FEMA

STATEMENT

OF

W. CRAIG FUGATE
ADMINISTRATOR
FEDERAL EMERGENCY MANAGEMENT AGENCY
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE
THE

COMMITTEE ON TRANSPORTATION AND INFASTRUCTURE
SUBCOMMITTEE ON ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS AND EMERGENCY MANAGEMENT

U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.

"BLACKOUT! ARE WE PREPARED TO MANAGE THE AFTERMATH OF A CYBER-ATTACK OR OTHER FAILURE OF THE ELECTRICAL GRID?"

Submitted
By

Federal Emergency Management Agency
500 C Street, S.W.
Washington, D.C. 20472

April 14, 2016

Introduction
Chairman Barletta, Ranking Member Carson and Members of this Subcommittee, good afternoon. My name is Craig Fugate and I am the Administrator of the Department of Homeland Security's (DHS) Federal Emergency Management Agency (FEMA). Thank you for the opportunity to discuss how FEMA fulfills its responsibility to lead the Nation's response and recovery efforts for all hazards, to include the physical impacts of a massive power outage.

The most effective way for the federal government to plan for and respond to the potentially life-threatening physical consequences of a cyber incident on our nation's power grid is to be as prepared as possible to handle the consequences of any type of catastrophic event, regardless of the cause. Whether it's a cyber incident, a space weather event, or a Category 5 hurricane making landfall, FEMA, in partnership with its federal partners, has the plans and resources in place for a robust federal effort to support state, local, tribal, territorial governments, the private sector, and citizens to appropriately respond to any hazard.

Over the past several years, FEMA – in close coordination with our federal interagency partners, the public and private sectors, and other key stakeholders – has made important progress in addressing ways in which we respond to, recover from, and mitigate all hazards, including malicious cyber activity and the physical consequences of cyber incidents.

In my testimony today, I will highlight the overarching catastrophic planning frameworks that guide FEMA's response to large-scale complex incidents; current efforts underway to supplement all-hazards plans to specifically address cyber incident considerations; and ways in which FEMA and other critical stakeholders exercise our ability to respond to catastrophic events, including the physical impacts of cyber incidents.

Overview of Planning and Catastrophic Planning Efforts

Response Planning
FEMA's Planning and Exercise Division is responsible for a number of planning actions, including developing and coordinating joint state and federal catastrophic plans; leading the development and alignment of regional-to-national-level interagency catastrophic planning efforts; supporting regional planning initiatives to align all catastrophic planning; and the overall development and delivery of the updated Power Outage Incident Annex, which I will discuss later in this testimony.

Additionally, we coordinate closely with our federal partners on other preparation efforts, including the development of pre-scripted mission assignments, interagency agreements, and advanced contracts for commodities. These partnerships are essential to FEMA's ability to carry out its mission by leveraging the full capacity of the federal government to prepare for, protect against, respond to, recover from and mitigate catastrophic incidents, including cyber incidents.

Presidential Policy Directive 8: National Preparedness
Recognizing that this nation's preparedness is a shared responsibility across all sectors of our society, on March 30, 2011, the President signed *Presidential Policy Directive (PPD)-8*: *National Preparedness*. PPD-8 aims to strengthen the security and resilience of this nation through systematic preparation for the threats and hazards that pose the greatest risk to national security.

PPD-8 called for a National Preparedness Goal to guide and align the nation's preparedness efforts at all levels. The National Preparedness Goal is: "A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk." The Goal is also the cornerstone for the implementation of PPD-8.

The President's issuance of PPD-8 significantly aided the alignment and integration of operational planning under a single National Preparedness System. The five mission frameworks – (Prevention, Protection, Mitigation, Response, and Recovery) – set forth the policy, roles and responsibilities of the community of partners across Federal, state, local, tribal and territorial governments, non-governmental organizations, and individual citizens.

National Response Framework

The National Response Framework (NRF) is an essential component of the National Preparedness System mandated in PPD-8. It is a guide to how the nation responds to all types of disasters and emergencies. It is built on scalable, flexible, and adaptable concepts identified in the National Incident Management System (NIMS) to align key roles and responsibilities across the nation. The NRF describes specific authorities and best practices for managing incidents that range from the serious, but purely local, to large-scale terrorist attacks or catastrophic natural disasters. The NRF defines a catastrophic incident as "any natural or manmade incident, including terrorism that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, or government functions." Furthermore, the NRF describes structures for implementing a nationwide response policy and operational coordination for all types of domestic incidents—underscoring the importance of how risk informs response planning. The Framework is always in effect and applies to all catastrophic incidents, including the physical impacts of malicious cyber activity.

The NRF organizes the implementation of federal response capabilities and expertise into 14 Emergency Support Functions (ESFs) to provide the planning, support, resources, program implementation, and emergency services needed during a disaster. The ESFs, coordinated by FEMA, serve as the primary operational-level mechanisms in support of state, local, tribal, and territorial efforts. During a cyber incident that results in physical impacts, most of the ESFs would play some role. For example, ESF #6: Mass Care would coordinate the delivery of federal mass care, emergency assistance, housing, and human services, while ESF #12: Energy would facilitate the restoration of damaged energy systems and components for incidents requiring a coordinated Federal response. Federal departments and agencies provide substantial disaster response assistance in their areas of expertise, as well as operational support when mission assigned to support the disaster response.

Revision of the National Response Framework (NRF)

Originally published in 2008 to replace the National Response Plan, the NRF was revised in 2013, to focus on how the NRF fits into the National Preparedness System called for in PPD-8. The NRF was refreshed again in 2015 to better integrate with the other mission areas. For example, the Framework describes in greater detail how "non-Stafford incidents" can employ and utilize the NRF to help organize, guide, and streamline incident response. The NRF is intended to be a

strategic document, with tactical planning and concept of operations content reserved for the Federal Interagency Operational Plans.

Federal Interagency Operations Plans (FIOPs)
The FIOPs build upon the National Planning Frameworks (including the NRF highlighted above), which set the strategy and doctrine for how the community partners at all levels build, sustain, and deliver the core capabilities identified in the National Preparedness Goal. The Response FIOPs is structured to address the "maximum of maximum" planning factors for the nation or any given region while being flexible and adaptable for the full range of threats that face the nation. A single all-hazard FIOP serves to operationalize the roles and responsibilities for each mission framework (Prevention, Protection, Mitigation, Response, and Recovery). This all-hazards approach includes events that would result from a cyber incident, including effects on infrastructure and individuals. The single operational plan for each mission framework allows for increased coordination across responders, including coordinated use and maintenance.

Incident Specific Annexes
The Incident Annexes to the FIOP address specific contingency or hazard situations or an element of an incident requiring specialized application of the general response concept of operations. They describe coordinating structures, in addition to the ESFs, that may be used to deliver core capabilities and support response missions that are unique to a specific type of incident. Incident annexes also describe specialized response teams and resources, incident-specific roles and responsibilities, other scenario-specific considerations and an execution schedule to guide the employment and deployment of assets. Incident Annexes currently under development include:

- Oil and Chemical Incident;
- Nuclear/Radiological Incident;
- Biological Incident;
- Food and Agriculture Incident;
- Mass Evacuation Incident; and
- Power Outage Incident.

Power Outage Incident Annex
FEMA is developing a new Power Outage Incident Annex to the Response and Recovery FIOPs, which will address the response and recovery to a mass or long-term power outage regardless of cause, but including the impacts of a cyber incident.

This annex is nearing completion of an operational draft in partnership with the Department of Energy, recognizing their role as the ESF #12 lead agency and as the Energy Sector Specific Agency (SSA), and with the Sector Coordinating Councils (SCCs) for critical infrastructure. This annex will address a serious threat: a significant disruption to our nation's energy grid–whether caused by a natural disaster, cyber or manmade event. FEMA expects that this incident annex will also be a valuable tool for other threats that may impact our energy infrastructure, such as significant space weather. We anticipate this annex will be released later this year.

In the coming years FEMA will expand this national planning effort to include joint federal-state plans conducted at our FEMA Regions to increase fidelity into our plans and expand our partnership to local and regional power providers.

FEMA will maintain the final versions of the annex via FEMA's interagency consequence management system and intranet websites, and will notify Congress and other key stakeholders (including the public and private sectors) when they are completed.

While we plan at the federal level, we are also developing tools to support planning across the whole community. FEMA is currently leading the development of cybersecurity resource typing definitions and job title position qualifications in collaboration with DHS' National Protection and Programs Directorate (NPPD), specifically the National Cybersecurity and Communications Integration Center (NCCIC). This will establish a common language for defining the capabilities of resources used to respond to cyber incidents via the NIMS. Also, FEMA will partner with relevant cyber subject matter experts across the federal government to support eligible jurisdictions on improving cybersecurity planning and increasing their ability to maintain cyber-dependent essential functions following a catastrophic event.

National Level Exercise (NLE) 2012

Many of the efforts I have previously described build on the lessons learned from our exercise program. NLE 2012 directly examined the nation's ability to coordinate and implement prevention, preparedness, response, and recovery plans and capabilities pertaining to a series of significant cyber events. The scenario of this major exercise was based on a nation state which sought to disrupt Critical Infrastructure and Key Resources, logistics systems, and communications capabilities of U.S. federal agencies as a way to erode the public's trust in its security and safety, and cause impacts to the U.S. economy. This scenario emphasized the shared responsibility among all levels of government, the private sector, and the international community to secure cyber networks and coordinate response and recovery actions. The exercise tested our national response plans and procedures, including the NRF.

The exercise:

- Evaluated government (federal, state, local, tribal, territorial, and international) roles and responsibilities in coordinating national cyber response efforts and their nexus with physical response efforts, including allocation of resources;
- Examined the ability to share information across all levels of government and with the private sector as well as the general public, to create and maintain cyber incident situational awareness, and coordinate response and recovery efforts; and
- Assessed key decision points and decision making in a significant cyber event.

As described in FEMA's NLE 2012 Quick Look Report, this exercise demonstrated the critical importance of coordinating national and international response efforts as well as integrating the private sector into decision-making. We continue to use lessons learned out of this and other exercises as we update and validate our response plans.

Conclusion

Our nation will continue to face significant and increasing malicious cyber activity. FEMA, working alongside our federal interagency partners, the public and private sectors, and other critical stakeholders, continues to lean forward to be able to respond to and recover from these ever growing and sophisticated threats.

Responding to events like these is a shared responsibility nationwide, including the federal government, states, local communities, businesses and individual families themselves. That is why we have partnered with communities across the nation to provide vital resources to make sure Americans know how to prepare for the potential physical consequences of a cyber incident like a major power failure—building understanding of what steps to take before, during, and after such an event.

As outlined in my testimony today, we remain steadfast and earnestly committed in our efforts to continue building robust planning capabilities and partnerships that strengthen our resilience to these types of incidents.

Chairman Barletta, and members of this subcommittee, thank you again for the opportunity to appear before you today to discuss FEMA's efforts in managing the physical consequences resulting from cyber incidents.

I look forward to your questions.