The White House
Office of the Press Secretary
For Immediate Release

July 26, 2016

FACT SHEET: Presidential Policy Directive on United States Cyber Incident Coordination

The new directive spells out how the Federal government will coordinate its incident response activities in the event of a large-scale cyber incident

Today, the President approved a **Presidential Policy Directive** (PPD) on United States Cyber Incident Coordination. This new PPD marks a major milestone in codifying the policy that governs the Federal government's response to significant cyber incidents. Since the beginning of his Administration, President Obama has emphasized that malicious cyber activity poses a serious threat to the national and economic security of the United States. As set forth in the **Cybersecurity National Action Plan**, over the last seven and a half years the Administration's cyber policy has been based on three strategic pillars: raising the level of cybersecurity in our public, private, and consumer sectors, in both the short and the long-term; taking steps to deter, disrupt, and interfere with malicious cyber activity aimed at the United States or its allies; and responding effectively to and recovering from cyber incidents.

Even as we have made progress on all three pillars, the United States has been faced with managing increasingly significant cyber incidents affecting both the private sector and Federal government. We have applied the lessons learned from these events, as well as our experience in other areas such as counterterrorism and disaster response. That experience has allowed us to hone our approach but also demonstrated that significant cyber incidents demand a more coordinated, integrated, and structured response. We have also heard from the private sector the need to provide clarity and guidance about the Federal government's roles and responsibilities. The PPD builds on these lessons and institutionalizes our cyber incident coordination efforts in numerous respects, including:

- Establishing clear principles that will govern the Federal government's activities in cyber incident response;
- Differentiating between significant cyber incidents and steady-state incidents and applying the PPD's guidance primarily to significant incidents;
- Categorizing the government's activities into specific lines of effort and designating a lead agency for each line of effort in the event of a significant cyber incident;
- Creating mechanisms to coordinate the Federal government's response to significant cyber incidents, including a Cyber Unified Coordination Group similar in concept to what is used for incidents with physical effects, and enhanced coordination procedures within individual agencies;
- Applying these policies and procedures to incidents where a Federal department or agency is the victim; and,
- Ensuring that our cyber response activities are consistent and integrated with broader national preparedness and incident response policies, such as those implemented through **Presidential Policy Directive 8-National Preparedness**, so that our response to a cyber incident can seamlessly integrate with actions taken to address physical consequences caused by malicious cyber activity.

We also are releasing today a **cyber incident severity schema** that establishes a common framework within the Federal government for evaluating and assessing the severity of cyber incidents and will help identify significant cyber incidents to which the PPD's coordination procedures would apply.

Incident Response Principles

The PPD outlines five principles that will guide the Federal government during any cyber incident response:

- **Shared Responsibility** – Individuals, the private sector, and government agencies have a shared vital interest and complementary roles and responsibilities in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences.
- **Risk-Based Response** – The Federal government will determine its response actions and resource needs based on an assessment of the risks posed to an entity, national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.
- **Respecting Affected Entities** – Federal government responders will safeguard details of the incident, as well as privacy and civil liberties, and sensitive private sector information.

- **Unity of Effort** – Whichever Federal agency first becomes aware of a cyber incident will rapidly notify other relevant Federal agencies in order to facilitate a unified Federal response and ensure that the right combination of agencies responds to a particular incident.
- **Enabling Restoration and Recovery** – Federal response activities will be conducted in a manner to facilitate restoration and recovery of an entity that has experienced a cyber incident, balancing investigative and national security requirements with the need to return to normal operations as quickly as possible.

Significant Cyber Incidents

While the Federal government will adhere to the five principles in responding to any cyber incident, the PPD's policies and procedures are aimed at a particular class of cyber incident: significant cyber incidents. A significant cyber incident is one that either singularly or as part of a group of related incidents is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

When a cyber incident occurs, determining its potential severity is critical to ensuring the incident receives the appropriate level of attention. No two incidents are the same and, particularly at the initial stages, important information, including the nature of the perpetrator, may be unknown.

Therefore, as part of the process of developing the incident response policy, the Administration also developed a common schema for describing the severity of cyber incidents, which can include credible reporting of a cyber threat, observed malicious cyber activity, or both. The schema establishes a common framework for evaluating and assessing cyber incidents to ensure that all Federal departments and agencies have a common view of the severity of a given incident, the consequent urgency of response efforts, and the need for escalation to senior levels.

The schema describes a cyber incident's severity from a national perspective, defining six levels, zero through five, in ascending order of severity. Each level describes the incident's potential to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. An incident that ranks at a level 3 or above on this schema is considered "significant" and will trigger application of the PPD's coordination mechanisms.

Lines of Effort and Lead Agencies

To establish accountability and enhance clarity, the PPD organizes Federal response activities into three lines of effort and establishes a Federal lead agency for each:

- Threat response activities include the law enforcement and national security investigation of a cyber incident, including collecting evidence, linking related incidents, gathering intelligence, identifying opportunities for threat pursuit and disruption, and providing attribution. *The Department of Justice, acting through the Federal Bureau of Investigation (FBI) and the National Cyber Investigative Joint Task Force (NCIJTF), will be the Federal lead agency for threat response activities.*
- Asset response activities include providing technical assets and assistance to mitigate vulnerabilities and reducing the impact of the incident, identifying and assessing the risk posed to other entities and mitigating those risks, and providing guidance on how to leverage Federal resources and capabilities. *The Department of Homeland Security (DHS), acting through the National Cybersecurity and Communications Integration Center (NCCIC), will be the Federal lead agency for asset response activities.* The PPD directs DHS to coordinate closely with the relevant Sector-Specific Agency, which will depend on what kind of organization is affected by the incident.
- Intelligence Support and related activities include intelligence collection in support of investigative activities, and integrated analysis of threat trends and events to build situational awareness and to identify knowledge gaps, as well as the ability to degrade or mitigate adversary threat capabilities. *The Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, will be the Federal lead agency for intelligence support and related activities.*

In addition to these lines of effort, a victim will undertake a wide variety of response activities in order to maintain business or operational continuity in the event of a cyber incident. We recognize that for the victim, these activities may well be the most important. Such efforts can include communications with customers and the workforce; engagement with stakeholders, regulators, or oversight bodies; and recovery and reconstitution efforts. When a Federal agency is a victim of a significant cyber incident, that agency will be the lead for this fourth line of effort. In the case of a private victim, the Federal government typically will not play a role in this line of effort, but will remain cognizant of the victim's response activities consistent with these principles and coordinate with the victim.

Coordination Architecture

In order to facilitate the more coordinated, integrated response demanded by significant cyber incidents, the PPD establishes a three-tiered coordination architecture for handling those incidents:

National Policy Level: The PPD institutionalizes the National Security Council-chaired interagency Cyber Response Group (CRG). The CRG will coordinate the development and implementation of United States Government policy and strategy with respect to significant cyber incidents affecting the United States or its interests abroad.

National Operational Level: The PPD directs agencies to take two actions at the national operational level in the event of a significant cyber incident.

- Activate enhanced internal coordination procedures. The PPD instructs agencies that regularly participate in the Cyber Response Group to develop these procedures to ensure that they can surge effectively when confronted with an incident that exceeds their day-to-day operational capacity.
- Create a Unified Coordination Group. In the event of a significant cyber incident, the PPD provides that the lead agencies for each line of effort, along with relevant Sector-Specific Agencies (SSAs), state, local, tribal and territorial governments, international counterparts, and private sector entities, will form a Cyber Unified Coordination Group (UCG) to coordinate response activities. The Cyber UCG shall coordinate the development, prioritization, and execution of cyber response efforts, facilitate rapid information sharing among UCG members, and coordinate communications with stakeholders, including the victim entity.

Field Level: The PPD directs the lead agencies for each line of effort to coordinate their interaction with each other and with the affected entity.

Integration with Existing Response Policy

The PPD also integrates U.S. cyber incident coordination policy with key aspects of existing Federal preparedness policy to ensure that the Nation will be ready to manage incidents that include both cyber and physical effects, such as a significant power outage resulting from malicious cyber activity. The PPD will be implemented by the Federal government consistent with existing preparedness and response efforts.

Implementation tasks

The PPD also directs several follow-on tasks in order to ensure its full implementation. In particular, it requires that the Administration develop and finalize the National Cyber Incident Response Plan – in coordination with State, Local, Territorial, and Tribal governments, the private sector, and the public – to further detail

how the government will manage cyber incidents affecting critical infrastructure. It also directs DHS and DOJ to develop a concept of operations for how a Cyber UCG will operate and for the NSC to update the charter for the CRG.