DHS ROLE IN CYBER INCIDENT RESPONSE

On July 26, 2016, President Obama signed Presidential Policy Directive (PPD) 41, *United States Cyber Incident Coordination*. The PPD sets forth principles governing the Federal Government's response to any cyber incident and, for significant cyber incidents, establishes lead federal agencies and an architecture for coordinating the broader Federal Government response.

PPD-41 refers to victims or other organizations that have been directly impacted by a cyber incident as "affected entities."

LINES OF EFFORT

The Federal Government has three lines of effort in cyber incident response. No single agency possesses all of the authorities, capabilities, and expertise to deal unilaterally with a significant cyber incident.

Asset Response: Asset response efforts involve furnishing technical assistance to affected entities to help them recover from the incident. The Department of Homeland Security (DHS), through the National Cybersecurity and Communications Integration Center (NCCIC), is the lead federal agency for asset response activities for significant cyber incidents.

Threat Response: Threat response efforts involve the investigation of the crime. The Department of Justice (DOJ), through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF), is the lead federal agency for threat response activities for significant cyber incidents.

Intelligence Support: Intelligence support efforts involve creating situational awareness about cyber threats. The Office of the Director of National Intelligence (ODNI), through the Cyber Threat Intelligence Integration Center (CTIIC), is the lead federal agency for intelligence support and related activities for significant cyber incidents. The CTIIC does not work with the affected entity; it supports the government effort.

Other federal agencies also have critical roles in cyber incident response. The U.S. Secret Service are experts in investigating financial crimes as part of threat response. DHS's Homeland Security Investigations provides threat response for cyber-enabled crimes, including illicit e-commerce and theft of intellectual property. Sector specific agencies, like the Department of Energy and the Treasury, provide their deep sector-level knowledge to asset response efforts. And DHS's Office of Intelligence and Analysis also participates in the intelligence support portion of cyber incident response.

NCCIC = FIREFIGHTER

As an analogy, think of a cyber incident as an arson: when you have a fire caused by arson, you want both the firefighters and the police to be present. The NCCIC is like a firefighter: its role is to put out the fire, prevent it from spreading to other buildings, determine how the fire started, and advise the building owner how to prevent future fires. That's asset response. The threat response role is the equivalent of the police role: their job is to figure out who the perpetrator is and bring them to justice.

NCCIC AND ASSET RESPONSE

At the tactical level, the NCCIC will help an affected entity:

- Find the adversary on its systems;
- Determine how the adversary broke in;
- Remove the adversary from its systems; and
- Help the affected entity rebuild its systems to be more secure.

Homeland Security

At the strategic level, the NCCIC will coordinate the asset response. It will:

- Coordinate the provision of assistance from all federal agencies to the affected entity;
- Share anonymized information about the incident from the affected entity so that other companies and governments can protect themselves;
- Distribute threat indicators of the incident through its Automated Indicator Sharing (AIS) capability (www.us-cert.gov/ais) to all AIS participants; and
- Identify and alert other entities that may be at risk from this particular incident.

PPD-41 OVERARCHING GUIDING PRINCIPLES

Shared Responsibility: We all have a shared 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 based on an assessment of the risks posed to an entity, our national security, foreign relations, the broader economy, public confidence, civil liberties, or public health and safety.

Respecting Affected Entities: Federal responders will safeguard details of the incident, as well as the affected entity's privacy and civil liberties and sensitive information.

Unity of Governmental Effort: The first federal agency aware of a cyber incident will rapidly notify other relevant federal agencies to facilitate a unified response.

Enabling Restoration and Recovery: Federal response activities will facilitate restoration and recovery of an entity that has experienced a cyber incident, balancing investigative and national security requirements, public health and safety, and the need to quickly return to normal operations.

NATIONAL CYBER INCIDENT RESPONSE PLAN

DHS, in coordination with DOJ and others, led the effort to write the National Cyber Incident Response Plan (NCIRP). The NCIRP outlines a nationwide approach to cyber incident response and formalizes the incident response practices that have been developed over the past few years.

Building upon PPD-41, the NCIRP provides more detail as to organizational roles, responsibilities, and actions to prepare for, respond to, and coordinate the recovery from a significant cyber incident.

To view the NCIRP, visit www.us-cert.gov/ncirp.

LINKS

PPD-41: www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

Cyber Incident Reporting: www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf