Charles Bethel <charles.bethel@wuhsd.org>

2023 NCSR Now Open!

1 message

MS- and EI-ISAC <noreply@msisac.org> Fri, Sep 29, 2023 at 7:01 AM

We are excited to announce the 2023 Nationwide Cybersecurity Review (NCSR) is now available! Your organization can utilize the NCSR to **measure your cybersecurity program** at no cost. After participating, you will then receive automated custom reporting and recommendations to improve your organization's cyber program.

This anonymous self-assessment will be open until February 29, 2024.

Why This Is Important

The NCSR provides access to a no-cost self-assessment and an associated portal containing reports and resources for mitigating common risks. The assessment is designed to help you measure your cyber program at a strategic level regardless of your level of cybersecurity maturity. You can then use the NCSR as a summary to identify gap areas that need funding and resource investments.

Grant Requirement Information

The NCSR is a post-award requirement for recipients and sub-recipients of the Homeland Security Grant Program (HSGP) – specifically, entities receiving funding through the State Homeland Security Program (SHSP) and the Urban Area Security Initiative (UASI).

The NCSR is also a post-award requirement for recipients of the State and Local Cybersecurity Grant Program (SLCGP). For questions specific to the grant process, please reach out to FEMA-Grants-News@fema.dhs.gov.

Accessing the NCSR Portal & Resources

Previously Established Users: Use https://cis.my.logicmanager.com/ to access the NCSR portal. Select "Get a new password" if a password reset is needed.

New Users: Register for the NCSR at https://www.cisecurity.org/ms-isac/services/ncsr/. The MS-ISAC will create your user account, at which point in time you will receive an email with login instructions.

Demo Presentations: The MS-ISAC is now offering individual 30-minute NCSR demo reviews for organizations that are new to the NCSR, the platform, and NCSR's associated benefits. Contact ncsr@cisecurity.org to schedule a NCSR demo.

2022 Participants: Please contact ncsr@cisecurity.org if you would like a majority of your 2022 NCSR answers imported to your 2023 assessment. You can then review and update your answers as needed.

Help Text: The majority of the NCSR assessment includes help text to assist you when reviewing and answering an applicable question. You can access the help text by selecting a gray question mark icon next to a specific question or by downloading the full Excel file located at the beginning of the assessment task view.

User Guide: Please consult the NCSR General User Guide for directions on navigating the NCSR portal, the assessment, and associated reporting. The NCSR portal also includes help text guidance that can assist end-users when reviewing the assessment and submitting answers.

Not sure where to begin with your results once you complete the assessment? We are now offering NCSR Maturity Reviews that are one-on-one meetings with a team member to review your results, identify available resources to implement, and key tips for drafting your cybersecurity plan. If you are interested, please email ncsr@cisecurity.org.

Thank you for your participation!

The MS-ISAC NCSR Team

31 Tech Valley Drive

East Greenbush, NY 12061

ncsr@cisecurity.org

TLP:CLEAR
https://www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

Please send all opt out requests to info@cisecurity.org.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.
This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

. . . . .