National Cyber Incident Response Plan (NCIRP)
Frequently Asked Questions (FAQs)

1. *What is the National Cyber Incident Response Plan (NCIRP)?*

The NCIRP describes the various roles and responsibilities in cyber incidents of the Federal Government, the private sector, and SLTT governments and how we will organize its activities to manage the effects of significant cyber incidents. The NCIRP, developed in accordance with Presidential Policy Directive (PPD) 41 on U.S. Cyber Incident Coordination, leverages doctrine from the National Preparedness System to articulate how the Nation responds to and recovers from cyber incidents. This alignment with the National Preparedness System also allows for cyber incident response to integrate seamlessly with physical incident response in cases where cyber incidents have physical impacts or vice versa.

2. *Why is the National Cyber Incident Response Plan being written?*

In July 2016, the President signed PPD-41 on U.S. Cyber Incident Coordination, filling a gap in policy about how the Federal Government prepares for, responds to, and recovers from significant cyber incidents. One of the tasks from PPD-41 was to create the NCIRP to address cybersecurity risks and coordinate activities to mitigate, respond to, and recover from cyber incidents.

The NCIRP retains key concepts and principles from the 2010 interim version, while incorporating lessons learned from exercises and real world incidents, best practices, and changes in national policy. The Department’s National Protection and Programs Directorate (NPPD) and Federal Emergency Management Agency (FEMA) strive to improve the Nation’s ability to manage cyber incidents, events, and emergencies.

3. *Who was involved in drafting the NCIRP?*

While NPPD led the drafting, the NCIRP refresh has been a collaborative effort with subject matter experts and stakeholders at the private sector, local, state, tribal, territorial and federal level.

NPPD and FEMA convened weekly stakeholder working groups consisting of private sector, local, state, tribal, and Federal Government subject matter experts to inform the draft of the NCIRP. These working groups covered diverse topics, including operations and coordination center systems and Incident Management and Assistance Teams.

Finally, the draft NCIRP was made available for public comment in October 2016 for a National Engagement Period during National Cybersecurity Awareness Month. The public National Engagement Period provided an opportunity for interested parties to provide comments on the NCIRP so that it reflected the collective expertise and experience of the whole community.

4. *When a significant cyber incident is determined, how does the Federal Government respond?*

The Federal Government uses a coordination structure known the Cyber Unified Coordination Group (UCG) to organize its activities into concurrent lines of effort:

- Asset Response, led by DHS through the National Cybersecurity and Communications Integration Center(NCCIC),
- Threat Response, led by the Federal Bureau of Investigation (FBI) and National Cyber Investigative Joint Task Force (NCIJTF),
- Intelligence Support, led by the Office of the Director of National Intelligence (ODNI) through the Cyber Threat Intelligence and Integration Center (CTIIC), and
- A fourth line of effort is the affected public or private entity's response efforts, which may include managing the effects of the cyber incident on its operations, customers, and workforce.

5. *How does the private sector participate with the Federal Government during a significant cyber incident?*

Depending on the nature and extent of a significant cyber incident, participation from the private sector in the Cyber UCG is voluntary and will be limited to organizations with significant jurisdiction, capability, or authority for response for that specific incident, which may not always include all organizations contributing resources to the response.

When a cyber incident affects a private entity, the Federal Government typically will not play a role in this line of effort, but it will remain cognizant of the affected entity's response activities, consistent with the principles above and in coordination with the affected entity.

6. *What is the Cyber Incident Severity Schema and how is it used?*

The Cyber Incident Severity Schema is a common method to describe the severity or impact of a cyber incident. The federal cybersecurity centers utilize the schema to evaluate and assess cyber incidents in a common and consistent manner to ensure the appropriate level of coordination is provided towards cyber incidents.

7. *How can organizations benefit from using the NCIRP?*

The NCIRP should serve as the basis when developing agency-, sector-, and organization-specific operational planning. Additionally, the NCIRP also contains information and resources to create incident response plans including the U.S. Cyber Incident Severity Schema.