# NATIONAL CYBER INCIDENT RESPONSE PLAN 2024

## OVERVIEW

In 2016, the National Cyber Incident Response Plan (NCIRP) was published to provide a framework for significant cyber incident coordination. A lot has changed over the past eight years, including across the cyber threat landscape and the cyber defense ecosystem, and the NCIRP must evolve accordingly. As directed in the National Cybersecurity Strategy, the Cybersecurity and Infrastructure Security Agency (CISA) is leading the effort to update the NCIRP to provide a modern, agile, flexible framework to enable coherent and repeatable national incident response across the federal government, private sector, and other key partners.

## WHAT IS THE NCIRP AND WHY WAS IT CREATED?

The NCIRP was developed in accordance with Presidential Policy Directive 41 (PPD-41) on U.S. Cyber Incident Coordination and describes how the federal government, private sector, and state, local, tribal, territorial (SLTT) government entities will organize to manage, respond to, and mitigate the consequences of significant cyber incidents. The NCIRP leverages principles from the National Preparedness System (NPS) to articulate how the nation responds to and recovers from significant cyber incidents. Alignment with the NPS also allows for significant cyber incident response to integrate with physical incident response in cases where cyber incidents may have physical impacts or vice versa.

## WHY IS THE NCIRP BEING UPDATED?

The nation's cyber defense ecosystem and the cyber threats faced by the nation have evolved significantly since 2016. There have been numerous changes to the organization and authorities of federal departments and agencies, including the creation of CISA and the expansion of its authorities, the overall growth in the capacity of federal agencies to engage in significant cyber incident response, increased international collaboration around cyber incident coordination, and, most importantly, the foundational role of the private sector in responding to and managing most cyber incidents without significant support from the federal government. The NCIRP 2024 will address these changes by incorporating lessons learned and feedback from stakeholders since the 2016 release, ensuring that the updated NCIRP is fully inclusive across non-federal stakeholders, and establishing a foundation for continued improvement of the nation's response to significant cyber incidents. Updating the NCIRP additionally addresses Strategic Objective 1.4 of the 2023 National Cyber Strategy, which calls for updating federal incident response plans and processes.

## WHO IS INVOLVED IN UPDATING THE NCIRP?

In addition to addressing the changes in the cyber defense ecosystem and evolving cyber threats, the NCIRP 2024 planning effort will bring together a community of stakeholders, including interagency partners, Sector Risk Management Agencies, regulators, and non-federal stakeholders such as the private sector, SLTT entities, and international partners.

## NCIRP 2024 WILL BE GROUNDED IN THE FOLLOWING PRINCIPLES:

1. **Unification.** National cyber incident response requires deeply committed partnerships across all levels of government, industry, and with our international partners. The NCIRP 2024 will bring together a diverse community of stakeholders to collaborate towards a more secure future.
2. **Shared Responsibility.** Cybersecurity is a team sport with players across the cybersecurity ecosystem playing unique roles in national cyber incident response. The NCIRP 2024 will challenge traditional ways of working with our partners to move toward more forward-leaning, action-oriented collaboration to realize the full potential of each players' authorities, capabilities, and expertise.

*This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.*

3. **Learning from the Past.** The past eight years have seen cyber incidents of unprecedented scale, impact, and sophistication. The NCIRP 2024 will explore past cybersecurity incidents to drive improvements and enable advances to national cyber incident response coordination efforts. By gleaning lessons from recent history, the NCIRP 2024 will fortify the nation's cyber environment, helping to safeguard it against the dynamic landscape of threats.
4. **Keeping Pace with Evolutions in Cybersecurity**. The cybersecurity landscape is a complex ever-evolving environment. The NCIRP 2024 will build processes mindful of this complex environment to ensure the agility to stay ahead of changes in the environment. This approach reflects a shift to clearly defining intended outcomes and becoming more proactive. It showcases our commitment to agility in a sophisticated cybersecurity landscape by remaining vigilant and acting quickly as a collective whole.

## WHAT'S COMING NEXT?

CISA is planning to use a variety of mechanisms to engage with its Federal, private sector, SLTT governments, and international partners. Engagement mechanisms may include one-on-one meetings, group listening sessions, briefings and discussions at conferences, or other standing meetings. CISA will take a phased approach to this effort building iteratively on each phase as they inform the process and illuminate areas for improvement in the NCIRP 2024.

CISA is currently in the "Planning Initiation" phase to solicit insights that will support the development of the NCIRP 2024. Stakeholder engagement with federal partners began in September and CISA plans to continue engaging additional stakeholders across the private sector, SLTT governments, and international partners through November. This initial engagement process is intended to collect insights on the planning process, based on lessons learned since 2016; identify opportunities for improving public-private significant cyber incident response and coordination; and to gauge stakeholders' interest in participating in the NCIRP 2024 Core Planning Team (CPT).

The NCIRP 2024 CPT will then transition to the "Planning and Development" phase in December. This phase will include a series of CPT working meetings or writing sessions to produce a draft of the NCIRP 2024 with regular input from federal, private sector, SLTT governments, and international stakeholders. The revised draft will be published for a public comment period to ensure relevant stakeholders have ample opportunity to provide input prior to publication. Upon adjudication of final comments, the NCIRP will be published and socialized across the cybersecurity community.

## WHEN WILL THE UPDATE BE COMPLETE?

As directed by the National Cybersecurity Strategy, the updated NCIRP is scheduled to be approved and published by the end of calendar year 2024.

## FOLLOW OUR PROGRESS.

To learn more about the NCIRP 2024, email us at ncirp@cisa.dhs.gov or go to our website.