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

Overview

Welcome to the first issue of “New and Noteworthy,” an update on the existing efforts to update the National Cyber Incident Response Plan (NCIRP) 2024. This publication will keep the public informed on planning processes, plan development, and stakeholder engagement efforts in support of the NCIRP 2024. This “New and Noteworthy” edition provides a brief overview of the NCIRP, information about the NCIRP Core Planning Team (CPT), and related engagement and outreach activities already underway. Our goal is to ensure the NCIRP 2024 reflects input from relevant stakeholder groups and is more operational and actionable.

Join the NCIRP virtual listening session on Wednesday, May 8, 2024 from 1-2 pm EST. If you are interested in attending, pre-register here: https://cisa.webex.com/weblink/register/rc3589e94b160fb45153c254f006646f5

Leveraging the Joint Cyber Defense Collaborative (JCDC), the Cybersecurity and Infrastructure Security Agency (CISA) is leading the national effort to update the NCIRP. CISA established JCDC to bring together public and private partners to plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents. Updating the NCIRP is foundational to the continued unity of effort that the JCDC is advancing. This month’s “New and Noteworthy” provides a brief overview of the broad group of stakeholders who represent the varied elements of national cyber response. This publication also serves to provide an overview of the NCIRP, detailing the existing efforts to make it more operational and actionable, related engagement and outreach activities, and the ongoing joint planning to ensure the new version of the NCIRP reflects input from relevant stakeholders. Many of these stakeholders are included in the Core Planning Team (CPT), which is a diverse and essential group of individuals who play a crucial role in the NCIRP 2024 planning process.

NCIRP Background

The NCIRP was initially developed and written to align with Presidential Policy Directive 41 (PPD-41) on U.S. Cyber Incident Coordination. The directive describes the Federal Government’s response to cyber incidents, whether involving government or private sector entities. The NCIRP leverages principles from the National Preparedness System (NPS) to articulate how the nation responds to and recovers from significant cyber incidents. Due to the evolving cyber threat landscape—including increased risks to critical infrastructure and public services—the need to update the NCIRP has never been greater.

CISA is working with JCDC participants and other partners to gather input and feedback that will be considered for the NCIRP 2024. The NCIRP 2024 update is one of the JCDC 2024 Priorities, which call for bringing together government and the private sector to prepare for major cyber incidents.

Making the NCIRP More Operationally Actionable

The NCIRP 2024 will incorporate lessons learned since the 2016 release, include contributions from public-private partners who play a critical role in national cyber incident response, and establish a foundation for continued improvement of the nation’s response to significant cyber incidents. The NCIRP 2024 will also address Strategic Objective 1.4 of the 2023 [National Cybersecurity Strategy](), which calls for updating federal incident response plans and processes.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

The NCIRP 2024 will clearly identify how federal and non-federal stakeholders, including private sector and State, Local, Tribal, and Territorial (SLTT) organizations, interact and collaborate during the lifecycle of significant cyber incidents. It will leverage the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 and Special Publication 800-61 to describe the nation's framework for detection of, response to, and recovery from significant cyber incidents. The NCIRP 2024 will also provide more practical, operationally actionable guidance across the lifecycle of a significant cyber incident.

Updates to the NCIRP 2024 will include two predetermined, broad focus areas: baseline updates and enhancements.

Baseline updates will address:

- Statutory changes expanding federal organizations and authorities (e.g., expansion of Sector Risk Management Agency [SRMA] responsibilities, issuance of National Security Memorandum-22.
- Agencies that have been created since 2016 (e.g., CISA and ONCD).
- Growth of federal partner capabilities and authorities.
- Changes in the cyber threat environment since the last NCIRP publication.

Enhancements will include:

- Improving transitions across the spectrum of routine cyber defense operations and significant incident response and recovery.
- Formalizing national cyber defense collaboration roles.
- Incorporating the central roles of private sector, SLTT, and key international stakeholders.
- Establishing a regular update cycle.

Core Planning Team

The NCIRP 2024 CPT was formed in December 2023 and has so far brought together 150 members representing 14 federal departments and agencies, 3 SLTT entities, and 26 private sector representatives—including JCDC participants and individuals from the Sector Coordinating Council (SCC) who are knowledgeable about specific industries. The CPT meets every two weeks to discuss important stakeholder input and feedback regarding proposed delivery of an effective, informative, and up to date plan. CPT members will continue to evolve and expand as our development efforts progress.

Engagement and Outreach

CISA is working to ensure the NCIRP 2024 addresses significant changes in policy and cyber operations that have occurred since 2016. In addition to NCIRP 2024 CPT meetings, CISA has solicited feedback and input from JCDC participants and other stakeholders during one on one discussions, informational listening sessions, voluntary office hours, and written feedback and documentation furnished to the NCIRP 2024 Planning Team. The initial phase for stakeholder engagement focused on outreach to federal and interagency partners, the private sector, and SLTT governments. This phase was intended to understand the roles, authorities, and capabilities of their significant incident response (as well as to solicit their participation in the NCIRP 2024 update).

A series of virtual listening sessions will be held with stakeholders who develop and exercise incident response plans for critical infrastructure to gather feedback about the NCIRP. Stakeholders will also impart their experience with incident response collaboration with the federal government. The first listening session is scheduled for May 8, 2024. Registration information is set to be published on the CISA NCIRP website. Please email ncirp@cisa.dhs.gov with any questions.

For more information, please visit the NCIRP webpage. Your feedback and thoughts are vital as the NCIRP 2024 CPT works to shape an informative and proactive plan to help the nation prepare for and respond to significant, disruptive cyber incidents. To share your suggestions, please email ncirp@cisa.dhs.gov and join our upcoming webinar series.