# Critical Partnerships: DHS, DoD, and the National Response to Significant Cyber Incidents

By Dr. Andy Ozment, Assistant Secretary for Cybersecurity and Communications, Department of Homeland Security and
Tom Atkin, Acting Assistant Secretary of Defense for Homeland Defense and Global Security, Department of Defense
with Eric Goldstein and Scott Mann.

## I. INTRODUCTION

Critical infrastructure provides the foundation for all aspects of modern life, from power to telecommunications to potable water. Over the past two decades, critical infrastructure entities have increasingly moved toward networked systems to improve their efficiency, accessibility, and reliability. But this increased connectivity has created new risks and vulnerabilities. If a legitimate user can remotely access a key component, such as a transformer, to conduct routine maintenance operations, a malicious actor may be able to exploit the same connectivity to inflict harm.

These risks are real, significant and increasingly salient. Last December, several Ukrainian power companies experienced a cyberattack that resulted in unscheduled power outages that impacted over 200,000 customers.[1] While there is no evidence of similar malicious activity affecting U.S. companies, the risk is clear. In March, the Department of Justice announced the indictment of seven Iranian hackers, who are accused of launching distributed denial of service operations against nearly 50 U.S. financial sector institutions between 2011 and 2013, as well as the repeated penetration of the computer systems tied to the Bowman Dam in Rye, NY.[2] These incidents collectively demonstrate the reality of the threat facing our nation's critical infrastructure.

Our nation's critical infrastructure owners and operators are increasingly aware of these risks and many have invested substantial resources in cybersecurity. Similarly, the Federal Government is clear-eyed about the potential impacts of such an attack, and we are actively working to prevent incidents—and to be ready to respond if they occur. Both the government and the private sector must work together to confront this evolving risk. To do so, we must first define a principal element of protecting U.S. critical infrastructure: an effective partnership with clearly understood responsibilities.

Partnership begins with a common understanding of the threat environment, the requirements for responding to a significant cyber incident, and proper roles and responsibilities across the public and private sectors to ensure a whole-of-nation response.

[1] Industrial Control Systems Cyber Emergency Response Team, Alert (IR-Alert-H-16-056-01), "Cyber-Attack Against Ukrainian Critical Infrastructure," February 25, 2016, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[2] Department of Justice, U.S. Attorney's Office. Southern District of New York, "Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyberattacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities, " March 24, 2016, https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated

## II. THE ANATOMY OF AN ATTACK

At this point, the effects of a major cyberattack are largely theoretical. The history of significant cyberattacks against critical infrastructure is a short one – few effects have been lasting, and almost none have caused loss of life or systemic costs. Examples are limited: intrusions targeting the Estonian government in 2007 and the Georgian government in 2008; a 2012 cyberattack against Gulf-nation oil and gas firms, and the most recent attack against the Ukrainian electric grid come to mind. While the list is short, a major cyberattack is, of course, theoretical only until it occurs.

A significant cyber incident would likely consist of two distinct but related parts: the actual network penetration (to include data theft or manipulation) and the resulting physical effects of that penetration. Initially, a network could be penetrated through a range of mechanisms, such as a phishing attack; the exploitation of vulnerabilities in unpatched systems; or through insider manipulation of systems (e.g. malware implantation) to permit remote access. Once inside, the intruder could steal data or alter the network.

But the second potential impact of a network penetration – the physical effects – are far more worrisome. With the right tools and intent, malicious actors could damage critical infrastructure in ways that replicate the effects of a major natural disaster. It is the physical effects of a cyberattack that are our focus here. [3]

## III. ANATOMY OF CYBER INCIDENT – FRAMING RESPONSE

With this in mind it is useful to think of a cyber incident in three phases: a pre-attack phase before an attack occurs, the actual conduct of an attack, and the post-attack phase after the attack has concluded. A common theme across all three phases is the need for cooperation across the Federal Government and with the private sector. For the moment, we will set aside the "pre-attack" phase and take for granted the many important (and no less essential) activities that ensure a cyber incident never occurs[4] and instead focus on the requirements for a post-attack scenario - that is, how do we respond?

### *A. Presidential Policy Directive-41: A Unified Response to a Cyber Incident:*

On July 26th, President Obama signed Presidential Policy Directive-41 (PPD-41) entitled *United States Cyber Incident Coordination.* This PPD sets forth principles governing the Federal

[3] Data manipulation is also a significant concern. The political and economic systems of this country rely on the integrity of the information on our key systems. Data manipulation risks a loss of trust in that information, and could undermine trust in the system.

[4] Before a cyber incident occurs, the U.S. government engages in three related activities to help prevent damaging attacks. The Department of Defense, for example, seeks to detect, and if necessary directly counter cyberattacks emanating from foreign states before they can be successfully launched. The Department of Homeland Security (DHS), US Secret Service, and the Federal Bureau of Investigation (FBI) share information about potential cyberattacks with the possible victims to inform targeted defensive measures. And DHS, in coordination with Sector Specific Agencies, provides more general guidance based upon the overall threat environment to help organizations improve their cybersecurity posture.

Government’s response to any cyber incident, whether involving government or private sector entities. For significant cyber incidents, the PPD establishes lead Federal agencies and an architecture for coordinating across the broader Federal Government. While this policy is new, there remains one constant unifying theme: as a first principle, the National Response Framework (NRF) applies equally to natural disasters and cyber incidents and provides a flexible, scalable, adaptable, and unified structure to handle a wide range of incident response requirements.

PPD-41 establishes three core responsibilities for Federal government cyber incident response: Threat Response, Asset Response, and Intelligence Support. An analogy may prove useful for explaining the roles and responsibilities described under PPD-41.

PPD-41 views significant cyber incidents as the equivalent of an arson in the real world: you want both the police and the firefighters to help you. In a significant cyber incident, the PPD assigns the lead for the “police” role, known as “Threat Response,” to the Department of Justice (DOJ), acting through the Federal Bureau of Investigation (FBI) and the National Cyber Investigative Joint Task Force (NCIJTF). The PPD assigns the lead “firefighter” role, known as “Asset Response” to the Department of Homeland Security (DHS) acting through the National Cybersecurity and Communications Integration Center (NCCIC). Finally, PPD-41 designates the Office of the Director of National Intelligence, acting through the Cyber Threat Intelligence Integration Center as the Federal lead agency for “Intelligence Support” and related activities. This intelligence organization will not interact directly with the victim or affected entity. Instead, it will provide behind-the-scenes support to government agencies during the response.

There has been particular interest in how DHS and the Department of Defense (DoD) will interact in the asset response role, so we will focus on that relationship.

### B. *ASSET RESPONSE: FRAMING DHS’ ROLE*

A truism of emergency response is that lifesaving activities must begin at the level closest to the affected population. In the case of a natural disaster, this is usually local public safety agencies. Those closest to an incident are likely the quickest to respond and have the best understanding of the facts on the ground. In the case of a cyber incident, the victim organization itself is usually the first to respond for precisely this reason.

As a tactical level “firefighter” during a cyber incident, DHS can help the victim: (1) find the adversary on its systems; (2) determine how the adversary broke in; (3) remove the adversary from its systems; and (4) rebuild its systems to be more secure.

At the strategic level, DHS will lead the asset response in a role somewhat more analogous to the Federal Emergency Management Agency, or FEMA. DHS will: (1) coordinate the provision of asset response assistance to the victim from all federal agencies; (2) share anonymized information about the incident from the affected entity so that other companies and governments can protect themselves; (3) distribute threat indicators of the incident through its Automated Indicator Sharing capability; and (4) work with DOJ/FBI to identify and alert other entities that may be at risk from this particular incident.

As noted, a cyber incident can also cause physical impacts. The approach to managing the physical impacts of a cyberattack are akin to the response to a major natural disaster – requiring efforts at all levels of society working in concert to return the affected entities to full functionality and capacity. The goal of such a response is to provide for the immediate needs of the community, reconstitute critical services while providing interim alternatives, and rebuilding as quickly as possible. This requires a coordinated effort at all levels – state, local, tribal, private sector, and the Federal Government. Just as these entities marshal resources to respond to the damage of a hurricane, they are ready and able to respond in the same way to the physical effects of a cyberattack.

### *C. DoD's Role - DEFENSE SUPPORT OF CIVIL AUTHORITIES*

DoD's core mission is to provide for the national defense, which includes providing the President with military options to deter or defeat adversaries. This mission remains a constant across all domains – air, land, sea, space, and cyberspace. Should a significant cyber incident be the result of an adversary attack, DoD is prepared to execute appropriate military options at the President's direction.

DoD has another role – providing support to civil authorities during national emergencies. DoD's Defense Support of Civil Authorities (DSCA) mission provides a well-exercised mechanism to bring the appropriate DoD resources, capabilities, and capacity to assist domestic response efforts. This applies equally to hurricanes and cyber incidents. Should a significant cyber incident exhaust the existing resources within DHS, DoD can, at the request of DHS, or at the direction of the Secretary of Defense or the President, support the response activities of civil authorities.

## IV. THE WAY AHEAD

Ultimately, effectively responding to a significant cyberattack requires a comprehensive, whole-of-nation approach. Neither the private sector nor the U.S. Government alone possess sufficient capability or capacity to address the risks to the Nation's most critical assets. Only through concerted, cooperative efforts can we be adequately prepared for a worst-case scenario. DHS and DoD are working with partners in government and the private sector to ensure that we are ready should a significant cyber incident affect critical infrastructure occurs.

Both PPD-41 and the NRF provide a solid set of universal principals to organize for cyber incident response. Both DoD and DHS have multiple on-going lines of effort to ensure Federal preparedness in the event of a major cyber incident.

### *A. Planning*

Crisis preparedness in any domain requires a deliberate approach. It requires identifying the available and essential resources, outlining clear roles and responsibilities, identifying the chain of command, and delegating where possible. As noted above, the principles of disaster response apply to the cyber domain as well. The NRF lays out a strategy for *all-hazards response*, providing a scalable, flexible, and adaptable foundation to meet the unique requirements of a given emergency. With this in mind, DHS is leading development of a National Cyber Incident Response Plan (NCIRP) to further extend the principles of the NRF into the cyber domain and codify how Federal agencies, State, Local, Tribal, and Territorial (SLTT) governments, and the private sector will work together to achieve a coordinated, cohesive cyber incident response.

### *B. Build Capability*

Plans require people to execute them. The core of domestic response efforts will occur within the affected entities themselves – indeed, the infrastructure owners remain responsible for and the locus of any response effort. It is important for the private sector to have a clear understanding of its capacity and as well as an understanding of the types of incidents that will require outside assistance.

To prepare for such an eventuality, DHS' NCCIC has cyber incident response teams that can deploy to assist victims of cyberattacks. The NCCIC has been deploying to help private sector and government agencies respond to attacks for years, but has always had a small number of teams. As part of the Cyber National Action Plan (CNAP) announced by the President in February of 2016, the President's Budget requests funding to expand DHS' NCCIC to include twenty-four teams of elite cyber first responders that can be deployed to help both private sector and government victims of cyber incidents. These teams encompass both regular cybersecurity responders and experts in industrial control systems.

DoD is in the process of building out the Cyber Mission Force (CMF), which is the nation's cadre of cyber soldiers. In the event of a major cyberattack, these forces may be called upon to respond in cyberspace to counter an adversary's aggression, much as the military does in other domains. They could also be called upon under DSCA to support civil authorities' domestic response efforts, much as logistics or search and rescue forces might be provided in a natural disaster. While remaining under the command and control of DoD, they would integrate fully to support a whole-of-nation response.

National Guard units serve an important role and may consult with government entities, public and private utilities, critical infrastructure owners, the Defense Industrial Base, and other non-governmental entities, as needed, in order to protect DoD information networks, software, and hardware, enhance DoD cyber situational awareness, provide for DoD mission assurance requirements, and support cybersecurity efforts in their respective States at the direction of the Governor.

### *C. Build Partnerships*

The foundation of effective response begins with establishing robust and enduring partnerships both across the Federal Government and with the private sector. We must collectively understand our capacity and capabilities, as well as the thresholds for requests for assistance.

These relationships are reinforced through effective communication and information sharing, whether it is DHS's NCCIC sharing threat signatures or providing advance warning of potential threats to public and private partners, or the private sector volunteering information regarding vulnerabilities or compromises. Open lines of communication contribute to shared situational awareness, provide effective avenues for prevention, and provide for rapid response in the event of an incident. These communication channels must be mature before an emergency occurs for them to function under the stress of a disaster.

The need for information sharing is a two-way street. It is incumbent upon all organizations to share information related to cyber threats and compromises broadly and rapidly. It is also important for organizations to remediate similar vulnerabilities across sectors to avoid repeated incidents. As required by the Cybersecurity Act of 2015, DHS has implemented a capability that allows real-time exchange of machine-readable cyber threat indicators between government and the private sector. As more organizations participate in this type of automated information exchange, our collective susceptibility to attack will be reduced. But this is a public good and requires broad voluntary participation to be truly effective. By sharing what is already known about threats and vulnerabilities, network defenders will be able to focus on combating sophisticated attacks rather than responding to myriad compromises using known vectors.

### *D. Exercise*

The best plans rarely survive contact with reality – it is impossible to plan for every contingency. This is why realistic exercises are essential. They provide opportunities to test assumptions, rehearse procedures, formalize communication channels, and execute plans in a controlled environment.

The Federal Government clearly recognizes the value of exercises, and employs a comprehensive set of exercises to test its capabilities and preparations. For example, Sector Specific Agencies like Treasury and the Department of Energy hold exercises with the financial and energy sectors, respectively.

DHS has conducted the CYBER STORM exercise series since 2004 as a capstone to test response capabilities across government and the private sector. In the most recent CYBER STORM V, over 1,200 individuals participated, representing more than 45 companies, 17 state governments, and 13 international partners.

Similarly, the DoD conducts its annual CYBER GUARD exercise in order to test a whole-of-government, whole-of-nation response. The 2016 CYBER GUARD was co-sponsored by DHS and the FBI, and included participants from the intelligence community, National Guard, and the private sector. This exercise, and ones like it, will be essential to ensuring the Nation is prepared in the event of a major cyberattack.

## V. Conclusion

Significant cyber incidents require a whole-of-government, whole-of-nation response. The processes outlined above for domestic incident response are just one of the necessary elements for responding to these emergencies, and are nested within a larger interagency framework that can bring the full tool chest of the Federal Government – diplomatic, informational, military, and economic levers - to respond to adversary aggression. Indeed, this concerted effort is required to effectively posture the Nation for a secure cyberspace.

To achieve the goals laid out in the PPD, the Federal Government has been, and will continue working closely with its partners, both in the interagency and with the private sector. By hiring and training dedicated personnel with cyber expertise, establishing information sharing channels to alert entities of network breaches and malware, and by establishing agreements and procedures to facilitate future unified and coordinated efforts, the ground work is being laid for effective incident response.

Together, we must undertake concerted effort to reduce the likelihood of a significant cyber incident. We cannot achieve perfect prevention. For this reason, the public and private sectors must continue to exercise, train, and plan together. In so doing, we will effectively manage both the cyber and physical effects of a significant cyber incident.