REQUEST FOR COMMENT: FOUNDATION FOR DEFENSE OF DEMOCRACIES

Cybersecurity and Infrastructure Security Agency

# National Cybersecurity Incident Response Plan Update

## (Docket No. CISA-2024-0037)


**SUBMITTED BY:**

**RADM (Ret.) Mark Montgomery**
*Senior Director of the Center on Cyber "and Technology Innovation at the Foundation for Defense of Democracies*

**Annie Fixler**
*Director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies*

**Jiwon Ma**
*Senior Policy Analyst of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies*



**Washington, DC**
**February 14, 2025**



FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Docket Number: CISA-2024-0037

**Public Comment on the National Cybersecurity Incident Response Plan**

The Foundation for Defense of Democracies (FDD) Center on Cyber and Technology Innovation appreciates the opportunity to comment on the draft National Cybersecurity Incident Response Plan (NCIRP).

The leadership of the Cybersecurity and Infrastructure Security Agency (CISA) in coordinating stakeholder and interagency engagement in drafting the NCIRP has been exceptional. As the designated National Coordinator for the security and resilience of the nation's critical infrastructure, the agency has demonstrated the ability to manage and coordinate responses to cyber threats across both the public and private sectors. The NCIRP, as drafted, provides a strong foundation and serves as a testament to CISA's dedication and its demonstrated capabilities over the years.

A clear and effective national response framework is critical for ensuring a well-coordinated response to cyber incidents threatening the security of U.S. critical infrastructure. The NCIRP could be refined further to provide greater clarity around the roles and responsibilities of key entities. Following the issuance of the final draft, we look forward to the implementation plans that will operationalize this framework.

**Further Recognition of Space as a Critical Infrastructure**

One notable aspect of the plan is its recognition of the space domain as a critical asset to our country. Space assets provide essential services for infrastructure systems we rely on every day, such as global positioning, satellite communications, and remote sensing, which support transportation, energy, emergency response, financial systems, and much more. Disruptions to these assets could have cascading effects across various sectors. However, the NCIRP's acknowledgment of this fact falls short of the needed step of formally designating space systems as critical infrastructure. National Security Memorandum 22 similarly fails to include space as a critical infrastructure, but this does not diminish its importance in national security.

Elsewhere, the NCIRP acknowledges Information Sharing and Analysis Centers (ISACs) as sector-specific entities with established relationships with CISA and Sector Risk Management Agencies (SRMAs). The Space ISAC, however, is only referenced in the final pages of the draft under "multi-sector resources," without a clear role articulated. More acknowledgment of space infrastructure in the NCIRP as a critical domain in cybersecurity would strengthen incident response capabilities for other critical infrastructures.

**CISA's Roles and Capabilities**

As the National Coordinator, CISA plays a pivotal role throughout the entire lifecycle of cyber incident response. During an incident, CISA's hunt and incident response teams provide direct support by investigating, mitigating, and containing cyber threats. The NCIRP should also

emphasize the teams' responsibilities following the incident investigation and analysis, such as publishing and amplifying mitigation guidance, issuing detailed reports, and documenting the types of incidents addressed, outcomes, and technical insights gained through incident response. The NCIRP should also more explicitly outline the hunt and incident response teams' responsibilities prior to incidents, particularly in the context of tabletop exercises and coordination efforts to improve the ability to withstand cyberattacks.

Furthermore, the role of CISA's regional Cybersecurity Advisors should be clarified, particularly in how they support state, local, tribal, and territorial (SLTT) entities and the private sector in responding to incidents. Similar to the details that are requested of the hunt and incident response teams, the NCIRP should define the regional Cybersecurity Advisors' responsibilities in incident recovery to ensure effective coordination.

**Sector Risk Management Agencies**

The NCIRP appropriately highlights the importance of clearly defined roles for SRMAs, specifically in how they assist critical infrastructure owners and operators in mitigating cyber risks, preparing for cyber incidents, and providing guidance during an incident. However, the draft does not explicitly mention their role during the post-incident phase during which it is critical for lessons learned to be shared both to improve future response efforts and to help other entities protect themselves against similar threats.

Additionally, the NCIRP should outline expectations for co-SRMAs to ensure they have established and exercised roles for effective collaboration during incidents. The plan should clarify the cycle for these exercises to ensure preparedness is continuously evaluated and refined. In turn, SRMAs should align all future budget allocations to reflect the importance of their roles.

**The Role of the Office of the National Cyber Director**

The Office of the National Cyber Director (ONCD) was a key partner in drafting the NCIRP, but further clarity around its role should be included. The NCIRP should recognize the role of the National Cyber Director as (according to statute) the principal advisor to the president on cybersecurity matters and therefore its ability to ensure improved coordination with federal agencies to prepare for and respond to cyber incidents. For instance, Table 6, which outlines coordinated activities during the response phase, should explicitly define ONCD's role, including its responsibility "to develop strategies for implementing, synchronizing, and measuring the effectiveness of response activities." Furthermore, as mentioned in the National Cybersecurity Strategy Implementation Plan, ONCD's role must include ensuring SRMAs and federal agencies evaluate the effectiveness of their contributions and their adherence to the NCIRP framework. In general, the NCIRP should more clearly articulate the ONCD's roles and responsibilities.

**State, Local, Tribal, and Territorial Governments and Private Sector**

The NCIRP should provide greater detail on how SLTT entities and the private sector fit into the cybersecurity response process. While the NCIRP mentions that adherence is voluntary for SLTTs, the private sector, and non-federal stakeholders, it also highlights the need to consider these entities for coordination structures, especially for regional coordination. Yet their role in incident response is omitted. It should be clearly delineated, including how they fit into the incident response framework.

The NCIRP should specify SLTT responsibilities both as directly impacted victims of a cyber incident and when incidents affect private companies in their jurisdiction. Moreover, the NCIRP should clarify the process by which SLTTs and private sector entities can seek federal support during a cyber incident. When they require federal support during an incident, it should be clear which agency — CISA, FBI, or SRMAs — serves as the primary lead in acquiring and sharing necessary information for coordination.

**The Role of the National Guard**

The role of the National Guard is noticeably absent from the NCIRP despite the guard's critical function in assisting SLTTs as first responders during cyber incidents. Under Title 32, the National Guard can provide vital support in emergency incident response and mitigation efforts. The plan should explicitly address how the National Guard coordinates with federal agencies during cyber incidents to ensure a more comprehensive response strategy.

**Conclusion**

The NCIRP is an essential governance document to guide national resilience and incident response efforts. It is a framework that benefits from CISA's leadership and expertise. By addressing gaps in key areas of this draft and refining clarification around coordination mechanisms, the NCIRP can better position federal agencies to protect the country from cyber incidents and enhance overall cybersecurity preparedness. Thank you for considering our input, and we look forward to seeing how these considerations are incorporated into the final plan.

**RADM (Ret.) Mark Montgomery** is the senior director at FDD's Center on Cyber and Technology Innovation, and a senior fellow at FDD. He also directs CSC 2.0, an initiative that works to implement the recommendations of the congressionally mandated Cyberspace Solarium Commission, where he served as executive director. Mark served for 32 years in the U.S. Navy as a nuclear-trained surface warfare officer, retiring as a rear admiral in 2017.

**Annie Fixler** is the director of FDD's Center on Cyber and Technology Innovation and a research fellow at FDD.

**Jiwon Ma** is a senior policy analyst at FDD's Center on Cyber and Technology Innovation, where she contributes to the CSC 2.0 project.