NEW AND NOTEWORTHY: AN UPDATE ON THE NATIONAL CYBER INCIDENT RESPONSE PLAN 2024

Overview

"New and Noteworthy" is a series of newsletters to inform the public of the Cybersecurity and Infrastructure Security Agency's (CISA) efforts to update the National Cyber Incident Response Plan (NCIRP). This third issue of "New and Noteworthy" contains important information about the upcoming public comment period and summarizes the June 27, 2024, NCIRP virtual public listening session, as well as other recent engagements and outreach activities.

NCIRP Update Available for Public Comment

The NCIRP Update draft is available for public comment from December 16, 2024, to January 15, 2025. We encourage stakeholders with a role in cyber incident response coordination at the national level to participate in this important update. Your input is extremely valuable to help inform the NCIRP Update.

To provide feedback on the NCIRP Update, please visit the Federal Register Federal Register :: Public Inspection: National Cyber Incident Response Plan to submit comments by January 15, 2025. The draft can also be found on CISA's NCIRP website - The National Cyber Incident Response Plan (NCIRP) | CISA. CISA's NCIRP Planning team will provide a high-level summary of the public feedback within 30 days after the close of the public comment period.

Engagement and Outreach

Core Planning Team (CPT)

CPT feedback is essential to the NCIRP Update. The CPT-- which is comprised of 60 distinct organizations from across federal departments and agencies, private sector, SLTT, and international organizations-- has supplied input on several iterations of the NCIRP Update. We anticipate holding a CPT meeting once public comments have been adjudicated to discuss final changes to the draft before it moves forward in the federal approval process.

Virtual Public Listening Session

On August 1, 2024, CISA held its third virtual public listening session. The NCIRP listening sessions provide stakeholders from across the critical infrastructure community an opportunity to reflect on 1) the adoption and use of the current NCIRP and 2) their experiences coordinating with the federal government during a significant cyber incident. The listening sessions attracted a diverse audience, allowing us to draw additional input from industry, state and local governments, federal agencies, and educational and international entities. During these sessions, CISA provided an overview of the NCIRP and outlined the process for informing the NCIRP Update. Some of the questions CISA's NCIRP Planning team addressed are as follows:

- **What are CISA's plans after the NCIRP Update is released?** CISA plans to work with stakeholders to update the NCIRP every two years to ensure it is aligned with changes in the cyber threat landscape and new capabilities and processes for collaborative incident response.
- **How will the NCIRP Update incorporate the incident response perspective of small and medium-sized businesses (SMBs)?** The NCIRP Update aims to describe expectations for national response activities more effectively to all elements of the private sector. In particular, the key decisions, activities, and coordinating structures in each phase of incident response are detailed so SMBs can more easily identify where they might participate in response.

- **Does the NCIRP Update integrate SLTT organizations into cyber response? The** NCIRP Update clarifies relevant partnerships, coordination structures, and information flow to allow the SLTT community to more effectively participate in national level incident response.
- **Does CISA see a role for cyber mutual assistance in cyber incident response?** The energy sector has pursued Cyber mutual assistance, and it is one of many potential solutions to enable robust incident response during a large-scale cyber incident.
- **Has CISA engaged with private sector standards and certification bodies?** CISA welcomes engagement with all stakeholders. Currently, most of our engagement in this arena has been with the National Institute of Standards and Technology (NIST), who is a regular participant in the CPT.
- **Since the NCIRP is so closely related to PPD-41, are there any plans to update that document to coincide with all the work being done to revise the NCIRP?** CISA is not aware of any plan to update PPD-41.
- **How can stakeholders offer feedback to CISA's NCIRP team?** To provide feedback on the NCIRP Update, navigate to the NCIRP webpage for instructions.

CISA is grateful to the participants who attended the virtual public listening session and will consider their comments during the update process.

Extended Engagement Outreach:

Since September 2023, the NCIRP team has conducted over 152 engagements outside of the CPT with federal, SLTT, industry, and international stakeholders. CISA continues to solicit feedback and input from a wide range of stakeholders from the federal and private sectors, as well as SLTT communities through the following forums:

- Outreach continues through additional stakeholder-specific engagements and other venues as we prepare for a final release of the NCIRP Update. We are particularly interested in engaging more with the SLTT and ICS sectors in the future.
- We encourage you to participate in the upcoming public comment period to share your perspectives.
- We welcome all requests for engagement via email to ncirp@cisa.dhs.gov.

Don't miss the opportunity to provide feedback during the public comment period! To learn more about the NCIRP, visit the NCIRP webpage for the most up-to-date information on the NCIRP Update development, public comment period, and access to the NCIRP newsletters.