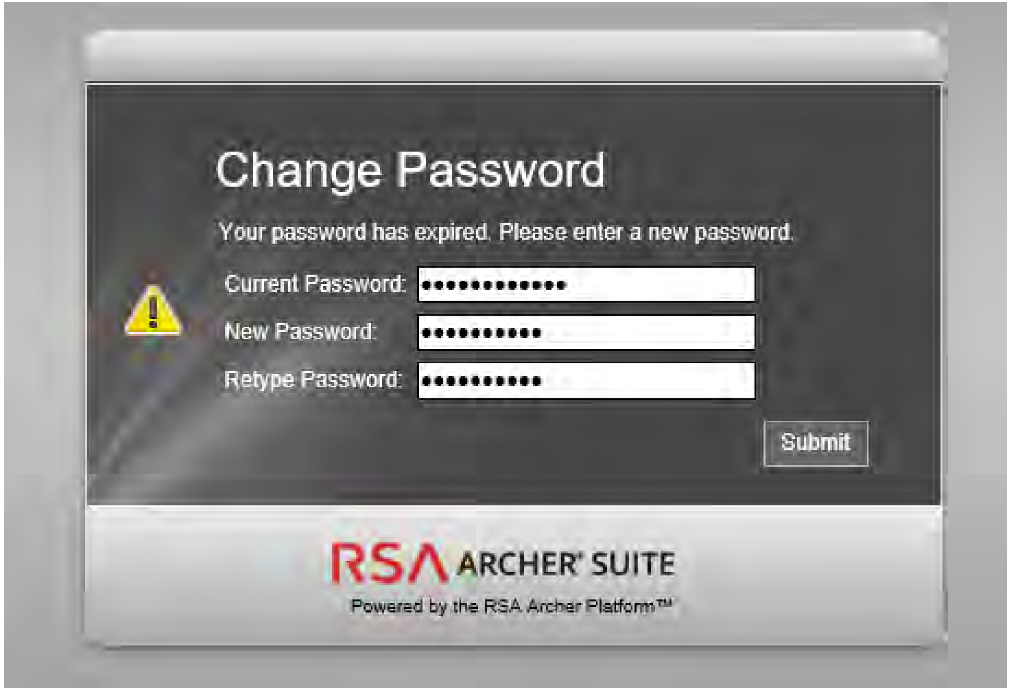
User Login

User Name: WEBINAR

Instance: 20244

Password: ••••••••••••••

User Login



Change Password

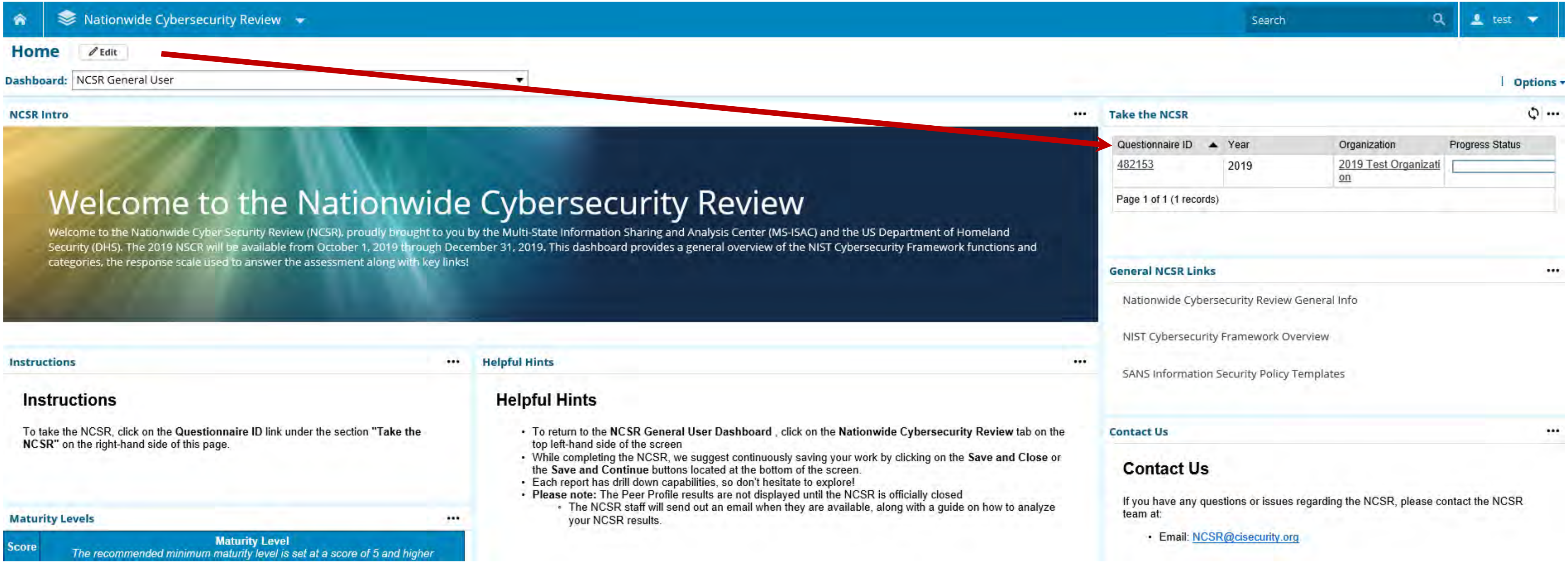
Your password has expired. Please enter a new password.

Current Password: ••••••••••••

New Password: ••••••••••

Retype Password: ••••••••••

Accessing the NCSR



Dashboard: NCSR General User

Welcome to the Nationwide Cybersecurity Review

Welcome to the Nationwide Cyber Security Review (NCSR), proudly brought to you by the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the US Department of Homeland Security (DHS). The 2019 NSCR will be available from October 1, 2019 through December 31, 2019. This dashboard provides a general overview of the NIST Cybersecurity Framework functions and categories, the response scale used to answer the assessment along with key links!

Questionnaire ID	Year	Organization	Progress Status
482153	2019	2019 Test Organization	

Page 1 of 1 (1 records)

Nationwide Cybersecurity Review General Info

NIST Cybersecurity Framework Overview

SANS Information Security Policy Templates

Instructions

To take the NCSR, click on the **Questionnaire ID** link under the section **"Take the NCSR"** on the right-hand side of this page.

Helpful Hints

- To return to the **NCSR General User Dashboard** , click on the **Nationwide Cybersecurity Review** tab on the top left-hand side of the screen
- While completing the NCSR, we suggest continuously saving your work by clicking on the **Save and Close** or the **Save and Continue** buttons located at the bottom of the screen.
- Each report has drill down capabilities, so don't hesitate to explore!
- **Please note:** The Peer Profile results are not displayed until the NCSR is officially closed
  - The NCSR staff will send out an email when they are available, along with a guide on how to analyze your NCSR results.

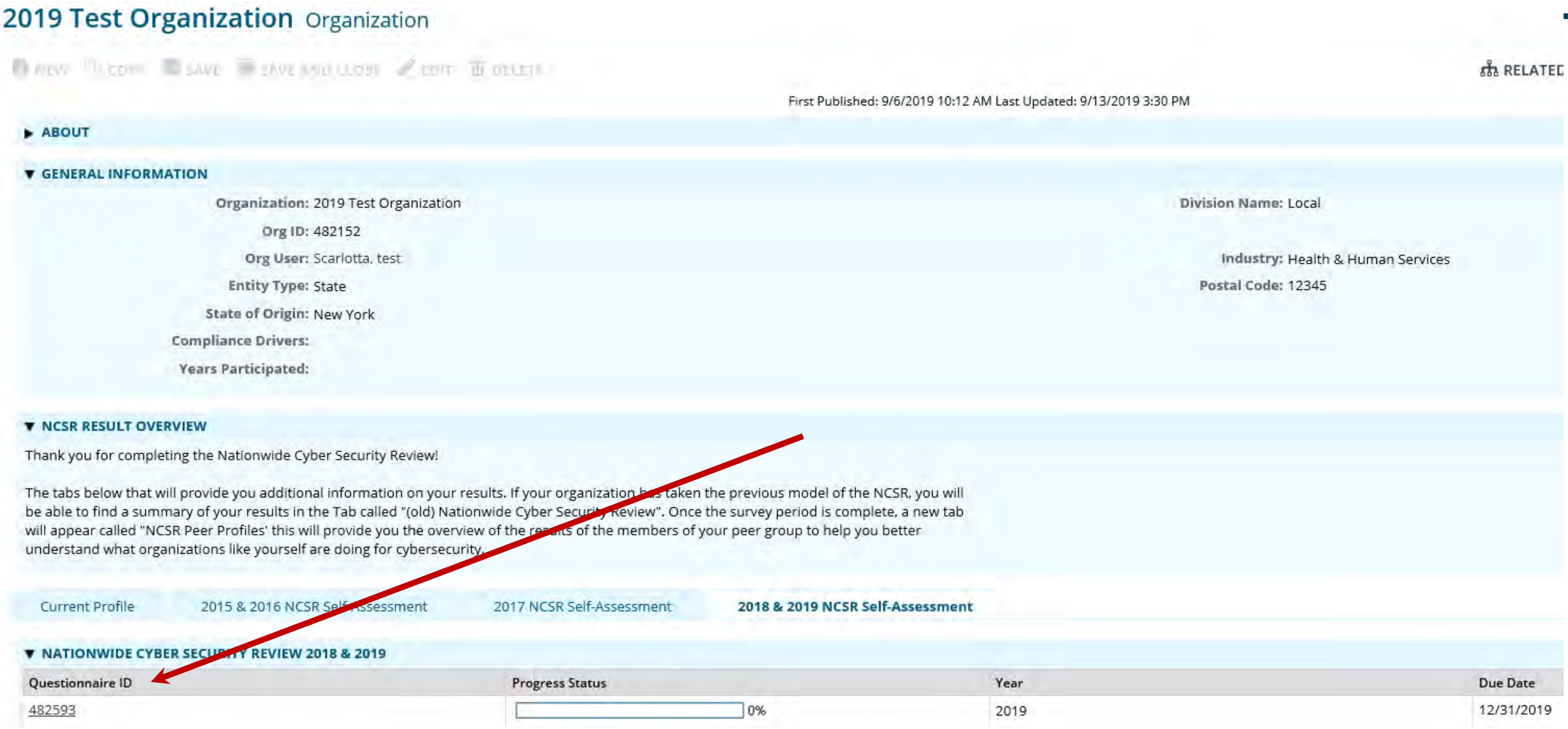
Contact Us

If you have any questions or issues regarding the NCSR, please contact the NCSR team at:

- Email: NCSR@cisecurity.org

Score	Maturity Level *The recommended minimum maturity level is set at a score of 5 and higher*

Accessing the NCSR


NEW
COPY
SAVE
SAVE AND CLOSE
EDIT
DELETE
RELATED
Current Profile
2015 & 2016 NCSR Self-Assessment
2017 NCSR Self-Assessment
2018 & 2019 NCSR Self-Assessment

2019 Test Organization Organization

First Published: 9/6/2019 10:12 AM Last Updated: 9/13/2019 3:30 PM

▶ ABOUT

▼ GENERAL INFORMATION

Organization:	2019 Test Organization	Division Name:	Local
Org ID:	482152		
Org User:	Scarlotta, test	Industry:	Health & Human Services
Entity Type:	State	Postal Code:	12345
State of Origin:	New York		
Compliance Drivers:			
Years Participated:			

▼ NCSR RESULT OVERVIEW

Thank you for completing the Nationwide Cyber Security Review!

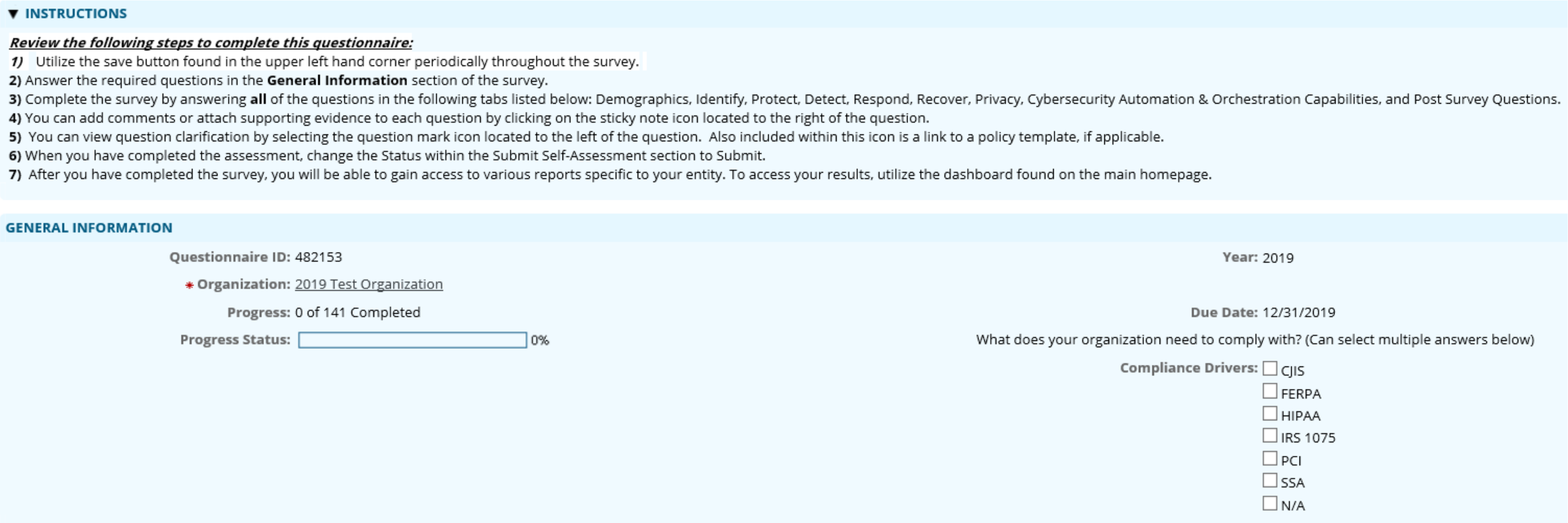
The tabs below that will provide you additional information on your results. If your organization has taken the previous model of the NCSR, you will be able to find a summary of your results in the Tab called "(old) Nationwide Cyber Security Review". Once the survey period is complete, a new tab will appear called "NCSR Peer Profiles' this will provide you the overview of the results of the members of your peer group to help you better understand what organizations like yourself are doing for cybersecurity.

▼ NATIONWIDE CYBER SECURITY REVIEW 2018 & 2019

Questionnaire ID	Progress Status	Year	Due Date
482593	0%	2019	12/31/2019

Navigating the NCSR

Questionnaire Heading:



▼ INSTRUCTIONS

Review the following steps to complete this questionnaire:

1) Utilize the save button found in the upper left hand corner periodically throughout the survey.

2) Answer the required questions in the **General Information** section of the survey.

3) Complete the survey by answering **all** of the questions in the following tabs listed below: Demographics, Identify, Protect, Detect, Respond, Recover, Privacy, Cybersecurity Automation & Orchestration Capabilities, and Post Survey Questions.

4) You can add comments or attach supporting evidence to each question by clicking on the sticky note icon located to the right of the question.

5) You can view question clarification by selecting the question mark icon located to the left of the question. Also included within this icon is a link to a policy template, if applicable.

6) When you have completed the assessment, change the Status within the Submit Self-Assessment section to Submit.

7) After you have completed the survey, you will be able to gain access to various reports specific to your entity. To access your results, utilize the dashboard found on the main homepage.

GENERAL INFORMATION

Questionnaire ID: 482153

* **Organization:** 2019 Test Organization

Progress: 0 of 141 Completed

Progress Status: 0%

Year: 2019

Due Date: 12/31/2019

What does your organization need to comply with? (Can select multiple answers below)

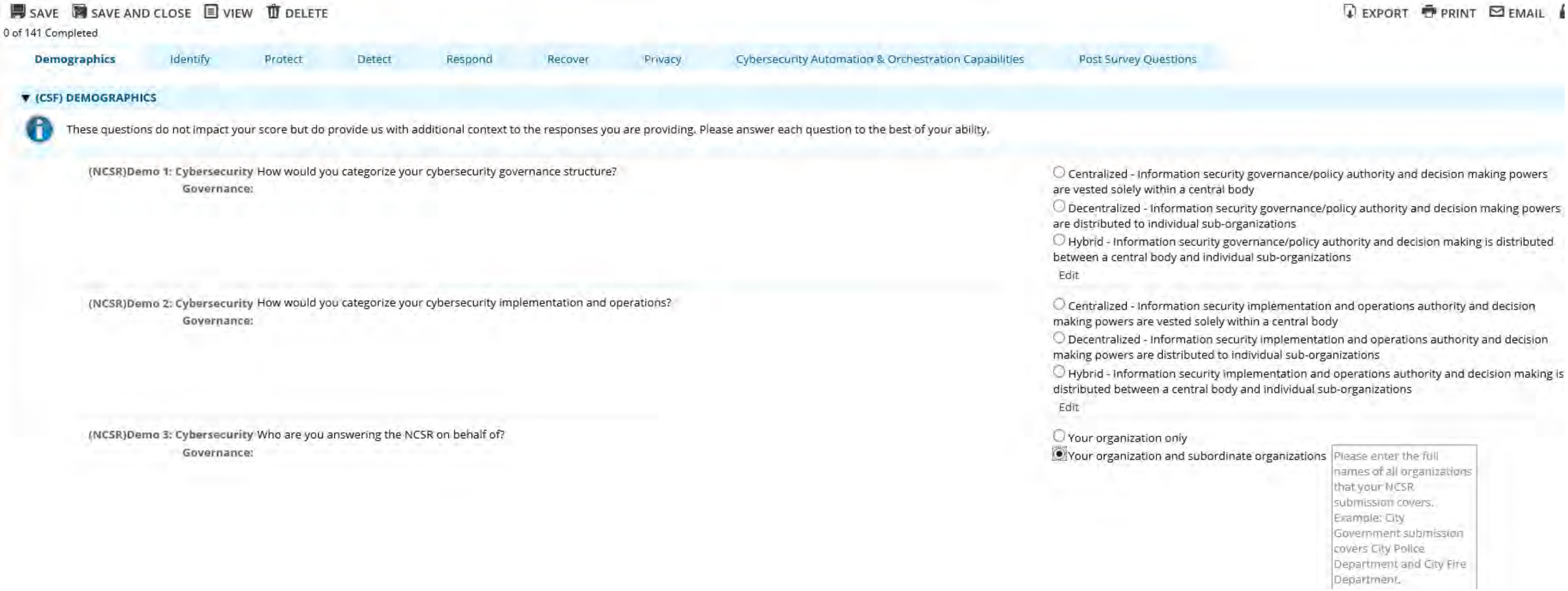
Compliance Drivers:
□ CJIS
□ FERPA
□ HIPAA
□ IRS 1075
□ PCI
□ SSA
□ N/A

MS-ISAC®

EI-ISAC®

Navigating the NCSR

Questionnaire Tabs with Questions Listed:



0 of 141 Completed

▼ (CSF) DEMOGRAPHICS

These questions do not impact your score but do provide us with additional context to the responses you are providing. Please answer each question to the best of your ability.

(NCSR)Demo 1: Cybersecurity Governance: How would you categorize your cybersecurity governance structure?

- ○ Centralized - Information security governance/policy authority and decision making powers are vested solely within a central body
- ○ Decentralized - Information security governance/policy authority and decision making powers are distributed to individual sub-organizations
- ○ Hybrid - Information security governance/policy authority and decision making is distributed between a central body and individual sub-organizations

Edit

(NCSR)Demo 2: Cybersecurity Governance: How would you categorize your cybersecurity implementation and operations?

- ○ Centralized - Information security implementation and operations authority and decision making powers are vested solely within a central body
- ○ Decentralized - Information security implementation and operations authority and decision making powers are distributed to individual sub-organizations
- ○ Hybrid - Information security implementation and operations authority and decision making is distributed between a central body and individual sub-organizations

Edit

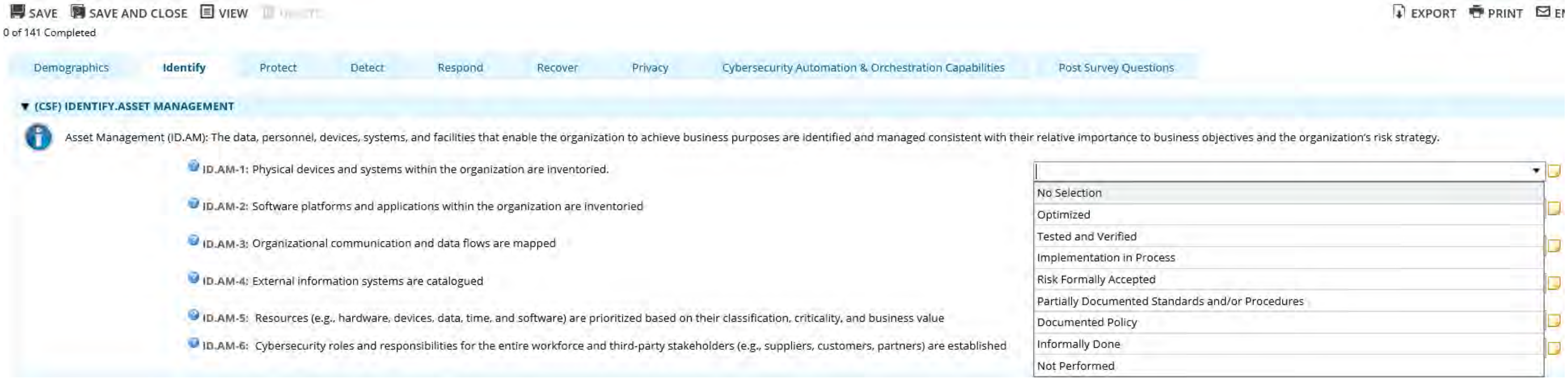
(NCSR)Demo 3: Cybersecurity Governance: Who are you answering the NCSR on behalf of?

- ○ 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.

Navigating the NCSR

Questionnaire Tabs with Questions Listed:



0 of 141 Completed

▼ (CSF) IDENTIFY.ASSET MANAGEMENT

Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

ID.AM-1: Physical devices and systems within the organization are inventoried.

ID.AM-2: Software platforms and applications within the organization are inventoried

ID.AM-3: Organizational communication and data flows are mapped

ID.AM-4: External information systems are catalogued

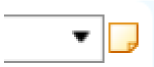
ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value

ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

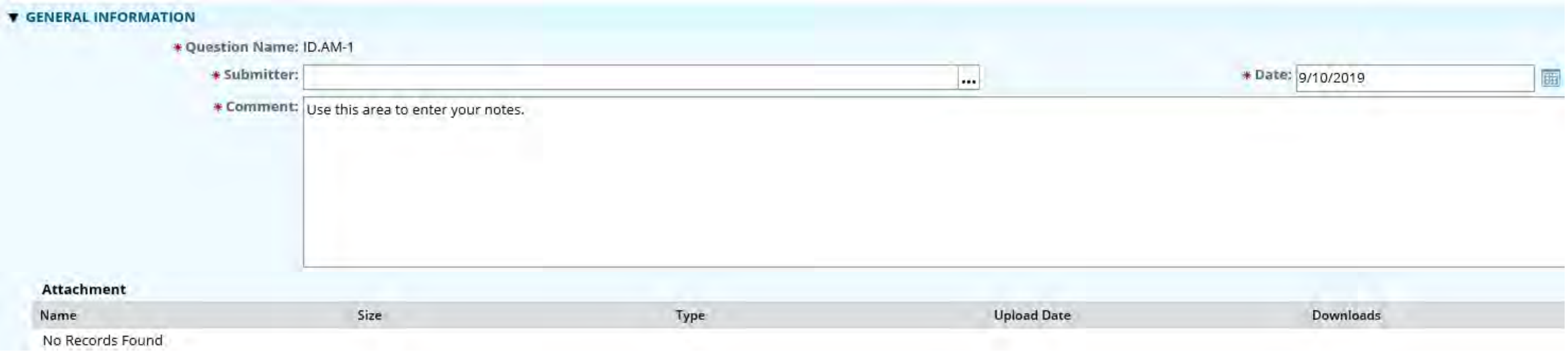
- No Selection
- Optimized
- Tested and Verified
- Implementation in Process
- Risk Formally Accepted
- Partially Documented Standards and/or Procedures
- Documented Policy
- Informally Done
- Not Performed

Documenting Notes

A sticky note icon is located to the right of the dropdown field for answer options:



This allows the end-user to enter and save notes on that specific question.



▼ GENERAL INFORMATION

* Question Name: ID.AM-1

* Submitter: ...

* Date: 9/10/2019

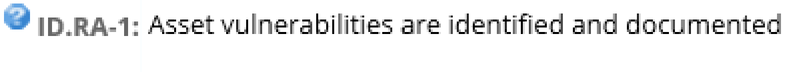
* Comment: Use this area to enter your notes.

Attachment

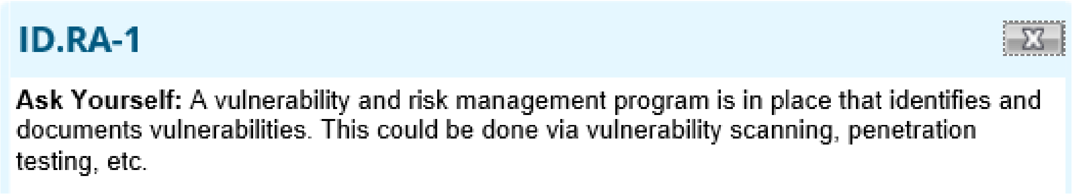
Name	Size	Type	Upload Date	Downloads
No Records Found				

Help Text – Question Clarification

A question mark icon is located to the left of a specific question, giving clarification on the question:



ID.RA-1: Asset vulnerabilities are identified and documented



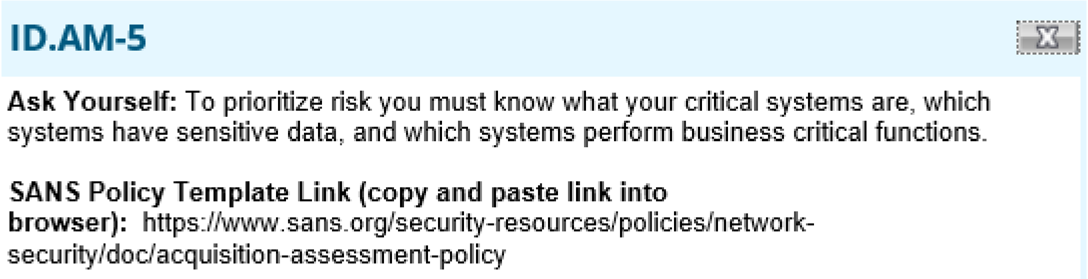
ID.RA-1

Ask Yourself: A vulnerability and risk management program is in place that identifies and documents vulnerabilities. This could be done via vulnerability scanning, penetration testing, etc.

Help Text – Policy Template Link

The Help Text will include a link to a SANS information security policy template, if applicable.

The policy templates can assist with establishing formal policies within an organization.



ID.AM-5

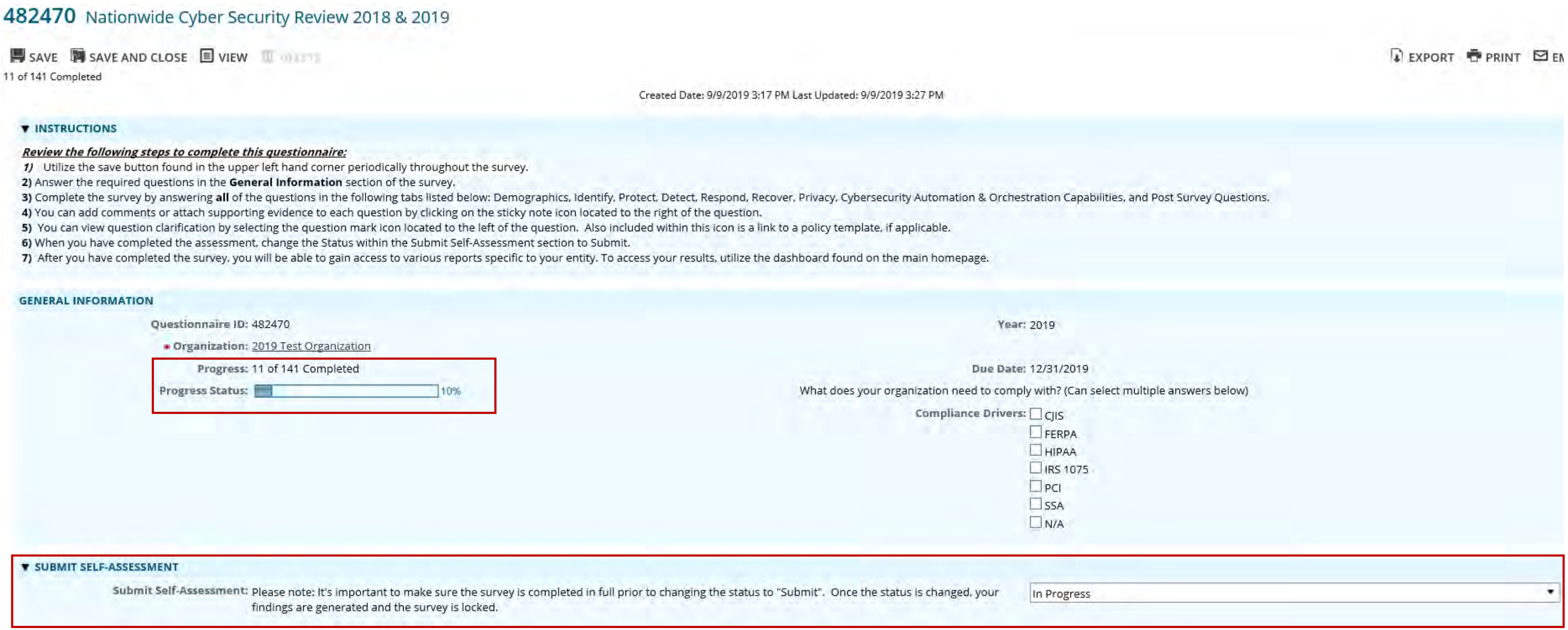
Ask Yourself: To prioritize risk you must know what your critical systems are, which systems have sensitive data, and which systems perform business critical functions.

SANS Policy Template Link (copy and paste link into browser): https://www.sans.org/security-resources/policies/network-security/doc/acquisition-assessment-policy

MS-ISAC®

Tracking Progress

EI-ISAC®



482470 Nationwide Cyber Security Review 2018 & 2019

11 of 141 Completed

Created Date: 9/9/2019 3:17 PM Last Updated: 9/9/2019 3:27 PM

▼ INSTRUCTIONS

Review the following steps to complete this questionnaire:

1) Utilize the save button found in the upper left hand corner periodically throughout the survey.

2) Answer the required questions in the **General Information** section of the survey.

3) Complete the survey by answering **all** of the questions in the following tabs listed below: Demographics, Identify, Protect, Detect, Respond, Recover, Privacy, Cybersecurity Automation & Orchestration Capabilities, and Post Survey Questions.

4) You can add comments or attach supporting evidence to each question by clicking on the sticky note icon located to the right of the question.

5) You can view question clarification by selecting the question mark icon located to the left of the question. Also included within this icon is a link to a policy template, if applicable.

6) When you have completed the assessment, change the Status within the Submit Self-Assessment section to Submit.

7) After you have completed the survey, you will be able to gain access to various reports specific to your entity. To access your results, utilize the dashboard found on the main homepage.

GENERAL INFORMATION

Questionnaire ID: 482470

Year: 2019

* **Organization:** 2019 Test Organization

Progress: 11 of 141 Completed

Progress Status: 10%

Due Date: 12/31/2019

What does your organization need to comply with? (Can select multiple answers below)

Compliance Drivers:
□ CJIS
□ FERPA
□ HIPAA
□ IRS 1075
□ PCI
□ SSA
□ N/A

▼ SUBMIT SELF-ASSESSMENT

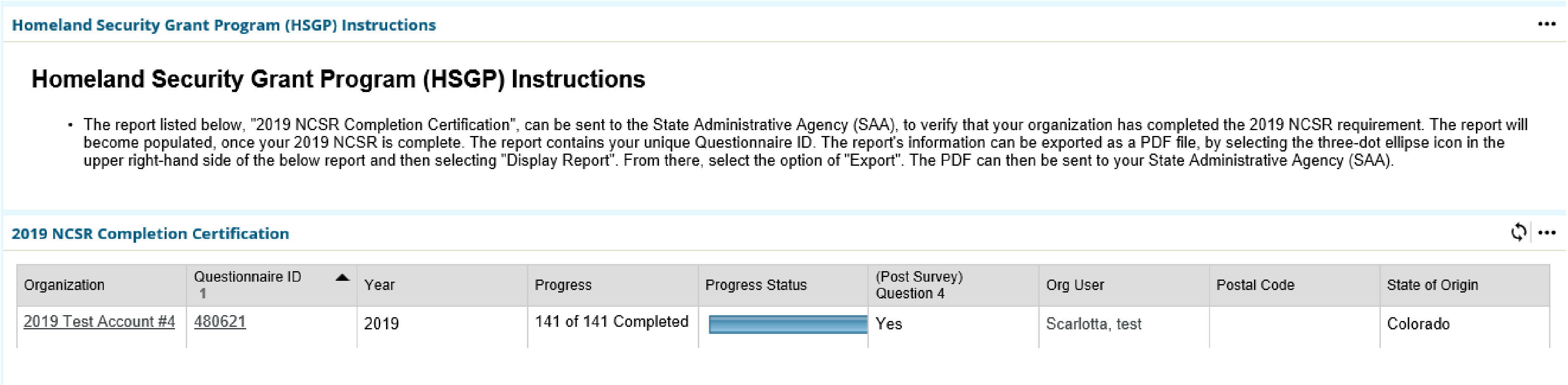
Submit Self-Assessment: Please note: It's important to make sure the survey is completed in full prior to changing the status to "Submit". Once the status is changed, your findings are generated and the survey is locked.

In Progress ▾

Completion Certification Export

- For those of you taking the NCSR to meet the SHSP or UASI grant requirement, there is a report named *“2019 NCSR Completion Certification”* on the home dashboard of the NCSR portal
  - This certifies that you took the NCSR and can be shared this with your State Administrative Agency (SAA).
- MS-ISAC will also be sending a bi-weekly report, to assist SAA’s with compliance.
- MS-ISAC is not sharing the data of organizations, only a listing of progress for organizations.

Completion Certification Export



Homeland Security Grant Program (HSGP) Instructions

Homeland Security Grant Program (HSGP) Instructions

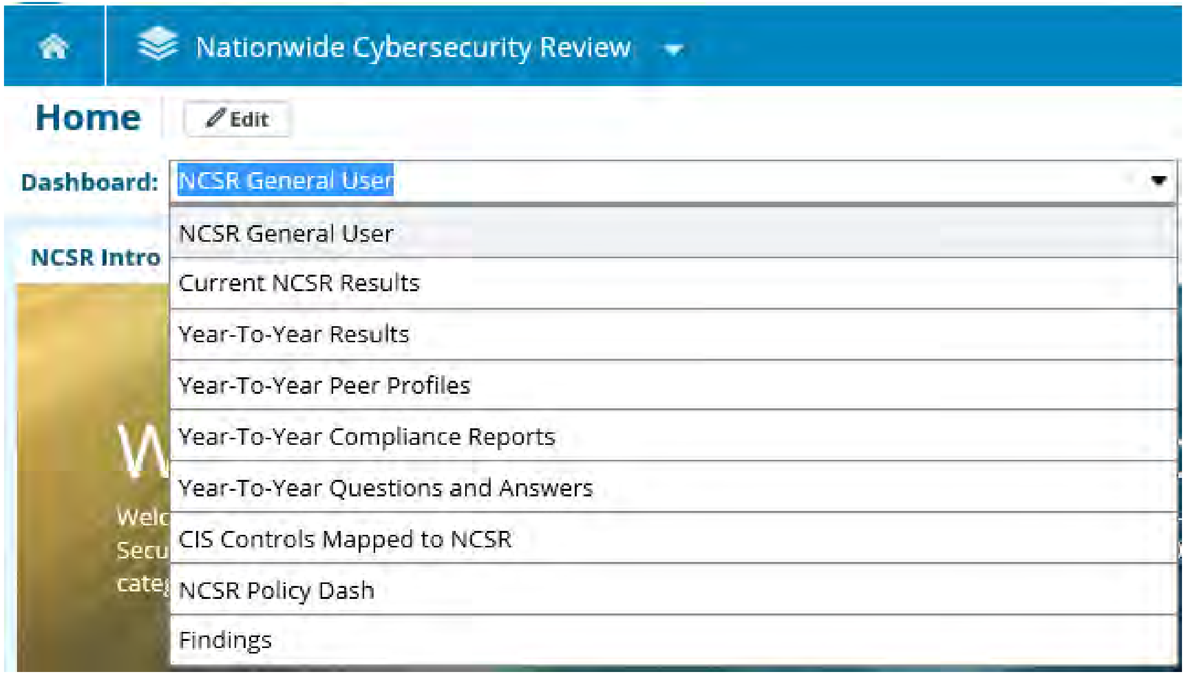
- The report listed below, "2019 NCSR Completion Certification", can be sent to the State Administrative Agency (SAA), to verify that your organization has completed the 2019 NCSR requirement. The report will become populated, once your 2019 NCSR is complete. The report contains your unique Questionnaire ID. The report's information can be exported as a PDF file, by selecting the three-dot ellipse icon in the upper right-hand side of the below report and then selecting "Display Report". From there, select the option of "Export". The PDF can then be sent to your State Administrative Agency (SAA).

2019 NCSR Completion Certification

Organization	Questionnaire ID ▲ 1	Year	Progress	Progress Status	(Post Survey) Question 4	Org User	Postal Code	State of Origin
2019 Test Account #4	480621	2019	141 of 141 Completed		Yes	Scarlotta, test		Colorado

Once Complete, Now What?

End-User Reports Listed on NCSR Portal Home:

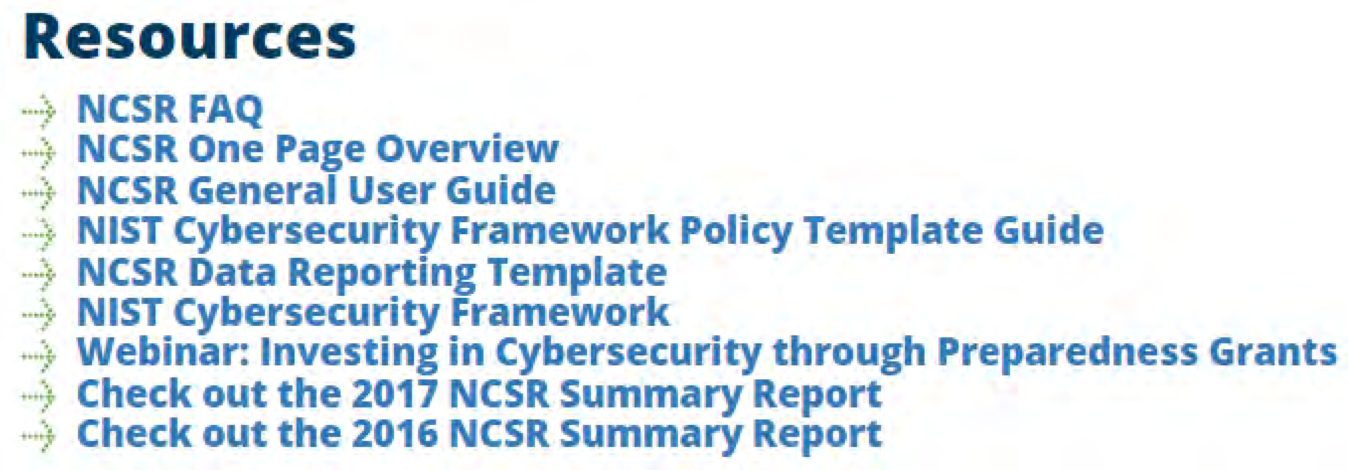


Dashboard: NCSR General User

- NCSR General User
- Current NCSR Results
- Year-To-Year Results
- Year-To-Year Peer Profiles
- Year-To-Year Compliance Reports
- Year-To-Year Questions and Answers
- CIS Controls Mapped to NCSR
- NCSR Policy Dash
- Findings

End-User Resources

Located Here: https://www.cisecurity.org/ms-isac/services/ncsr/



Resources

- NCSR FAQ
- NCSR One Page Overview
- NCSR General User Guide
- NIST Cybersecurity Framework Policy Template Guide
- NCSR Data Reporting Template
- NIST Cybersecurity Framework
- Webinar: Investing in Cybersecurity through Preparedness Grants
- Check out the 2017 NCSR Summary Report
- Check out the 2016 NCSR Summary Report

Contact Information

- For questions related specifically to the NCSR or the MS-ISAC, please contact **ncsr@cisecurity.org**
- To register for the 2019 NCSR, please visit: **https://www.cisecurity.org/ms-isac/services/ncsr/**
- For questions regarding the SHSP and UASI programs or allowable expenditures, please contact **AskCSID@fema.dhs.gov** or consult the HSGP NOFO.
- For questions related specifically to cybersecurity and developing the cyber-focused investment justification, please contact **SLTTCyber@hq.dhs.gov** and include “FEMA Grant” in the subject line.

Q & A Session

MS-ISAC Members & Metrics Workgroup:

- Gary Coverdale – CISO - Mono County, California
- Jim Cusson – Security Liaison - Commonwealth of Massachusetts
- Joe Frohlich – Enterprise Security Program Manager - State of Montana
- Kim LaCroix – NYS Chief Information Security Office, Security Governance, Risk & Compliance - State of New York

DHS & FEMA:

- Tom Filippone – Partnerships Branch - Stakeholder Engagement Division of CISA
- Madelyn Weingast – Partnerships Branch - Stakeholder Engagement Division of CISA
- Margaret Wilson – Senior Advisor, GPD - FEMA

Nationwide Cybersecurity Review (NCSR)

NATIONWIDE CYBERSECURITY REVIEW

NCSR 2019 October 1–December 31

The Nationwide Cybersecurity Review (NCSR) is a no cost, anonymous, annual self-assessment that is designed to measure gaps and capabilities of state, local, tribal and territorial (SLTT) governments' cybersecurity programs.

Benefits

- Receive metrics specific to your organization to identify gaps and develop a benchmark to gauge year-to-year progress, as well as anonymously measure your results against your peers
- For HIPAA compliant agencies, translate your NCSR scores to the HIPAA Security Rule scores of an automatic self-assessment tool
- Access to informative references such as NIST 800-53, COBIT, and the CIS Controls that can assist in managing cybersecurity risk
- Nationally, aggregate NCSR data provides a baseline, foundational understanding of SLTT cybersecurity posture to help drive policy, governance, and resource allocation
- Results enable Federal partners to better understand the status quo and engage in more strategic, cyber-specific planning and preparedness to help manage national risk and improve SLTT core capabilities

https://www.cisecurity.org/ms-isac/services/ncsr

MS-ISAC®

EI-ISAC®

Thank You