Today, President Obama signed a policy on Cyber Incident Coordination. This document outlines the federal government's roles and approach for responding to significant cyber incidents. (See the URLs at the bottom of this message for more about this document, which is also known as Presidential Policy Directive, or PPD, 41).

The PPD articulates the significant role of the Department of Homeland Security (DHS) in cyber incident response, and I want to give you more information on our role.

By analogy, think of each cyber incident as the equivalent of a fire in the physical world. When a building is on fire, you want both the firefighters and, if the fire is suspicious, the police to be present. DHS' National Cybersecurity and Communications Integration Center (NCCIC) is like the firefighter, helping the owner of the building put out the fire and then rebuild it to be more fire-proof. The NCCIC also works on fire prevention, to prevent these incidents from happening in the first place or to keep fires from spreading to nearby structures. Our federal law enforcement agencies, including the U.S. Secret Service (USSS), U.S. Immigration and Customs Enforcement/Homeland Security Investigations (HSI), and the Federal Bureau of Investigations (FBI), are the equivalent of the police. They work to identify and catch the criminal that set the fire.

In all of these activities, we respond in a coordinated way as a united government, and we will place the victim or the affected entity's needs first.

Asset Response

Within a Cyber Unified Coordination Group (UCG), which will be stood up in the event of a significant cyber incident, the NCCIC will act as the lead Federal Government coordinator for "asset response" activities. This is the "firefighter" role.

At the tactical level, the NCCIC will continue to help affected entities:

- Find the adversary on its systems;
- Learn how the adversary broke in;
- Remove the adversary from its systems; and
- Rebuild its systems to be more secure moving forward.

At the strategic level, the NCCIC will coordinate the asset response within a Cyber UCG. In essence, the NCCIC's role will be analogous to the role of FEMA in physical events. The NCCIC will:

- Coordinate the provision of assistance from all government agencies to the victim;
- Use anonymized information from the affected entity and share it broadly, so that other companies and governments can protect themselves;
- Distribute threat indicators through its Automated Indicator Sharing system, which was established by the Congress in December 2015; and
- Identify other entities that may be particular at risk from this attack and alert them.

In all of these activities, the NCCIC will work closely with other members of the Cyber UCG, including the appropriate Sector Specific Agency – the government agency that works most

closely with a given sector. Those agencies bring a wealth of knowledge, relationships, and capability to support their sectors.

Threat Response

DHS also plays an important role in "threat response" activities to cyber incidents. In our arson analogy, this is the equivalent to the police role. DHS law enforcement components—specifically, the USSS and HSI—will continue to conduct criminal investigations into cyber incidents in coordination with other law enforcement agencies. Within a Cyber UCG, these activities will be coordinated with the National Cyber Investigative Joint Task Force, as the lead coordinator for "threat response" activities to a significant cyber incident.

We cannot make progress in cybersecurity without deterring, disrupting, and dismantling our adversaries' malicious cyber capabilities and activities, and threat response is critical to that mission. These investigative activities will ensure that the resources of the entire federal law enforcement community as well as state, local, tribal, and territorial law enforcement communities are brought to bear against cyber criminals.

NCIRP

Aside from its work in both asset and threat response activities, DHS is also leading the effort to write the National Cyber Incident Response Plan (NCIRP). The plan will formalize the incident response practices that have been developed over the past few years and will in further detail clarify organizational roles, responsibilities, and actions to prepare for, respond to, and coordinate the recovery from a significant cyber incident. This plan will build upon the PPD and include the private sector and other levels of government.

We began the effort to write the NCIRP last month and will coordinate with all critical infrastructure sectors, sector coordinating councils, government coordinating councils, Sector Specific Agencies, states, and private sector organizations to seek their input on the NCIRP, so expect to hear from us soon if you haven't already. We anticipate releasing a draft of the NCIRP for public comment in September 2016.

Of course it's voluntary, but please continue to report cyber incidents to the federal government, whether via the NCCIC, USSS, HSI, FBI, or any other agency with whom you have an established relationship. By reporting an incident, you help us protect you and others. Be assured that we will continue to coordinate closely to ensure that any damage is quickly mitigated and that the perpetrators are brought to justice.

Best,
Phyllis Schneck & Andy Ozment

Links:

- DHS Secretary Johnson's Statement: https://www.dhs.gov/news/2016/07/26/statement-secretary-jeh-c-johnson-regarding-ppd-41-cyber-incident-coordination

- PPD-41: https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
- Annex: https://www.whitehouse.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident
- Fact Sheet: https://www.whitehouse.gov/the-press-office/2016/07/26/fact-sheet-presidential-policy-directive-united-states-cyber-incident-0