United States Cyber Incident Coordination Policy

The Obama Administration recently released Presidential Policy Directive-41 (PPD-41) on United States Cyber Incident Coordination. This directive establishes a unified federal government response to potential cyber incidents and highlights the important role that the FBI plays in cyber incident response. PPD-41 not only sets forth principles that will govern the federal government's response to any cyber incident but also develops architecture for how different agencies will coordinate and interact.

Guiding Principles

PPD-41 directs a unified federal government strategy for cyber incident response which incorporates several key principles: utilization of the unique skills, authorities, and resources of each agency; assessment of the risks posed to U.S. security, safety, and prosperity; and a focus on enabling the restoration and recovery of the affected entity. PPD-41 also recognizes the importance of protecting privacy and civil liberties and sensitive private sector information. The PPD directs that during federal response to a cyber incident, details of the incident and sensitive private sector information be safeguarded through coordination with affected entities. Significantly, PPD-41 also acknowledges that prevention and management of cyber incidents is a shared responsibility among the government, private sector, and individuals.

The FBI's Role in Cyber Incident Response

FBI designation as lead Threat Response agency

PPD-41 organizes the federal government's response to cyber incidents into three distinct lines of effort: threat response, asset response, and intelligence support, and designates agency leads to take ownership of each. The Department of Justice, through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF), has been named as the lead for threat response activities. Threat response activities include the investigative actions related to the cyber incidents, such as collecting evidence, determining attribution, conducting law enforcement activity, and identifying opportunities for further investigative action, intelligence collection, or disruption strategies. Asset response activities involve the mitigation of vulnerabilities and identification of any potential risks to other organizations or sectors that may be affected while also reducing the overall impact of the incident. Intelligence support activities involve building a broader picture of the incident as it relates to other events or intelligence, as well as analyzing trends and events and identifying intelligence gaps.

FBI role in Unified Coordination Group (UCG)

For a significant cyber incident, the PPD directs the formation of a Cyber Unified Coordination Group (UCG) to be comprised of the leads for threat response, asset response and intelligence support. As warranted, UCG participation will be extended to relevant organizations, to include Sector-Specific Agencies (SSAs); other federal agencies; state, local, tribal, and territorial (SLTT) governments; nongovernmental organizations; international counterparts; and the private sector.

Because the victim of cyber incidents is often a private sector entity, PPD-41 clarifies for affected entities how elements of the federal government will organize, respond and coordinate during a cyber incident. This structure allows for enhanced coordination between the FBI and all other agencies and organizations and will ensure the incident is managed as effectively and efficiently as possible.

PPD-41 codifies the essential role the FBI plays in cyber incident response and recognizes the FBI's unique expertise, resources, and capability to lead threat response activities. As the FBI continues to evolve to keep pace with the cyber threat, PPD-41 will empower to FBI to help shape the nation's strategy for addressing cyber incidents of significant national impact. Please see the White House website to read the PPD in its entirety.