Homeland Security Advisory Council

FINAL REPORT OF THE CYBERSECURITY SUBCOMMITTEE: Part I - Incident Response

June 2016

This page is intentionally left blank.

This publication is presented on behalf of the Homeland Security Advisory Council, Cybersecurity Subcommittee, co-chaired by Steve Adegbite, Juliette Kayyem, Jeff Moss and Dr. Paul Stockton as ***Part I – Incident Response*** of the final report and recommendations to the Secretary of the Department of Homeland Security, Jeh C. Johnson.

<Signature on file>

Steve Adegbite
Chief Information Officer
E*Trade Financial Corp

<Signature on file>

Juliette Kayyem
Founder
Kayyem Solutions, LLC

<Signature on file>

Jeff Moss
Found
Black Hat and DEF CON Conferences

<Signature on file>

Dr. Paul Stockton
Managing Director
Sonecon LLC

This page is intentionally left blank.

CYBERSECURITY SUBCOMMITTEE MEMBERS: Incident Response Group

Steve Adegbite (Co-Chair) – Chief Information Security Officer, E*TRADE Financial Corporation; Member of Homeland Security Advisory Council
Juliette Kayyem (Co-Chair) – Founder, Kayyem Solutions, LLC; Member of Homeland Security Advisory Council
Jeff Moss (Co-Chair) – Founder of Black Hat and DEF CON Conferences; Member of Homeland Security Advisory Council
Paul Stockton (Co-Chair) – Managing Director, Sonecon LLC; Member of Homeland Security Advisory Council

Incident Response Group

Barry Bates – Executive Vice President at National Defense Industrial Association, Major General (ret)
Richard Bejtlich – Strategist at FireEye, Brookings Institution non-resident Fellow, Incident Response Author
Scott Charney – Corporate Vice President for Trustworthy Computing, Microsoft
Richard Danzig – Senior Advisor, Johns Hopkins Applied Physics Laboratory; Member of Homeland Security Advisory Council
Thomas Fanning – Chairman, President, Chief Executive Officer, Southern Company
Russ Fitzgibbons – Chief Risk Officer, The Clearing House
Carie Lemack – Cofounder and Chief Executive Officer of DreamUp, Cofounder, Global Survivors Network and Families of September 11; Member of Homeland Security Advisory Council
Danny McPherson – Chief Security Officer, Verisign
John Stankey – Chief Executive Officer of Entertainment and Internet Services, AT&T
Michael J. Wallace – Senior Advisor, Center for Strategic and International Studies (CSIS)

The Cybersecurity Subcommittee would like to ***thank*** the following individuals for their excellent support and service to the Subcommittee:

Christopher J. Boyer, Assistant Vice President, Global Public Policy, AT&T
Michele L. Guido, Security Policy Manager, Southern Company
Christopher Krebs, Director, Cybersecurity Policy, Microsoft

HOMELAND SECURITY ADVISORY COUNCIL STAFF

Sarah Morgenthau, Deputy Assistant Secretary for the Private Sector Office and Executive Director, Homeland Security Advisory Council
Erin Walls, Director, Homeland Security Advisory Council
Mike Miron, Staff, Homeland Security Advisory Council
Jay Visconti, Staff, Homeland Security Advisory Council
Katrina Woodhams, Staff**,** Homeland Security Advisory Council

This page is intentionally left blank.

TABLE OF CONTENTS

This page is intentionally left blank.

I. INTRODUCTION

This report offers recommendations to meet a poorly understood but absolutely vital challenge for U.S. cybersecurity: ensuring that *interdependent* infrastructure sectors can work together to restore critical services after a cyberattack, in partnership with the Department of Homeland Security (DHS) and other Federal and state agencies.

Secretary of Homeland Security, Jeh C. Johnson, requested such recommendations in his August 6, 2015 message to the Homeland Security Advisory Council (HSAC) in which he directed the HSAC to create a Cybersecurity Subcommittee (Subcommittee). Secretary Johnson noted that "The Department and its public and private sector partners are making significant progress to protect the electric grid, water and wastewater systems, and other lifeline infrastructure sectors from attack." However, he also emphasized that "Given the increasing severity of the cyber threat, it is essential to strengthen U.S. plans, capabilities, and coordination mechanisms to restore infrastructure services if our defenses fail."

Secretary Johnson asked the Subcommittee to support DHS's development of an improved National Cyber Incident Response Plan (NCIRP) with two analytic efforts:

- "Identify the readiness of our lifeline sectors to meet the emerging cyber threat;" and
- "Provide recommendations for building cross-sector capabilities to rapidly restore critical functions and services following a significant cyber event."

A. REPORT SCOPE

Given the brief period within which we were asked to complete our report, the Subcommittee determined that it would be impractical to provide cross-sector recommendations encompassing all 16 critical infrastructure (CI) sectors. These sectors widely vary in their composition, collaborative mechanisms, and cross-sector interdependencies. Rather than provide a generalized overview of their sector-specific restoration challenges, the Subcommittee decided to instead conduct a detailed analysis of three sectors: financial services, communications, and electricity.[1]

Of course, the other 13 critical infrastructure sectors also provide essential services. The Subcommittee recommends that as soon as possible, DHS request follow-on studies to assess their cross-sector interdependencies and recommend how U.S. response plans and capabilities should be structured to help them meet their sector-specific restoration challenges.

Nevertheless, the electricity, financial services, and communications sectors provide a valuable starting point to fulfill the Subcommittee taskings provided by Secretary Johnson.

[1] PPD-21 identifies 16 critical infrastructure sectors. The Directive categorizes finance and communications as sectors, electricity is a subsector of the Energy Sector. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

These sectors are highly interdependent and support the operations of many other infrastructure sectors. They are vital to the U.S. economy, national security, and the well-being of the American people -- and therefore may be especially attractive targets for cyberattack in future crises.

These three sectors also face rapidly growing cyber threats. Mary Jo White, chair of the U.S. Securities and Exchange Commission (SEC), recently designated cyber security as the biggest risk facing the financial system.[2] The power grid and U.S. communication systems face escalating cyber threats as well, both to their information technology (IT) systems and to the industrial control systems and other operational technology (OT) systems on which they increasingly rely.[3]

B. STRUCTURE OF THE REPORT

Section II of our report examines the emerging cyber threat in greater detail. In particular, we examine how cyber threats will create cross-sector restoration challenges different from those from other hazards, and recommend how all-hazards incident response plans and capabilities need to account for these differences.

Section III summarizes our assessment of the readiness of the communications, financial services, and electricity subsectors to restore critical services against the emerging threat, given their interdependencies and risks of cross-sector disruptions. The summary draws on detailed, sector-specific studies included as appendices to the report. These three studies document the important progress that each of the sectors are making in restoration preparedness, including for cross-sector support, and identify additional gaps to fill.

Section IV offers recommendations on how a new National Cyber Incident Response Plan should be structured to account for these risks, and help the three sectors and their government partners prioritize and accelerate restoration of services in a contested environment. Our focus is improving the functional capabilities of the NCIRP to facilitate such cross-sector restoration.

What the report does *not* do is recommend how specific roles and missions should be allocated between DHS, the Federal Bureau of Investigation (FBI), the Sector-Specific Agencies (SSAs) that lead the Federal Government's interaction with particular infrastructure sectors, and other Federal Departments and Agencies. DHS has informed the Subcommittee that the Executive Branch will soon issue a document clarifying their organizational responsibilities. Within that allocation of roles and missions, this Subcommittee report offers recommendations on how the NCIRP should help strengthen coordination across the Federal Government, state governors, and – especially – with the private sector.

[2] Lambert, Lisa and Barlyn Suzanne. "SEC says cyber security biggest risk to financial system," *Reuters*, May 18, 2016. http://www.reuters.com/article/us-finance-summit-sec-idUSKCN0Y82K4

[3] Clapper, James R. Worldwide Threat Assessment of the US Intelligence Committee, Office of the Director of National Intelligence, February 9, 2016. http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf

II. THE EMERGING CYBER THREAT

To help provide recommendations for building cross-sector capabilities to rapidly restore critical functions and services following a significant cyber event, the Subcommittee developed a notional baseline threat to help identify key preparedness shortfalls and opportunities for progress. Appendix A provides an overview of the baseline threat. The analysis below summarizes our findings and recommendations drawn from that threat, and highlights the implications for cross-sector support requirements and the design of the new NCIRP.

As provided for in the 2011 Interim NCIRP, the Subcommittee anticipates that the communications, financial, and electric sectors (and individual companies within them) will continue to refine their restoration plans and "playbooks" based on the emerging, sector-specific threats against them. Information Sharing and Analysis Centers and other mechanisms for sharing information on the threat will provide crucial support for this refinement process. The analysis below provides a broader assessment of the cross-sector challenges that should help drive the development of the NCIRP.

A. DEFINING A "SIGNIFICANT" CYBER EVENT

Secretary Johnson's tasking to the Subcommittee was to provide recommendations on restoration of services following a "significant cyber event." Clarifying the characteristics of such an event will be essential to provide a benchmark for assessing cross-sector restoration requirements. More broadly, the NCIRP will need a system to categorize events by their severity in order to establish thresholds for triggering the use of appropriate coordination mechanisms, the employment of specific sets of authorities, and (depending on the degree of disruption to communication sector) fallback onto emergency communications systems.

Finding: The National Cyber Risk Alert Level (NCRAL) System is inadequate for characterizing event severity and setting response thresholds.

The Interim National Cyber Incident Response Plan (2011), which DHS will replace with an improved version, relies on the (*NCRAL*) system to characterize threats in terms of severity.[4] DHS' Cyber Storm III exercise in 2011 found that significant improvements were needed to the NCRAL system. The DHS report on that exercise found that to increase NCRAL effectiveness, the thresholds that precipitate an alert level change, the communications and messaging that accompany a level change, and the recommended security posture and actions at each level would need to be more clearly defined.[5]

[4] U.S Department of Homeland Security (DHS), National Cyber Incident Response Plan, Interim Version, September 2010, Appendix K, http://www.federalnewsradio.com/wp-content/uploads/pdfs/NCIRP_Interim_Version_September_2010.pdf

[5] U.S Department of Homeland Security, Cyber Storm III, Final Report, July 2011, p. 3, https://www.dhs.gov/sites/default/files/publications/CyberStorm%20III%20FINAL%20Report.pdf

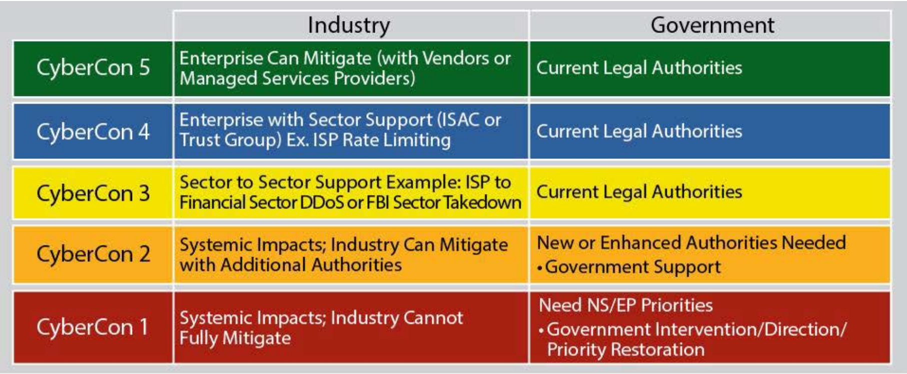
The Subcommittee found that the NCRAL system continues to lack the clarity needed to characterize the severity of attacks on critical infrastructure, and to set thresholds to trigger different types of response operations and the use of tiered government authorities (including Presidential emergency authorities at the highest end of the spectrum). The new NCIRP should jettison any reliance of the NCRAL system and adopt a more operationally useful way of categorizing threats.

Recommendation (1): Use the five-tier "Cyber Condition (CyberCon)" system as the starting point to replace the NCRAL for critical infrastructure event characterization

National Security Telecommunications Advisory Committee (NSTAC), which reports to the President on Information and Communications Technology (ICT) Mobilization (November 2014) provides the basis to develop an improved system for categorizing threats and setting response thresholds. Secretary Johnson's tasking requested that our Subcommittee account for the recommendations in the ITC Mobilization Report. The Subcommittee has done so, and concurs with the ITC Report's assessment of problems in threat characterization and recommended solutions.

The NSTAC report concludes that there is no effective methodology to support rapid mobilization and coordination of critical communications sector assets to respond to large-scale cyber incidents. In particular, despite recent progress, "there is not yet an effective methodology in place to coordinate Government and industry's operational response capabilities across the full spectrum of national security and emergency preparedness (NS/EP) events with cyber implications."[6]

Creating an improved way to categorize events and trigger coordination protocols would help support the development of such coordination mechanisms not only for the communications industry, but also for other infrastructure sectors. The ICT Mobilization report also proposes to classify cyber events based upon a five-tier "Cyber Condition (CyberCon)" scale from 5 to 1, or green to red (Fig. 1). The following graphic illustrates the CyberCon escalation process contemplated in the report:



	Industry	Government
CyberCon 5	Enterprise Can Mitigate (with Vendors or Managed Services Providers)	Current Legal Authorities
CyberCon 4	Enterprise with Sector Support (ISAC or Trust Group) Ex. ISP Rate Limiting	Current Legal Authorities
CyberCon 3	Sector to Sector Support Example: ISP to Financial Sector DDoS or FBI Sector Takedown	Current Legal Authorities
CyberCon 2	Systemic Impacts; Industry Can Mitigate with Additional Authorities	New or Enhanced Authorities Needed •Government Support
CyberCon 1	Systemic Impacts; Industry Cannot Fully Mitigate	Need NS/EP Priorities •Government Intervention/Direction/ Priority Restoration

Fig. 1: Cyber-Con Escalation Scale

[6] *Information Technology* Mobilization *Scoping* Report, The President's NSTAC, May 21, 2014.

The NSTAC report states that "the orange level represents the domain of extensive coordination and collaboration between Government and industry in terms of dynamic protocols and procedures" and describes the red level as "represent[ing] a cyber emergency of the severest nature and greatest potential impact" where industry cannot resolve the issue on its own and where "Government will be expected to convey priorities and industry will do all that is possible to support national survival, under Government direction and within a comprehensive, legal, and operational framework."[7]

As part of the NCIRP development effort, DHS should structure consensus-building process with the representatives selected by each infrastructure sector (such as their Information Sharing and Analysis Centers, Sector Coordinating Councils, or other sector-wide representative organizations) to refine and build out a new event categorization system based on the NSTAC report's CyberCon approach.

In particular, this consensus-building process should further specify the event characteristics that will help differentiate CyberCon levels, and help trigger the use of NCIRP coordination capabilities and mechanisms appropriate for those levels. Characteristics to be considered could include the likely impact of the event on:

- Public health and safety
- National security
- National economy
- Public confidence in the ability of the United States government to protect the Nation and defend its interests;
- Civil liberties of the American people

Recommendation (2): The baseline threat for assessing CI preparedness and assessing cross-sector coordination requirements for the NCIRP should initially be set at CyberCon 2 level.

Rather than assess the readiness of the electric, financial, and communications sectors against a catastrophic "Cyber Pearl Harbor" threat in the CyberCon 1 category, or a relatively minor attack that each sector could handle largely on its own, a CyberCon 2 event should be used as the starting point for assessing cross-sector restoration challenges and NCIRP requirements.

The sector-specific analysis summarized in Section III of this report (and provided in greater detail in the report's appendices) found that a CyberCon 2 event would create serious shortfalls in the ability of each sector to support the others' restoration operations. A CyberCon 2 threat could also require government to provide substantial assistance to CI restoration operations, and require regulatory relief and other measures by the Federal Government above and beyond those that are currently provided for. Section IV of this report offers specific recommendations for how the NCIRP should be structured to fill such shortfalls.

[7] *NSTAC Report to the President on Information and Communications Technology Mobilization*, page 13, Section 3.1.3, November 19, 2015.

Over time, however, it will also be necessary to assess CI restoration requirements against CyberCon 1-level threats. The new NCIRP should be scalable in terms of event severity and have the capabilities necessary to help coordinate industry-government responses to catastrophic attacks by peer or near-peer adversaries. Industry should play a key role in helping to shape those coordination capabilities to ensure they will be of greatest value for infrastructure owners and operators in restoration operations, in ways that also account for the government's national security priorities in extreme events.

Finding: While an all–hazards approach to incident management is appropriate, that approach must account for the fact that cyberattacks will pose qualitatively different challenges than natural hazards or industrial accidents.

The Subcommittee strongly supports the progress being made by DHS and its federal and state partners to position cyber response operations within a broader, all-hazards context for incident management. CyberCon 2-level cyberattacks on the power grid and other infrastructure sectors will inevitably have physical consequences. Such attacks are also likely to require incident response operations under the National Response Framework (NRF) to save and sustain lives.[8] Given that both CI restoration and more traditional consequence management operations will need to go forward at the same time, creating consistent, mutually supportive mechanisms based on the NRF and the all-hazards National Incident Management System (*NIMS*)[9] will help provide for coordinated responses to significant cyber events.

However, cyber events will pose challenges for critical infrastructure restoration very different from those created by traditional hazards, including hurricanes and other severe weather events. Clarifying the differences in kind and degree between cyber restoration requirements and those for traditional hazards will be crucial for designing the new NCIRP and specifying the capabilities it should have. Key findings and recommendations identified by the sector-specific studies included in this report:

- *Potentially unlimited geographic scope.* Hurricanes, earthquakes, industrial accidents, and other familiar hazards tend to be geographically localized. Through mutual assistance agreements and other support arrangements, companies from outside the stricken region can send assets to help restoration knowing that their own service areas will escape damage. In contrast, cyberattacks can occur anywhere, potentially on a multi-region or even nationwide basis. Mutual assistance arrangements within each sector, and NCIRP coordination mechanisms for cross-sector/government support, will need to be structured accordingly. The NCIRP should also draw on lessons learned from coordination planning against pandemic threats that can have similarly widespread geographic scope.

[8] Federal Emergency Management Agency (FEMA), National Response Framework. http://www.fema.gov/national-response-framework

[9] The National Incident Management System (*NIMS*) is a systematic, proactive approach to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sector to work together seamlessly and manage incidents involving all threats and hazards—regardless of cause, size, or location. http://www.fema.gov/national-incident-management-system

- *Uncertainty over threat characterization, damage assessment, and remediation measures.* In a hurricane or ice storm, assessing physical damage to infrastructure systems is a familiar and straightforward challenge. So, too, are processes for replacing damaged or destroyed equipment. It will be far more difficult to determine whether and how a cyberattack has caused service interruptions, rapidly characterizing the threat, assess the extent of damage to/corruption of key system components, and acquiring and implementing malware eradication measures (including against malware never before seen). All of these tasks present radically different challenges for infrastructure sectors and their government partners than traditional hazards. The coordination capabilities of the NCIRP will need to be structured accordingly.

- *Risks of re-attack.* Once a hurricane has passed over an area, that area -- and the new infrastructure installed to replace damaged equipment -- is safe until the next storm or other event strikes. Our baseline CyberCon 2 threat assumes that adversaries will employ advanced persistent threats (APT) in their attack.[10] Unless APTs are completely eradicated from communications, financial and electric grid networks, that malware will continue to disrupt restoration operations and create further cascading infrastructure failures and system instability.[11] The NCIRP's capabilities should account for this risk of re-attack.

  These challenges include 1) communicating with the public concerning infrastructure restoration timelines while risk of re-attack persists; and 2) how to determine – and perhaps even certify – that a given system is malware-free, and can be linked to other sector systems without fear of infecting them. In particular, the NCIRP and additional coordination capabilities should address the issue of how networks, services, and the companies that rely on them will determine the extent of compromise of the impacted systems. As a critical task within these coordination capabilities, the NCIRP will also need to clarify the procedures and required capabilities to access any necessary software updates, and effectuate any necessary malware eradication tools. It will also be essential to create a process to determine that the impacted systems are clean, and can be brought back on-line without introducing further instability.

- *Data corruption/ destructive malware.* Traditional hazards do not attack the data on which financial institutions and other infrastructure sectors depend. Our baseline threat assumes that adversaries will seek to destroy and/or corrupt data so that it is no longer usable or reliable. The NCIRP and cross-sector restoration playbooks should account for these risks.

- *The political goals of the attack and implications for coordinated public messaging.* Natural disasters do not intend to create political effects. In contrast, cyber adversaries will design their attacks to achieve specific political objectives, such as creating disaffection between U.S. citizens and their government, or the incitement of panic to put

[10] Hardy, Mark. APT Dot Gov: Protecting Federal Systems from Advanced Threats, A SANS Whitepaper, October 2011. https://www.sans.org/reading-room/whitepapers/analyst/apt-dot-gov-protecting-federal-systems-advanced-threats-35085

[11] Ibid

pressure on U.S. leaders to back down in the crisis that prompted the cyberattack. The NCIRP should be structured to facilitate the development and coordination of strategic messaging in a white-hot political environment that would include adversary misinformation campaigns.

- *Disruption of communications systems.* While the electric, financial, and communications sectors are all vitally important, a severe disruption of the communications would create challenges for coordination of response operations across these sectors and with the government. Such disruptions could result either from the direct effects of a cyberattack on the communications sector, or indirectly (via the disruption of the electric power supplies on which communications infrastructure depends). The coordination mechanisms established by a new NCIRP will be useless if industry and government leaders cannot communicate adequately to use them. As part of the NCIRP effort, DHS, the communications sector, and other infrastructure sectors should identify options to sustain essential emergency communications in a severely disrupted environment, and develop a plan to ensure the availability of such communications for leaders guiding response operations.

III. ADDITIONAL SECTOR ASSESMENTS: READINESS TO MEET THE EMERGING THREAT

The sector-specific studies included as appendices to this report provide detailed analyses of the progress each sector is making for post-cyberattack restoration of services. These studies also examine cross-sector dependencies, and recommendations on how the NCIRP should be structured to help accelerate service restoration. This section identifies overarching findings and proposals that pertain to all three sectors.

Finding: Significant improvements are needed in assessments of cross-sector vulnerabilities and in mechanisms to prioritize restoration operations accordingly

While each sector has an increasingly strong understanding of the sector-specific restoration challenges it confronts, and is rapidly improving plans and capabilities to meet those challenges, cross-sector vulnerabilities in a significant cyber event are not nearly as well understood.

The Subcommittee developed a typology to help infrastructure sectors and their government partners systematically categorize and address such threats. Categories include:

- *Direct, sector-specific effects*. A cyberattack on the financial, communications or electric sector will disrupt each of their abilities to operate and sustain critical services. The three sectors have been building preparedness against these threats for many years, though (as the sector-specific studies note) significant challenges remain.

- *Indirect, collateral impacts.* The financial, communications, and electric sectors have significant interdependences. If a cyberattack disrupts one of them – for example, the electric sector – the other two sectors will suffer collateral effects from the loss of electric service, even if their own systems were not directly attacked. In turn, because the electric sector depends on both the communications and financial sectors to sustain and restore electric service, the collateral effects on those two sectors will severely disrupt power restoration operations (leading to still further cross-sector disruptions).

- *Multi-sector, cascading failures.* Adversaries may not do the United States the kindness of attacking only a single sector. In the attack on the Ukraine power grid, the perpetrators struck both power distribution systems and the phone system; the latter attack prevented customers from reporting outages and disrupted the ability of grid operators to focus on restoration operations accordingly.[12] To achieve similar synergistic effects~~,~~ adversaries may launch simultaneous attacks on the electric, communications, and financial sectors. Such multi-sector attacks (and the cascading failures they would produce) compound problems for infrastructure restoration.

[12] ICS-CERT, Cyber-Attack against Ukrainian Critical Infrastructure, February 25, 2016. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

Recommendation (1): Cross-sector exercises should be ramped up to reveal unanticipated risks of cross-sector failure.

A series of exercises have helped reveal cross-sector vulnerabilities and identified options to help mitigate them. In November 2015, GridEx III examined the cascading failures that would be created by an attack on the power grid, and the ways in which resulting disruptions in the communications and financial sector would disrupt power restoration operations.[13] The summer 2016 Hamilton exercise[4] will further assess the impact of power outages on the financial sector. The DHS Cyber Storm V exercise[5], conducted in March of 2016, also examined cross-sector restoration challenges for the health, retail, and communications sectors.[14]

These cross-sector exercises provide an invaluable discovery tool. They should be expanded in a systematic way to encompass all 16 CI sectors and their government partners. These exercises should include participation by relevant Information and Sharing and Analysis Centers (ISACs) and other participants who will play a crucial role in restoration of services. To help facilitate discovery of cross-sector interdependencies, consideration should also be given to expanding exercise programs sponsored by the National Cybersecurity and Communications Integration Center (NCCIC).

Recommendation (2): Such exercises should be specifically designed to develop and assess cross-sector support options and requirements for regulatory relief or new authorities.

Exercises can not only reveal unexpected dependencies but also generate new proposals to address them. For example, GridEx III participants determined that if adversaries are able to create long-duration outages, utilities will come under intense financial pressure. They lose their revenue from delivering electricity but still need to meet their debt servicing obligations and pay their staffs (including personnel responsible for restoring service). Exercise participants determined that utilities may require blacktop financing such as loan guarantees in order to meet these challenges.[15] Preliminary discussions are now underway with the financial sector and government partners on how to provide for such emergency support.

The Subcommittee recommends that those discussions be intensified, and that future exercises develop and assess equivalent opportunities for cross-sector support. One especially promising opportunity lies in the ability of the financial and communications sectors to further clarify priorities for restoration of electric service, given the severely disrupted environment that adversaries may be able to create and the criticality of particular assets (and their fallbacks) for restoration of financial and communications services.

Recommendation (3): The NCIRP's coordination capabilities should be structured to account for collateral, cross-sector impacts and multi-sector attacks.

[13] North American Electric Reliability Corporation (NERC). GRID Security Exercise: GRIDEXIII Report, March 2016. http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf

[14] U.S Department of Homeland Security, Cyber Storm: Securing Cyber Space. https://www.dhs.gov/cyber-storm. See also U.S DHS, Informing Cyber Storm V: Lessons Learned from Cyber Storm IV, June 2015. https://www.dhs.gov/sites/default/files/publications/Lessons%20Learned%20from%20Cyber%20Storm%20IV.pdf

[15] NERC, p. 2.

Given the potential attractiveness of multi-sector attacks for adversaries seeking to maximize the effectiveness of their strike, or to demonstrate unexpected cross-sector vulnerabilities to U.S. leaders in the midst of an escalating political crisis, the NCIRP's coordination mechanisms should be designed to handle such attacks (as well as meet the more limited requirements that single-sector attacks would create). Multi-sector attacks and cascading failures across infrastructure sectors will create significant coordination challenges for government and industry. The section that follows examines those challenges and makes recommendations to meet them.

This page is intentionally left blank.

IV. ACCELERATING CROSS-SECTOR RESTORATION OF SERVICE: CAPABILITY REQUIREMENTS FOR THE NCIRP

Industry and its government partners should seek to resolve four closely related problems to facilitate cross-sector coordination for incident response: 1) how the three sectors -- and eventually many more -- should self-organize, collaborate in restoration operations, and assist each other as cyber incidents require; 2) how DHS and the White House should strengthen operational coordination across the Department of the Treasury (Treasury), the Department of Energy (DOE), and other Sector Specific Agencies (SSAs) who lead federal collaboration with each infrastructure sector;[16] 3) how to bring state governors into an appropriate role within the NCIRP; and 4) how to provide for a centralized but flexible mechanism for coordination between multiple sectors and their federal and state partners.

A. ORGANIZING ACROSS THE PRIVATE SECTOR

In a cyberattack that disrupts the electric, communications, and financial sectors, all three sectors will need the ability to collaborate with each other to help establish a shared situation awareness of the effects of the attack (including cascading failures) and prioritize restoration support for each other. No such mechanism for large-scale operational coordination exists today. The cyber incident playbooks developed by the electric subsector and other infrastructure sectors have largely focused on coordinating operations within each sector. The Electric Subsector Coordinating Committee and equivalent bodies in other sectors have begun inviting cross-sector partners to meetings on cyber response issues. However, the three sectors will also need to establish a mechanism to coordinate actual cross-sector operations, and do so even if normal voice and data communications systems are disrupted.

Finding: Significant diversity exists between infrastructure sectors in terms of how they are structured and organized for collaboration.

The communications, electricity, and financial sectors share a strong commitment to strengthening cross-sector coordination of restoration operations. However, there are a variety of ways to do so. One promising option would be to leverage an existing initiative by the National Infrastructure Advisory Council (NIAC). In the March 2015 Final Report by the NIAC, the Council proposed to establish a Strategic Infrastructure Executive Council (SIEC). In particular, the NIAC recommended that the President direct the Secretary of Homeland Security to work with the Sector Specific Agency heads for the electricity, water, transportation, communications and financial services sectors to establish an SIEC composed of Chief Executive Officers (CEO)

[16] SSAs are responsible for working with Department of Homeland Security (DHS) to implement the NIPP sector partnership model and risk management framework, develop protective programs and related requirements, and provide sector-level CI/KR protection guidance in line with the overarching guidance established by DHS pursuant to HSPD-7. Working in collaboration with security partners, they are responsible for developing and submitting Sector Specific Plans and sector-level performance feedback to DHS to enable national cross-sector CI/KR protection program gap assessments. In accordance with HSPD-7, SSAs are also responsible for collaborating with private sector security partners and encouraging the development of appropriate information sharing and analysis mechanisms within the sector. See National Infrastructure Protection Plan, Sector Overview, DHS. https://www.dhs.gov/xlibrary/assets/NIPP_SectorOverview.pdf

or Senior Executive decision-makers from these sectors and their counterpart agencies. The SIEC would “identify national priorities and develop joint or coordinated action plans and agreements to implement them.”[17]

The NIAC’s proposal was not framed to provide for operational decision making and cross-sector collaboration in the midst of a cyberattack. The SIEC or some sub-component of it might be adapted to provide for such operational coordination.

However, infrastructure sectors vary widely in the way they are structured to make operational decisions, in the ability of a small number of industry leaders to make commitments on behalf of the sector as a whole, and in the way they are organized to reach consensus. These differences are especially significant across the larger set of infrastructure sectors to be incorporated in the SIEC, including the communications, water, and transportation sectors, where it may not be as practical to have a small number of industry leaders represent the sector as a whole.

The Communications sector has advanced another promising option. That sector proposes to build upon existing industry relationships to create an operationally-focused Cross-Sector Emergency Response Team. As events move up the CyberCon scale, the Team would convene to coordinate cross-sector emergency response operations. The communications sector is also recommending the establishment of a strategic steering committee that can meet periodically to ensure executive level engagement in the process. Further, the Communications sector proposes that industry convene the “enablers” group of Internet and Communications Technology (ICT) companies that are best positioned to help respond to especially severe cyber incidents, and ensure the engagement of the key players across the Internet ecosystem (and in particular, from the IT realm).

The bottom line: while a variety of options exist to strengthen cross-sector coordination in response operations, the three sectors are unanimous in their commitment to achieving practical, near-term progress towards that goal.

Recommendation (1): On a voluntary basis, representatives of the communications, electricity, and financial sectors should build consensus on how best to provide for cross-sector restoration coordination.

Such discussions could leverage not only the SIEC and Emergency Response Team options, but also the capabilities provided by other organizations, including the Partnership for Critical Infrastructure Security (PCIS) and the National Council of Information Sharing and Analysis Centers.[18]

[17] Wallace, Michael and Kepler, David. Executive Collaboration for the Nation’s Strategic Critical Infrastructure: Final Report and Recommendations, National Infrastructure Advisory Council, March 20, 2015, p. 7, https://www.dhs.gov/sites/default/files/publications/niac-executive-collaboration-final-report-508.pdf

[18] Testimony of Thomas I. Farmer, Chair, Cross-Sector Council Partnership for Critical Infrastructure Security, Before the U.S Senate Committee on Homeland Security and Government Affairs, “Hearing on Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities and Solutions, May 18, 2016. http://www.hsgac.senate.gov/hearings/assessing-the-security-of-critical-infrastructure-threat-vulnerabilities-and-solutions

Recommendation (2): To pilot the development of a near-term capability for operational coordination, the electric, financial, and communications sectors could explore options for an interim coordinating body.

These three sectors are likely to have significant differences in the way they would prefer to be represented and organized for cross-sector collaboration in restoration operations. One way to proceed may be to begin by specifying the functions that such a coordinating body should be able to perform. These could include the ability for each sector to provide prioritized requests for support from other sectors, and also commit major company or sector-wide resources to meet requests for cross-sector assistance. Then, based on these functional requirements, each sector would decide on how it would be represented at an appropriate level in the coordinating body -- ideally, with the smallest number of representatives essential to facilitate decision making. Conducting exercises with that organization would be essential to refine its coordination mechanisms and deriving lessons for possible expansion to include additional sectors over time.

B. ORGANIZING ACROSS THE FEDERAL GOVERNMENT

A forthcoming Executive Branch document is expected to specify how cyber incident management roles and missions will be allocated between DHS, the FBI, Treasury, and other Federal Departments and Agencies. It is also expected that in a significant cyber event, a Cyber Unified Coordination Group (UCG) would coordinate the development and execution of response and recovery tasks, priorities, and planning efforts necessary to appropriately respond to the incident, speed recovery, and facilitate the rapid and appropriate sharing of information amongst Cyber UCG participants. Depending on the scope of a particular significant cyber incident, the Cyber UCG would also be expected to include includes participation from the private sector; state, local, tribal, and territorial (SLTT) governments; nongovernmental organizations; or international counterparts

Within this UCG system, it will be crucial to develop a mechanism that maintains an appropriate balance between the expertise and authorities of Sector-Specific Agencies, and the authorities of DHS to provide for overall event coordination.

Recommendation: The electric, communications, and financial sectors have very effective working relationships with their respective SSAs – the DOE, DHS, and Treasury, respectively. Consistent with the overall framework that the Executive Branch document is expected to provide, the NCIRP should ensure that each of the SSAs can bring their specialized expertise and unique industry connectively to bear in support of cross-sector restoration operations.

However, there is no need for the SSAs to replicate the capabilities for cross-sector coordination that DHS will provide in a significant cyber event. This DHS coordination role must not only be consistent with NIMS and the NRF, but should also be refined to meet industry priorities for support of their restoration operations.

C. BRINGING GOVERNORS INTO THE COORDINATION PROCESS

Governors have primary responsibility in their states for public health and safety, both of which can be jeopardized by major power outages and other infrastructure disruptions *regardless of their cause.* During Superstorm Sandy, Governor Cuomo, Governor Christie, and other governors in the region were intensely focused on restoration operations for the grid and other critical infrastructure sectors. Consistent with the National Response Framework, governors also took the lead in requesting and prioritizing federal assistance during the storm.

Finding: The involvement of governors in responding to cross-sector disruptions caused by cyberattacks will be at least as significant as in natural hazard events.

Governors across the United States are developing plans to help strengthen situational awareness in cyber events and to use state resources to help meet requests for assistance (RFAs) from infrastructure owners and operators. In particular, California and other states are creating plans and capabilities for their state National Guard organizations to establish cyber protection teams that could help respond to industry RFAs. [19] Significant challenges remain for making these initiatives effective. Nevertheless, to provide for unity of effort between state and Federal agencies in CyberCon 2 events, bringing governors into the response coordination process will be essential. Engaging with governors will also be essential to provide for unity of messaging in such events.

Recommendation (1): The NCIRP should provide for deeper engagement with governors in the coordination of CI restoration operations.

The 2011 Interim NCIRF failed to specify how governors would help partner with the Federal Government and industry to coordinate cyber response efforts in their own states. As DHS and other Federal Agencies continue to make the cyber response system as consistent as possible with the all-hazards response system guided by the NRF and NIMS, the new NCIRP should expand engagement with governors accordingly.

Recommendation (2): The Secretary of Homeland Security should request the Council of Governors (working in consultation with the National Governors Association) to propose specific mechanisms to include states in NCIRP coordination mechanisms.

The Council of Governors (Council) was established in 2012 to enable governors to address issues involving the homeland defense, and related matters with the leadership of Federal Emergency Management Agency (FEMA), DHS, Department of Defense (DOD), and the White House.[20] The Council and its federal participants have adopted a *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity* (2014) that provides a "framework for establishing a collaborative environment for states, territories, and the Federal government to expedite and

[19] See, for example, State of Michigan Executive Office, *Michigan Cyber Disruption Response Strategy* (Lansing, MI: State of Michigan Executive Office, September 16, 2013), https://www.michigan.gov/documents/cybersecurity/Michigan_Cyber_Disruption_Response_Strategy_1.0_438703_7.pdf.

[20] Exec. Order No. 13528 ("Establishing Council of Governors") (January 11, 2010), https://www.whitehouse.gov/the-press-office/president-obama-signs-executive-order-establishing-council-governors.

enhance the nation's response to cyber incidents."[21] DHS should ask the Council to recommend ways to provide for appropriate state-level engagement in CI restoration operations under the NCIRP, with appropriate consultation between the Council and the National Governors Association.

D. GOVERNMENT-INDUSTRY COORDINATION FOR CROSS-SECTOR RESTORATION OPERATIONS

The three forgoing efforts to develop coordination mechanisms will help contribute to the final challenges: that of structuring the NCIRP to facilitate multi-sector, Federal/State collaboration in significant cyber events. The sector-specific studies that follow in Appendices B, C and D provide additional recommendations on the capabilities that the NCIRP will need to enable industry-government collaboration. As DHS goes forward in drafting the Plan, these recommendations will provide a strong basis for progress.

[21] Council of Governors, *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity* (Washington, DC: National Governors Association, July 2014), http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1407CouncilofGovernorsCyberJointActionPlan.pdf.

This page is intentionally left blank.

APPENDIX A – BASELINE THREAT

I. Key Baseline Threat Characteristics

A. Political/Military Context for Attack

The baseline threat assumes that a significant cyberattack by a state actor on U.S. Critical Infrastructure (CI) is most likely to occur in the context of an escalating regional crisis or other political confrontation, rather than as a "bolt from the blue" attack. That escalating crisis would provide infrastructure owners/operators and their government partners with advance warning that the risk of a cyberattack was increasing; coordination mechanisms and cross-sector consultations could be activated accordingly before the attack occurs. In particular, electric, communications, and financial sector organizations could also take pre-attack initiatives to strengthen defensive measures and (through cross-ISAC calls and other coordination mechanisms) pre-plan for coordinated restoration operations.[22]

However, against terrorist organizations and non-state actors that are already targeting U.S. interests and assets, an attack on U.S. infrastructure could occur with little or no warning as soon as those adversaries gain the ability to do so. It will also be necessary to hedge against the risk that state adversaries will strike without warning. Accordingly, mechanisms for cross-sector coordination (by both industry and government) will require significant survivability against no-notice attacks, and should be exercised to ensure their effectiveness in such contingencies.

B. Categories of Disruption

In a sequential manner, the baseline threat will account for three categories of damage that cyberattacks can inflict on U.S. infrastructure. Each of these categories are examined in the report, and provide the basis for both near-term recommendations and proposals for follow-on stages of analysis.

- *Direct, sector-specific effects*. A cyberattack on the financial, communications or electric sector will disrupt each of their abilities to operate and sustain critical services. The sections that follow identify the sector-specific effects that the baseline threat will entail.

- *Indirect, collateral impacts.* The financial, communications, and electric sectors have significant interdependences. If a cyberattack disrupts one of them – for example, the electric sector – the other two sectors will suffer collateral effects from the loss of electric service, even if their own systems were not directly attacked. In turn, because the electric sector depends on both the communications and financial sectors to sustain and restore electric service, the collateral effects on those two sectors will severely disrupt power restoration operations (leading to still further cross-sector disruptions).

[22] ISAC stands for Information Sharing and Analysis Center. The electricity, financial services and communications sectors each have an ISAC tailored to meet the needs of their sector-specific needs. https://www.dhs.gov/topic/cybersecurity-information-sharing

- *Multi sector, cascading failures.* The adversary may not do us the kindness of attacking only a single sector. In the attack on the Ukraine power grid, the perpetrators struck both power distribution systems and the phone system; the latter attack prevented customers from reporting outages and disrupted the ability of grid operators to focus restoration operations accordingly.[23] To achieve similar synergistic effects~~,~~ adversaries may launch a simultaneous attack on the electric, communications, and financial sector. Such a multi-sector attack (and the cascading failures they would produce) will provide still further problems for infrastructure restoration.

These three categories of disruption differ in the degree to which infrastructure owners and operators are prepared to meet the restoration challenges they entail. Direct, sector-specific threats are relatively well understood. Efforts to identify indirect, collateral impacts are less advanced. A series of exercises are helping to reveal these indirect effects. Grid Ex 3 examined the cascading failures that would be created by an attack on the power grid, and the ways in which resulting disruptions in the communications and financial sector would disrupt power restoration operations.[24] The summer 2016 Hamilton exercise[4] will further assess the impact of power outages on the financial sector. The DHS Cyber Storm V exercise[5], conducted in March of 2016, also examined cross-sector restoration challenges for the health, retail and communications sectors.[25]

Multi-sector cascading failures are the least well understood. Further analysis will be essential to examine how cyberattacks could create such failures, assess their consequences for restoration of critical services, and identify opportunities for cross-sector support to mitigate their effects. Cross-sector analysis by the three ISACs would offer an excellent starting point to better assess these risks and mitigation opportunities.

C. Cyber-Response versus Consequence Management

This baseline recognizes that a cyberattack on U.S. critical infrastructure would not only disrupt CI networks ~~(~~and require cyber response operations~~)~~, but also create physical consequences, including threats to public health and safety. Our report recognizes this dual challenge and, recommends how the revised NCIRP should be structured to support an integrated approach to cyber response/consequence management.

The Subcommittee report also leverages the findings of the 2015 NSTAC ICT Mobilization Report, which highlighted the need to simultaneous address to the need to align

[23] https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[24] http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf

[25] https://www.dhs.gov/cyber-storm. See also https://www.dhs.gov/sites/default/files/publications/Lessons%20Learned%20from%20Cyber%20Storm%20IV.pdf

cyber incident management with consequence management in a cyberattack.[26] Using that Report's terminology~~,~~ the NCIRP should help support:

(1) Incident management (focusing on addressing the underlying "cyber" root-causes and ICT-related challenges), and
(2) Consequence management (focusing on the manifestation of impacts across the various infrastructure sectors as a result of the underlying cyber issues).

D. Overall Attack Severity

This baseline threat posits a mid-tier attack rising to Cyber Condition (CyberCon) level 2 on the CyberCon scale proposed in the NSTAC ICT Mobilization Report. This level of attack can be addressed by industry via cross-sector cooperation under existing legal authorities, and would not require new or enhanced authorities to be provided by government. Those more severe types of events (CyberCon 1) are-also considered in the ICT Mobilization report but are not included as part of this baseline threat.

E. Key Attack Characteristics

The attacks will utilize destructive malware. For the financial system, the attack will destroy and/or corrupt data so that it is no longer usable or reliable. In all three sectors~~,~~ system components will be disrupted or otherwise limited, negatively impacting service availability and will need extensive repairs or replacement.

Unless the advanced persistent threats employed in the attack are completely eradicated from the communications, financial and electric grid networks, that malware will continue to disrupt restoration operations and create further cascading infrastructure failures and system instability.[27] The NCIRP should account for the challenges that this risk of re-attack-creates.

In particular, the NCIRP and additional coordination mechanisms should address the issue of how networks, services, and the companies that rely on them, will determine the extent of compromise of the impacted systems. These coordination mechanisms will also need to clarify the procedures and required capabilities to access any necessary software updates, and effectuate any necessary malware eradication tools. It will also be essential to create a process to determine that the impacted systems are clean, and can be brought back on-line without introducing further instability.

The adversary will design the attacks to achieve specific political and/or operational objectives, such as creating disaffection between U.S. citizens and their government, impeding U.S. military deployments and/or the incitement of panic to put pressure on U.S. leaders to back

[26] *NSTAC Report to the President on Information and Communications Technology Mobilization*, November 19, 2015. https://www.dhs.gov/sites/default/files/publications/ICTM%20Final%20Draft%20Report%2011-2014%20(2).pdf

[27] Hardy, Mark. APT Dot Gov: Protecting Federal Systems from Advanced Threats, A SANS Whitepaper, October 2011. https://www.sans.org/reading-room/whitepapers/analyst/apt-dot-gov-protecting-federal-systems-advanced-threats-35085

down in the crisis that prompted the cyberattack. The NCIRP should have the capabilities necessary to facilitate the development and coordination of strategic messaging in a white-hot political environment that would include adversary misinformation campaigns.

Illustrative, sector-specific attack characteristics that may also be considered in developing scenarios:

- *Financial sector*: As the Financial sector is comprised of broadly dispersed firms, operating individually, the most likely attack would be on specific “key” financial institutions and/or the exchanges and clearing houses they connect to. That has been the premise of the Hamilton exercises.

  Additionally, the financial services sector would feel the cascading effects of an attack on the Electric and/or Communications sectors, owing to its dependencies on these components of critical infrastructure and creating potential for broader, regional disruption of services.

- *Electric Sector:* The baseline scenario assumes that a previously unknown malicious code is discovered on industrial control systems used across multiple critical infrastructure sectors including Energy, Water, Transportation, Chemical, and Manufacturing. Widespread reports of organizations infected by the malware confirm it adversely impacts the ability to receive telemetry data and safely and effectively operate assets. Impacts have been noted in several sectors, creating disruption and potential damage to assets.

  In lieu of clear understanding of what may be compromised and lack mechanisms and information to reliably ascertain this, some companies are taking systems offline to prevent damage even if the system is not known to be compromised, creating broader impact. In the electric sector, generating units have either been forced offline by malicious software or taken offline intentionally as a precaution, creating either reductions in reserve margin or localized and distributed power outages.

  Given the necessity of a rapid response~~,~~ it is not clear how to identify the range of damage to impacted systems, how to determine if a system is compromised, and how to achieve high confidence with any remediation. Therefore~~,~~ components may need to be replaced and / or systems rebuilt using vendor-supplied software and hardware. The simultaneous activation of this malware, spanning numerous organizations across sectors, has created severe contention for replacement components and access to software as well as expert personnel from the vendor to respond and assist with replacement and recovery.

APPENDIX B – COMMUNICATIONS SECTOR READINESS FOR CYBER RESPONSE AND CROSS-SECTOR RECOMMENDATIONS FOR THE NCIRP

I. EXECUTIVE SUMMARY

The Cybersecurity Subcommittee of the Homeland Security Advisory Council (HSAC) was established in 2015 and is tasked with providing the Secretary of Homeland Security with actionable findings and recommendations related to "the readiness of lifeline sectors to meet the emerging cyber threat and… for building cross-sector capabilities to rapidly restore critical functions and services following a significant cyber event".[28] The Subcommittee is also required to consider the National Security Telecommunications Advisory Council ("NSTAC") Report to the President on Information and Communications Technology Mobilization ("ICT Mobilization Report").[29]

In order to develop these recommendations, the Cybersecurity Subcommittee has created three sector specific working groups, one each for communications, electricity, and financial services. This document provides the findings of the communications sector identifying gaps that exist in current preparedness to respond to cyber-attacks and recommendations for DHS to improve incident response building upon recent NSTAC reports. This document also provides recommendations on how to improve cross-sector incident response in the event of a significant cascading cybersecurity attack impacting multiple critical infrastructure sectors including addressing the recommendations from the energy sector to establish a Strategic Infrastructure Executive Council ("SIEC"). The following is a summary of the critical findings of the communications sector sub-group:

- **Finalize a National Cybersecurity Incident Response Plan (NCIRP).** One critical finding from recent exercises, including Cyber Storm V and the National Level Exercise conducted in 2012, in which the communications sector participated, is the absence of clear organizational processes guiding both private sector and government incident response activities. This gap can be addressed by finalizing a national response plan or framework.

- **Develop an operation process flow to organize incident response.** As part of this plan, government must develop a flow chart or operational process flow for how incident response will occur so that industry knows how, when, where and with whom to engage as events occur. This operational process flow is particularly needed for large scale cyber-attacks that rise to the red or orange level as designated in the ICT Mobilization report.

- **Convene the enablers outlined in the ICT Mobilization Report.** One of the findings in the ICT Mobilization report is that there is a small group of Internet and Communications Technology (ICT) companies who are uniquely positioned to share

[28] Tasking memo from Secretary Johnson to the HSAC regarding establishment of a Cybersecurity Subcommittee.
[29] *NSTAC Report to the President on Information and Communications Technology Mobilization*, November 19, 2015.

information and help with large-scale incident response (the "enablers") whereas there are other sectors; *e.g.*, energy and financial services, that are downstream ("consequence") organizations. The private sector should work jointly with DHS to convene this group and determine how these industries can work together and with government in the event of a major cyber incident as recommended in the NSTAC report. The enablers would be different from the Cross-Sector Emergency Response Team concept mentioned below in that it sits upstream from the lifeline sectors with the exception of communications.

- **Determine critical infrastructure at greatest risk and focus activities in those areas.** The private sector and government should work together to determine critical infrastructure that are the most systemically critical and should be prioritized for response and recovery activities in the wake of an incident.

- **The existing Unified Coordination Group ("UCG")[30] should either be replaced or modified**. The communications sector currently participates in the UCG and its experience is that the UCG as currently structured is not effective for incident response. . DHS should re-evaluate and/or make process improvements to ensure the effectiveness of either an enhanced UCG or successor organization.

- **Improve cross-sector collaboration on incident response.** One finding of the communications sub-group is that there is a need for enhanced cross-sector organization in the event of a significant cyber incident that rises to the orange and red levels in the ICT Mobilization report. To address this issue we are making two recommendations.

    - *Establish a cross-sector emergency response team.* This entity would be a cross-sector, operationally-focused entity comprised of representatives of the major lifeline sectors that could be called upon to convene in the event of a major (red or orange in the ICT Mobilization Report) cybersecurity incident, particularly those events with the potential for cascading effects on multiple sectors in order to assist and inform any prioritization of restoration activities. The representatives for each sector would be operationally focused and have the ability to escalate to senior management as events require. This entity would be different from the enablers and sit more downstream representing the "consequence" organizations impacted by the attack and where there is a need to organize restoration activities and prioritization to mitigate the impact of an attack while in progress.

    - *Establish a lifeline sector executive steering committee.* Additionally an executive steering committee should be established that meets periodically to ensure resources levels and set the strategic direction to ensure the viability of the cross-sector emergency response team. This recommendation partially addresses the call from the energy sector for the creation of the SIEC in that this entity would be at the senior executive level and could meet annually or semi-annually for cross-sector engagement at the C-suite or senior management levels for

[30] The Unified Coordination Group (UCG) is the present entity assigned with the task to coordinate across agencies and sectors of critical infrastructure in the event of a major cyber-attack.

planning activities; however, it would not operate as a new Federal advisory committee like the SIEC. As envisioned, this group would meet periodically, potentially around the NSTAC meetings, similar to when the Electricity Sub-Sector Coordinating Council executives were invited to participate in the November 2014 NSTAC meeting.

- **Expand the availability of prioritized services**. As technology evolves communications would benefit greatly from the development of prioritized restoration services from other lifeline sectors (such as electricity) comparable to the Telecommunications Service Priority Services (TSP) offered today. Communications is as dependent upon energy as energy is on communications for incident response and in the event of a large scale outage similar prioritized services would greatly benefit response activities.

- **Test incident response procedures and develop a timeline for implementation.** Government should test these processes at least annually to ensure their effectiveness and revise accordingly. Further, DHS should shut down or eliminate redundant advisory committees and other activities. The Secretary should develop a timeline and roadmap to achieve the recommendations of the Subcommittee to ensure that DHS and other agencies remain focused on these activities.

- **Eliminate redundancies**. Finally, these activities should become the focal point for cross-sector and incident response activities. DHS should work with the private sector to identify redundant and overlapping initiatives and eliminate them.

II. ASSUMPTIONS

The Cybersecurity Subcommittee developed a hypothetical scenario that each sub-group was asked to evaluate in the process of making their recommendations that contemplates a simultaneous cascading cyber-attack impacting all three sectors which are the focus of this report: communications, energy, and financial services (*see the Baseline Threat Scenario in Appendix A*). The Communication sub-group developed its recommendations under an assumption that the impact of this scenario is a condition of degraded service, not a universal outage of communications capabilities, given the diversity and resiliency of communications networks. This point is noted in the NSTAC Communications Resiliency Task Force report (“Resiliency Report”) published in 2011 which discusses that the “diversity in communications systems components, including software, hardware, networking paths, design approaches, and operational procedures, will increase resiliency to attacks that target specific technologies or operational procedures.”[31]

III. OBSERVATIONS ON GAPS IN CYBER-SECURITY PREPAREDNESS

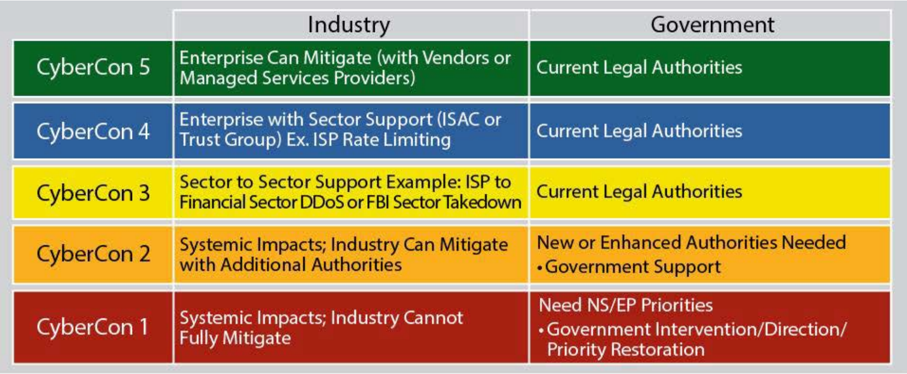
A. NSTAC ICT Mobilization Report

[31] See NSTAC Communications Resiliency Task Force Report at p. 29 https://www.dhs.gov/sites/default/files/publications/NSTAC-Report-to-the-President-on-Communications-Resiliency-2011-04-19.pdf

In November 2014 the NSTAC completed the ICT Mobilization Report providing a series of recommendations to the President to close gaps in the Nation's cybersecurity preparedness. The report is instructive as the problem statement for this exercise is similar in scope.

The NSTAC report highlights that awareness exists and investments are being made by industry to respond to cyber threats; however, the report also concludes that there is no effective methodology to support rapid mobilization and coordination of critical sector assets to respond to a large-scale incident. That is, despite progress, "there is not yet an effective methodology in place to coordinate Government and industry's operational response capabilities across the full spectrum of national security and emergency preparedness (NS/EP) events with cyber implications".[32]

The ICT Mobilization report also proposes to classify cyber events based upon a five-tier "Cyber Condition (CyberCon)" scale from 5 to 1, or green to red (Fig. 2). The following graphic illustrates the CyberCon escalation process contemplated in the report:



	Industry	Government
CyberCon 5	Enterprise Can Mitigate (with Vendors or Managed Services Providers)	Current Legal Authorities
CyberCon 4	Enterprise with Sector Support (ISAC or Trust Group) Ex. ISP Rate Limiting	Current Legal Authorities
CyberCon 3	Sector to Sector Support Example: ISP to Financial Sector DDoS or FBI Sector Takedown	Current Legal Authorities
CyberCon 2	Systemic Impacts; Industry Can Mitigate with Additional Authorities	New or Enhanced Authorities Needed • Government Support
CyberCon 1	Systemic Impacts; Industry Cannot Fully Mitigate	Need NS/EP Priorities • Government Intervention/Direction/ Priority Restoration

Fig. 2: Cyber-Condition Escalation Scale

The NSTAC report states that "the orange level represents the domain of extensive coordination and collaboration between Government and industry in terms of dynamic protocols and procedures" and describes the red level as "represent[ing] a cyber emergency of the severest nature and greatest potential impact" where industry cannot resolve the issue on its own and where "Government will be expected to convey priorities and industry will do all that is possible to support national survival, under Government direction and within a comprehensive, legal, and operational framework."[33]

The report proceeds to identify operational gaps in each of these levels discussing a variety of factors such as gaps between the capabilities of various sector ISACs, varied participation by sectors and that the ability to quickly assess and identify potential cyber impacts within all sectors is still not fully developed. The report also discusses that liability concerns

[32] *Information Technology* Mobilization *Scoping* Report, The President's NSTAC, May 21, 2014.

[33] *NSTAC Report to the President on Information and Communications Technology Mobilization*, page 13, Section 3.1.3, November 19, 2015.

associated with information sharing are still frequently cited as a limitation, and that the capability for coordination between ISACs is limited with notable exceptions between the Financial Services Sector, the Communications Sector, the Defense Industrial Base Sector, and the IT Sector. The ICT Mobilization report concludes that "at lower levels, current practiced behavior should be sufficient to maintain stability and response to cyber incidents; however, much changes in the industry-Government relationship as industry moves from utilizing existing authorities within yellow to requesting incremental Government authorities in orange."[34]

The report recommends that government "develop specific new protocols, authorities, expectations, and procedures well in advance of the need, and to exercise and train to these protocols to ensure progressive refinements over time."[35] Thus a primary gap is the development of these new protocols, authorities, expectations, and procedures to support response as events move from the first three levels, which can largely be addressed under existing processes, and events that rise to the level of orange or red where new authorities and planning is required. The report elaborates that "at this level, highly cyber-dependent organizations from industry and Government could experience degradation resulting in catastrophic impacts to our national security, economic security, public health and safety and that is currently no protocol for the Government to convey in advance the national cyber priorities for protection, reconstitution, or recovery in the event an incident surpasses industry's mitigation ability".[36]

In conclusion, based upon the ICT Mobilization Report the primary gaps appear to be the following:

- The lack of a fundamental framework and process methodology on the part of government to support and sustain infrastructure in the event of circumstances that arise to the orange and red CyberCon levels as outlined in the ICT Mobilization report which would require potentially new authorities and closer collaboration between government and industry beyond existing methodologies and may involve cross-sectoral efforts to mitigate the attack.
- A related inability for government to prioritize critical "systems and assets" that could lead to a national cyber level incident and the need for a more robust industry/government dialog on priorities for the communications sector and protocols to convey those priorities from government to industry, and
- Determining how industry and government work together to protect those specific "systems and assets" under fire, during an attack in both the orange and red scenarios outlined in the ICT Mobilization report.

B. NSTAC Communications Resiliency Task Force

[34] Ibid

[35] *NSTAC Report to the President on Information and Communications Technology Mobilization*, page 12, Section 3.1.2, November 19, 2015.

[36] Ibid.

The NSTAC Communications Resiliency Task Force recommendations developed in 2011 also address gaps in preparedness. One of the findings in that report was that while nearly all carriers and ISPs have relied on command and control structures within their company's incident response procedures for determining how an incident is handled and how the company coordinates with other entities on mitigation activities, there is a need for a centralized coordination structure rather than the ad hoc methods that existing today which are largely based on personal and business relationships. The Resiliency Report then further discusses the need for the development of a National Cyber Incident Response Plan (NCIRP) to improve private and public collaboration. [37]

IV. STRATEGIC INFRASTRUCTURE EXECUTIVE COUNCIL ("SIEC")

One of the recommendations from the energy sector is the establishment of the SIEC which is a recommendation that the National Infrastructure Advisory Council (NIAC) made to the Secretary in 2015. This recommendation calls for the establishment of a C-level executive committee that would be available to address restoration activities in the event of a major cyber incident. While communications recognizes the need for coordinated response activities, we do not see the need to create yet another advisory committee. The communications sector has been partnering with the Federal government, initially in the National Communications System (NCS) and its successor organizations dating back to 1962.

On the policy level the communications industry has one of only three Presidential level advisory committees in the NSTAC that regularly convenes to provide policy advice to the President on National Security and Emergency Preparedness ("NS/EP"). On the planning level the Communications Sector Coordinating Council ("CSCC") has been in existence since 2006 and is fully vested in organizing planning activities on behalf of the sector. And on the operational level the communications sector is co-located with DHS in the National Communications and Cybersecurity Integration Center ("NCCIC") and has personnel that are designated to coordinate response activities with the Federal government in the event of a major cyber incident.

In order to facilitate improved cross sector collaboration, in particular between the lifeline sectors, during an incident impacting multiple sectors, we are recommending two steps to improve cross-sector collaboration:

- First, establish a cross-sector emergency response team. This entity would be a cross-sector operationally focused entity comprised of representatives of the major lifeline sectors that could be called upon to convene in the event of a major (red or orange in the ICT Mobilization Report) cybersecurity incident with cascading effects on multiple sectors to prioritize restoration activities. We recognize that major cyber incidents might impact a non-lifeline sector and the response team would necessarily work with representatives of the impacted entities at that time. Nonetheless, under all major cyber incidents, the need to ensure continuity and availability of lifeline sectors services suggests a closer, ongoing operational relationship. The cross-sector group would be responsible for organizing response activities related to that specific incident. The

[37] See NSTAC Communications Resiliency Task Force at 32

representatives for each sector would be operationally focused and have the ability to escalate to senior management as events require. This entity would be different from the enablers and sit more downstream representing the "consequence" organizations impacted by the attack and where there is a need to organize prioritization and restoration activities to mitigate the impact of an attack while in progress.

- Second, establish a lifeline sector executive steering committee. This executive steering committee should be established and meets periodically to set the strategic direction and ensure resource level and assure the viability of the cross-sector emergency response team. This recommendation partially addresses the call from the energy sector for the creation of the SIEC in that this entity would be at the senior executive level and could meet annually or semi-annually to ensure cross-sector engagement at the C-suite or senior management levels for planning activities; however, it wouldn't comprise a new Federal advisory committee. This group as envisioned would meet periodically, potentially around the NSTAC meetings, such as what occurred in 2014 when the Electricity Sub-Sector Coordinating Council executives were invited to participate in the NSTAC meeting.

V. RECOMMENDATIONS

The following are the Communications sector subgroup recommendations building upon NSTAC ICT Mobilization and Resiliency Reports and the previous Subcommittee discussions.[38]

1. **Adopt the Cyber Condition scale in the NSTAC report and focus on incidents rising to the ORANGE or RED levels.** The Subcommittee should build out recommendations focused on the orange or red level incidents as defined in the NSTAC ICT Mobilization report that may rise to the level of being beyond existing standard processes and procedures for government and privacy sector collaboration to address cyber-attacks.

2. **Prioritize which infrastructure is of the greatest risk to cyber-attack.** Government, in consultation with the private sector, should determine priorities in terms of critical infrastructure at greatest risk so that response, recovery, and restoration priorities are clearly understand in the immediate aftermath of an incident. To the extent possible, this pre-identification would lead to increased attention to "left-of-boom" activities, including relationship building between appropriate stakeholders. This process should include identifying specific systems and assets that may be at risk (using classic risk formulation of Risk = Threat x Consequence x Vulnerability) as opposed to simply identifying companies.

3. **Develop an organizational flowchart for how government will respond to a major cybersecurity incident.** One of the gaps identified in the ICT mobilization report, and confirmed by the Communications industry's recent experience in the Cyber Storm V exercise, is that there is not a good organizational flow chart as to how to respond to attacks. Such a flow chart would identify:

[38] These are tentative recommendations subject to further input from the sector as discussed in the proposed approach outlined below.

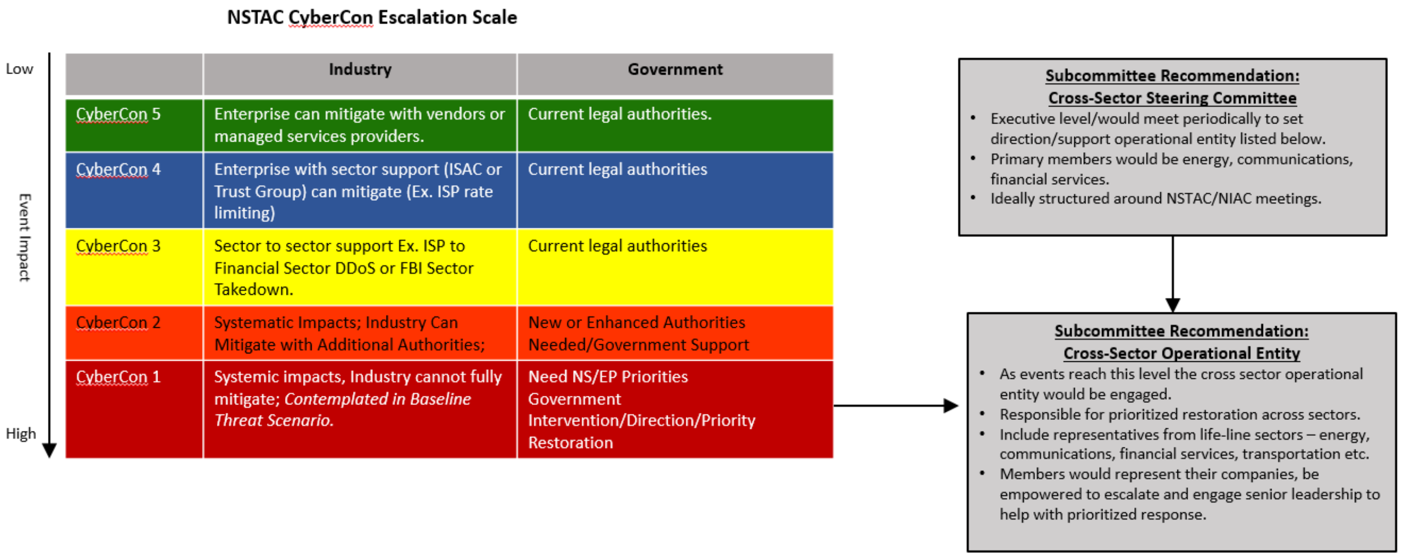
a) Who does what when there is a cyber incident,
b) What organization to contact in the event of an attack,
c) Defining which attacks rise to what level of significance, and
d) Other basic tasks that should be included either as part of the eventual incident response plan or related documents.

In developing this plan, DHS should collaborate with industry to ensure planning requirements for all stakeholders are reflected. Once developed, those stakeholders (critical infrastructure sectors) fully understand these processes and are aware of the appropriate government incident response stakeholders. These processes should then be the focal point of future exercises similar to Cyber Storm V.

4. **Convene a group of ICT Enablers**. One of the findings of the ICT Mobilization report is that there some entities, largely in the Internet and Communications Technology ("ICT") space, referred to in the report as "enablers", comprised of IT and communications companies that are uniquely positioned to have visibility into and aid the incident management elements of a large scale cyber-attack. The report then makes various recommendations to the President of how to incorporate this finding into cyber emergency preparedness. Although there are existing coordination bodies, like the Cyber Unified Coordination Group (UCG), they do not bring together the appropriate ICT sector stakeholders, nor is the UCG focused on incident response. Accordingly, the government should work with industry to create a flexible, scalable, and adaptable coordination mechanism that brings together these ICT enablers.

5. **Improve cross-sector collaboration.** As noted above regarding the SIEC, collaborate with industry to develop a private sector led cross-sector emergency response team comprised of the lifeline sectors such as communications, energy and financial services that can be convened as events rise to the RED and ORANGE levels on the CyberCon scale. This group, identified in advance, would be an ad hoc entity that could be called upon as events merit comprised predominantly of the lifeline sectors that may be impacted by the cyber-attack, as well as government representatives, to help coordinate prioritized response. This entity would be downstream from the enablers mentioned above as they represent the "consequence" or organizations impacted by the attack and where there is a need to organize specific restoration activities and prioritization to mitigate the impact of an attack. The representatives within this group should be at the operational level and empowered to escalate to senior management within their respective firms as appropriate. A principle role for this group, given cross sector dependencies would be to coordinate prioritization of the restoration of service in the event of a major orange or red level attack. Related to the cross sector emergency response team an executive steering committee could meet annually comprised of executive members from each sector. The goal of the steering committee would be to meet annually, potentially around a corresponding NSTAC or NIAC meeting to review status, clear roadblocks and ensure support for the emergency response team discussed above.

The following diagram (Fig. 3) illustrates this proposed process flow:



NSTAC CyberCon Escalation Scale

	Industry	Government
🟩 CyberCon 5	Enterprise can mitigate with vendors or managed services providers.	Current legal authorities.
🟦 CyberCon 4	Enterprise with sector support (ISAC or Trust Group) can mitigate (Ex. ISP rate limiting)	Current legal authorities
🟨 CyberCon 3	Sector to sector support Ex. ISP to Financial Sector DDoS or FBI Sector Takedown.	Current legal authorities
🟧 CyberCon 2	Systematic Impacts; Industry Can Mitigate with Additional Authorities;	New or Enhanced Authorities Needed/Government Support
🟥 CyberCon 1	Systemic impacts, Industry cannot fully mitigate; *Contemplated in Baseline Threat Scenario.*	Need NS/EP Priorities Government Intervention/Direction/Priority Restoration

Subcommittee Recommendation:
Cross-Sector Steering Committee

- Executive level/would meet periodically to set direction/support operational entity listed below.
- Primary members would be energy, communications, financial services.
- Ideally structured around NSTAC/NIAC meetings.

Subcommittee Recommendation:
Cross-Sector Operational Entity

- As events reach this level the cross sector operational entity would be engaged.
- Responsible for prioritized restoration across sectors.
- Include representatives from life-line sectors – energy, communications, financial services, transportation etc.
- Members would represent their companies, be empowered to escalate and engage senior leadership to help with prioritized response.

Fig. 3: NSTAC Cybercon Escalation Scale

6. **Streamline or eliminate redundant government initiatives.** The recommendations above should be the principle vehicle for cross-sector engagement. While we anticipate that the various sector coordinating councils and others will continue to meet as usual DHS should streamline other operationally oriented cross-sector activities to avoid redundancy.

7. **Charge DHS with continuing to develop and test the successor to the NCIRP.** DHS should recognize that the rapidly changing technologies and threats in the cyber domain dictate that the incident response plan or framework be constantly tested and updated in order to remain relevant.

8. **Direct DHS to institute an expanded program of exercises that include government agencies and infrastructure providers.** These exercises should be designed to: 1) broaden the base of organizational engagement; 2) progressively increase the scope, complexity and potential-consequence scenarios of such exercises, to permit further refinement, testing and exercising of plans and procedures by both government and industry; 3) identify and detail systemic effects and interdependencies of all kinds; and 4) support development of and continued exercising of out-of-band and autonomous coordination capabilities and procedures to restore Internet infrastructure services.

9. **Conduct joint exercises involving multiple critical infrastructure sectors.** The Communications sector participated with the Energy sector in the 2015 Grid Ex exercise. As part of continuing to test incident response, DHS could conduct joint exercises of

contemplate threat scenarios in exercises, such as what occurred in Cyber Storm V, that impact multiple sectors or entities.

10. **Consider the expansion of priority services across sectors.** The communications sector has created high availability National Security and Emergency Preparedness (NS/EP) priority services based upon market and government critical infrastructure needs. An example of this is the Telecommunications Service Priority (TSP) program which authorizes organizations to receive priority restoration treatment for vital voice and data circuits or other telecommunications services before any non-TSP service. These services are leveraged by companies, including Critical Infrastructure and Key Resources (CIKR) to manage risk. The communications sector has also developed business continuity capabilities (e.g., fixed & mobile generators) to manage power availability risk. The Communications Sector is interested in exploring the potential for the development of comparable priority restoration programs among all the lifeline sectors, and particularly with the Electric subsector to develop and offer comparable commercial offerings for high availability and/or priority restoration for NS/EP needs.

11. **Determine how to integrate State, Local, Tribal, and Territorial entities into incident response.** The State Local Tribal and Territorial (SLTT) sub-group should also contemplate undertaking a comparable prioritization effort within states, developing comparable escalation scales that might invoke the support of ICT enablers, and align State processes with the federal processes to avoid conflicting protocols and facilitate state response to cyber incidents.

APPENDIX C – FINANCIAL SERVICES SECTOR READINESS FOR CYBER RESPONSE AND CROSS-SECTOR RECOMMENDATIONS

I. INTRODUCTION

U.S. Department of Homeland Security (DHS) Secretary Johnson tasked the HSAC to "provide recommendations for building cross-sector capabilities to restore critical functions and services following a significant cyber event." To complete that assignment, the HSAC Cybersecurity Subcommittee's Incident Response sub-group decided to focus initially on recommendations pertaining to the financial sector, communications sector, and electricity subsector.

The analysis below describes the financial sector's preparedness for cyberattacks, its ongoing initiatives for responding to them, and its recommendations for developing cross-sector capabilities to rapidly restore critical functions and improve the National Cyber Incident Response Plan (NCIRP).

II. BASELINE THREAT

A. CHARACTERISTICS OF THE FINANCIAL SECTOR

The unique characteristics of the financial sector determine that cyber-attacks on it will manifest themselves in unique ways.

1. ***Geographic Effects of a Cyber Attack on the Financial Sector.*** As the Baseline Threat Assessment indicates, the financial sector is comprised of connected, but dispersed, financial institutions, including exchanges and clearing houses.

    - **Not Organized Geographically.** The financial sector is not arranged geographically, but along market and product lines. An attack would most likely manifest itself at the institution level, although the criticality of that institution could lead the attack to have a cascading impact on other components in the sector, which would be dispersed geographically.

    - **Attack Effects Not Geographic.** The results of such an attack, even on a critical component, could negatively affect a market, but not necessarily a geographic area. An attack on a bank or two would not necessarily spread to all nearby banks, while an attack on an exchange would not spread to other nearby financial institutions.

    - **Attacks on Other Sectors Could Have Geographic Impacts.** The Baseline Threat Assessment notes that an attack on electricity or communications, however, could affect the financial sector in a geographic fashion. In that case, the sector would rely on its regional coalitions as a source of support locally and intelligence nationally. It would also rely on its cross-sector relationships to address the matter. These would include the Tri-Sector Advisory Group consisting of electricity, communications, and finance, as well as the relationships developed among the ISACs through the National Council of ISACs.

2. ***Implications for Resource Sharing.*** The financial sector realizes that the life and safety of people affected by an attack are of paramount importance and, therefore, take precedence over the financial sector. All necessary resources should be dedicated to that effort.

3. ***The Importance of Responding Quickly.*** The need to respond to an attack swiftly cannot be overstated. The attacker may well attempt to disable the financial sector's detect-respond-and-recover capabilities and procedures. The attacker may also adapt to the sector's response to the incident, further highlighting the importance of responding quickly.

B. FINANCIAL SECTOR DEPENDENCIES ON COMMUNICATIONS AND ELECTRICITY

An attack on communications or electricity would affect the financial sector's response in a manner differently than a direct attack.

1. ***Responding to an Attack on Communications*.** In a crisis, the financial sector will tend to rely upon traditional communication channels to respond and recover, but utilize redundancy, geographic dispersion, and dedicated lines in light of regulatory requirements.

   The needs of the sector are too complex and integrated to accommodate a simple solution, such as satellite phones or ham radios. Such tools may offer some help, but they would not effectively replace existing communication capabilities. (If the communications circuits are active, but just overloaded, the use of the GETS/WPS could be used to help prioritize emergency communications.)

   - **Redundancy**. Sector participants have invested heavily in building redundancy into communication capabilities, as well as the ability to fail over to other sites in the expectation that they will not be disrupted. In many cases, critical firms have global fail over capabilities.

   - **Geographic Dispersion.** Sector participants have also moved their redundant data centers and operational units hundreds of miles from one another to avoid the geographic effects of an attack.

   - **Dedicated Communications Lines.** Many significant firms have invested in dedicated communication lines to conduct their critical operations.

   - **Broad Disruption.** In a widely-dispersed attack, less significant institutions may lack the above capabilities. In such a case, communications among clients, participants, and markets may not fully exist. This would reduce the ability of the market to function. Firms would fail over to backup locations to conduct operations.

2. ***Responding to an Attack on Electricity.*** The financial sector relies in many cases on power substitutes that may be needed in the absence of electricity. Regulatory requirements have also led to this approach.

   - **Redundancy Sources.** Some also have multiple sources of electricity in the event that one or more fails for some reason.

   - **Generators and Uninterruptable Power Supplies (UPS).** Many financial institutions rely on generators and/or UPS to bridge gaps in the availability of electricity.

   - **Broad Disruption.** In a widely-dispersed loss of power, neither redundancy nor short-term alternative sources of power will suffice. Firms would fail over to backup locations to conduct operations.

III. SECTOR READINESS, KEY CHALLENGES, AND ONGOING INITIATIVES FOR RESPONDING TO CYBER ATTACKS

A. SECTOR READINESS

The financial sector has been and continues to be a prime target for cyber threat activity, as the recent incidents involving banks utilizing SWIFT illustrate. As these attacks have continued to evolve in terms of complexity and impact, the sector has strived to develop defenses and resilience to keep pace with the threat.

Lessons learned from the Iranian distributed denial of service (DDoS) attacks of 2012 and 2013, affecting 46 financial institutions, showed that enhanced coordination, readiness, and response capabilities were required. As the sector continued to evolve its capabilities, there were several key themes that came into focus.

1. ***Cybersecurity Operational Capabilities Assessment (COCA) Framework.*** COCA was developed as a model to support the structured integration of all sector operational threat and hazard response projects through a mutually supporting framework allowing each element to logically coordinate with and flow into the superseding activity (Fig. 4). The Framework draws inspiration from the National Response Framework and adapted versions of some of its principles:

   - **Engaged Partnership.** Leaders across private sector and public partners at all levels collaborate to develop shared response goals and align capabilities to meet the needs of the situation. This collaboration is designed to provide transparency, coordination, and effective management for potentially cascading impacts.

- **Tiered Response.** Efficient incident management, so that such incidents are handled at the lowest possible level and supported by additional capabilities only when needed.

- **Scalable, Flexible, and Adaptable Operational Capabilities.** These capabilities are implemented as incidents evolve in size, scope, and/or complexity, so that the response to an incident or combination of incidents adapts to meet the requirements. Processes for engaging Cybersecurity Operational Resources across individual firms, the sector, commercial, and government organizations are understood and utilized in a prioritized manner. Their engagement and effectiveness for each contingency and incident is reviewed and lessons learned captured and implemented.

- **Unity of Effort.** Sector coordination requires the consideration of each impacted or participating organization's needs with an emphasis on seamless coordination across sector organizations in support of common, agreed priorities and objectives.

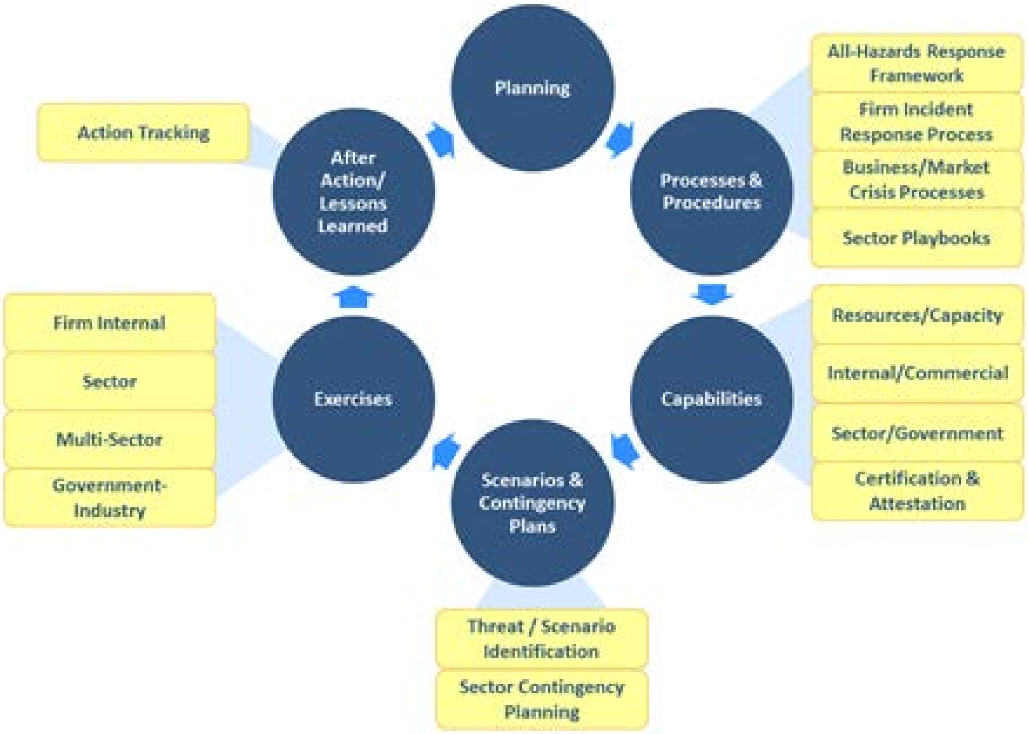

Planning
Processes & Procedures
All-Hazards Response Framework
Firm Incident Response Process
Business/Market Crisis Processes
Sector Playbooks
Capabilities
Resources/Capacity
Internal/Commercial
Sector/Government
Certification & Attestation
Scenarios & Contingency Plans
Threat / Scenario Identification
Sector Contingency Planning
Exercises
Firm Internal
Sector
Multi-Sector
Government-Industry
After Action/ Lessons Learned
Action Tracking

Fig. 4: Cybersecurity Operational Capability Assessment (COCA) Framework

2. ***Enhancements to the Financial Sector Cyber Response Coordination Guide.*** This is the sector specific annex to the National Cyber Incident Response Plan (NCIRP) that has been maintained by the sector, even though the NCIRP was never published. The Guide is in the process of being further revised and integrated with the updated All-Hazards Playbook. This document has benefitted from lessons learned in the sector's response to the DDoS attacks and from input from Treasury, DHS, FBI, and other agencies.

B. ONGOING INITIATIVES

1. ***Communications Task Group.*** A significant cyber incident will require consistent messaging from the sector to address questions from the media and public. This task group is working with representatives in the private and public sector to develop a communications playbook as well as establish the appropriate contact lists to facilitate outreach between government and private sector. The Financial Services Sector Coordinating Council (FSSCC), Financial Services-Information Sharing and Analysis Center (FS-ISAC), and public sector members seek unity in messaging in the event of significant cyber incident.

2. ***Cross-Sector.*** A 2016 financial sector exercise will be conducted with the electricity subsector. The communications sector will be present at that exercise as an observer. Their participation will strengthen their awareness of the activities and capabilities of the financial sector, identify cross-sector impacts, identify opportunities to integrate cross sector elements of responsiveness into each other's plans, and -- most importantly -- begin to coalesce on a common escalation typology for coordination and decision making at the national level.

3. ***Information Sharing Cross-Sector.*** Coordination of information sharing and communication between sectors continues to grow. The respective ISACs are now communicating cross sector regularly and looking for opportunities to further enhance those capabilities. Moreover, the National Council of ISACs facilitates an extensive amount of cross-sector sharing among the ISACs.

4. ***Tri-Sector Advisory Group***. The finance, communications, and electricity sectors have begun to meet as a group to discuss common areas of tactical and strategic importance. Participants include representatives from the respective Coordinating Councils, with the intent to include their ISAC and other sector representatives. Reporting to sector C-suite, or inclusion of such representatives is being contemplated.

C. KEY CHALLENGES

The process of improving financial sector capabilities has led to the development of closer relationships with other critical sectors, especially electricity and communications. Each of these sectors confronts common threats, requires the same information about these threats, and the impact of these threats expands beyond any one sector.

Cross-sector collaboration ensures that there will be appropriate coordination across the many shared requirements of preparedness and responsiveness. These efforts have been matched by a corresponding effort from these same sectors to establish the same cross-sector capabilities. This cross-sector outreach recognizes sector interdependencies, as well as the potential for simultaneous attacks on multiple sectors, as appropriately contemplated in the Baseline Threat Assessment.

1. ***Dependency on Communications.*** From an impact perspective, the financial sector is dependent on the electricity sector for the power necessary to run its infrastructure and

networks. Critical financial institutions have redundant power providers and backup generators, but there is a dependency on infrastructure outside the control of any individual financial institution. The impacts could cascade into other elements of infrastructure and networks, becoming increasingly problematic. Getting primary power restored is essential to minimize the broader impact.

2. ***Dependency on Electricity.*** There are many similarities with the communications sector in terms of the financial sector's dependency and resiliency. While critical financial institutions have alternate providers to account for outages, there are points within the network where communications carriers share infrastructure and thereby create vulnerabilities. As the communications networks are stressed the effect will cascade through the various components of the financial system, from the public to the financial institutions to the clearing and settlement exchanges.

IV. CROSS-SECTOR CAPABILITIES: RECOMMENDAITONS FOR THE NATIONAL CYBER INCIDENT RESPONSE PLAN (NCIRP) AND CAPABILITY DEVELOPMENT

A. RECOMMENDATIONS FOR THE NCIRP

A national response plan must address a vast array of firms within each of the 16 critical sectors, as well as incorporate the numerous federal agencies with authority in the event of an incident. This requires a plan both general enough to be applicable across that disparate set of entities, as well as sufficiently concrete to be actionable. By way of example, the financial sector reduced the size of its sector playbook to 10 pages from more than 100. Specific and detailed appendices exist, but the basic approach to ANY incident can be covered in relatively few pages.

1. ***Leverage the Unified Coordination Group (UCG).*** The UCG exists as a vehicle to bring together the necessary parties to address a significant incident, including a cyber-attack against one or more sectors.

   - **Develop Process for Identifying Those Needed in UCG.** The key to implementing the UCG in an effective manner is knowing who must be part of it for any particular incident. The financial sector is too diverse for any handful of participants, whether CEOs, ISAC, or FSSCC leaders, to represent the entire sector. As a result, the sector has developed a process for identifying who needs to "be at the table." This approach would work well for the UCG across sectors.

     - The financial sector consists a large number of companies offering a variety of products and services. The leadership of a firm involved in one product/service line would not have the expertise to address issues affecting another firm in a different business. Thus, those key firms affected by an incident would be the private sector leads, but speaking for their firms only. In practice, response has involved collaboration among affected firms, with the participation of FSSCC and FS-ISAC, as well as key trade associations, as necessary.

- The financial sector will rely on the U.S. Department of the Treasury as its intermediary with the White House and even the President. As a mature sector, the necessary people can be brought to a meeting as needed. The U.S. Department of the Treasury has a view of the entire sector, as do FSSCC and FS-ISAC, while key trade associations have expertise across a swath of firms in various lines of business.

2. ***Leverage the Tri-Sector Advisory Group.*** The finance, electricity, and communications sectors have formed an advisory group comprised of representatives from each sector, which should serve as a key source of intelligence, mutual aid, and expertise in the event of significant cyber incident.

   - **Connect the Advisory Group to the UCG.** The Advisory Group may be leveraged by the UCG, for example, in light of an incident for guidance in identifying who should be part of the UCG and for the expertise necessary to address the incident.

   - **Expand the Advisory Group.** As the Advisory Group develops and becomes effective, it should expand its membership to other critical sectors, albeit in a deliberate and careful manner. To be useful for both the private and public sectors, it must avoid becoming unwieldy or bureaucratic.

3. ***Develop a Senior Level Tri-Sector Council.*** The Advisory Group should be overseen by the leaders of the respective sectors comprising it. These could be CEOs and/or other senior leaders, depending upon the nature of the participating sectors. This Council could meet relatively infrequently, compared with the Advisory Group.

   - **Connect the Council to the UCG.** The Council may be leveraged by the UCG, for example, in light of an incident for guidance in identifying who should be part of the UCG and for the expertise necessary to address the incident.

   - **Expand the Council.** As the Council develops and becomes effective, it should expand its membership to other critical sectors, albeit in a deliberate and careful manner. To be useful for both the private and public sectors, it must avoid becoming unwieldy or bureaucratic.

B. RECOMMENDATIONS FOR CAPABILITIES DEVELOPMENT

In addition to the NCIRP, capabilities must continue to be developed, both within, between, and among critical sectors.

1. ***Initiate a Communications R&D Project.*** The financial sector's communications needs are so complex and integrated that no backup communications tool or suite of tools exists. R&D funding should be allocated to developing either new communications capabilities as a widely-shared fallback system or rendering existing ones more resilient.

2. ***Continue to Develop the Financial Sector Communications Task Group on a Cross-Sector Basis.*** The sectors and government need to continue to develop a process whereby the industry and relevant public agencies speak with one voice. The goal is to maintain public confidence in the financial sector, while conveying necessary information to the public. As this effort matures, the process should be expanded to the electricity and communications sectors. Coordinated messaging among the sectors should be developed. Respective corporate communication teams should hold a series of meetings to plan this.

3. ***TSP, GETS, and WPS.*** The benefits of the TSP, GETS, and WPS programs should be leveraged and implemented within all sectors to the greatest extent possible.

4. ***Private Sector Participation in Setting Priorities for Restoration of Service.*** In the event restoration decisions cannot be predetermined, ensure a robust process for quickly making those determinations during an incident leveraging private sector input. This may well involve the Tri-Sector Advisory Group and/or Council, as well as the UCG.

    - **Restoration within the Financial Sector.** Financial sector restoration differs from those in other sectors. The highest priority will be collaborating with the U.S. Department of the Treasury as a sector, with the emphasis on section 9 firms.

    - **Regulatory Restoration Requirements.** The financial sector has restoration priorities, as provided in the 2003 Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System. For example, it states that the ability of firms playing significant roles in critical financial markets to recover clearing and settlement activities depends on the timing of the recovery of core clearing and settlement organizations for those markets. These critical functions must be recovered within the same business day as the disruption, with some required to become operational again in four hours or two hours.

5. ***Clarify Federal Agency Roles.*** Clarify federal agency roles, responsibilities, and capabilities in support private sector restoration efforts.

6. ***Collaboration at the State and Local Levels.*** The financial sector collaborates with local and state governments in various ways. These procedures should be coordinated with other sectors, beginning with the Tri-Sector Advisory Group.

    - **Collaboration with the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC).** Financial services collaborates extensively with the members of the SLTTGCC on cybersecurity issues to understand how non-federal entities will respond to such an incident. These efforts should also be conducted on a cross-sector basis, utilizing the Tri-Sector Advisory Group.

    - **Financial Sector Regional Coalitions.** Regional coalitions within the financial sector offer another vehicle for cross-sector collaboration and crisis response. There are 17 communities of financial institutions across the country that collaborate regularly with state and local first responders and emergency management so as to be prepared for incidents. These entities complement the national sector partnerships, serving as means of handling incidents that are geographic in nature. Some are cross-sector, and each could collaborate with Tri-Sector Advisory Group.

7. ***Continued Importance of Sector-Specific Planning.*** The importance of continued sector-specific planning must be recognized. Such efforts address the unique needs of each sector and provide a clear mechanism for sector-specific plans to "plug in" to the UCG framework. This planning may also develop best practices of use to other sectors, as well as uncover gaps with other sectors that might otherwise go unnoticed.

8. ***Addressing Corrupted or Destroyed Data.*** The Hamilton Series included a recommendation to develop a solution to the problem of destructive malware corrupting or destroying financial data, a potential problem noted in the Baseline Threat Assessment. In response to that recommendation, the financial sector is creating a process for financial institutions to maintain daily account balances in a secure environment so that there is a record that can be used in the event data is corrupted or destroyed. While unique to the financial sector, it may provide insights for how other sectors could address this problem.

This page is intentionally left blank.

APPENDIX D – ELECTRICITY SUBSECTOR READINESS FOR THE EMERGING THREAT AND RECOMMENDATIONS FOR CROSS-SECTOR RESILIENCE

I. INTRODUCTION

The electricity subsector is rapidly improving its ability to restore power after a significant cyber event. However, as cyber threats become more severe, electric utilities will need to strengthen their restoration plans and capabilities accordingly. This will be especially true against the baseline threat scenario provided in Appendix A, which posits the use of Advanced Persistent Threats in a simultaneous attack on the electric, financial and communications sectors.

This subsector analysis finds that utilities will be heavily dependent on the availability of communications links to coordinate their operations with other electric systems (and, in some cases, to guide and sustain their own restoration efforts). Attacks on the financial system could create additional problems for the electric subsector, especially in extreme events where utilities might need access to emergency loans. There is evidence that attackers have considered these cross-cutting effects. As defenders we must do the same. Establishing a Strategic Infrastructure Executive Council (SIEC) would help meet these coordination requirements. An aggressive exercise program, building on GridEx III and other exercises, will also be necessary to reveal underlying interdependencies and to develop and test options to mitigate them.

On the government side, a forthcoming President Decision Directive (PDD) is expected to lay out how Federal agencies will be organized for incident response. However, as the PDD is implemented and operationalized, it will be critical to ensure that the Department of Energy -- the Sector Specific Agency (SSA) for the electricity subsector -- will continue to play a crucial role in coordinating government-industry collaboration. That role will remain vital in cross-sector attacks, even as the Department of Homeland Security and the Cyber Unified Coordination Group help provide for cross-sector coordination.

Section II examines the progress that the electric sector is making to meet the challenges of post-cyberattack power restoration, and offers recommendations to fill key gaps in preparedness that remain. Section II analyzes how a cross-sector attack (striking the electric, communications, and financial sectors) would complicate power restoration, and proposes options to strengthen cross-sector resilience. Section III offers recommendations on how a new National Cyber Incident Response Plan (NCIRP) should be structured to support cross-sector restoration of services.

II. CYBER RESPONSE INITIATIVES WITHIN THE ELECTRICITY SUBSECTOR: PROGRESS AND REMAINING CHALLENGES

In assessing the readiness of the electricity subsector to restore power against the baseline threat used by this report, three aspects of that threat will be particularly challenging for the grid – and will require response mechanisms that differ significantly from those that the electric industry has refined over many decades of experience with natural hazards. These threat characteristics help drive the electric subsector findings and recommendations that follow.

The first challenge is that of the potential geographic scope of such attacks. Unlike hurricanes and other traditional hazards, cyberattacks can occur simultaneously or at intervals on a multi-region or even nationwide basis. Broad attacks will not only multiply demands for restoration assets but also create uncertainties and potential conflicts over restoration priorities. These challenges will put a premium on close operational coordination and rapid information sharing between utilities and with the government. The risk of multi-region attacks will require significant adjustments to the mutual assistance agreements on which the industry relies to accelerate power restoration.

The second challenge lies in rapidly detecting the threat, characterizing the malware used in the attack, and assessing damage to utility networks and other systems. Knowing that an ice storm may soon hit a utility is relatively easy; identifying that the storm has hit is typically straight forward; so, too, is the process of identifying damaged or destroyed equipment to replace. Rapidly characterizing and assessing damage in a cyber-event will be far more difficult. Warning will be still more difficult to obtain, especially if an adversary seeks to “spoof” monitoring systems. Compared to restringing wire and other familiar restoration tasks, the utility-specific nature of many industrial control systems (ICS) will also require specialized training and exercise initiatives to eradicate malware and conduct other cyber remediation operations.

The third problem stems from the risk of re-attack. Once a hurricane has passed over an area, utilities in that area will remain safe until the next storm or other event strikes. This report’s baseline CyberCon 2-level threat assumes that adversaries will employ advanced persistent threats in attacking the grid.[39] Unless utilities and their partners can completely eradicate APTs from electric grid networks, that malware could:

- Continue to disrupt restoration operations and create further cascading infrastructure failures and system instabilities;[40]
- Infect replacement equipment;
- Infect additional networks and equipment as systems are reconnected; and
- Create problems for communicating with the public and elected officials regarding Estimated Times of Restoration (ETRs).

A. ELECTRICITY SUBSECTOR COORDINATION FOR POWER RESTORATION

The electricity subsector has a well-established, all-hazards foundation on which to build for post-cyberattack power restoration. The Electricity Subsector Coordinating Council (ESCC) provides an exceptionally strong basis for collaborative progress by all components of the

[39] Hardy, Mark. APT Dot Gov: Protecting Federal Systems from Advanced Threats, A SANS Whitepaper, October 2011. https://www.sans.org/reading-room/whitepapers/analyst/apt-dot-gov-protecting-federal-systems-advanced-threats-35085

[40] Ibid

industry.[41] The ESCC was formed to help coordinate these efforts and to ensure utilities are appropriately deploying each other's expertise, capabilities, and assets. The ESCC consists of electric company CEOs and trade association leaders who represent all segments of the electric sector and actively partner with government executives to prepare for, and respond to, national-level incidents or threats to critical infrastructure.[42]

A key characteristic of the ESCC is executive engagement. In addition to providing resources and accountability that have pushed both the government and industry to work very closely and very quickly, senior executives on both sides also help to ensure unity of effort and unity of message among their organizations. During an incident, the ESCC provides situational awareness, helps align messaging, and coordinates with government on response and recovery efforts. However, the ESCC does not play an *operational* role in coordinating restoration efforts.[43]

As a starting point to build such an operational role, the ESCC might leverage its current ability to convene senior executives during an incident. In past events, such as Superstorm Sandy, the ESCC has served as an effective "center of gravity" for increasing situational awareness across the sector (and throughout electricity companies).

These executives can use the ESCC framework to break down barriers and bureaucracy as they partner with senior government officials, help make real-time hard decisions that standard operating procedures wouldn't allow for, and resolve difficult decisions under duress.

Finding: Significant operation coordination between utilities, and between electric subsector and senior government officials, will be essential in significant cyberattacks. Rapid sharing of situational awareness (supported by industry and government sharing mechanisms) will be critical in such events. Moreover, utility leaders may have to make difficult decisions on network isolation/grid segmentation, prioritized allocation of scarce ICS restoration assets, and other operational issues.[44]

Recommendation: Rather than build a cyber-specific coordinating body from scratch, the electric subsector should create an operational sub-component within the ESCC. A very small number of utility CEOs might be selected by the ESCC to convey the sector's priorities and perspectives to the Cyber Unified Coordination Group (C-UCG). These CEOs could also work with the C-UCG on decisions involving waivers or use of Federal authority, requests for

[41] U.S Department of Homeland Security (DHS), Energy Sector – Electricity Subsector: Council Charters and Membership. https://www.dhs.gov/energy-electricity-subsector-charters-and-membership

[42] Statement of Scott I. Aaronson, Managing Director, Cyber and Infrastructure Security Edison Electric Institute, Before the U.S Senate Homeland Security and Government Affairs Committee, "Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities, and Solutions," May 18, 2016, p.4. http://www.hsgac.senate.gov/hearings/assessing-the-security-of-critical-infrastructure-threat-vulnerabilities-and-solutions. As in the case of superstorm Sandy, however, the ESCC has helped "convene" CEO discussions on operational issues

[43] Aaronson, op cit. , p. 5

[44] NERC, Cyber Attack Task Force, May 9, 2012, http://www.nerc.com/docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf; Report on the FERC-NERC-Regional Entity Joint Review of Restoration and Recovery Plans," FERC/NERC/Regional Entities, January 2016, http://www.ferc.gov/legal/staff-reports/2016/01-29-16-FERC-NERC-Report.pdf

government assistance, and other operational matters, and convey C-UCG recommendations back to the ESCC for fuller consideration.

B. INFORMATION SHARING AND ANALYSIS

The Electricity Information Sharing and Analysis Center (E-ISAC) and other sources of threat data and situational awareness data will be essential for supporting restoration operations. The E-ISAC establishes situational awareness, incident management, coordination, and communication capabilities within the electricity sector through timely, reliable, and secure information exchange. In collaboration with DOE and the ESCC, the E-ISAC serves as the primary security communications channel for the electricity sector and enhances the sector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.

The E-ISAC:

- Identifies, prioritizes, and coordinates the protection of critical power services, infrastructure support services, and key resources;
- Facilitates sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, potential protective measures, and practices;
- Provides rapid response through the ability to effectively contact and coordinate with member companies, as required;
- Issues alerts to industry ranging from advisory notices to essential actions requiring recipients to respond as defined in the alert; [45]
- Provides and shares campaign analysis, which includes capturing, correlating, trending data for historical analysis, and sharing that information within the sector;
- Receives incident data from private and public entities;
- Assists DOE, Federal Energy Regulatory Commission (FERC), and DHS in analyzing event data to determine threats, vulnerabilities, trends and impacts for the sector, as well as interdependencies with other critical infrastructures (this includes integration with the DHS National Cybersecurity and Communications Integration Center (NCCIC));
- Analyzes incident data and prepares reports based on subject matter expertise in security and the bulk power system;
- Shares threat alerts, warnings, advisories, notices, and vulnerability assessments with the industry;
- Works with other ISACs to share information and provide assistance during actual or potential sector disruptions whether caused by intentional, accidental, or natural events;
- Develops and maintains an awareness of private and governmental infrastructure interdependencies;
- Provides an electronic, secure capability for the E-ISAC participants to exchange and share information on all threats to defend critical infrastructure;
- Participates in government critical infrastructure exercises; and
- Conducts outreach to educate and inform the electricity sector. [46]

[45] NERC Alerts, http://www.nerc.com/pa/rrm/bpsa/Pages/Alerts.aspx

[46] Testimony of Gerry Cauley, President and Chief Executive Officer, NERC, to House Transportation and Infrastructure Committee, Subcommittee on Economic Development, Public Buildings and Emergency Management, April 14, 2016, pp. 4-5. http://transportation.house.gov/uploadedfiles/2016-04-14-cauley.pdf

All of these functions will be vital for accelerating post cyberattack power restoration. However, information sharing and analysis systems and capabilities will need to continue improving if the industry is to strengthen its preparedness against the increasingly severe threat. One important initiative to do so is provided by the Cyber-security Risk Information Sharing Program (CRISP), a public-private partnership, co-funded by DOE-OE and industry. 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. CRISP leverages advanced sensors and threat analysis techniques developed by DOE along with DOE's expertise as part of the National Intelligence Community to better inform the energy sector of the high-level cyber risks. Current CRISP participants provide power to over 50 percent of the total number of continental U.S. Electricity Subsector customers.[47]

Finding: Information sharing and analysis systems and capabilities within the electricity subsector are improving, and must continue to do so to stay ahead of the threat. To help meet this challenge, the ESCC has established initiatives on 1) Tools & Technology, focused on deploying government technologies that improve situational awareness and enable machine-to-machine information sharing; and 2) Information Flow, aimed at ensuring that actionable intelligence and threat indicators are communicated to the right people at the right time.

These improvements within the electricity subsector are vital but not sufficient. In an attack that hits multiple sectors simultaneously, cross-sector information sharing capabilities will also be essential. Early threat detection, characterization and conveyance of information about attacks on the communications sector, for example, could provide critical situational awareness for electric utilities as they consider relying on that sector's services for their own restoration operations.

Recommendation: The ESCC's working groups on Cross-Sector Coordination and Incident Response should make it a priority to explore opportunities for improved cross-sector information sharing and analysis for restoration operations. One option would be for the National Council of ISACs or other organizations (including government agencies) to provide for increased and more operational cross-sector information sharing.[48] Collaborative efforts by the E-ISAC, the FS-ISAC, and the Communications ISACs should also continue to expand. Within the next two years, an exercise should stress these three sectors by simulated simultaneous attacks.

C. CYBER MUTUAL ASSISTANCE

[47] Testimony of Patricia A. Hoffman, Assistant Secretary for Office of Electricity Delivery and Energy Reliability, U.S Department of Energy, to Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings and Emergency Management, U.S House of Representatives, April 14, 2016, p. 3. http://transportation.house.gov/uploadedfiles/2016-04-14-hoffman.pdf

[48] National Council of ISACs. http://www.nationalisacs.org/#!about-isacs/vu5l7

The electric power industry has built an impressive, voluntary system of mutual support. Under this system, utilities that are not at risk of being struck by a hurricane or other hazard can send restoration assets to those that are. The overall restoration capacity of the industry is immense; the mutual assistance system enables utilities to target support when and where specific utilities request aid. Drawing on the lessons learned from Superstorm Sandy, utilities are expanding the mutual assistance system to bring to bear still greater restoration capabilities in future catastrophes.[49]

Adapting the current restoration system for post-cyberattack operations will entail major challenges.[50] During hurricanes, utilities sending assistance to the impact zone were secure in the knowledge that they were safely beyond the reach of the storm. No power company will be beyond harm's way during a nationwide cyberattack. Unless the electric industry can adjust mutual assistance agreements to account for such challenges, utility CEOs are likely to be less willing to share assets in a cyberattack

Differences among the industrial control systems (ICSs) utilities use to manage their operations, pose an additional problem. When ice storms or other natural hazards strike, repair crews from outside the stricken region can provide immediate assistance because restringing power lines and other restoration tasks are similar from one utility to the next. Much greater variation exists across ICS software, applications, and system designs. Restoring these operational technology (OT) systems after a cyberattack requires specialized, utility-specific training, which will limit mutual assistance operations unless such challenges are resolved.

As cyber risks proliferate, the industry is organizing itself to pool resources in the face of incidents that exceed the capacity of individual companies to respond. In its early stages now, a framework is being developed to identify and share resources during incidents. Over the long term, this project—with the backing and leadership of senior industry executives—will evolve based on the cyber incident response needs of the industry. In addition, electric companies work to maintain and strengthen their ties to state agencies, state and local law enforcement, and state Fusion Centers that receive, analyze, gather, and share threat information.[51]

Difficulties in cyber information sharing are intensified by two collateral considerations. One is the paucity of cyber skilled personnel. We estimate that the number utility workers capable of restoring the grid from physical damage exceeds by an order of magnitude the number able to do so against cyber threats. The second is that physical restoration does not normally involve potential breach of confidential information. Cyber restoration does. Both these considerations intensify the requirements for special planning for cyber emergencies.

Finding/recommendation: The efforts being made by the subsector to overcome the challenges to cyber mutual assistance are extremely important. In a significant cyberattack using APTs,

[49] Edison Electric Institute, *Before and after the Storm,* Appendix C.
[50] This analysis of mutual assistance challenges draws in part on Stockton, Superstorm Sandy: Implications
[51] Statement of Scott I. Aaronson, Managing Director, Cyber and Infrastructure Security Edison Electric Institute, Before the U.S Senate Homeland Security and Government Affairs Committee, "Assessing the Security of Critical Infrastructure: Threats, Vulnerabilities, and Solutions," May 18, 2016, pp. 5-6. http://www.hsgac.senate.gov/hearings/assessing-the-security-of-critical-infrastructure-threat-vulnerabilities-and-solutions

even well prepared utilities may not have the capabilities in-house necessary to entirely eradicate malware and conduct other restoration operations. As against natural hazards, the ability of utilities to support each other in cyber events should become a linchpin of preparedness.

III. CROSS-SECTOR ATTACKS: IMPLICATIONS FOR POWER RESTORATION

The financial and communications sectors are heavily dependent on the flow of electricity to function. Although emergency power generators can help keep their critical facilities and systems functioning during short duration outages, problems of generator burn-out and sustaining refueling operations will create growing disruptions as a blackout continues. Restoring grid-provided power (whenever practical, in a way that reflects communications and financial system priorities) will be crucial for accelerating getting financial and communications services back on-line.

A. COLLABORATION WITH THE COMMUNICATIONS SECTOR

In turn, the electric subsector also depends on communications systems to function. The North American Electric Reliability Corporation (NERC) has established communications and coordination standards for power generators, high voltage transmission companies, and other Bulk Electric System (BES) entities to confer.[52] Power distribution utilities (which are regulated by State Public Utility Commissions) also generally have redundant communications systems so they can sustain control of their operations if their primary communication systems go down. Additional utility measures to ensure that they will have essential communications links for utility operations:

- Utility emergency response plans and/or business continuity plans typically cover communications system restoration planning. These plans address the recovery of key communication functions for IT, data, and voice communications, as well as connectivity for essential personnel and offsite locations.

- Many utilities also are laying dark fiber and taking other high-tech measures to strengthen communications system survivability. They have also made provisions for more elementary, low-tech communications media if systems and networks shut down during recovery and restoration efforts. HAM Radio can be particularly useful as a communication channel of last resort, because it can communicate and even access the internet when landlines are down and cell traffic is overloaded, and it can run on battery power for extended periods of time. HAM radio was used extensively during Hurricane Sandy, the 2003 New York City blackout, and many other significant events.

- A growing number of utilities also have also established collaborative relationships with their communications providers to help mitigate the loss of service due to natural disasters. On a utility-by-utility basis, these relationships can help prioritize the restoration of critical communications services.

[52] See, for example, NERC Standard COM-002-2 — Communications and Coordination, http://www.nerc.com/files/COM-002-2.pdf

- New technologies, such as M2M technology or private clouds to give utility personnel access to data and files when primary systems go down, can provide additional system redundancy -- as long they are not themselves degraded by a cyberattack underway against the communications and electricity subsectors.[53]

However, building the resilient communications required in cross-sector attacks will also require additional technical initiatives and collaborative efforts. Four levels of effort will be required for such communication initiatives: 1) long term, sustainable communications between utilities for subsector-wide coordination of restoration and "new normal" operations; 2) resilient emergency communications necessary for coordinated incident response between the finance, electricity, and communications senior executives; 3) communications between these executives and their counterparts in government; and 4) communications with the American people.

1. **Communications within the Electricity Subsector.** NERC's study on Severe Impact Resilience (2012) noted that in a significant cyberattack or other event, and emergency situation so catastrophic may emerge that complete restoration of electric service is not possible for many weeks or even months. The Bulk Electric System (BES) system would need to operate at a reduced state of reliability and supply for months or possibly years during this "new normal" period, as utilities worked to stabilize power islands and gradually integrate them on a regional basis. Having reliable backup communications systems that utilities could rely on to conduct such operations will be vital.[54] Systems that can survive cyberattacks on the communications sector and operate in disrupted power environments will also be critical to enable CEO collaboration on power restoration efforts in less severe events.

2. **Cross-Sector Communications.** If the three sectors are to help each other accelerate restoration of service by identifying key support priorities, and sharing situational awareness of restoration timelines and emerging threats to restoration efforts, minimalist but highly survivable communications links will also be needed to link sector leaders. One model to leverage might be the Department of Defense's "thin line" for nuclear force command and control. The thin line provides a survivable, secure, and enduring communications architecture to ensure connectivity between the President, the Secretary of Defense, and other officials.[55]

   Developing an equivalent survivable, bare-bones architecture for communications between sector leaders would be enormously valuable to support cross-sector coordination on service restoration. High Frequency (HF)/shortwave backup

[53] Krachenfels, Jim, The Role of Communications in the Smart Grid, *Electric Light & Power*, November 1, 2012. http://www.elp.com/articles/powergrid_international/print/volume-17/issue-11/features/the-role-communications-smart-grid.html; Unger, Eileen, Planning for Disaster – Ensuring Utility Communication System Resilience, *Energy Central*, May 20, 2015. http://www.energycentral.com/gridtandd/communicationsandsecurity/articles/3167/Planning-for-Disaster-Ensuring-Utility-Communication-System-Resilience/

[54] NERC, Severe Impact Resilience: Considerations and Recommendations, May 9, 2012, p. 11, http://www.nerc.com/docs/oc/sirtf/SIRTF_Final_May_9_2012-Board_Accepted.pdf

[55] Nuclear Matters Handbook 2015, Office of the Deputy Assistant Secretary of Defense for Nuclear Matters. http://www.acq.osd.mil/ncbdp/nm/NMHB2015/chapters/chapter_6.htm

communications systems may provide one viable option to do so, since many companies already have such systems.

3. **Communications with the Government.** Unless reliable communications exist between the Cyber UCG and sector leaders, the coordination mechanisms provided for in the NCIRP will be of limited value. In addition to the HF options above, emergency communications networks maintained by the National Guard and other government agencies might be considered to help meet these requirements.

4. **Communicate with the Public.** A key conclusion of the GridEx III exercise was that:

   “Industry and government need to provide the public with meaningful information so they are aware of the situation and what is being done about it. This helps individuals decide what they need to do to look after their own interests. Utilities and government at all levels, local, state/provincial, and federal, will need to communicate with the public. Social and traditional media capabilities drive an ever-increasing demand for timely and accurate information. Widespread and prolonged power outages will disrupt the ability of traditional media (television, radio, print) to function. [56]

Being prepared to communicate despite thee disruptions will be especially critical in cyberattacks, where the adversary may be seeking to incite panic and create uncertainty among U.S. citizens as to whether the government is able to protect them.

B. COLLABORATION WITH THE FINANCIAL SERVICES SECTOR

Another key finding of GridEx III exercise was that as a cyber-induced power outage continues, electric companies will come under intense financial pressure. If the financial sector is simultaneously disrupted, the ability of utilities to conduct normal business operations that depend on financial services will be challenged. Moreover, utilities will have little or no revenue coming in if their customers are no longer receiving power. At the same time, however, those utilities will need to meet their payroll needs and fund service restoration operations, as well as be expected to service any debt obligations. Companies could quickly find themselves on the brink of financial default. Accordingly, the exercise found that “Utilities will need unprecedented levels of financial resources in order to restore their facilities and eventually resume normal operations.”[57] The electric sector should partner with the financial services sector and the government agencies (including Treasury) to explore options to provide for emergency liquidity in significant cyberattacks.

IV. RECOMMENDATIONS FOR THE NCIRP

As the PDD on cyber incident management is implemented, two lines of follow-on work will be needed to support its implementation. The first is that of clarifying how industry will be

[56] NERC, Grid Security Exercise, GridEx III Report, March 2016, p. 14. http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf

[57] NERC, Grid Security Exercise, GridEx III Report, March 2016, p. 15. http://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf

represented in the Cyber UCG and other fora. One prime option: as proposed in the March 2015 Final Report of the National Infrastructure Advisory Council (NIAC), a Strategic Infrastructure Executive Council (SIEC) should be established to facilitate cross-sector collaboration for incident response planning and coordination. Proposed next steps:

- Examine how the NIAC's proposed creation of an SIEC might help meet the needs of the Electricity Subsector for support from the Financial and Communications Sectors for post-cyberattack power restoration (follow-on work would explore broader cross-sector coordination).

- Consider how the proposed makeup and staff support of the SIEC could be most effective in addressing the highest priority issues requiring engagement of industry senior executives and senior government executives. Given the limited role that the SIEC is envisioned to play in supporting cross-sector operations during a cyber-event, the Group will identify requirements for such operational coordination, and develop options to meet them.

As the Energy SSA, DOE also serves as the day-to-day Federal interface for the prioritization and coordination of activities to strengthen the security and resilience of critical infrastructure in the energy sector. This involves building, maintaining and advancing relationships and collaborative efforts with the energy sector. DOE has invested in public/private partnership programs and initiatives that involve sharing real time information, assessing vulnerabilities, clarifying responsibilities, and engaging in training and exercises. [58]

No other Federal agency can or should attempt to replicate the deep expertise that DOE has on electric subsector issues, including power restoration challenges. DOE will need to be a lead federal partner for the electric industry in significant cyber events. This is all the more essential because DOE will work with its interagency partners to coordinate appropriate waivers, when needed, to further speed restoration efforts. In extreme cases, DOE can also use its legal authorities under the Federal Power Act, the Defense Production Act, and the recently-passed FAST Act (Fixing America's Surface Transportation Act, P.L. 114-94) to assist in response and recovery operations.[59] DOE is also the Federal lead for Emergency Support Function 12 (Energy), which will continue to serve as a foundational document for coordination on electricity restoration operations.

However, the question remains as to how SSAs will be integrated into the Cyber UCG and other coordinating mechanisms in cross-sector events, and provide sector-specific expertise within the overall cross-sector incident management roles that the PDD is expected to assign to DHS. As the implementation of the PDD goes forward, the crucial, sector-specific role of DOE will need to be preserved.

[58] Testimony of Patricia A. Hoffman, Assistant Secretary for Office of Electricity Delivery and Energy Reliability, U.S Department of Energy, to Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings and Emergency Management, U.S House of Representatives, April 14, 2016, p. 3. http://transportation.house.gov/uploadedfiles/2016-04-14-hoffman.pdf

[59] Ibid.

APPENDIX E – INCIDENT RESPONSE GROUP MEMBER BIOGRAPHIES

Steve Adegbite (Co-Chair)

Steve Adegbite is the Chief Information Security Officer at E*Trade. Prior to joining E*Trade, he was the Senior Vice President in charge of the Enterprise Information Security Program Oversight and Strategy Organization at Wells Fargo & Co. Mr. Adegbite has also served as the Director, Cyber Security Strategies at Lockheed Martin Information Services and Global Services. Prior to joining Lockheed Martin, Mr. Adegbite was the Chief Security Strategist for Adobe Systems Inc. within the Adobe Secure Software Engineering. Mr. Adegbite has also worked with Operations positions at the National Security Agency, the National Geospatial-Intelligence Agency and the Defense Intelligence Agency, both as a government employee and as an associate consultant for Booz Allen Hamilton, a strategy and technology consulting firm.

Juliette Kayyem (Co-Chair)

Juliette Kayyem has spent over 15 years managing complex policy initiatives and organizing government responses to major crises in both state and federal government. She is the founder of *Kayyem Solutions, LLC*, providing strategic advice in technology, risk management, mega-event planning and more. Currently, Kayyem serves on the faculty at Harvard's Kennedy School of Government. She is an on-air security analyst for CNN and hosts a regular podcast entitled "Security Mom" for WGBH, Boston's local NPR station.

Previously, Kayyem was President Obama's Assistant Secretary for Intergovernmental Affairs at the Department of Homeland Security. Her book, "Security Mom: An Unclassified Guide to Protecting Our Homeland and Your Home," was published by Simon & Schuster in 2016.

Jeff Moss (Co-Chair)

Jeff Moss is a Nonresident Senior Fellow at the Atlantic Council within the Brent Scowcroft Center on International Security. He is the former Chief Security Officer for the Internet Corporation for Assigned Names and Numbers (ICANN). Prior to joining ICANN, Mr. Moss served as the Director of Black Hat and Techweb. Prior to founding Black Hat, Mr. Moss was a Director at Secure Computing Corporation, where he helped establish the Professional Services Department in the United States, Asia, and Australia. Mr. Moss has also worked for Ernst & Young, LLP in their Information System Security division. Mr. Moss speaks frequently on topics of computer and information security.

Paul Stockton (Co-Chair)

Paul Stockton is the managing director of Sonecon LLC, an economic and security advisory firm in Washington, DC. Before joining Sonecon, he served as the assistant secretary of defense for Homeland Defense and Americas' Security Affairs from May 2009 until January 2013. In that position, he was the secretary of defense's principal civilian advisor on providing defense support to FEMA and DHS during Superstorm Sandy, Hurricane Irene, and other disasters. Dr.

Stockton also served as DOD’s domestic crisis manager and was responsible for Defense Critical Infrastructure Protection policies and programs. In addition, Dr. Stockton served as the executive director of the Council of Governors.

Prior to being confirmed as assistant secretary, Dr. Stockton served as a senior research scholar at Stanford University’s Center for International Security and Cooperation and associate provost of the Naval Postgraduate School (NPS). Dr. Stockton was twice awarded the Department of Defense Medal for Distinguished Public Service, DOD’s highest civilian award. DHS awarded Dr. Stockton its Distinguished Public Service Medal. Dr. Stockton holds a PhD from Harvard University and a BA from Dartmouth College. He is the lead co-author of “Curbing the Market for Cyberweapons” (*Yale Law & Policy Review*, 2013) and numerous other studies on cybersecurity issues. Dr. Stockton is senior fellow of the Johns Hopkins University Applied Physics Laboratory and serves on the boards of Analytic Services, Inc, Idaho National Laboratory, and the Center for Cyber and Homeland Security Studies at the George Washington University.

General Barry D. Bates

General Barry D. Bates is a retired Major General in the U.S. Army. He retired on 1 January 2003, after serving as the Commander, 19th Theater Support Command, Eighth U.S. Army, Republic of Korea. In this capacity, he was responsible for logistics support and installation management for U.S. Army forces in Korea, as well as for planning wartime logistics to support U.S. Army units deploying to Korea in the event of hostilities. General Bates previously led the worldwide retail operations of the Army and Air Force Exchange Service as its Commander and CEO. General Bates is currently the Executive Vice President at NDIA, where he is responsible for logistics and administrative support for 37 functionally oriented, corporate leader-populated industrial base committees. He further leads a team responsible for planning and executing more than one hundred government-industry meetings, conferences, and symposia annually. General Bates has worked at NDIA since February 2003.

Richard Bejtlich

Richard Bejtlich is Chief Security Strategist at FireEye, and was Mandiant's Chief Security Officer. He is a nonresident senior fellow at the Brookings Institution and an advisor to Threat Stack, Sqrrl, and Critical Stack. He is pursuing a Doctor of Philosophy in War Studies at King's College London. He was previously Director of Incident Response for General Electric, where he built and led the 40-member GE Computer Incident Response Team (GE-CIRT). Richard began his digital security career as a military intelligence officer in 1997 at the Air Force Computer Emergency Response Team (AFCERT), Air Force Information Warfare Center (AFIWC), and Air Intelligence Agency (AIA). Richard is a graduate of Harvard University and the United States Air Force Academy. His fourth book is "The Practice of Network Security Monitoring" (nostarch.com/nsm).

Scott Charney

Scott Charney is Corporate Vice President for Microsoft's Trustworthy Computing Group, which is responsible for the security of Microsoft's products and services, as well as a range of corporate programs enforcing Microsoft's mandatory engineering policies. Prior to joining Microsoft, Mr. Charney served as a Principal at PricewaterhouseCoopers where he led the firm's Digital Risk Management and Forensics Practice. Before that, Mr. Charney served as Chief of the Computer Crime and Intellectual Property Section (CCIPS) where he was responsible for implementing the Justice Department's computer crime and intellectual property initiatives. Under his direction, CCIPS investigated and prosecuted national and international hacker cases, economic espionage cases, and violations of the federal criminal copyright and trademark laws. His section also proposed and commented on legislation, represented the United States internationally, and supported the development and implementation of U.S. information technology policy. Prior to leading CCIPS, Mr. Charney served an Assistant United States Attorney responsible for the investigation and prosecution of complex cases involving organized crime and as an Assistant District Attorney in Bronx County, New York, where he was responsible for prosecuting persistent violent felony offenders and then served as Deputy Chief of the Investigations Bureau. Mr. Charney has received numerous awards during his career, including the Justice Department's John Marshall Award for Outstanding Legal Achievement and the Attorney General's Award for Distinguished Service. He currently serves on the President's National Security and Telecommunications Advisory Committee, was a co-chair of the CSIS Commission on Cybersecurity for the 44th Presidency, and served three years as Chair of the G8 Subgroup on High-Tech Crime.

Richard Danzig

Richard Danzig is a Senior Advisor to the Johns Hopkins Applied Physics Laboratory, a consultant to the Intelligence Advanced Research Projects Activity (IARPA), Chair of the Advisory Panel for Idaho National Laboratories' Innovation Center, and a member of the Toyota Research Institute Advisory Board. He is also a member of the Defense Policy Board, The President's Intelligence Advisory Board, and the Homeland Security Secretary's Advisory Council, a Trustee of Reed College and of the RAND Corporation, a Director of the Center for a New American Security and a Director of Saffron Hill Ventures (a European investment firm).Dr. Danzig was a Professor of contract law at Stanford and Harvard Universities between 1972 and 1977. He was the Under Secretary of the Navy between 1993 and 1997 before serving as the 71st Secretary of the Navy from November 1998 to January 2001.

Thomas A. Fanning

Thomas A. Fanning is chairman, president and chief executive officer of Southern Company, one of America's largest electricity producers. Fanning has worked for Southern Company for more than 30 years and has held 15 different positions in eight different business units, including numerous officer positions with a variety of Southern Company subsidiaries in the areas of finance, strategy, international business development and technology. Prior to assuming the role of chief financial officer, Fanning was president and CEO of Gulf Power, a Southern Company subsidiary. Fanning chairs and serves on numerous boards spanning his areas of interest and expertise, including acting as chair of the Electricity Subsector Coordinating Council, which serves as the principal liaison between the federal government and the electric power sector to protect the electric grid from threats that could impact national security.

Russell Fitzgibbons

Russell Fitzgibbons is the Executive Vice President and Chief Risk Officer for The Clearing House, a financial institution that provides clearing and settlement services for financial commodities derivatives and securities transaction. Mr. Fitzgibbons and is responsible for Enterprise Risk Management, Information Security and Business Continuity. He has more than 30 years of management experience in various operations, payments and payments-related services. Prior to joining The Clearing House, Mr. Fitzgibbons held a number of positions at Deutsche Bank, most recently as the Global Head of Cash Operations, where he was responsible for successfully processing all payment and payment-related transactions, including high-value payments, ACH transactions, and checks worldwide. He also managed Deutsche Bank's Messaging Network and Regulatory Filtering. Prior to joining Deutsche Bank, Mr. Fitzgibbons worked for Bankers Trust, and for First Chicago's Edge Act offices in Boston, Los Angeles and New York as its Operations Manager. He is Chairman of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. He also has participated on the Payment Risk Committee at the Federal Reserve Bank of New York and on the BAFT-IFSA Board.

Carie A. Lemack

Carie A. Lemack, currently the Cofounder and CEO of DreamUp, a provider of space-based education and media services, is a cofounder of Global Survivors Network, a global organization for victims of terror to speak out against terrorism and radicalization. Ms. Lemack has coordinated and inspired events in Jordan, Pakistan, and Indonesia, produced the award-winning documentary film *Killing in the Name*, spearheaded a website, www.globalsurvivors.org, and generated interest and coverage in media outlets worldwide. Ms. Lemack cofounded and led the non-profit, non-partisan organization Families of September 11th. She was previously an International Affairs Fellow at the Council on Foreign Relations and is currently a Senior Fellow at the Center for Cyber and Homeland Security at George Washington University.

Danny McPherson

Danny McPherson is a Senior Vice President and the Chief Security Officer for Verisign where he is responsible for all aspects of security and IT functions. He currently serves on the FCC's Communications Security, Reliability and Interoperability Council (CSRIC), ICANN's Security and Stability Advisory Committee 9SSAC), and several other industry forums. Previously, Mr. McPherson was CSO of Arbor Networks, and prior to that he held technical leadership positions with Amber Networks, Qwest Communications, Genuity, MCI Communications, and the U.S. Army Signal Corps, and has also served multiple terms on the Internet Architecture Board (IAB) along with numerous IETF leadership positions. He has been active within the Internet operations, security, research, and standards communities for over 20 years, and has authored a number of books, standards, research papers, and other publications related to these topics.

John Stankey

John Stankey, CEO – AT&T Entertainment Group, is responsible for the company's position facing the consumer market segment. He leads strategy, marketing and operations around the development and distribution of a premier entertainment experience. John oversees AT&T's entertainment offerings including TV, video and content development, its consumer mobility and wireless products, and its high speed Internet services as well as its advertising business.

John previously served as Chief Strategy Officer, where he led the company's corporate strategy, M&A, and business development initiatives. Before that, John served as President and CEO of AT&T Business Solutions, where he was responsible for serving AT&T's business customers worldwide and all of AT&T's shared services including capital planning, engineering, network operations, information technology, supply chain and corporate real estate. In his three-decade career, John also has served as President and Chief Executive Officer of AT&T Operations, Inc. and as Group President-Telecom Operations, where he was responsible for the company's former five regional telecom units. His responsibilities also have included Chief Technology Officer, Chief Information Officer, President and CEO of AT&T's Southwest Region, and President of Industry Markets.

John is on the Board of Visitors at the Anderson Graduate School of Management at UCLA. He also serves on the board of directors of UPS and the Cotton Bowl Athletic Association. John also served for several years on the National Security Telecommunications Advisory Committee.

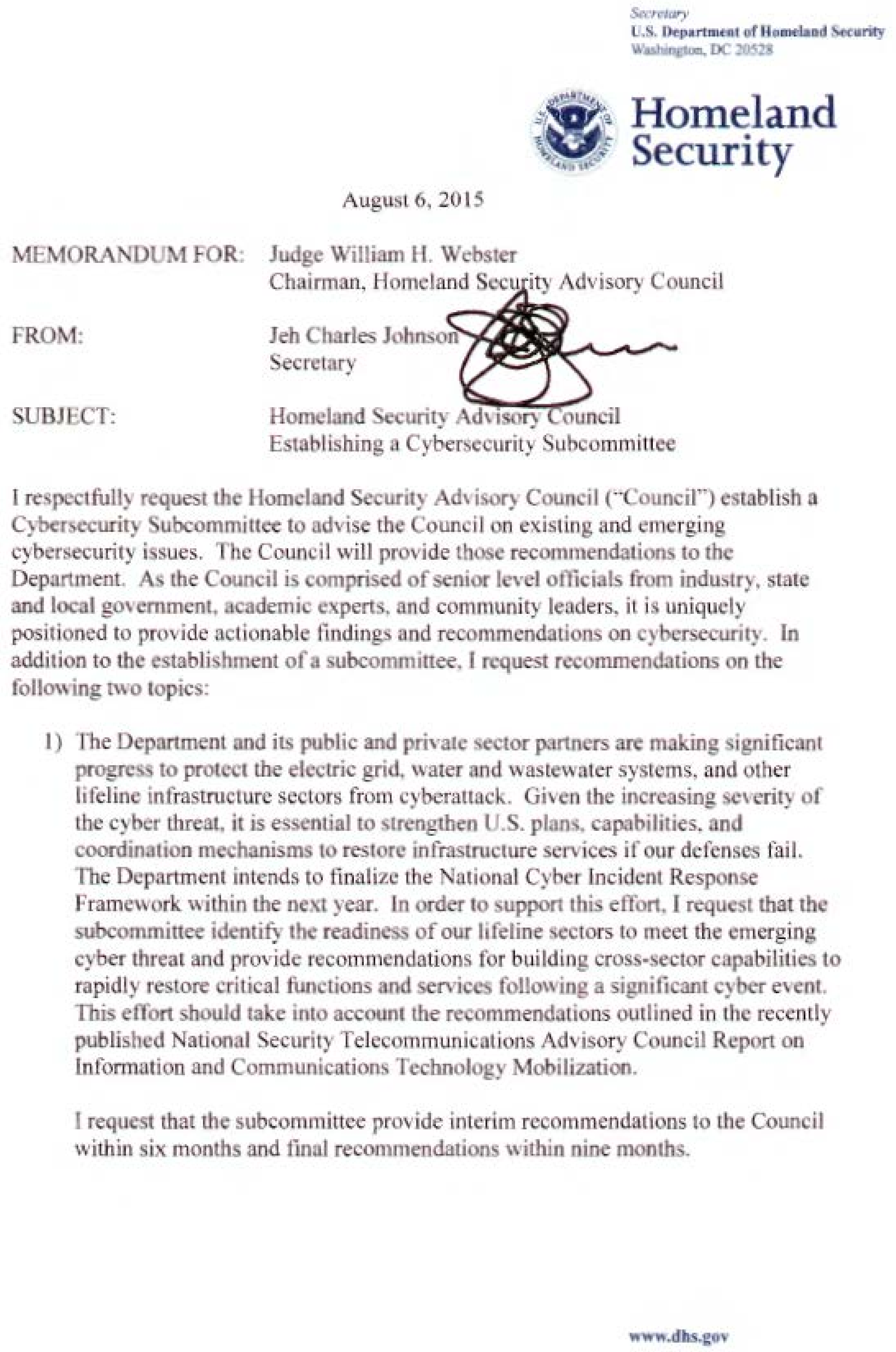
A native of California, John earned a bachelor's degree in finance from Loyola Marymount University in Los Angeles in 1985 and a master's degree in business administration from UCLA in 1991.

Michael J. Wallace

Michael J. Wallace is a senior advisor at the Center for Strategic and International Studies, where he served as director of the Nuclear Energy Program and co-chairman of the Commission on Nuclear Energy Policy in the U.S. He is engaged in two broad based areas: nuclear energy, and critical infrastructure security. He serves as a member of the National Infrastructure Advisory Council, which advises the President of the United States on matters related to Homeland Security. He also serves as a Senior Advisor to the North American Electric Reliability Corporation (NERC). Mr. Wallace is a member of Draper Laboratories' corporation, the Advisory Board of Centrus Corporation, the U.S. Naval Historical Foundation Advisory Council, and the Board of Emirates Nuclear Energy Corporation. Mr. Wallace was previously the Vice Chairman and COO of Constellation Energy and Chairman of Constellation Energy Nuclear Group. As COO, Mr. Wallace had direct responsibility for several different business groups, including its wholly owned subsidiary Baltimore Gas and Electric. Before joining Constellation Energy, Mr. Wallace was Managing Director of Barrington Energy Partners, LLC, a strategic consulting firm specializing in energy industry transactions and advisory services, which he co-founded. Prior to co-founding Barrington Energy, Mr. Wallace had more than 25 years of senior executive and utility operations experience. He also proudly served as a naval officer in the U.S. Navy nuclear submarine force.

This page is intentionally left blank.

APPENDIX F – TASK STATEMENT



Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

August 6, 2015

MEMORANDUM FOR: Judge William H. Webster
Chairman, Homeland Security Advisory Council

FROM: Jeh Charles Johnson
Secretary

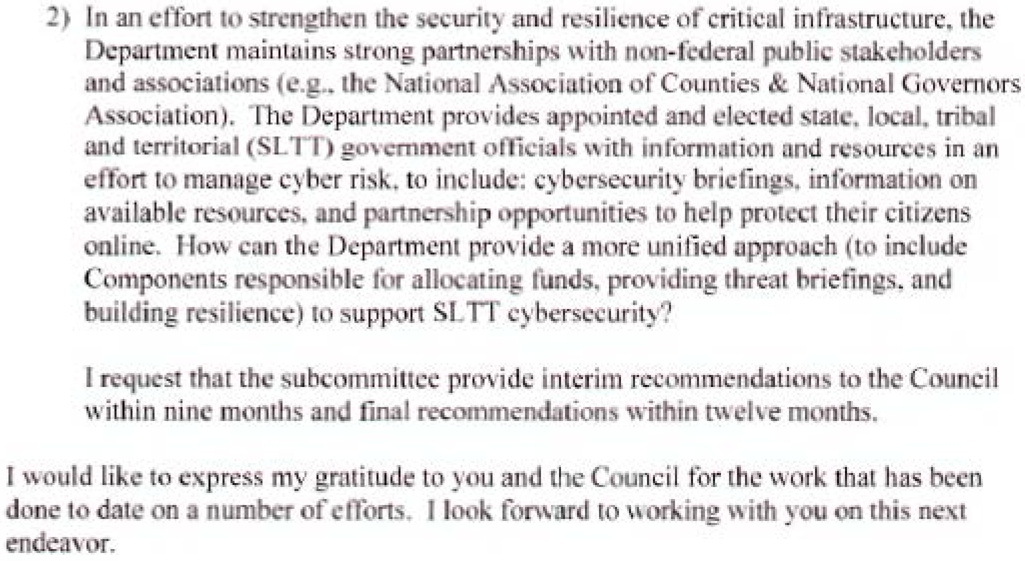
SUBJECT: Homeland Security Advisory Council
Establishing a Cybersecurity Subcommittee

I respectfully request the Homeland Security Advisory Council ("Council") establish a Cybersecurity Subcommittee to advise the Council on existing and emerging cybersecurity issues. The Council will provide those recommendations to the Department. As the Council is comprised of senior level officials from industry, state and local government, academic experts, and community leaders, it is uniquely positioned to provide actionable findings and recommendations on cybersecurity. In addition to the establishment of a subcommittee, I request recommendations on the following two topics:

1) The Department and its public and private sector partners are making significant progress to protect the electric grid, water and wastewater systems, and other lifeline infrastructure sectors from cyberattack. Given the increasing severity of the cyber threat, it is essential to strengthen U.S. plans, capabilities, and coordination mechanisms to restore infrastructure services if our defenses fail. The Department intends to finalize the National Cyber Incident Response Framework within the next year. In order to support this effort, I request that the subcommittee identify the readiness of our lifeline sectors to meet the emerging cyber threat and provide recommendations for building cross-sector capabilities to rapidly restore critical functions and services following a significant cyber event. This effort should take into account the recommendations outlined in the recently published National Security Telecommunications Advisory Council Report on Information and Communications Technology Mobilization.

   I request that the subcommittee provide interim recommendations to the Council within six months and final recommendations within nine months.

www.dhs.gov



2) In an effort to strengthen the security and resilience of critical infrastructure, the Department maintains strong partnerships with non-federal public stakeholders and associations (e.g., the National Association of Counties & National Governors Association). The Department provides appointed and elected state, local, tribal and territorial (SLTT) government officials with information and resources in an effort to manage cyber risk, to include: cybersecurity briefings, information on available resources, and partnership opportunities to help protect their citizens online. How can the Department provide a more unified approach (to include Components responsible for allocating funds, providing threat briefings, and building resilience) to support SLTT cybersecurity?

   I request that the subcommittee provide interim recommendations to the Council within nine months and final recommendations within twelve months.

I would like to express my gratitude to you and the Council for the work that has been done to date on a number of efforts. I look forward to working with you on this next endeavor.

APPENDIX G – SUBJECT MATTER EXPERTS

Lisa Beury-Russo – National Cyber Exercises and Planning Program (NCEPP), Office of Cybersecurity & Communications (CS&C), National Protectorate & Programs Directorate (NPPD)

Chris Boyer – Assistant VP, Global Public Policy, AT&T

John Carlson – Financial Service Sector Coordinating Council and Financial Sector Information Sharing and Analysis Center (FS-ISAC)

Caitlin Durkovich – Assistant Secretary, Office of Infrastructure Protection, NPPD

Tom Fanning – CEO, Southern Company

John Felker – Director, National Cybersecurity and Communications Integration Center (NCCIC), CS&C, NPPD

Leonard Gentile – Office of Intelligence and Analysis, DHS

Amias Gerety – Acting Assistant Secretary for Financial Institutions, Department of the Treasury

Jennine Gilbeau – Chief, NCEPP, CS&C, NPPD

Greg Gist – Financial Services Sector Coordinating Council

Patricia A. Hoffman – Assistant Secretary for the Office of Electricity Delivery and Energy Reliability, Department of Energy

Helen Jackson – Section Chief, Stake Holder Engagement, CS&C, NPPD

Neil Jenkins – Acting Director for Enterprise Performance Management, CS&C, NPPD

Sean Kanuck – Office of the Director of National Intelligence

Laura Laybourn – Director, Stakeholder Engagement and Cyber Infrastructure Resilience Division, CS&C, NPPD

Donald 'Doc' Lumpkins – Director, National Integration Center, FEMA

Jeanette Manfra – Counselor to the Deputy Secretary

Mark Neighbors – DHS Office of Policy

Jon Noetzel – NCEPP Support Task Lead, CS&C, NPPD

Andy Ozment – Assistant Secretary, CS&C, NPPD
Ed Roback – Deputy Director, Office of Critical Infrastructure Protection and Compliance Policy, Department of the Treasury

Susan Rogers – Director, Financial Sector Information Sharing and Analysis Center

Phyllis Schneck – Deputy Under Secretary, CS&C, NPPD

Jennifer Silk – Senior Advisor, Office of the Secretary, Department of Energy

Suzanne Spaulding – Under Secretary, NPPD

Lisa Devon Streit – Deputy Assistant Secretary, Infrastructure Security and Energy Restoration, Department of Energy

John Suver – Financial Sector Information Sharing and Analysis Center

Brian Tishuk – Financial Services Sector Coordinating Council

Greg Touhill – Deputy Assistant Secretary, CS&C, NPPD

Brandon D. Wales - Director, Office of Cyber and Infrastructure Analysis (OCIA), NPPD

This page is intentionally left blank.