U.S. DEPARTMENT OF ENERGY

Office of Electricity Delivery & Energy Reliability

Cyber Incidents - Federal Roles and Responsibilities

Liberty Eclipse

Northeast and Mid-Atlantic Regional Energy Assurance Exercise
December 8, 2016

Fowad Muneer, Program Manager, Cybersecurity
Infrastructure Security & Energy Restoration (ISER) Division

Agenda

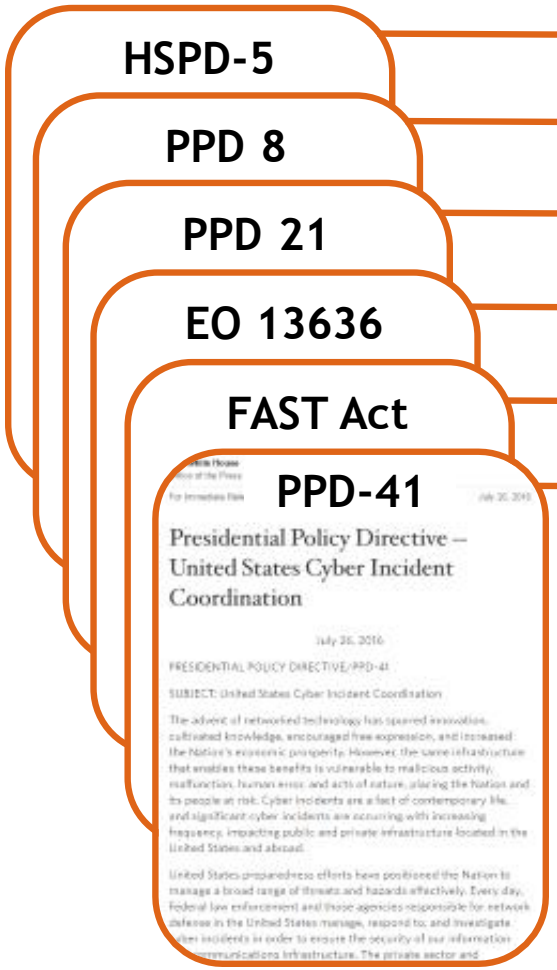
A- ROLES & RESPONSIBILITIES – CRITICAL INFRASTRUCTURE SECURITY

1. Policies and Laws
2. Sector Specific Agency (SSA) Role
3. Energy Sector Cybersecurity Considerations
4. Energy SSA - Cybersecurity Activities

B- ROLES & RESPONSIBILITIES – SIGNIFICANT CYBER INCIDENTS

1. Presidential Policy Directive (PPD) 41
2. Significant Cyber Incidents
3. Cyber Unified Coordination Group (UCG)
4. Cyber UCG - Lines of Effort
   - Identification & Notification
   - Determining Severity
   - Activating Cyber UCG
   - Response Activities
   - Deactivation & Reporting

Policies and Laws



- National Incident Management System
- National Preparedness Goals & Capabilities
- Security of Critical infrastructure Sectors
- Improving Critical infrastructure Cybersecurity
- Energy SSA Roles and Authorities
- Cyber Incident Coordination

Sector Specific Agency (SSA) Role

Critical Infrastructure Sectors

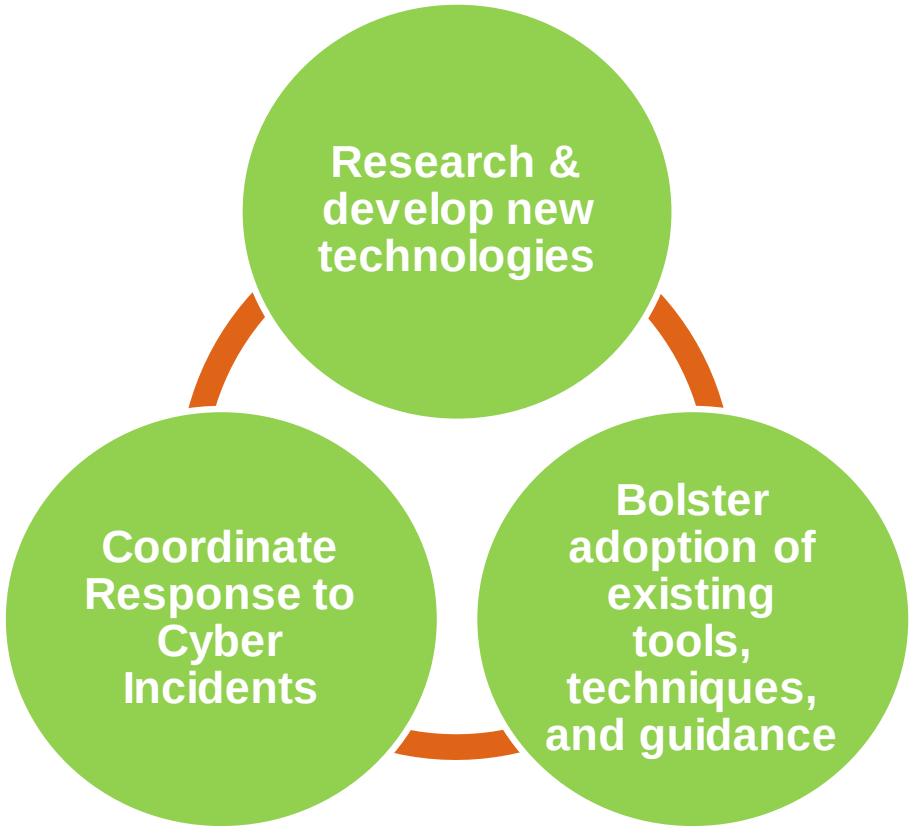
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, & Waste
- Transportation Systems
- Water and Wastewater Systems

Energy Sector Cybersecurity Considerations

Energy Delivery Control Systems ≠ **Business IT Systems**

Different Priorities

Energy SSA - Cybersecurity Activities

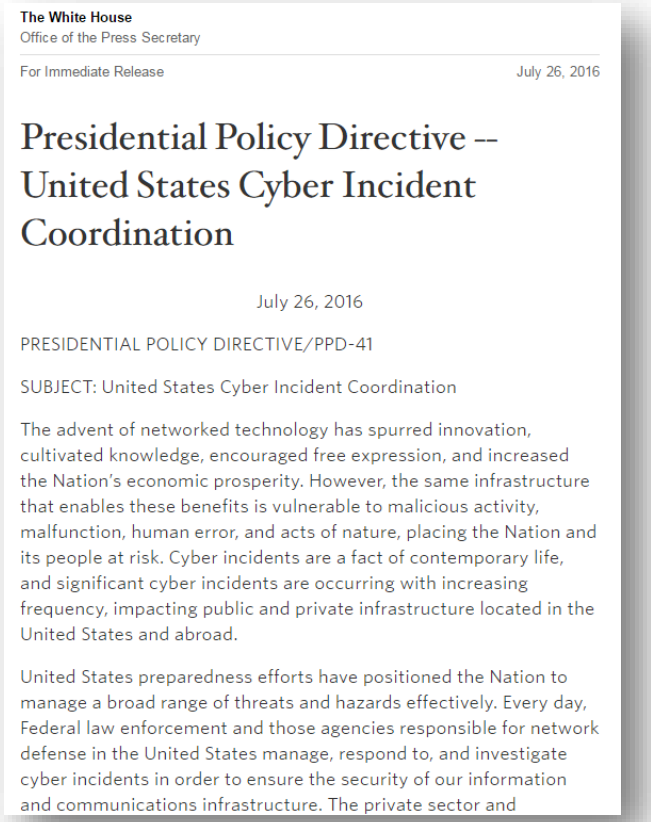


Sector security and resilience goals are achieved through partnerships with industry, federal agencies, national labs, and academia.

Energy SSA - Cybersecurity Activities

Presidential Policy Directive 41

- **Applies to Federal government's activities**
- **Applies to both incidents impacting critical infrastructure sectors, and to incidents where a Federal department or agency is the victim**
- **Establishes principles that govern Federal government's activities in cyber incident response**



The White House
Office of the Press Secretary

For Immediate Release July 26, 2016

Presidential Policy Directive -- United States Cyber Incident Coordination

July 26, 2016

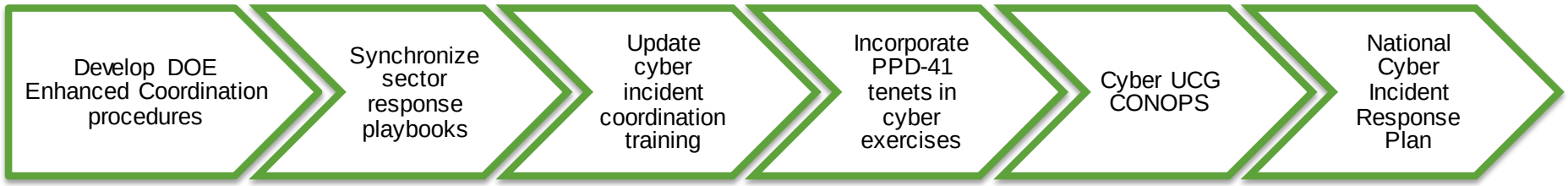
PRESIDENTIAL POLICY DIRECTIVE/PPD-41

SUBJECT: United States Cyber Incident Coordination

The advent of networked technology has spurred innovation, cultivated knowledge, encouraged free expression, and increased the Nation's economic prosperity. However, the same infrastructure that enables these benefits is vulnerable to malicious activity, malfunction, human error, and acts of nature, placing the Nation and its people at risk. Cyber incidents are a fact of contemporary life, and significant cyber incidents are occurring with increasing frequency, impacting public and private infrastructure located in the United States and abroad.

United States preparedness efforts have positioned the Nation to manage a broad range of threats and hazards effectively. Every day, Federal law enforcement and those agencies responsible for network defense in the United States manage, respond to, and investigate cyber incidents in order to ensure the security of our information and communications infrastructure. The private sector and

Presidential Policy Directive 41 (Contd.)



Presidential Policy Directive 41 (Contd.)

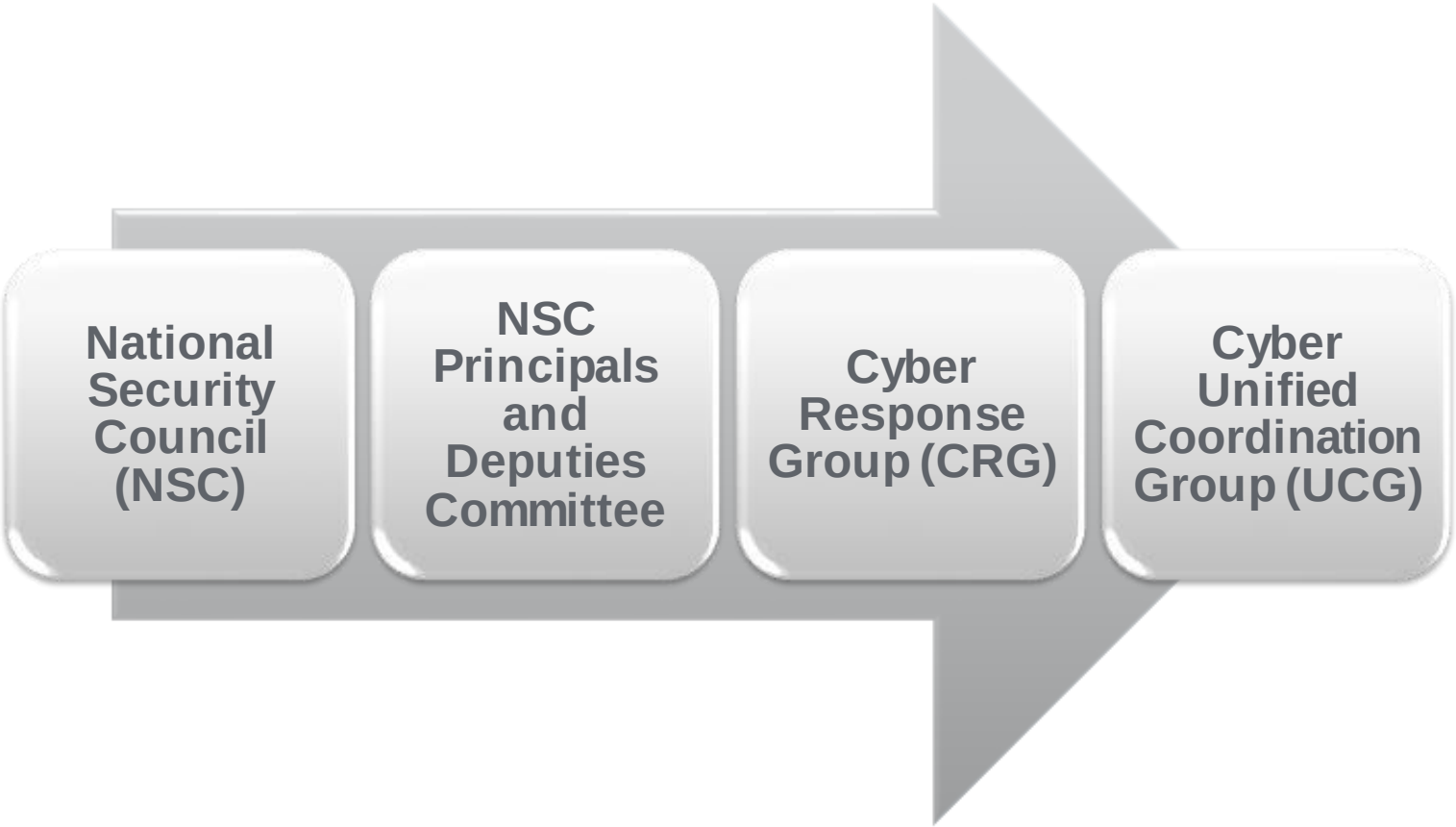
- Defines "Significant" cyber incidents and distinguishes significant cyber incidents with steady-state incidents

- Establishes policy that governs Federal government's response to significant cyber incidents
  - Specific lines of efforts
  - Designated lead agency for each line of effort
  - Mechanisms to coordinate Federal government's response

Significant Cyber Incidents

- **CYBER INCIDENT**
  - **Actual or imminent**
  - **Jeopardizes integrity, confidentiality, or availability**
  - **Virtual or Physical infrastructure controlled by information systems or information resident thereon**
  - **Includes vulnerabilities that could be exploited by a threat source.**
- **SIGNIFICANT CYBER INCIDENT**
  - **A cyber incident that is (or group of related cyber incidents that together are) 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.**

Cyber Unified Coordination Group (UCG)



Cyber UCG - Lines of Effort

Significant Cyber Incident

Likely to result in demonstrable harm to National Security, Foreign relations, Economy, Public confidence, Civil liberties, Public health and Safety

Threat Response

Efforts to address threat aspects of cyber risk, e.g., attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity.

NCIJTF

Asset Response

Provide technical assistance to protect victim assets, mitigate vulnerabilities, & reduce impacts. Identify other entities at risk of same vulnerabilities and assess risks to sector or region

NCCIC

Intelligence Support

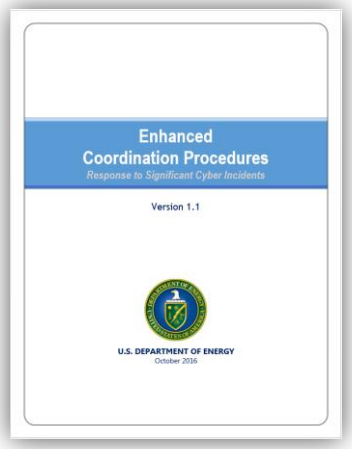
Enable situational threat awareness and sharing of related intelligence and analysis and mitigating adversary threat capabilities

CTIIC

DOE

Enhanced Coordination Procedures

Procedures that bring dedicated leadership and resources to impacted entity, enabling it to manage an incident under demands that would exceed its capacity to coordinate under normal operating conditions.



Identification & Notification

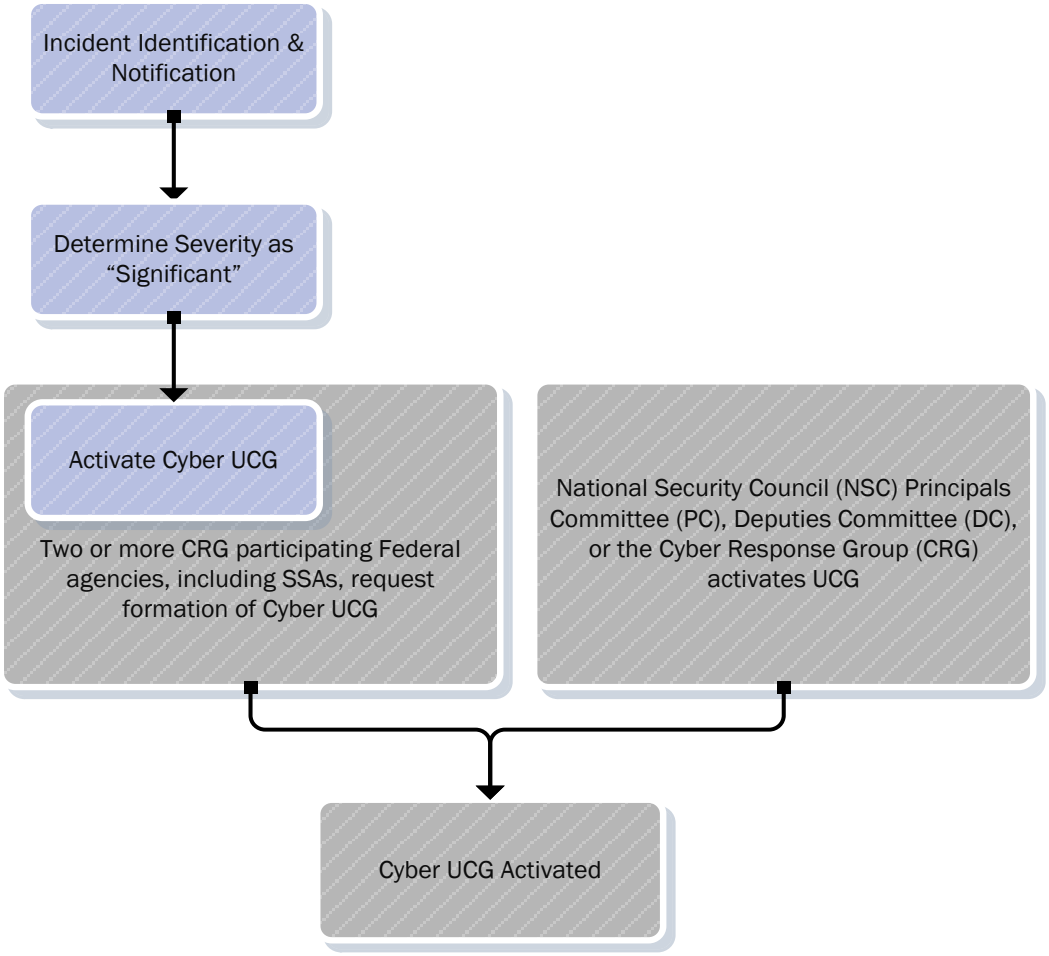
- **Whichever Federal agency first becomes aware of a cyber incident will rapidly notify other relevant Federal agencies in order to facilitate a unified Federal response and ensure that the right combination of agencies responds to a particular incident.**
- **Adhere to victim privacy protocol requirements**

Determining Severity

- **Response actions and resource needs based on assessment of risk to entity, national security interests, foreign relations, economy, public confidence, civil liberties, or public health and safety.**
- **Level 3 and above is deemed Significant Cyber Incident**

Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

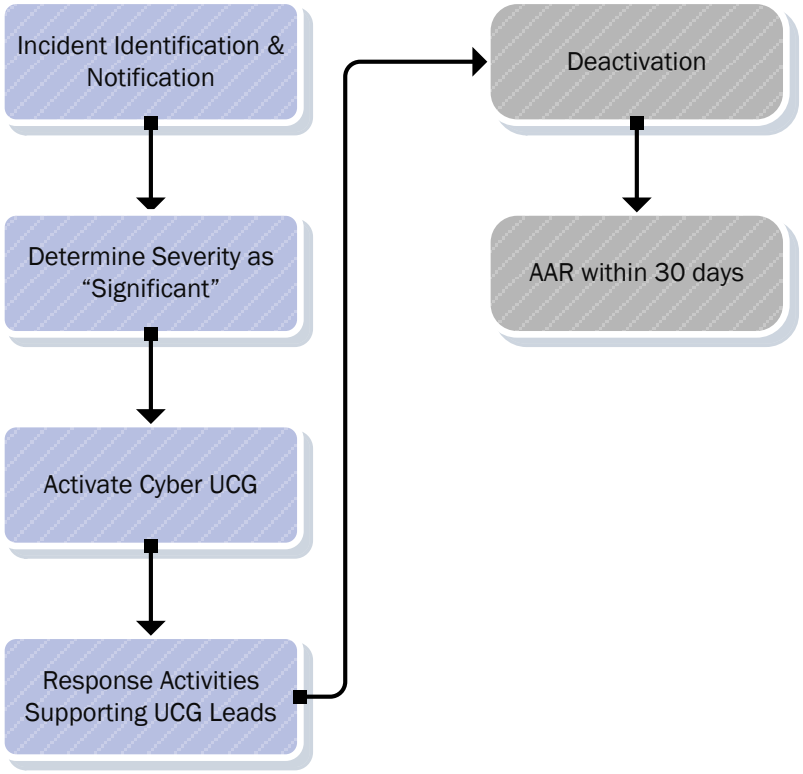
Activating Cyber UCG



Response Activities

- **SSA response actions will be performed in support of Cyber UCG Leads for Asset, Threat, and Intelligence Response**
- **Leverage Sector Specific expertise, capabilities, protocols, and authorities to support incident response**

Deactivation & Reporting



- **After Action Report to be provided to the CRG within 30 days.**
- **Federal agencies will modify relevant plans or procedures as appropriate or necessary in light of that report.**

CyberEnergy@hq.doe.gov
www.energy.gov/oe/services/cybersecurity