MANAGING A CYBER ATTACK ON CRITICAL INFRASTRUCTURE:

CHALLENGES OF FEDERAL, STATE, LOCAL, AND PRIVATE SECTOR COLLABORATION

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

INSA TABLETOP EXERCISE AFTER-ACTION REPORT

August 2018

INSA

CONTENTS

01 GLOSSARY

01 EXECUTIVE SUMMARY

03 INTRODUCTION

04 LEADERSHIP AND COORDINATION OF EFFORT

06 RESOURCES NEEDED TO RESPOND TO AND MITIGATE A CYBER ATTACK

- 06 1. Personnel to match key elements of preparedness plans
- 07 2. Government personnel with waiver authorities
- 07 3. Prepositioned equipment

08 ACTIONS TO RESPOND TO AND MITIGATE A CYBER ATTACK

- 09 1. Understand the attack
- 10 2. Contain the Attack
- 10 3. Communicate and Coordinate Additional Steps
- 11 4. Restore Services
- 12 5. Capture Lessons Learned to Improve Future Response Capability

12 THE IMPORTANCE OF SHARING INFORMATION AMONG INCIDENT RESPONDERS

- 13 1. Quickly establish communications between all relevant actors
- 13 2. Identify information sharing venues prior to a crisis
- 13 3. Identify all actors' information requirements
- 14 4. Create a mechanism for sharing intelligence information
- 14 5. Create incentives to share information
- 14 6. Establish redundant communications

15 PUBLIC COMMUNICATIONS

- 15 1. Use communications to maintain public confidence
- 16 2. Centralize public communications
- 16 3. Make use of existing electronic communications tools

17 ADVANCE PREPARATIONS: THE IMPORTANCE OF PLANNING AND EXERCISING

- 18 1. Develop cross-jurisdictional public-private plans for coordinating during a crisis
- 18 2. Identify and harden critical assets, infrastructure, and networks that are needed to continue operation during an incident
- 19 3. Pre-position critical equipment at critical sites
- 19 4. Develop plans for prioritizing restoration of services
- 20 5. Exercise plans to restore services

21 CONCLUSIONS

22 RECOMMENDATIONS

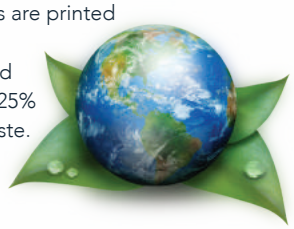
24 APPENDIX A – Information Provided to Exercise Participants

27 APPENDIX B – Participating Organizations

29 ACKNOWLEDGEMENTS

INSA SUPPORTS A HEALTHY PLANET

INSA White Papers are printed on recycled paper that is 50% recycled content including 25% post consumer waste.



GLOSSARY

CRISP	Cybersecurity Risk Information Sharing Program
CTIIC	Cyber Threat Intelligence Integration Center
COOP	Continuity of Operations Plan
DHS	Department of Homeland Security
DoD	Department of Defense
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
INSA	Intelligence & National Security Alliance
ISAC	Information Sharing and Analysis Centers
MOA / MOU	Memorandum of Agreement / Memorandum of Understanding
NCICC	National Cybersecurity and Communications Integration Center (DHS)
NCIRP	National Cyber Incident Response Plan
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
ODNI	Office of the Director of National Intelligence
PPD	Presidential Policy Directive
SCC	Sector Coordinating Council
SLFC	State and Local Fusion Center
TTX	Tabletop Exercise
UIC	Unified Incident Commander

EXECUTIVE SUMMARY

On November 8, 2017, the Domestic Security Council and the Cyber Council of the Intelligence and National Security Alliance (INSA) organized a tabletop exercise (TTX) to examine the effectiveness of mechanisms to respond to and recover from a cyber attack on critical infrastructure. The TTX was intended to generate lessons and recommendations for improving responses to cyber attacks that affect multiple critical infrastructures, with an emphasis on the energy and transportation sectors.

In the scenario for this exercise, power companies in the Baltimore, Maryland region suffered a cyber attack that took much of the power grid offline, with cascading impacts on regional transportation infrastructure (roads and rail, as well as the Baltimore airport and seaport).[1] Five teams, consisting of cybersecurity, energy, transportation, and communications experts, as well as government professionals, were presented with three moves (an initial crisis scenario and two changes in the situation) and were asked to recommend courses of action to the Secretary of Homeland Security and to state-level government officials. The exercise's three moves were structured around selected phases in the National Institute of Standards and Technology (NIST) Cybersecurity Framework: Detect, Respond, and Recover.[2]

[1] *Background provided to all TTX participants is included at Appendix A.*

[2] *National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018. At https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.*

Participants in the TTX included professionals from federal and state government agencies, infrastructure operators, industry experts in cybersecurity and infrastructure protection, and non-profit institutions.[3] The TTX was conducted at ICF International's Executive Conference Center in Fairfax, VA. A brief recap of the event's preliminary findings and recommendations is available on INSA's website.[4]

Extensive reliance on integrated information and computer systems makes the nation's critical infrastructures vulnerable to cyber attacks from a wide range of actors with broad implications for public safety, commerce and national security. Critical infrastructures are linked intrinsically; a cyber incident affecting one infrastructure would simultaneously affect other infrastructures. The TTX made evident the interdependence of energy and transportation infrastructures. In addition, a local event (e.g., affecting a major metropolitan area) could have important implications for other regions, and for the nation. The interdependence of energy and transportation infrastructures is likely to grow as technology in both infrastructures become "smarter" and are managed in common by complex IT systems.

The scenario attempted to reflect a complex international and national environment, one in which a myriad of adversaries might attempt one or more computer network attacks against local, regional or national infrastructures. As a result, decision makers and operators must learn to regard the cyberspace on which our critical infrastructure depends as a contested environment in which adversaries willfully seek to cause damage to U.S. networks and adapt to our efforts to deal with them.

The TTX also demonstrated that effective communication – using communication channels and mechanisms defined and tested prior to a cyber emergency – and coordination among numerous stakeholders at various levels of government and the private sector are important to mitigating the effects of and recovering from a cyber attack.

While the TTX scenario was challenging – posing a dynamic situation, myriad effects and uncertain attribution – it was also clear that stakeholders were already well prepared; many participants knew with whom they needed to coordinate, how to assess the situation, and what actions to take.

Several recommendations follow from observations and analysis of the TTX:

- While many organizations play an important role in mitigation and recovery, lack of clear operational authority can hamper the collective effectiveness of these organizations. In cases of emergency, consideration should be given to the appointment of a Unified Incident Commander (UIC) by a state's Governor.
- Consideration should be given to clarifying safe harbor provisions – rules that indemnify organizations from liability for actions taken in emergency situations -- which would empower local and regional responders to take effective action.
- The regulatory authorities and policy guidelines pertinent to cyber emergencies are complex and relatively new. Consequently, they should be exercised regularly by the Department of Homeland Security (DHS), state and local officials, and their private sector partners. Multi-sector and inter-jurisdictional exercises should explore the real-world applicability of policy guidance contained in relevant Executive Orders and Presidential Policy Directives, and test the mechanisms for coordinating incident response and recovery among all relevant stakeholders.
- The challenges of information sharing remain significant. Information Sharing and Analysis Centers (ISACs) for every critical infrastructure sector should clarify and standardize the ways in which they can facilitate information sharing among the public and private sectors. In addition, more work appears necessary to facilitate information sharing between the government generally – and the Homeland Security and Intelligence Communities specifically – and the nation's critical infrastructure sectors.

[3] *A list of organizations represented by participants is provided in Appendix B.*

[4] *The TTX event recap is available online at https://www.insaonline.org/wp-content/uploads/2017/12/INSA-Tabletop-Exercise-8Nov2017-Event-Recap.pdf.*

- Monitoring across all infrastructure sectors should continue to be improved, both to detect cyber vulnerabilities and to provide effective situational awareness during a cyber emergency. For example, the Department of Energy, working in concert with the private sector, has developed the CRISP program which may prove a useful model for other infrastructure sectors.[5]
- The observations, findings, and recommendations generated by this exercise are offered to strengthen the resilience of the nation's critical infrastructures and promote greater public-private collaboration on incident response and recovery. Additional work must be undertaken to identify and develop solutions to specific shortcomings in policies, procedures, and response mechanisms.

INTRODUCTION

Extensive reliance on computer networks and information systems makes the nation's critical infrastructure especially vulnerable to cyber attacks from foreign states, non-state actors, and criminal elements. Essential services across a variety of sectors – including energy, transportation, and communications – are all vulnerable to attacks, with wide-ranging ramifications for public safety, commerce, and national security.[6]

While most organizations have some level of cyber defense in place to repel or mitigate such attacks, the next step forward in cyber defense is ensuring coordinated responses to cyber attacks by all actors who could be affected – e.g., government agencies at the federal, state and local levels, as well as privately owned infrastructure operators. Only by working together closely can these public and private sector organizations contain and mitigate cyber attacks and restore critical services.

On November 8, 2017, INSA's Domestic Security Council and Cyber Council hosted an exercise to evaluate these stakeholders' responses to a cyber attack. The scenario was designed to:

- Assess cooperation and information sharing among intelligence agencies, law enforcement, and the private sector;
- Identify gaps in incident response planning, authorities, knowledge, and processes;
- Identify obstacles to prompt restoration of critical services after a cyber attack; and
- Provide insights on how government and private industry can better work together to counter future cyber threats.

[5] *According to the Department of Energy (DOE): "The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership, co-funded by DOE and industry and managed by the Electricity Information Sharing and Analysis Center (E-ISAC). The purpose of CRISP is to collaborate with energy sector partners to facilitate the timely bi-directional sharing of unclassified and classified threat information and to develop situational awareness tools that enhance the sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources."*

[6] *We expect the dependence of critical infrastructure on complex information technology systems will continue to grow, as will the interconnection between and interdependence among infrastructures as the resources that comprise them become "smarter."*

The exercise included more than 70 participants from federal and state agencies, cybersecurity companies, the energy and transportation sectors, and crisis communications firms. Divided into five teams, participants worked through a scenario simulating a cyber attack on the Baltimore power grid that had cascading effects on the regional transportation infrastructure. In the exercise's three moves, stakeholders detected, responded to, and recovered from the cyber attack; these moves were structured around phases in the NIST Cybersecurity Framework.

Exercise participants identified several core issues that, as they worked through the crisis scenario, proved critical to address: (1) the importance of clear leadership; (2) the need for an effective, rapidly applicable methodology to contain the attack; (3) the value of disseminating information to direct response efforts; and (4) the importance of multi-sector communication in coordinating efforts and smoothing response processes.

Preparation for the TTX included an examination of relevant issues at an INSA panel discussion on Cyber Threats to Critical Infrastructure that took place on October 4, 2017 – roughly one month before the exercise. Speakers included representatives from the U.S. Department of Energy; the Maryland Governor's Office of Homeland Security; the Virginia Office of Public Safety and Homeland Security; the National Academies of Sciences, Engineering, and Medicine; and ICF International. A summary of this discussion is available on INSA's web site.[7]

LEADERSHIP AND COORDINATION OF EFFORT

The TTX illustrated that effective response can be hampered by a lack of understanding at the federal, state, local levels of government, as well as and in each infrastructure sector regarding the responsibilities that must be fulfilled, and who is accountable for fulfilling – or not fulfilling – those responsibilities. Throughout the exercise, all teams of participants repeatedly asked questions regarding who is in charge (e.g., what are the roles of the federal government and state governments in responding to a crisis? Who leads, and who plays supporting roles? Do all entities responding to the crisis have a shared understanding of roles, responsibilities, protocols, and authorities?)

Once a cyber attack is detected, government and industry organizations move into mitigation and response phases, during which clear, effective leadership becomes increasingly important. Several themes emerged from the TTX team discussions. While these themes do not necessarily guide this report's recommendations, it is important to acknowledge their prevalence among TTX participants.

[7] *A summary of the panel discussion is available at https://www.insaonline.org/cyber-threats-to-critical-infrastructure-recap/. The panel discussion agenda and speaker list are online at https://www.insaonline.org/event/cyber-threats-panel-oct-4-2017/.*

1. ***Roles of state and federal government agencies must be deconflicted and clearly defined.*** During the response phase, players expressed confusion about whether the state or the federal government was in charge (i.e., should the federal government lead with state support, or should the state lead with federal support?). State officials, not surprisingly, tended to believe the state government should be in charge. Power companies did as well, since state regulation of this industry creates close ties between energy companies and their state government counterparts. Conversely, some participants advocated for federal government agencies, like the DHS National Cybersecurity and Communications Integration Center (NCICC), Federal Emergency Management Agency (FEMA), or Federal Bureau of Investigation (FBI) to take control early in the response. Beyond issues of capabilities and effectiveness, participants noted a lack of legal clarity regarding state and federal agencies' jurisdictions to intercede in the crisis.

2. ***If state officials lead response efforts, federal government assistance should only be deployed if the state requests it.*** Some participants supported the view that the federal government should only play a supporting role – particularly if state officials do not ask it to engage actively. The National Security Council, these participants suggested, should convene a senior-level meeting to direct prioritization of federal response efforts and stand by to declare a power grid security emergency through the Department of Energy.[8] However, these participants argued, the federal government should only provide assistance if it is requested by state officials.

3. ***Attribution of the attack could influence who is in charge.*** Difficulty in determining attribution for the attack yielded some confusion regarding who should be in charge. Some argued that FEMA should lead the response until the attacker had been identified. If the attack was determined to have originated from a foreign state, some argued that it would be Department of Defense's (DoD) responsibility to assume leadership for the response, even though mounting an overseas response (e.g., retaliation against the attacker) would involve different legal authorities, capabilities, and resources than undertaking a domestic response (e.g., working with civil authorities on recovery and service restoration). Moreover, DoD Homeland Defense authorities typically place DoD in a supporting role to civil officials, so the Department probably would not lead a domestic response/recovery effort.

   Second, some argued, the recovery operation should not depend on whether the attacker was a nation-state, a foreign non-state actor, or a domestic hacker. Others noted that responsibility for response and recovery domestically should not change based on attribution, as it could take quite a long time to identify an attacker, and switching lead agencies mid-course could disrupt the recovery effort.

4. ***Effective incident responses need a Unified Incident Commander.*** A common concern for participants was the lack of a centralized leadership hub. Many participants supported the designation of a UIC who could direct response and recovery efforts and provide a clear understanding of where federal, state, and local level agencies as well as affected infrastructures should direct their efforts. Whether the incident commander is a state or federal official, and what agency provides the person to serve in this role, first requires a decision regarding whether the federal or state government is the lead authority. In any case, this UIC should be prepared to operate in a manner consistent with the National Cyber Incident Response Plan (NCIRP).[9]

   One complication in developing an effective UIC is establishing the metaphorical meeting table: At whose facility should response leaders meet and from where should operations be coordinated? Who should be invited? Who should not be invited but nevertheless be involved in some of the decisions? Ideally, such determinations would be made in advance of a crisis so debates over participation do not delay response and recovery efforts.

[8] *The Federal Power Act, as amended by the Fixing America's Surface Transportation Act (FAST Act), authorizes the Secretary of Energy to order emergency measures, following a presidential declaration of a grid security emergency, to protect or restore the reliability of critical electric infrastructure or defense critical electric infrastructure during the emergency. See 16 USC 824o-1 and 16 USC 824a(c).*

[9] *See U.S. Department of Homeland Security (DHS), National Cyber Incident Response Plan, December 2016. At https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.*

5. *Politics could affect incident response.* Exercise participants noted the potential for politics to complicate decisions regarding leadership and collaboration among government entities from different jurisdictions. They noted that a Governor from one party might be reluctant to request federal assistance from – or even cooperate with – a President of the opposite party during an election season (e.g., a Governor wants to appear self-sufficient and avoid appearing indebted to an official from the other party; a Governor requests federal assistance, only to find that a President who advocates smaller government provides little or no federal resources). While it is impossible to predict the exact impact of political dynamics, cyber attack response plans should anticipate that political dynamics will complicate and delay federal government decisions on whether and to what extent assistance should be provided.

RESOURCES NEEDED TO RESPOND TO AND MITIGATE A CYBER ATTACK

The most critical resources for responding to a cyber attack are human resources. Organizations in both government and industry need personnel with the skills to identify and mitigate the attack, execute legal authorities, restore critical services, and communicate with counterparts and with the public. In many cases, the skills required to recover from a cyber attack are like those employed during the recovery effort from a natural disaster: both situations require public-private coordination, interpretation of legal authorities, and communication with key partners and audiences. While human resources are most critical, those personnel will nonetheless require the equipment necessary to implement response and recovery activities.

1. PERSONNEL TO MATCH KEY ELEMENTS OF PREPAREDNESS PLANS.

Organizations must ensure they can gather the skilled teams needed to execute an emergency response plan even in the midst of a crisis situation. The skills needed to execute cybersecurity functions, such as attribution, malware isolation, and network restoration, are likely to reside in the organizations' IT or security staffs. However, it may be necessary to identify outside experts, such as cyber threat analysis specialists, who can be summoned on short notice.

What may be more challenging in a crisis situation is bringing in competencies that are not typically exercised in the course of normal (non-emergency) business, such as understanding applicable legal authorities and limitations, coordinating ad-hoc activities with government and industry partners, and negotiating with regulators and government entities regarding issues that do not generally arise in normal business operations. The personnel who may play these roles in a crisis are likely to work in an organization's offices of general counsel, privacy, civil rights and civil liberties, policy, government affairs and, to some extent, core operational functions. To ensure that such officials can contribute in a crisis, they should be engaged in all planning activities and develop networks of contacts on whom they can call in the wake of a cyber attack.

2. GOVERNMENT PERSONNEL WITH WAIVER AUTHORITIES

Public sector organizations may need to provide (or at least identify) officials who are empowered to execute certain authorities or waive certain requirements that constrain infrastructure operators under normal conditions. For example, if a memorandum of agreement (MOA) is in place that permits officials from different jurisdictions to assist each other, the official(s) who can invoke such an agreement must be integrated into the crisis response. Similarly, if a water utility is prohibited from discharging untreated wastewater except under certain conditions, the officials who can attest to the existence of those conditions must be available to engage on short notice if a cyber attack incapacitates the utility's water treatment capability.

3. PREPOSITIONED EQUIPMENT

Pre-positioned critical equipment and supplies can enable critical facilities (such as hospitals, gas stations, etc.) to resume operations quickly. Pre-positioned materiel should include equipment needed to restore communications (e.g., radios, cell phones) and power (e.g. backup generators, transformers, fuel, batteries, and renewable energy-generating equipment such as solar chargers). These items can be pre-deployed to the facilities most likely to need them in a crisis, such as electric power sub-stations or regional train depots, or they can be distributed throughout a service area. If critical equipment and supplies are pre-positioned, local first responders will be better positioned to restore essential services quickly, safeguard public health and safety, and boost public confidence that recovery efforts are underway.

> Organizations must develop and test a thorough response mechanism, capture it in writing, and practice it regularly.

ACTIONS TO RESPOND TO AND MITIGATE A CYBER ATTACK

Any large organization – especially one with access to sensitive, privileged, or valuable information – should not expect to be immune from cyber attacks. Every organization's policy and planning processes must address ways to mitigate and respond to cyber attacks.

Organizations must develop and test a thorough response mechanism, capture it in writing, and practice it regularly. Development of a formalized response plan should involve a broad group of relevant offices and individuals beyond traditional IT and security, such as teams and individuals with roles in business operations. Such a group should be able to identify dependencies and systemic weaknesses and plan responses that mitigate effects and maintain critical functions. The same group will also create awareness and knowledge of the plan within the organization, thereby increasing its usefulness during a cyber attack.

During the tabletop exercise, the teams identified several guiding principles to frame response planning. Stated concisely, the principles of response may be summarized as:

- Understand the attack
- Contain the impact
- Communicate and coordinate additional steps
- Restore services
- Capture lessons learned to improve future response capability

1. UNDERSTAND THE ATTACK

A. ***An effective response relies on understanding the attack as quickly as possible and avoiding knee-jerk decisions based on narrow considerations or incomplete information.*** Mapping essential functions, and socializing plans that account for those functions ahead of a crisis, will make it easier to apply the 'do-no-harm' principle during an attack.

The group identified several questions that leaders should ask when determining the nature of an attack and, as a result, the nature of an effective response:

- Have we seen similar attacks before; have others?
- Does this attack demonstrate known or previously attributed tactics, techniques, and procedures?
- Is this a single strike? Should we expect follow-up attacks regionally or nationally?
- Is this a smokescreen for a broader attack?
- Does this seem like an experimental attack aimed at testing defenses, or an attack with a specific target?
- Is this a zero-day attack?
- Does the attack have a lateral impact, either inside or outside our organization? Could the effects spread and compromise more networks?

Answering these questions – which requires research and coordination that depends on previously established planning and relationships – will inform the nature of response required.

B. ***Work to attribute responsibility for the attack.*** Taking steps to support attribution will bolster an organization's long-term risk management efforts. Restoring business functions and industrial controls will be the priority in the initial response phase, especially for industry. While attribution of the attack may not be directly relevant to initial response efforts, it remains important for understanding adversary intent and capabilities, mapping out a response, and detecting and defending against future attacks.[10]

From the government's perspective, attribution is critical. The "who" and "how" of a cyber attack will determine the government's posture, define its mitigation approaches, and identify whether there is a risk of escalation to military hostilities with a nation-state.

From private industry's perspective, attribution will be important in the longer term after the response and the restoration of services. Industry, for example, needs to know whether the attack was an act of industrial espionage or theft of intellectual property.

Preserving evidence – even during the process of isolating and removing malware – will assist in attribution and can bolster the response. If evidence is preserved and shared with the FBI during the response, the FBI may be able to identify and provide relevant tactics, techniques, and procedures that were previously effective in resolving a similar cyber attack. Cybersecurity managers should have some understanding of how to preserve data in a way that is useful to law enforcement – both as investigative leads and as potential evidence for a prosecution.[11]

[10] *Attribution and understanding adversary intent can be helpful in judging the likelihood that a cyber incident will be of a prolonged nature or is likely to be repeated, depending on an adversary's interests and operational concepts.*

[11] *Presidential Policy Directive 41 (PPD-41) outlines Federal cybersecurity incident response intelligence, operational, and law enforcement responsibilities. See The White House, Presidential Policy Directive PPD-41, "United States Cyber Incident Coordination," July 26, 2016. At https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.*

2. CONTAIN THE ATTACK

A. ***First, do no harm: Avoid making the situation worse with premature conclusions or poorly considered actions.*** In the exercise, participants emphasized that, despite the need for immediate action, the *wrong* action may play into the attacker's hands or may exacerbate the negative consequences of the attack. An initial response team with the best of intentions (i.e., to remedy the situation) but operating without deep knowledge of essential business functions may damage an organization's essential functions in pursuit of a solution. For example, taking an airport's network offline for 24 hours to isolate an attack may require inbound aircraft to divert to other airports; such diversions would significantly disrupt airline operations. As the response team considers steps to mitigate the attack, it could consider whether a more nuanced response could minimize airline disruptions – for example, by taking the network offline for a shorter period of time or by providing airlines with sufficient notice that they can augment airport customer service staffs to help affected customers.

B. ***Take speedy action to halt the spread of an attack.*** Detection of a cyber attack does not mean that the attack has ended. Although victims will want to conduct a thorough analysis to determine the full range of effects and identify all system breaches, a swift response to the attack increases the likelihood that damage can be contained and mitigated. It may be wise to disconnect affected networks from broader systems to isolate malware before it can spread further. Similarly, it may also be wise to take backup systems offline to increase the likelihood that uncontaminated backups can be used to restore services.

C. ***Reduce the number of people in the affected area and prevent people from entering it.*** Exercise participants found that response and recovery efforts were complicated by the presence of civilians in areas where power and transportation services were impacted. While teams would work to get stranded civilians out of affected areas, they were concerned that additional people would enter the area because they did not understand the scale of the crisis. For example, if commuters who were unable to take their normal train to work instead drove their cars, the roads would become jammed – thereby stranding additional people in the affected region and complicating recovery workers' ability to move around.

3. COMMUNICATE AND COORDINATE ADDITIONAL STEPS

A. ***Communicating with partners is a prerequisite for an effective and coordinated response.*** In fact, robust communication and collaboration among government and industry organizations can be the determining factor in whether a response effort is successful. Creating or connecting to a common operational picture will require advanced identification of critical dependencies and first, second and third-order effects, including beyond the immediate target sector or region. For an extensive discussion of the importance of communication during a crisis, see Section VI and VII.

> Robust communication and collaboration among government and industry organizations can be the determining factor in whether a response effort is successful.

B. *Apply relevant incident response and/or emergency management protocols – even if they are not related to cyber.* Federal, state, local, and private sector officials have developed robust protocols for natural disasters and other emergencies that address challenges like intergovernmental collaboration, public-private information sharing, and public communication. One example is the National Incident Management System, which is a playbook for consequence management and lifeline service restoration. Although these protocols were developed for non-cyber emergencies, their organizing principles can often be applied to cyber attack response.

- Many organizations have developed cyber-specific protocols based on Executive Order 13636[12] and Presidential Policy Directives (PPD) 21[13] and 41.[14] In cases of massive, widespread or strategic impact, incidents may rise to the level of national significance. In such situations, the National Cyber Incident Response Plan (NCIRP) and its associated mechanisms come into play.

- Understanding the applicable protocols for the incident at hand – and applying effective management and communications techniques that have been developed and exercised for other types of emergencies – can help facilitate an effective and timely response to a cyber attack.

C. *Know what public-private coordinating mechanisms exist and can be used by the organization.* State and Local Fusion Centers (SLFCs) and sector-specific Information Sharing and Analysis Centers (ISACs) can be used to share information and coordinate decision making by government and industry.

D. *For industry, it is also important to know in advance what safe harbors exist for information sharing.* To ensure rapid information sharing with parties who may be able to help, infrastructure operators should develop in advance a legal interpretation of what information can be shared and with whom. Asking fundamental legal questions in the middle of a crisis about what is permissible could waste valuable time and resources.

4. RESTORE SERVICES

A. *Prioritize Service Restoration:* Many exercise participants grappled with decisions about what services to reestablish first. Before a crisis, state and local officials, in coordination with infrastructure operators, should prioritize the services that need to be restored, with a focus on public health and safety and national security concerns. This plan should then be reevaluated in the context of the crisis at hand. This could entail placing certain services ahead of others – for example, getting power back to hospitals before activating road and rail infrastructure necessary for economic activity and public convenience. However, it could also involve decisions as to which regions or neighborhoods should get services first, or whether to prioritize residential areas over commercial sites – decisions that are politically sensitive and economically consequential.

Although it will be difficult to know ahead of time what essential services might be affected by a cyber attack, it is critical for state and local officials to outline the relative importance of various public services so that it will be easier to prioritize the restoration of disrupted functions. During a crisis, it is easier to adapt an existing comprehensive plan than to develop a plan from scratch.

[12] *Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," 78 C.F.R. 11739 (2013). At https://www.gsa.gov/cdnstatic/ATTCH_1_-_CyberEO-FedReg.pdf.*

[13] *The White House, Presidential Policy Directive PPD-21, "Critical Infrastructure Security and Resilience," February 12, 2013. At https://www.gsa.gov/cdnstatic/ATTCH_2_-_PPD-21.pdf.*

[14] *The White House, Presidential Policy Directive PPD-41, "United States Cyber Incident Coordination," July 26, 2016. At https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.*

B. *Begin restoring services, consistent with prioritization decisions,* in the most comprehensive manner as quickly as possible. Exercise participants proposed several ways to restore critical services, including relying upon backup systems (if they are operable and unaffected by the attack); resorting to manual operations of critical systems, such as manually opening valves and turning switches instead of relying upon computers to do so; and arranging for the delivery of critical equipment and supplies into the affected area as soon as possible.

Taking such steps requires planning. For example, personnel may need to be trained in the manual operation of equipment that has been automated for many years and they will need to practice doing so periodically. Similarly, extra equipment and supplies will need to be on hand, if not already pre-deployed to areas where they are likely to be needed in a crisis (e.g., to electric power sub-stations or regional train depots).

5. CAPTURE LESSONS LEARNED TO IMPROVE FUTURE RESPONSE CAPABILITY

A. *Use incidents as opportunities to improve security.* Although cyber incidents are unwelcome, they do highlight shortcomings and enable cybersecurity analysts to identify needed improvements. Where possible during or immediately after the restoration of services, organizations should identify opportunities to enhance the security posture of affected systems. Likewise, lessons learned can be shared among ISACs and used to inform future exercises that bring together players from government and industry.

THE IMPORTANCE OF SHARING INFORMATION AMONG INCIDENT RESPONDERS

One of the principal takeaways from the INSA tabletop exercise was the need to share information widely. Exercise participants highlighted that government and industry stakeholders needed to establish – and even incentivize the use of – mechanisms for sharing information on the attack. Role-players also made clear that affected agencies and infrastructure operators should communicate frequently and openly with each other and with the public, both to facilitate recovery and to maintain public confidence. In a potential challenge to information sharing and transparency, role-players noted that it is often difficult for affected organizations to know what information other organizations need – a compelling reason to consult widely and share thoroughly.

1. QUICKLY ESTABLISH COMMUNICATIONS BETWEEN ALL RELEVANT ACTORS

"Share early and share often" is a mantra often repeated in both government and industry, but it is essential in times of crisis. A cyber attack on critical infrastructure can have a cascading impact on multiple sectors across multiple jurisdictions, providing little time to contain and mitigate damage and prevent any follow-on attacks. It is vital to establish trusted relationships among key stakeholders before a crisis hits. And, while inevitably there will be a "fog of war" during a crisis, role-players concluded that it is essential to quickly establish and maintain communications between relevant federal, state, local, and industry actors.

2. IDENTIFY INFORMATION SHARING VENUES PRIOR TO A CRISIS.

State and local fusion centers and ISACs can play a valuable role in facilitating communications regionally and nationally and coordinating efforts to ensure a successful response and recovery effort. Fusion centers can connect state and local officials with their federal partners, while industry-specific ISACs are prepared to share information between government officials at all levels and with infrastructure operators in affected industries.

Exercise participants pointed out that several entities exist to facilitate communication among infrastructure operators within a sector, as well as between private and public sector entities. These structures include ISACs, Information Sharing and Analysis Organizations (ISAOs), the Critical Infrastructure Partnership Advisory Council (CIPAC),[15] Sector Specific Agencies (SSA), Sector Coordinating Councils (SCC) and their companion Government Coordinating Councils (GCC), the Federal Senior Leadership Council (FSLC), and the Regional Consortium Coordinating Council (RC3),[16] among others.

3. IDENTIFY ALL ACTORS' INFORMATION REQUIREMENTS

While it is important to identify essential stakeholders early in the crisis, it is equally critical to understand and respond to their varying information needs, as different actors will have different information requirements and priorities. Stakeholders should provide a list of their information needs to the UIC, whose personnel should then disseminate each stakeholder's list to all other to stakeholders.

Federal officials will largely require strategic information on the nature and consequences of the attack and the varying needs of industry. They will also seek information that will help identify the attacker, as the federal government may need to assess whether, how, and under what circumstances it should attempt to name, shame, or otherwise retaliate against a foreign state or non-state attacker. State and local officials will require information needed to keep the public safe and to mitigate the impact of the attack on the community (for example, local officials may set up cooling centers if the power is brought down on a sweltering day, or they may deploy extra traffic police if disrupted rail service sends commuters onto the roadways). Industry needs operational and tactical information necessary for the quick restoration of services and the prevention of any follow-on attacks.

In the exercise, government and industry role-players did not fully understand each other's information needs. Government representatives, for example, thought industry did not need to know certain information regarding the source of the attack, as industry would not have any role in retaliating against the attacker. However, industry representatives asserted that information on the attacker's objectives, motivations, and methods of attack could have helped them identify the scope of potentially affected systems and the possible extent of the damage.

[15] *See information at https://www.dhs.gov/critical-infrastructure-partnership-advisory-council.*

[16] *See information at https://www.dhs.gov/critical-infrastructure-sector-partnerships.*

4. CREATE A MECHANISM FOR SHARING INTELLIGENCE INFORMATION

The Intelligence Community should create a clear channel for declassifying and disseminating actionable threat information, whether classified (to be shared with appropriately cleared individuals), or which could be downgraded or, in some instances, disseminated to cleared private sector decision-makers. In the exercise, government representatives had little unclassified information, which made it difficult for intelligence and law enforcement agencies to share information with the private sector operators of affected infrastructure. Industry representatives asked government representatives to transfer more actionable intelligence from the Intelligence Community to the infrastructure operators.

Per PPD-41, the Office of the Director of National Intelligence (ODNI), through the Cyber Threat Intelligence Integration Center (CTIIC), will act as lead for intelligence support and related activities. This role includes the declassification of intelligence and/or "tear-line" reports at various classification levels. This role is crucial in allowing for the dissemination of actionable information, particularly for private sector stakeholders. In conjunction, coordinating groups like ISACs and SCCs will ensure communication between and among the various affected entities, especially regarding multi-sector, multi-jurisdictional cyber incidents.

5. CREATE INCENTIVES TO SHARE INFORMATION

Policymakers and legislators at all levels of government should consider ways to incentivize companies and government agencies to share information and coordinate in a crisis. Good will exists in a crisis; affected stakeholders desire to quickly resolve a crisis through collaborative engagement. Challenges abound, however, when it comes to information sharing between government and industry. Industry may be reluctant to share information with government partners if doing so could create risks related to legal compliance, civil liability, customer privacy, or the corporation's reputation. Government officials, for their part, may be constrained in sharing information with industry partners who may lack necessary security clearances. In some cases, government officials with little private sector experience simply may lack understanding of industry business practices and information needs. To overcome the challenges associated with sharing information, organizations that already bring together government and industry stakeholders – such as fusion centers and ISACs – could facilitate collaboration and build trust that would enable more direct cooperation.

6. ESTABLISH REDUNDANT COMMUNICATIONS

Given the potential for wide-ranging power outages in the aftermath of a cyber attack, it is also essential to stand up tested and redundant means of communication among recovery officials and infrastructure operators. Since the September 11, 2001 attacks, communications interoperability among first responders and other stakeholders, particularly across jurisdictions, has greatly improved. However, the effectiveness of these communications systems must be tested periodically to ensure that they connect the full range of emergency responders when needed.

> It is important to keep the public informed so they remain calm and safe — and so they do not take actions that complicate recovery and service restoration activities.

PUBLIC COMMUNICATIONS

The most important audience in a crisis response is the public. They are the constituents of the federal, state, and local officials who work to ensure national security, public safety, economic prosperity, and economic security; they are also the customers for the infrastructure operators who provide power, healthcare, transportation services, banking services, and other critical functions. In responding to any crisis, it is important to keep the public informed so they remain calm and safe – and so they do not take actions that complicate recovery and service restoration activities.

Government and industry officials engaged in recovery operations should keep in mind three communications principles.

1. USE COMMUNICATIONS TO MAINTAIN PUBLIC CONFIDENCE

All actors should communicate transparently and frequently to sustain public confidence. Exercise participants noted that many components of critical infrastructure – such as the banking sector – depend on public confidence in their resilience and continued long-term availability (despite short-term interruptions of service). Providing a consistent, credible voice in communicating with the public can help avoid communication overload and ensure proper focus on public health and safety, setting realistic expectations for restoration of services, and addressing what the public itself can do to assist. By maintaining timely, transparent, and frequent communications with the public, officials can convey what is being done to address the situation, identify the resources being applied, and recommend steps the public can take to facilitate the overall response (such as staying off the roads or using less water or power) while also addressing inaccurate reports that could create panic or impede the response effort.

2. CENTRALIZE PUBLIC COMMUNICATIONS

Government and industry responders should establish a process for communicating consistent messages to the public in a crisis. Care should be taken to correct information that was previously released but found to be erroneous or incomplete. Exercise role-players broadly agreed that creating a communications hub could improve the efficiency and effectiveness of information sharing by distilling the data provided by disparate entities and by supplying needed direction. In the aftermath of a highly disruptive cyber attack, it will be essential for government and industry officials to communicate consistent messages, lest they unknowingly complicate recovery efforts or create confusion among the public. Government and industry organizations may wish to stand up a public communications cell to coordinate messages and deliver them in a coordinated fashion (e.g. a daily press conference involving all critical stakeholders). Such a cell may wish to designate a single principal spokesperson who can provide a strategic overview of response and recovery operations on behalf of all affected organizations.

3. MAKE USE OF EXISTING ELECTRONIC COMMUNICATIONS TOOLS

All agencies and infrastructure operators should make use of social media and existing emergency alert systems to communicate. Regular press briefings and statements from composed public affairs officers enable thorough and nuanced messaging. At the same time, emergency response officials use emergency alert systems and social media to communicate critical updates in a timely fashion, as well as to enable two-way interactive communications. Exercise participants noted that emergency alert systems that send text messages to warn of disruptions ranging from forest fires to highway accidents can be used to disseminate information that the public needs to remain safe or to shape their behavior in ways that facilitate emergency responses. Social media platforms enable government agencies and critical service providers to disseminate information to the public as well as to receive information – such as reports of power outages – that is needed to direct response and recovery efforts. Smartphone apps can often play a similar role; regional power companies, for example, often have apps that allow their customers to report outages and see what areas of their community are experiencing service disruptions. There is no shortage of communications methods; the challenge is to use such redundant tools to disseminate consistent, coordinated, accurate, and timely information from both public and private sector stakeholders.

ADVANCE PREPARATIONS: *THE IMPORTANCE OF PLANNING AND EXERCISING*

Extensive reliance on computer networks and information systems makes the nation's critical infrastructure especially vulnerable to cyber attacks from foreign states, non-state actors, and rogue elements. Essential services across a variety of sectors – including energy, transportation, shipping, and communications – are all vulnerable to attacks, with wide-ranging ramifications for public safety, commerce, and national security.

While infrastructure operators work diligently to enhance the *resistance* of infrastructure to a cyber attack, the significant risk that operations will be disrupted at some point – whether through a successful cyber attack, a natural disaster, or simple equipment failure – means that operators must also work diligently to improve the *resiliency* of their critical operations. Pre-crisis planning must therefore include steps to repel cyber attacks and to implement comprehensive and thoroughly exercised service restoration plans.

During the tabletop exercise, participants identified several areas in which advance preparation would have strengthened responses by individual institutions and enhanced coordination among the myriad public and private sector organizations involved.

Participants recommended six steps which both government and industry entities should take to prepare and test contingency plans before a crisis hits:

- The first step – developing cross-jurisdictional public-private response plans – requires government and industry stakeholders to agree upon a joint crisis response plan.
- The remaining five steps should be undertaken by individual stakeholders – particularly critical infrastructure providers – to ensure they can both prevent cyber attacks and promptly restore operations in the wake of one. These steps include:
  - Identifying and hardening critical assets
  - Backing up data
  - Pre-positioning critical equipment
  - Prioritizing the services to be restored, and
  - Exercising crisis response plans to ensure they work.

1. DEVELOP CROSS-JURISDICTIONAL PUBLIC-PRIVATE PLANS FOR COORDINATING DURING A CRISIS

Creating response plans before a cyber incident occurs should be a high priority, not only for the federal government, but also for other public sector and private sector entities. The federal government developed two key action plans to implement strategic guidance approved at the presidential level: the National Cyber Incident Response Plan (NCIRP), developed pursuant to Presidential Policy Directive (PPD)-41, and the National Infrastructure Protection Plan (NIPP),[17] pursuant to PPD-21. The NCIRP details a strategic cyber incident plan for the United States, outlines roles and responsibilities of different organizations, identifies core capabilities, and discusses coordinating structures and integration, while the NIPP details risk mitigation and coordination efforts concerning critical infrastructure. It should be noted that both the NCIRP and NIPP are strategic, not operational, documents. They provide guidance for various organizational entities on developing an operational plan.

The NCIRP established which agency will be the lead federal agency for a given action. However, other federal agencies and private sector organizations that would be involved in a crisis response must also develop plans for coordination. (The NCIRP's Appendix F, Task 10, discusses the need for formal agreements and partnerships between governmental and private sector organizations, and between varying private sector entities.) To implement the NCIRP, government agencies and critical infrastructure operators could develop Memoranda of Understanding (MOUs) or Memoranda of Agreements (MOAs) to define in advance of a crisis each organization's roles and responsibilities. State and local planners should understand the NCIRP's provisions, whether or not the federal government leads the response to a given crisis.

2. IDENTIFY AND HARDEN CRITICAL ASSETS, INFRASTRUCTURE, AND NETWORKS THAT ARE NEEDED TO CONTINUE OPERATION DURING AN INCIDENT.

The NIPP (particularly chapters 5 and 6) also presents planning steps that can facilitate incident response. It lays out a Risk Management Framework in Chapter 5, and specific action items in Chapter 6. The NIPP recommends the development of a Risk Management Framework to identify critical assets, infrastructure, and networks that are needed to continue operation during an incident. Once identified, organizations can work to harden such assets or systems to ensure they are functional when needed. The Framework also calls for risk mitigation planning. One element of mitigating risk is to identify and prepare for threats, which could include preparing backup equipment for critical systems or isolating critical networks to allow them to continue functioning. Another element is to actively reduce vulnerabilities by, for example, making critical systems as resistant to attack or disruption as possible.

Employing a risk-based approach may help organizations assess the consequences of a cyber attack on public safety and infrastructure operations. A risk-based approach looks at the likelihood that a given system would be damaged or taken off-line by a cyber attack, the extent to which a given system would be damaged or taken off-line, and the consequence of the diminished capability or loss of that system. Mitigating such cybersecurity risks may include the design, development, and deployment of security controls in the enterprise architecture and changes to operational and maintenance processes. Using a risk management approach promotes resiliency, which includes the ability to contain the threat and restore services to a certain operational level in a timely manner.

[17] *U.S. Department of Homeland Security (DHS), National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience, December 2013. At https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.*

Best practices promote the idea of "defense in depth,"[18] the concept of implementing multiple levels of security controls that can prevent, detect, and respond to an intrusion. Security controls may manifest as physical controls (e.g., locked doors), procedure controls (e.g., incident response and contingency training), technical controls (e.g., firewalls, redundant backup systems) and policy controls (e.g., data management policies). For a critical infrastructure, participants cited the need to think holistically about what security controls to implement (e.g., technical controls may require appropriate procedures and policy controls to ensure a protected system).

3. PRE-POSITION CRITICAL EQUIPMENT AT CRITICAL SITES

As noted earlier, pre-positioning critical equipment and supplies at critical sites can enable essential services to resume operations quickly. Both government and industry organizations should develop and implement plans to deploy mission-essential equipment where it can be installed swiftly to replace affected systems.

4. DEVELOP PLANS FOR PRIORITIZING RESTORATION OF SERVICES

Organizations should develop, practice, continuously update, and convey plans for prioritizing restoration of services in preparation for potential cyber incidents which may degrade or destroy these services, systems, or critical infrastructure.

Since the September 11th attacks, many organizations have developed all-hazards continuity of operations plans (COOP); given the omnipresent threat of cyber attacks, every organization should have COOP plans which identify and prioritize key services and determine the order in which they should be brought back online. Achieving enhanced organizational resilience requires that communication channels are in place both internally and externally, service level agreements are written, and assets are well understood and managed. System restoration should be built into plans that are regularly tested, updated, and communicated.

- *Identifying Key Services:* Guidelines such as Federal Information Processing Standard (FIPS) 199[19] and 200[20] assist in identifying and categorizing a wide variety of federal information systems. A basis for categorization, such as FIPS, can help an organization understand which systems and services it should prioritize for restoration in the event of a cyber attack. Once these systems and services are identified, each organization must develop their own restoration plans as discussed in the above data back-up planning section.
- *Prioritizing Service Restoration:* When determining recovery priorities, organizational and stakeholder value must first be considered, as well as legal, regulatory, and operational requirements. In its Cybersecurity Framework 1.0 (CSF),[21] the National Institute of Standards and Technology (NIST) outlines the importance of understanding and managing assets (such as data, systems, facilities) relative to their criticality of achieving organizational mission goals.

[18] *U.S. Department of Homeland Security, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, September 2016. At https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.*

[19] *National Institute of Standards and Technology (NIST), Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards (FIPS) Publication 199, February 2004. At https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.*

[20] *National Institute of Standards and Technology (NIST), Minimum Security Requirements for Federal Information and Information Systems, Federal Information Processing Standards (FIPS) Publication 200, March 2006. At https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.*

[21] *National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014. At https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.*

5. EXERCISE PLANS TO RESTORE SERVICES

The best way to respond quickly and confidently is to plan and rehearse multi-actor responses ahead of time. Response protocols should be in place to ensure that responsible parties know when and what to communicate well in advance of a cyber attack. Good planning creates shared knowledge in many areas (e.g., stakeholder equities and tradeoffs, roles and responsibilities, taxonomies and terminology, availability of critical information) that will accelerate and improve the effectiveness of response. For minor or localized incidents, the response can be as simple as identifying an ongoing attack, triaging affected resources, and initiating the response protocol. For more severe incidents, the organization must be aware of its role within the broader operational picture: What sector-wide and government organizations must be engaged? What other sectors may be affected? What are the thresholds for elevating issues to higher external authorities? In any case, planning is critical both for identifying triggers and training users to recognize them.

Effective execution of any plan requires regular practice – particularly for contingency or backup procedures to reduce the impact of loss of operations, as ingrained manual contingency processes are key for successfully managing a crisis. Indeed, NIST's Guide for Cybersecurity Event Recovery[22] calls for plans to be tested and updated continuously.

In addition, it is also critical for an organization to monitor and test the implemented security capabilities to ensure they are still able to detect and isolate any cyber attacks.

[22] *Michael Bartock, Jeffrey Cichonski, Murugiah Souppaya, Matthew Smith, Greg Witte, and Karen Scarfone, Guide for Cybersecurity Event Recovery, NIST Special Publication 800-184, December 2016. At https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf.*

CONCLUSIONS

Four core themes are apparent when considering the experience of the exercise participants: (1) the centrality of leadership; (2) the need for an effective, rapidly applicable methodology to contain the attack; (3) the value of information to direct response efforts; and (4) the importance of communication in coordinating efforts and smoothing response processes.

Leadership, especially in the beginning of the response phase, is vital to ensuring an effective response and recovery from an attack. While participants in response and recovery efforts must have a clear understanding of their own roles and responsibilities, they must also know who is in charge. Clarifying who will lead a response effort under varying circumstances, perhaps in MOUs to which stakeholders across federal and state governments and private industry agree, will enable a smoother, more coordinated response.

> Fusion centers and ISACs are essential to sharing information and should be designated as communication channels in standard emergency response plans.

Effective mitigation begins with understanding the attack as quickly as possible to begin response efforts immediately. Likewise, determining attribution provides greater clarity for federal, state, and local governments in establishing who should take the lead in the response efforts, and to what extent other entities should engage. Mitigation should be guided by effective communication and coordination to contain the attack as quickly and thoroughly as possible. Prioritizing areas that need attention will further enable appropriate mitigation responses.

To facilitate the mitigation efforts, the right entities must be equipped with the right information at the right time. State and local fusion centers and ISACs are essential to sharing information and should be designated as communication channels in standard emergency response plans. Likewise, these organizations can help coordinate efforts with federal and private sector partners. Understanding the information needs of different actors is essential to sharing the right information with the right people and allowing mitigation efforts to progress. Sharing classified information, however, presents a significant challenge: many private firms that would be engaged in crisis response have few, if any, cleared individuals who can receive classified information from the government. Government agencies can declassify information to share with infrastructure operators; however, the declassification process may take too long to aid in the timely restoration of critical services. Nonetheless, the inability to access such information could be a stumbling block to coordinated, rapid, effective mitigation efforts, as some contributors to service restoration will lack information that others are using to guide their response.

Communication between all stakeholders is critical to coordinating response efforts, de-conflicting authorities, and maintaining public cooperation and confidence. Communication should represent a unified front and be clear, transparent, and frequent to ensure public confidence. Moreover, officials should employ all available platforms to inform the public and shape their response to the crisis.

RECOMMENDATIONS

A. LEADERSHIP

1. Define and deconflict federal and state governments' leadership roles in advance of crises. Ensure that federal and state agencies know when to engage in a crisis, agree on who has legal jurisdiction, and clarify reporting mechanisms for local authorities and the private sector.

2. Determine attribution for the attack as soon as possible to enable rapid, effective mitigation efforts and help both state and federal governments respond in appropriate manners.

3. Establish a Unified Incident Commander (UIC) to oversee a leadership, communication, and information hub. The UIC should be able to direct response efforts and gather the right agencies and organizations at the table.

B. MITIGATION: RESOURCES

1. Ensure organizations can provide all the skilled personnel necessary to carry out emergency plans during a cyber attack.

2. Grant government agencies the authority to waive certain procedural (or even regulatory) requirements to enable faster incident response. Public sector organizations may need to provide (or at least identify) officials who are empowered to execute certain authorities or waive certain requirements that constrain infrastructure operators under normal conditions.

3. Pre-position mission-essential infrastructure equipment so it is easily accessible and ready to use. Pre-positioned equipment can enable critical facilities, such as hospitals and gas stations, to resume operations quickly.

C. MITIGATION: PROCESSES

1. Understand the attack. A measured and effective response relies on understanding the attack as quickly as possible.

2. Work quickly to contain the attack. Avoid making the situation worse with premature conclusions or poorly considered courses of action.

3. Reduce the number of people present in the affected area and prevent people from entering it unnecessarily to improve the efficiency of responders.

4. Communicate with partners to ensure an effective and coordinated response. Apply relevant incident response and/or emergency management protocols – even if they are not related to cyber. Know what public-private mechanisms exist and can be used by each organization. Industry should know in advance what safe harbors exist for information sharing.

5. Prioritize the restoration of services with an emphasis on ensuring public health and safety and national security.

6. Capture lessons learned to improve security and response capability for the long term.

D. INFORMATION SHARING

1. Establish communications quickly among all relevant actors.
2. Identify information sharing mechanisms prior to a crisis. State and Local Fusion Centers and/or ISACs can be especially helpful in facilitating communication.
3. Identify all actors' information needs and information sharing requirements proactively so they can respond appropriately and improve mitigation efforts.
4. Create a mechanism for sharing intelligence information. The IC should create clear channels for disseminating both classified and unclassified information to both public and private sector partners, and a mechanism to quickly declassify actionable intelligence to share with industry in times in crises.
5. Policymakers at all levels of government should consider ways to incentivize companies and government agencies to share information, coordinate and collaborate in a crisis.
6. Establish redundant communications in case primary means fail.

E. PUBLIC COMMUNICATION

1. Use communication to maintain public confidence. Providing a consistent, credible voice can avoid communication overload, ensure proper focus on public health and safety, set realistic expectations for the restoration of services, and address what the public itself can do to assist.
2. Centralize public communications. Establish a means for communicating a consistent message to the public in crises, such as a communications hub and a primary spokesperson for the UIC.
3. Make use of existing electronic communication tools. Use multiple communication tools, especially social media and alert systems, to communicate with the public.

F. PLANNING AND EXERCISING:

1. Develop cross-jurisdictional, public-private plans for coordinating during a crisis.
2. To implement the National Cyber Incident Response Plan (NCIRP), which outlines roles and responsibilities of different organizations during a cyber incident, government agencies and critical infrastructure operators should develop MOUs or MOAs to define such roles in advance of a crisis.
3. Identify and harden critical assets, infrastructure, and networks that are needed to continue operation during an incident. Use a risk management approach to promote resiliency, contain the threat, and restore services to a certain operational level in a timely manner.
4. Develop plans for prioritizing the restoration of services to improve the timeliness of the response and ensure the optimal allocation of time, resources, and personnel.
5. Plan and rehearse multisector responses ahead of time.

APPENDIX A – *INFORMATION PROVIDED TO EXERCISE PARTICIPANTS*

BACKGROUND INFORMATION

Exercise Goals and Objectives

The Intelligence and National Security Alliance (INSA) is organizing a tabletop exercise on cyber threats to critical infrastructure, with a focus on the energy and transportation sectors and the critical dependencies that exist between the two. Key findings from the exercise will inform the development of an INSA white paper that will identify threats and vulnerabilities, assess relevant policies and crisis response procedures, and recommend steps that would help strengthen partnerships and infrastructure resiliency.

The exercise is intended to address at least a subset of the following:

- Explore the intersection of intelligence, law enforcement, and private sector information sharing and the intersection of cyber and physical threats as they affect US critical infrastructure.
- Identify shortfalls in authorities between federal, state, local and industry elements involved in responding to cyber attacks on critical infrastructure.
- Identify processes, procedures, roles, responsibilities and red lines for coordination between government and industry in responding to a cascading event that crosses two critical infrastructure sectors.
- Identify how threat information is shared between critical infrastructure sectors when the result of a cyber event could have a cascading impact.
- Establish insight into how government and industry can work together to build resiliency and "harden" US critical infrastructure against future attacks.

INSA's mission is to promote public-private collaboration on national security challenges; this exercise has been developed by two of INSA's policy councils, which focus on cybersecurity and domestic security, respectively.

Exercise Overview and Orientation

On November 8, 2017, the Intelligence and National Security Alliance (INSA) will conduct a tabletop exercise (TTX) to examine the challenges of ensuring effective public-private collaboration across multiple levels of government and multiple infrastructure sectors during a cyber attack. The TTX will encompass three of the five NIST Cybersecurity Framework Phases (Detect, Respond, and Recover). Five teams will be convened simultaneously to role-play a crisis scenario during these phases.

In the scenario being simulated, the United States is experiencing a cyber attack that affects the power grid in the Baltimore area and has cascading impacts on the regional transportation infrastructure. Your team will take on the role of experienced experts with background in cyber, energy, transportation, government, and communications assembled to advise the Secretary of Homeland Security and, through the Secretary, the White House. You can also anticipate that your advice will be communicated to Cabinet Departments, including the Departments of Homeland Security, Justice, Energy and Transportation and, through DHS, to infrastructure owners and operators, industry officials, and officials in state and local governments.

Each team member will play the role of a certain stakeholder with a role to play in a cyber crisis (e.g., federal government, state government, energy utility, transportation operator, etc.) Each team member should attempt to represent the views, perspectives, and interests of the organizations they personify. Key issues to consider include:

- What are my organizations' core interests (e.g., containing the cyber attack, public safety, service restoration)?
- What do I need to do to advance these core interests (e.g., attribute the source of the attack, enlist government public safety agencies, secure prompt access to power, prioritize customers to receive restored power, etc.)?

- What information would my organizations possess, need, disseminate, or withhold?
- With what other actors – public or private – would my organizations need to collaborate? What forms would such collaboration take (e.g., information sharing, operational coordination, etc.)?
- What information and actions would my organizations offer, and what would they demand from others?
- What do non-represented stakeholders – e.g., the American public, the media, other energy consumers – need from my organization?

At the end of the exercise, your team will provide insights into the dynamics that both inhibited and facilitated the effective mitigation of the attack and restoration of critical services. You may offer recommendations to improve processes, transparency, reporting, or other dynamics that you identify during your deliberations. You should approach your 10 - 15 minute briefing as if you are informing senior DHS officials who will share your insights with stakeholders in industry and at all levels of government to improve the processes for responding to future cyber incidents.

Scenario Structure

At the beginning of each move of the exercise, you will be provided fictional information regarding a major cyber incident affecting critical infrastructure in the United States. The attacks notionally take place in November 2017 as the United States heads into the holiday and New Year's season. The scenario presents a fictional account of security and political developments, along with fictional public reporting surrounding the cyber incident. You are to consider as facts the following pages for formulating your response.

The move is divided into three moves structured around three key stages in the NIST Cybersecurity Framework:

1. Move 1 will focus on ***detecting*** the threat – understanding attack targets and methods, correlating data from multiple sources, and assessing the impact of events. This move will last 45 minutes.
2. Move 2 will focus on ***responding to*** the cyber attack – promoting public-private collaboration, including sharing information and coordinating actions with key stakeholders, to contain and mitigate the cyber attack. This move will last 45 minutes.
3. Move 3 will focus on ***recovering from*** the attack – restoring key services and communicating recovery activities to critical stakeholders. This move will last 90 minutes.

Role-Playing Tips

- **Don't fight the scenario.** Assume all scenario information presented is possible, observed, or reported as written. Use your energy to explore the implications of that information, not the plausibility.
- **Play a broad role.** Your team may only have two players representing a range of stakeholders, such as "federal government agencies." If so, consider how you might convey the interests, perspectives, and knowledge of all relevant stakeholders. For "federal government agencies," this might include intelligence agencies, law enforcement agencies, industry oversight agencies (such as the Departments of Energy and Transportation), and other organizations that might plausibly be involved in the scenario.
- **Think multi-dimensionally.** When analyzing the scenario, remember to consider implications for other organizations and domains (e.g. private sector, military, law enforcement, diplomatic, etc.) and incorporate these insights along with cybersecurity.
- **Be creative.** Cyber policy and operations are an evolving discourse, and there is no single correct response option to the scenario information provided. There are many ideas to consider in responding to the crisis.
- **Analyze the issues.** The goal of the TTX is for us to grapple with complex issues and weigh the strengths and weaknesses of sometimes conflicting interests. Priority should be given to analysis of the issues and not to listing all possible issues or solutions.

Schedule

After a short overview of the scenario, participants will break into five multi-disciplinary teams and disperse to breakout rooms. After three short moves, teams will compile their findings during a working lunch and then brief their insights to all participants.

The day will proceed as follows:

8:15 – 9:00 AM	REGISTRATION AND BREAKFAST
9:00 – 9:20 AM	WELCOME REMARKS / FORM TEAMS
9:20 – 9:30 AM	Break / Move to Team Rooms
9:30 – 10:15 AM	MOVE 1 – DETECT
10:15 – 11:00 AM	MOVE 2 – RESPOND
11:00 – 11:15 AM	Break / Refreshments
11:15 AM – 12:45 PM	MOVE 3 – RECOVER
12:45 – 1:00 PM	Break / Pick Up Lunch
1:00 – 2:00 PM	WORKING LUNCH / TEAMS COMPILE FINDINGS AND PREPARE OUTBRIEFS
2:00 – 2:15 PM	Break / Refreshments / Move to Auditorium
2:15 – 3:15 PM	TEAMS BRIEF FINDINGS AND RECOMMENDATIONS (10 - 12 minutes each)
3:15 – 4:00 PM	DISCUSSION – THEMES AND LESSONS LEARNED
4:00 PM	Exercise Ends

BACKGROUND FOR SCENARIO – DHS GUIDANCE

DATE: 20 November 2017 0715

FROM: Chief of Staff to the Secretary of Homeland Security

SUBJECT: Cyber Attack Against Critical Infrastructure

A major cyber incident is occurring that could affect US national security and public safety. The Department of Homeland Security is contacting your team to identify responses to the unfolding situation. While we cannot share classified information with you via this channel, please be advised that we have received from several managed security service providers corroborating information that a cyber attack is underway affecting critical infrastructures.

Given the unprecedented nature of this incident, the Secretary of Homeland Security is asking that your team – representing major stakeholders in government and industry – develop responses that mitigate the cyber attack and restore services. At the end of the crisis, the Secretary asks that you brief her on the dynamics that facilitated and hindered effective collaborative responses.

As we respond to and manage this crisis, the Secretary requests that you consider the following potentially conflicting interests. These are provided as suggested starting points and are not meant to limit your policy responses.

- **Attribution vs. Mitigation.** How important is it to attribute the actors and motivations behind the attack? Is attribution necessary to mitigate the damage and restore services?
- **Government Response vs. Private Sector Response.** What actions taken in response to the reports and incidents should be led by the private sector and what actions should be under the government's leadership?
- **Information vs. Action.** How much information is needed before public safety and critical services can be restored?

APPENDIX B – PARTICIPATING ORGANIZATIONS

PANEL DISCUSSION

The following organizations provided speakers for the October 4, 2017, panel discussion on cyber threats to critical infrastructure:

- ICF International
- Maryland Governor's Office of Homeland Security
- Office of Public Safety and Homeland Security, Commonwealth of Virginia
- Transportation Research Board, The National Academies of Sciences, Engineering, and Medicine
- U.S. Department of Energy

TABLETOP EXERCISE

The following organizations sent representatives to participate in the November 8, 2017 tabletop exercise as facilitators, participants, or observers:

TTX Facilitators

- ICF International
- The MITRE Corporation
- Parsons
- RAND Corporation
- Shulman Rogers
- Thomson Reuters

TTX Participants – Public Sector (Federal)

- Amtrak
- Federal Bureau of Investigation (FBI)
- National Maritime Intelligence-Integration Office
- Office of the Director of National Intelligence, National Counterintelligence and Security Center (ODNI/NCSC)
- Transportation Security Administration (TSA)
- U.S. Department of Defense, Office of Command, Control, and Communication (C3), Cyber, and Business Systems (OSD/C3CB)
- U.S. Department of Defense, Office of the Deputy Assistant Secretary for Energy, Installation & Environment
- U.S. Department of Energy (DOE)
- U.S. Department of Homeland Security, Office of Intelligence and Analysis (DHS/I&A)
- U.S. Navy, Naval Network Warfare Command

TTX Participants – Public Sector (State and Local)

- Kansas Intelligence Fusion Center
- Maryland Coordination and Analysis Center (MCAC)
- Maryland Department of Transportation
- Maryland Governor Larry Hogan's Office
- Maryland State Police
- Maryland Transit Administration
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Northern Virginia Regional Intelligence Center
- Virginia Fusion Center
- Washington Metropolitan Area Transit Authority (WMATA)

TTX Participants – Private Sector

- American Gas Association
- ArcBest Technologies
- Deloitte
- Edison Electric Institute
- Goldman Sachs
- ICF International
- Institute of Transport Engineers
- Iron Net Cybersecurity
- Johns Hopkins University Applied Physics Lab
- Lockheed Martin
- Mission Secure Inc.
- Morigi Strategies
- National Emergency Number Association
- New America
- Northern Virginia Electric Cooperative (NOVEC)
- PulsePoint Group (an ICF subsidiary)
- Raytheon
- Security Awareness Lab
- Skadden, Arps, Slate, Meagher & Flom LLP
- Smart City Works
- Transportation Research Board
- Vencore (now Perspecta)

TTX Observers

- Federal Bureau of Investigation, Baltimore Field Office
- Federal Bureau of Investigation, Office of Private Sector
- ICF International
- Maryland Transit Authority Police
- Office of the Director of National Intelligence, Office of Partner Engagement (ODNI/PE)
- Spadaro & Associates
- U.S. Department of Homeland Security, Office of Intelligence and Analysis (DHS/I&A)
- Vencore (now Perspecta)

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff members who contributed their time, expertise, and resources to develop the TTX scenario, contributed to the exercise's implementation, prepared the October panel discussion, and wrote this report:

INSA MEMBERS

Dawn Scalici, Thomson Reuters;
Chair, INSA Domestic Security Council

Mark Rosenthal, MITRE;
Vice Chair, INSA Domestic Security Council

Kevin Zerrusen, Goldman Sachs;
Chair, INSA Cyber Council

Samuel Visner, *MITRE*

David Luckey, *RAND Corporation*

Marianne Meins, *Parsons*

Emily Frye, *MITRE*

Mark Maier, *Shulman Rogers*

Sean Plankey, *BP*

Tommy Gardner, *HP*

Barbara Alexander,
General Dynamics Information Technology

Dennis Hunt, *AECOM*

Todd Rosenblum, *IBM*

Christian Faust

INSA STAFF

Chuck Alsup, *President*

Suzanne Wilson Heckenberg, *Chief Operating Officer*

Larry Hanauer, *Vice President for Policy*

Ryan Pretzer, *Senior Manager, Policy and Public Relations*

Toya Cribbs, *Director, Meetings and Events*

Lauren Parker, *Membership Manager*

Alexzandra Smith, *Intern*

Amrutha Prasad, *Intern*

John Hastings, *Intern*

Kathryn Rowan, *Intern*

Nathaniel Morra, *Intern*

Colin Blowers, *Intern*

INSA also expresses its appreciation to INSA member firms, which provided facilities, support, as well as a significant amount of staff time and expertise, for the October panel discussion and the November tabletop exercise:

ICF International

Raytheon

MITRE

Spadaro & Associates

Vencore *(now Perspecta)*

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit forum for advancing intelligence and national security priorities through public-private partnerships. INSA's government and private sector members collaborate to make government more effective and efficient through the application of industry expertise and commercial best practices. INSA's 160+ member organizations are leaders in intelligence collection and analysis, data analytics, management consulting, technology development, cybersecurity, homeland security, and national security law, and its 4,000 individual and associate members include leaders, senior executives, and intelligence experts in government, industry, and academia.

ABOUT THE INSA CYBER COUNCIL

INSA's Cyber Council seeks to lead, facilitate and deliver authoritative and influential insight around national security challenges present in the cyber domain by fusing knowledge from industry, government, and academic experts. The Council works to promote a greater understanding of cyber threats, challenges, and opportunities that can be addressed effectively through public-private collaboration.

ABOUT THE INSA DOMESTIC SECURITY COUNCIL

INSA's Domestic Security Council works to identify, develop, and promote innovative solutions for the homeland intelligence enterprise. INSA established the forum (initially known as the Homeland Security Intelligence Council) in 2008 to promote understanding of the role of intelligence in the homeland enterprise, the successes it has achieved, and evolving challenges that continue to threaten our nation.

INSA

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Building a Stronger Intelligence Community

(703) 224-4672 | www.INSAonline.org