THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on Information and Communications Technology Mobilization

November 19, 2014

TABLE OF CONTENTS

EXECUTIVE SUMMARY

"*Cyber threats pose one of the gravest national security dangers that the United States faces… (I)t's clear that much more work needs to be done to enhance our cybersecurity. America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas.*"[1] – President Barack Obama

In February 2014, the National Institute of Standards and Technology (NIST) released a Cybersecurity Framework highlighting best practices and standards across the categories of identify, protect, detect, respond, and recover to assist organizations with better managing cyber risk to our critical infrastructure. The year-long development of the Cybersecurity Framework reflected the changing environment within which the Nation operates, an environment where threats, both natural and man-made, could threaten the "engine for economic growth and platform for the free exchange of ideas."[2]

The evolving cybersecurity threat landscape is increasingly complex and poses challenges of an unprecedented magnitude. Studies estimate that global crime extracts 15-20 percent of the value created by the Internet ($375 billion) and that cybercrime is approximately 0.64 percent of U.S. GDP ($107 billion).[3] At the same time, 33 nations include cyber warfare in their military planning and organization and "some states include specific plans for informational and political operations."[4] Further complicating the environment are other sophisticated threat actors, including cyber terrorists, organized crime, and "hacktivist" groups such as Anonymous. While most media attention focuses on criminal and nation-state actors, catastrophic natural events, such as disruptions in space or weather, add an additional layer of complexity and could also lead to a national security event with a cyber component.

Industry in general, and the President's National Security Telecommunications Advisory Committee (NSTAC) members' companies in particular, are aware of and responding to this challenging reality, making constant improvements to better identify, protect, detect, respond to, and recover from cyber events, and investing in people, processes, and technology innovation to deliver network and system resilience and protect customers. In the course of examining historic cyber events, the NSTAC noted that what were formerly considered high-profile events are now routinely treated as "business as usual." However, the evolving cyber risk environment may soon present national and economic security challenges that test industry's capability to respond alone, requiring the Nation to evolve, strengthen and clarify roles in the essential partnership between the private sector and Government. While Government and industry have developed or are currently advancing or evolving programs, practices, and methodologies to share threat

[1] White House, Statement by the President on the Cybersecurity Framework, February 2, 2014, www.whitehouse.gov/the-press-office/2014/02/12/statement-president-cybersecurity-framework.
[2] Ibid.
[3] Center for Strategic and International Studies (CSIS), *Net Losses: Estimating the Global Cost of Cybercrime*, June 2014, http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.
[4] James A. Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization," CSIS, 2011.

information, there exists no effective methodology that currently supports the rapid mobilization and coordination of critical commercial sector assets to respond to a large-scale incident of national security concern. To address this national security and emergency preparedness (NS/EP) communications need, the National Security Council of the Executive Office of the President asked the NSTAC to:

- Identify conditions, triggers, thresholds, and situations that might require increased operational coordination across industry, as well as between industry and Government;
- Identify critical commercial assets, functions, and/or capabilities that, if operationally coordinated, would be helpful or are necessary to respond to a cyber-related event of national significance;
- Recommend an operational framework that: (1) allows for agile, effective, and distributed implementation across numerous stakeholders, resulting in a coherent, unified, and dynamic national response; and (2) guides, informs, and prioritizes response across the full spectrum of NS/EP events with cyber implications; and
- Identify an operational structure or construct to coordinate assets at each threshold considered, detailing which entities would exercise what roles, as well as suggested approaches for training and exercises of such contingencies.

Numerous NSTAC reports to the President address operational, coordinated, Government-industry activity in support of NS/EP goals. One of these reports led to the creation of the National Coordinating Center for Telecommunications (1984). More recently, the NSTAC's *Cybersecurity Collaboration Report* was instrumental in addressing the environment and capabilities now evidenced by the Information Sharing and Analysis Centers referenced throughout this report.[5] In this tasking, the NSTAC is specifically focused on addressing how commercial capabilities or functions could be operationally coordinated to address a national security event with a cyber component. While current information sharing and collaboration across the total national cybersecurity enterprise remains unfinished work, this is not the NSTAC's focus. Instead, the NSTAC was specifically asked to focus on Government-industry collaboration at the highest levels of threat and national emergency.

In addition, the NSTAC did not address laws associated with current information sharing or large-scale cyber incident response. The NSTAC is fully aware of concerns associated with legal limitations regarding information sharing as well as uncertainties associated with Government's authority to provide the waivers or indemnifications that might be necessary to support cyber incident response *in extremis*. At the outset, the NSTAC tasking excluded an analysis of legal authorities since a determination of the operational efficacy of the NSTAC's recommendations would be a pre-requisite to an examination of legal authority.

In this report, the NSTAC outlines a unified risk assessment approach that suggests when increased operational coordination within industry, as well as between industry and Government, might be required, and highlights the level of Government support and collaboration in a five-

[5] NSTAC *Cybersecurity Collaboration Report: Strengthening Government and Private Sector Collaboration Through a Cyber Incident Detection, Prevention, Mitigation, and Response Capability.* May 2009. Available at: https://www.dhs.gov/sites/default/files/publications/NSTAC%20CCTF%20Report.pdf

level cyber condition graphic. The NSTAC finds that certain information and communications technology (ICT) functions are likely necessary to support incident management for large-scale cyber events. Those functions are provided by a diverse set of organizations, referred to as ICT enablers. The NSTAC provides insights into characteristics of the ICT enablers and highlights some of the unique challenges facing the global ICT enabler community while norms for behavior are being developed. Finally, the NSTAC provides a notional template for how the ICT enablers could collaborate with each other, as well as how ICT-enabler support might be integrated into current national cyber incident response plans and response bodies.

Given the delicate state of international dialogue on Government and industry ICT activities, it became increasingly clear throughout the NSTAC examination and development of this report that industry mobilization activities, particularly those directed by or in coordination with a national Government, must be as transparent, inclusive, and respectful of the complexities of the global economy as feasible. Many of the companies that would be critical to a successful mobilization framework, both U.S.-based and foreign-owned, are multi-national corporations with significant international business operations; valid concerns surrounding the nature of that collaboration could undermine the ability of those companies to operate globally. The resulting reduced competiveness within the global ICT industry has a measureable negative impact both domestically and globally. At the levels contemplated, any ICT mobilization truly becomes an international undertaking with global implications and consequences, given the interconnected nature of the cyber ecosystem, the global distribution of cyber ecosystem functions and capabilities, and the decentralized operations of cyber bad actors. Consequently, successful cyber response must be a multi-stakeholder, multi-jurisdictional endeavor.

With these challenges in mind, and during its deliberations, the NSTAC frequently articulated a number of principles to guide the appropriate interaction of industry and Government during mobilization activities. These principles are not limited to the U.S. Government; in fact, these principles may provide a solid foundation to guide Government-industry cyber response planning in any forum worldwide.

- Governments should not interfere with industry cyber risk management objectives and actions, and should limit requests for industry action to preservation, protection, defensive or sustainment objectives;
- Governments should consider the international nature of the cyber ecosystem when examining response actions, and should collaborate with other governments on mobilization objectives and actions; and
- Government should consult with industry on mobilization objectives and actions to the extent industry could be involved or implicated.

With these principles in mind, the NSTAC found that between "business-as-usual" cyber response and "national emergency" response, there lies a transitional zone wherein closely-coordinated information flow and actions would likely help to contain developing crises, minimize duration and impact, and accelerate return to normal operations. At the extreme, it is also possible to envision some set of conditions, events or circumstances—in isolation or linked to geopolitical or economic events—where Government direction may be needed in order to ensure continuity of Government and the national economy, and to mitigate damage. In the absence of a clear understanding of what must be preserved, protected, or recovered in a cyber

event of national significance, however, it is difficult to meet the full objectives of the ICT mobilization tasking.

The NSTAC recognizes certain limitations in its own ability to progress beyond this design phase. Principal among these limitations is the fact that the discussions necessary to complete the tasking will require great sensitivity. Further, these discussions must include both representatives of the ICT enablers and Government representatives from across the national security domain. As presently constituted, the NSTAC cannot adequately represent all the ICT enabler domains.

To that end, the NSTAC recommends a path and process detailed within this report to meet the last objectives of the initial tasking: to better guide, inform, and prioritize response across the full spectrum of NS/EP events with cyber implications; and to identify an operational structure to coordinate assets at each threshold considered, detailing which entities would exercise what roles, as well as suggested approaches for training and exercises of such contingencies.

The NSTAC recommends the President take the following actions to ensure the Nation is prepared to manage a cyber-related event of national significance:

- Identify and convene a representative group of organizational representatives reflecting the defined ICT functions as described herein and national security organizations of Government.
  - — Appoint a suitable Federal official to coordinate and facilitate the work of this group.
  - — Charge the group to describe mutual national priorities and objectives for protection, prioritization, and/or recovery, and to define in actionable detail the actions, options, authorities, statutory provisions, indemnifications, information flow, waivers, and other processes specific to requesting resources from both Government and industry for those circumstances.
  - — Having thus defined the national priorities and objectives, identify the key functions and related stakeholders necessary to support them, and the specific events, conditions, circumstances and/or actions which will serve to trigger and invoke the protections defined above.
  - — Conduct an analysis of current NS/EP legal and policy authorities implicated by the identified national priorities and associated actions as identified above. To the extent current legal frameworks do not provide sufficient authorities to meet NS/EP goals, identify the maximum capabilities currently supported by law, thus establishing current operational boundaries, and produce a report identifying changes in current laws that would facilitate the level of coordinated protections desired.
  - — Examine existing response frameworks, mechanisms, bodies, and constituencies, and adapt, expand, or revise them, as appropriate, to meet recommended ICT response capabilities.
- Create a comprehensive training, education, and exercise regime designed to enhance and maintain readiness by all Government and industry participants in this program.
  - — Develop a timeline for introduction and testing of these procedures in progressively-

complex and large-scale exercises, leading to involvement in the National Exercise Program and National-Level Exercises as soon as practicable.

— Provide processes to examine feedback and exercise lessons learned, in order to revise and refine procedures as appropriate and as threat conditions evolve.

— Establish accountability and ownership across the Federal Government for follow-up on lessons learned and identified gaps to produce an improvement plan, a plan of action, and milestones, and to create a methodology for testing those improvements in succeeding exercises.

- Develop global norms for national cyber response in partnership with industry, incorporating industry expertise and experience to the maximum extent possible.

1.0 INTRODUCTION

1.1 Scoping, Charge, and Methodology

In November 2013, the Executive Office of the President requested the President's National Security Telecommunications Advisory Committee (NSTAC) examine the implications of the operational coordination of critical commercial assets or capabilities to facilitate a coordinated information and communications technology (ICT) response to a cyber-related event of national significance. In May 2014, the NSTAC concluded its scoping effort and determined that the policy and doctrine needed to govern a response to cyber events of national significance are incomplete. Furthermore, the effort found that there was a need for, and benefits from, developing a national ICT response coordination capability. The NSTAC indicated it would further examine three fundamental areas: (1) the conditions, triggers, and thresholds for increased coordination across industries, as well as between industry and Government; (2) a methodology and process for identifying assets, functions, and/or capabilities; and (3) an operational framework and operational structure for this coordination effort. Specifically, the NSTAC determined that it would:

- Research and identify conditions, triggers, thresholds, and situations that might require increased operational coordination across industry, as well as between industry and Government;
- Research and recommend a methodology by which Government and industry can identify critical commercial assets, functions, and/or capabilities that, if operationally coordinated, would be helpful or are necessary to respond to a cyber-related event of national significance;
- Research and recommend an operational framework that: (1) allows for agile, effective, and distributed implementation across numerous stakeholders, resulting in a coherent, unified, and dynamic national response; and (2) guides, informs, and prioritizes response across the full spectrum of national security and emergency preparedness (NS/EP) events with cyber implications; and
- Identify an operational structure or construct to coordinate assets at each threshold considered, detailing which entities would exercise what roles, as well as suggested approaches for training and exercises of such contingencies.

Through the course of the initial scoping effort, the NSTAC received a number of Government briefings on plans, exercises, programs and policies associated with this topic, including: (1) the Department of Homeland Security's (DHS) Cyber Capabilities Planning Framework; (2) the interim draft *National Cyber Incident Response Plan* (NCIRP); (3) the Cyber Storm Exercise Series; (4) the 2012 National Level Exercise; and (5) the Civil Reserve Air Fleet Program. During the scoping effort, the subcommittee also recognized that if a cyber-related event of national significance occurred, there may be international implications; the Government may have unique authorities necessary to address the issues; and citizens may expect their Government to act and even lead. That said, the capabilities necessary to develop and implement an effective response would largely reside within the private sector.

As such, the activities during the research phase first focused on current industry practices and how industry engages with Government for support or assistance at less extreme levels to respond to cyber events. In particular, the subcommittee assessed if the private sector could mobilize collectively on its own and, if so, what triggered industry self-mobilization and if this mobilization was sufficient. If mobilization gaps existed, the NSTAC assessed if there were further steps industry could take to improve this capability. The NSTAC then turned its focus to the touch-points or intersections where Government support, collaboration, or coordination better enabled private sector response. During this stage, the NSTAC sought to determine if there were barriers to private sector response activities that Government might remove upon request, how industry could make these requests and to whom, as well as what type of support industry might ask of Government; in particular, the NSTAC considered regulatory relief, indemnification, public outreach and education, and international coordination. The NSTAC recognized these as several potential tools available to help the Nation approach strategic cyber defense policies. The NSTAC also considered if there were triggers that might lead Government to request industry mobilization and if there were triggers or thresholds after which the presumption of "industry-led mitigation with Government support" might become "Government-led mitigation with industry support."

The synthesis of these two stages of review permitted the NSTAC to understand how industry and Government respond to cyber-related crises within their own domains, powers, and capabilities. In so doing, the NSTAC identified opportunities to enhance these respective approaches by viewing national cyber defense holistically. This report provides recommendations towards these ends.

To inform its research, the NSTAC received briefings from subject matter experts representing Government and industry on different topics, including:

- Industry incident response capabilities at the company, Information Sharing and Analysis Center (ISAC), and trust-group levels;
- How past cyber incidents were addressed by industry, the National Cybersecurity and Communications Integration Center (NCCIC), and the Cyber Unified Coordination Group (UCG);
- The emerging role of the National Guard in support of the Department of Defense's (DOD) domestic cyber defense strategies;
- A baseline understanding of what Government might consider important to protect or recover in the aftermath of a cyber event of national significance; and
- The role of the private sector response in creating an environment of cyber deterrence and stability globally.

In addition, the NSTAC was briefed on findings from a cyber exercise conducted by the National Council of ISACs through the course of this initiative. These briefings and the NSTAC's discussion provided the foundation for the foundational findings and analysis outlined below.

2.0 FOUNDATIONAL FINDINGS

During the scoping and research phase, the NSTAC engaged subject matter experts across a broad community of industries, as well as cybersecurity experts from the Federal Government, to receive additional knowledge and insights regarding cyber incident response and mitigation practices. As a result of its examination of both the Government and industry current practices to addressing cyber threats, the NSTAC identified a number of findings, highlighted below. These findings provided the foundation for the NSTAC to recommend the conditions, triggers, and thresholds for increased coordination; a methodology and process for identifying assets, functions, and/or capabilities; and an operational framework or structure for coordination and collaboration during a cyber event of national significance.

2.1 Findings – Government Briefings

The NSTAC identified the following findings from Government briefings:

- Substantive progress has been made within Government to more effectively coordinate with each other and with industry.
- While the United States is working with international allies to examine the challenge of blended international networks or assets, the protocols or doctrine associated with cyber response for U.S. interests located internationally are unclear.
- The goal of creating a common operating framework for Government and industry remains elusive. This limits Government's and industry's ability to assess impacts and develop an effective response strategy.
- Recent cyber exercises consistently highlight weaknesses in the current interim draft NCIRP, such as:
  - There are no defined thresholds for what constitutes a cyber event of national significance;
  - There are no definitive guidelines on how to respond to a cyber incident;
  - The interim draft NCIRP is Government-centric and does not articulate how activities and capabilities between the private sector and Government can be coordinated for a unity-of-effort; and
  - The current Cyber UCG process does not lend itself to the development of response mitigations in a timeframe necessary to mitigate a cyber incident of national significance.
- Government response support plans are generally built upon geographic or national boundaries, though cyber events are not bound by the geographic jurisdictions.
- The Government considers the primary role of the private sector is to serve as a first responder during cyber incidents. The ability of the private sector (e.g., ISACs) to aggregate and correlate like incidents is considered foundational to cyber awareness and the creation of a common operating framework.
- The Government has identified what it considers to be the Nation's most cyber-dependent critical infrastructures under Section 9 of Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*. It has begun to mature, identifying high-level cyber

functions—in both the private sector and Government—that should be the focus of protection or restoration efforts before, during, or after a cyber incident.

- The interim draft NCIRP identifies the Cyber UCG as the interagency and inter-organizational coordination body that incorporates public and private sector officials to collaborate identification, protection, detection, response, and recovery actions in a significant cyber incident; however, current UCG industry and Government participation needs to mature from a situational awareness body to one that can form action-oriented incident management teams.
- The DHS Cyber Capabilities Planning Framework provides an initial means to identify and organize cyber-related capabilities across the Government and the private sector. With the exception of enterprise-level requests for technical assistance, it is not clear how industry would request Government capabilities to address a national security event with a cyber component.
- The National Security Council has identified four gaps in the Government's ability to effectively execute cyber response, including: (1) understanding and identifying the kind of response options and capabilities and courses of action industry has; (2) receiving private sector corroboration of threats and a perspective on the potential consequence of threats; (3) knowing private sector's current posture and ability to handle threats; and (4) identifying what the private sector might expect, request, or need from Government to address threats.

2.2 Findings – Industry Briefings

The NSTAC identified the following findings from industry briefings:

- In general, industry cyber response is built upon the foundation of incident response at the enterprise (i.e., corporate information technology [IT] asset) level. The enterprise response capabilities are a function of enterprise and their vendor capabilities.
- At a high level, the step-phases for current industry response protocol include:
  - If an enterprise detects and cannot mitigate an incident, then, optimally, the enterprise seeks information and/or support from similar enterprise entities within their sector through an ISAC or trust group. In addition, enterprises optimally report on incidents they were able to mitigate, through their ISACs, for dissemination to sector and cross-sector peers. The sector-ISAC or trust group serves several functions:
    - The ISAC acts as an information-sharing and support mechanism for the impacted enterprise;
    - It aggregates and correlates instances of incidents within the sector and acts as a conduit to other sector ISACs for support, if required;
    - The ISAC generally acts as the point for notification to Government (e.g., NCCIC) if potential or actual impacts are likely to implicate other entities within that sector or may affect other sectors, or if there are impacts within the sector that are occurring in more than one geographic region;
    - ISACs act as the NCCIC's primary point for information dissemination if the NCCIC needs to send information to a specific sector(s); and

  - ISACs share and disseminate information through the National Council of ISACs. Based on the criticality and scale of the potential impact on the sector, it is possible that a sector issue may rise to a level warranting national attention.

— If multiple sector ISACs report potential or actual impacts related to the original incident, then this issue may rise to a level warranting national attention. Some entities belong to more than one ISAC, which also provides some level of multi-sector awareness.

- While ISACs provide correlated information sharing for the benefit of enterprises within their sector, their ability to correlate enterprise-related threat information among and between the sector-ISACs is limited and needs to be enhanced.
- While the framework for the UCG contemplated representation from each of the 16 critical infrastructure sectors, not all sectors are represented. Representation of all 16 critical infrastructure sectors was perceived as a means to ensure early situational awareness of potential sector impacts. In addition, as structured, the Cyber UCG is not sufficiently agile or effective in responding to incidents.
- With the exception of coordinated law enforcement activities, private sector entities have driven historical cyber response events. Therefore, mobilization efforts should remain aligned with industry as the first responder; should meet the privacy, security, and trust concerns of industry; and should focus on developing a unity-of-effort approach between industry and Government.
- While there is inter-sector cyber correlation and coordination, the goal of a joint, integrated, and cross-sector information sharing and analysis capability to produce timely, reliable, and actionable situational awareness remains elusive and must be enhanced.

3.0 ANALYSIS: FOCUS ON CONDITIONS FOR INCREASED COORDINATION

Listed in Section 1.1, this section addresses the NSTAC's "Research and [identification of] conditions, triggers, thresholds, and situations that might require increased operational coordination across industry, as well as between industry and Government."

In the analysis to identify conditions, triggers, thresholds, and situations that might require increased operational coordination across industry, as well as industry and Government, the NSTAC reviewed more than 20 historical cyber events as well as six events of potentially high impact.[6] The NSTAC leveraged the NCCIC Critical Information Requirements (CIR) Impact Scale as a rough guide for an initial characterization of escalation of an actual or potential cyber-related event. The CIR Impact Scale is used to guide the NCCIC's incident assessment and immediate NCCIC actions, notifications, and reporting requirements. While Table 1 is not intended to define "cyber incidents of national significance," the following impact levels provide a useful example of an incident scale.

[6] Please refer to Appendix D, List of Historical Events, for a listing of historical cyber events.

Table 1: Sample Incident Scale Impact Levels

Impact Level	Impact Characterization
National	• Actual or potential impacts are likely to occur on a national scale. • Any actual or potential impact occurring in more than one sector or region. • Threats to cyber and communications infrastructures on a national scale.
Sector	• Actual or potential impacts are likely to occur in one of the Nation's 16 critical infrastructure sectors. • Entities within sectors often share the same types of infrastructure and therefore share similar risks, thus warranting escalated attention.
Regional	• Actual or potential impacts are likely to occur in one specific geographic location. • Current or potential impacts to a specific region could cause serious harm to the region, thus warranting escalated attention.
Entity (Enterprise)	• Actual or potential impacts are likely applicable to only one organization. • The possibility of cascading or potential impacts to a sector or region is unlikely, or cannot be ascertained at this time.

Implicit in the CIR approach is concern that the incident's characteristics could escalate to disruption, corruption, or destruction of sector and/or regional resources, or critical infrastructures where a cybersecurity incident could reasonably cause catastrophic impacts to our national security, economic security, public health and safety.[7]

Using this impact scale to review recent and historical incidents, the NSTAC noted that incident response at the entity or enterprise level is ongoing, constant, and considered business as usual (BAU). If the enterprise cannot address the incident, which might indicate that other enterprises are equally unable to mitigate, then the enterprise would escalate the incident through trust groups or ISACs. In this event, the vast majority of enterprise incidents are resolved with the support and collaboration of similar enterprises. This finding affirms the value and role of information sharing at the enterprise level through ISAC mechanisms.

At the opposite end of the scale, the NSTAC noted that while there have been numerous high-profile cyber events that warranted national attention, using the NCCIC CIR as an approximate gauge, none ultimately were considered a cyber event of national significance. Upon review of these high-profile events, the NSTAC noted that the fundamental incident management actions occurred through private sector collaboration or mobilization at a much smaller scale, limited to a group of actors that had the technical competence and ability to develop and propose appropriate mitigations to address the core vulnerability. This group is distinct from the affected community, which constitutes those end users with the responsibility for managing the actual manifestations of the consequences of the attack.

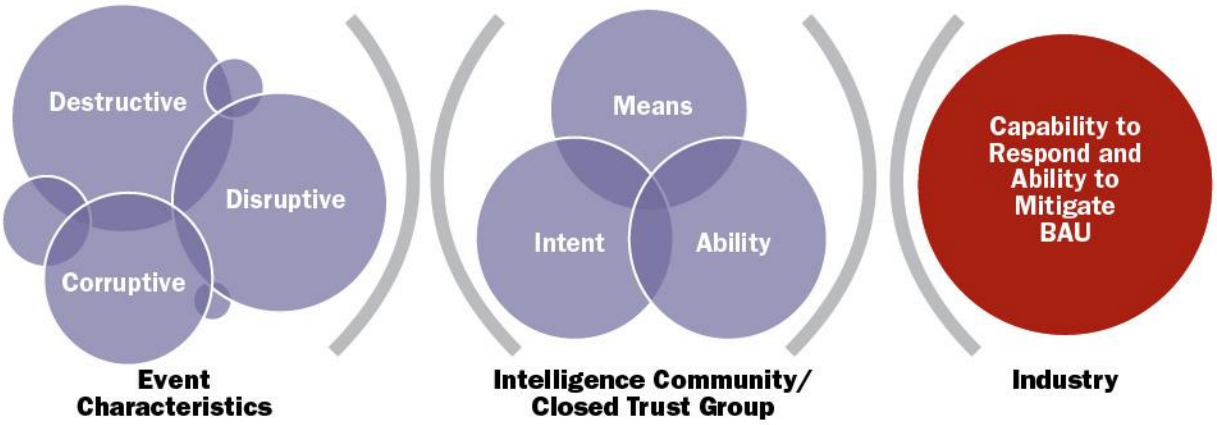
[7] White House. Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, and Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, February 12, 2013.

The NSTAC then focused on events where there was collaboration with Government to mitigate ongoing cyber incidents. In these cases, the nature of the incident was fostered by threat actors with the intent, means, or capability to continue escalating the cyber event. Under these circumstances, representatives from industry and other trust groups felt that the incident would continue unabated without collaboration and support from Government, in the form of law enforcement. With this view, the NSTAC developed a means to understand both potential and actual incidents from a unified risk assessment approach to assess if an incident would or should escalate.

Finding: The unified risk assessment of a potential or actual impact provided an indicator of whether an issue should escalate or de-escalate. The assessment is a function of three criteria/parameters, including:

- Event Characteristics: Does the potential or actual event (or series of events) manifest characteristics that could result in substantive disruption, corruption, or destruction of critical infrastructure, EO 13636 Section 9 entities, and sector resources?
- Intelligence Sources: Do the perpetrators (i.e., threat actor[s]) have the means, intent, or ability to escalate the potential or actual event to an event of national significance?
- Capability to Respond: Based upon prior knowledge, does industry have the capability to respond and address the incident, without changes in legal authority, rules of engagement, or operating framework?

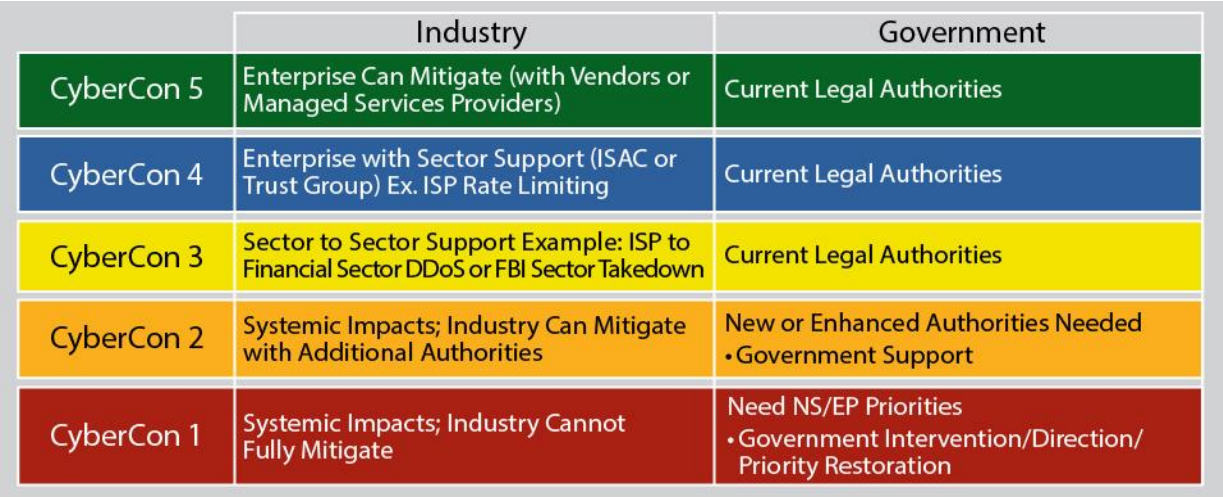
Figure 1: Notional Unified Risk Assessment Process for Mobilization



Combining this assessment protocol with the NCCIC impact criteria, the NSTAC generated a means to characterize the Cyber Condition (CyberCon) at any given time, reflecting the increased level of collaboration and/or support required for enterprises and sectors to respond to cyber incidents, as well as when an incident would likely warrant increased coordination between industry and Government. Similar to the NCCIC CIR, and predicated on the foundation of enterprise/entity response, the five-level CyberCon represents an escalation tier reflecting the increased level of collaboration and/or support required for enterprises and sectors to respond to

cyber incidents. Shown in Figure 2, below, this CyberCon was developed solely for the purposes of the NSTAC analysis and is not intended to replace any existing industry or Government alert condition protocols.

Figure 2: Escalation-Cyber Event Graphic



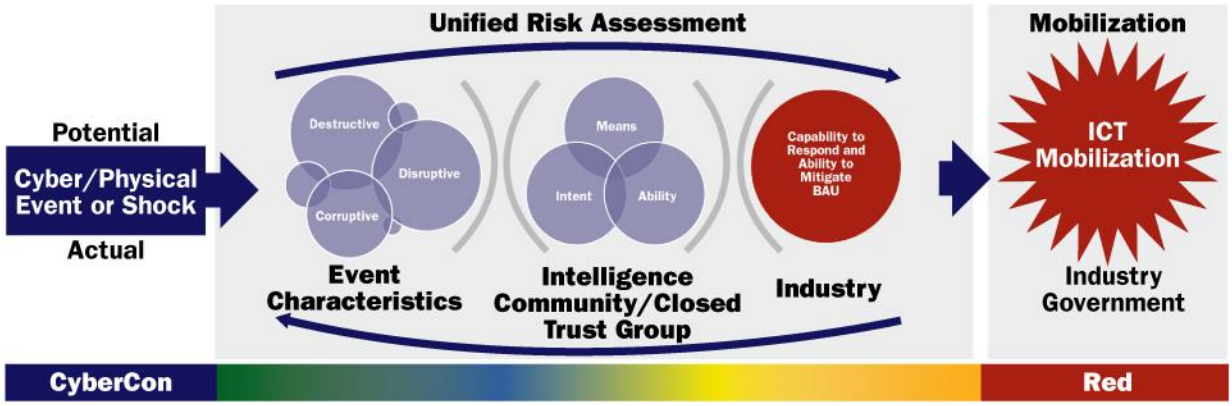
The five CyberCon tiers are described as follows:

- GREEN: The enterprise/entity (with vendors) alone can address the cyber event.
- BLUE: The enterprise can address the cyber event with support from sector resources, such as ISACs and trust groups. One example of this level would be an Internet service provider (ISP) requesting short-term rate limiting support from fellow ISPs.
- YELLOW: At this level, support to mitigate an event is drawn from resources outside an individual sector using current legal authorities. Two recent activities that would be categorized as yellow include ISP defense against financial services distributed denial-of-service attacks and the recent criminal takedowns coordinated across sectors by the National Cyber-Forensics and Training Alliance.
- ORANGE: At this level, the assessment suggests that industry can mitigate and respond; however, new or incremental Government support would likely be indicated, which may take various forms. At the same time, at this level, the Government would enhance its own attention and response to the incident at hand, which would likely yield increased Government-industry coordination.
- RED: At this level, industry is unable to fully mitigate the incident, even with additional authorities. If the incident cannot be fully mitigated, industry would want recommendations or direction on the priorities for protection (e.g., pre-incident) or recovery (e.g., post-incident). Specification of national security priorities is a responsibility inherent to

Government. For purposes of this NSTAC report, the RED level is characterized as ICT mobilization.[8]

Figure 3, below, provides an alternative way to characterize the iterative, escalatory process of the five CyberCon levels.

Figure 3: Notional Unified Risk Assessment Process for Mobilization with Cyber Condition Levels



In general, the GREEN/BLUE/YELLOW levels can be characterized as BAU, where industry can mitigate and respond without new or incremental Government authorities. Collaboration and cooperation with Government is considered BAU at these stages, as the response can utilize existing legal authorities. It is important to note that the CyberCon determination is a mutual assessment within industry at lower levels, and between Government and industry at higher levels.

To some degree, the five-level CyberCon aligns with the NCCIC CIR, which incorporates entity, sector, and regional impacts throughout the alert levels and identifies the potential need for additional authorities to address a multi-sector threat. The potential need for additional authorities suggests enhanced pre-coordination and collaboration mechanisms with Government to mitigate those concerns. The distinction between the CyberCon developed for this report from other alert condition guidelines is that "ability (and authority) to mitigate" is the factor to determine if the issue must be escalated.

3.1 Current Operational Gaps

In general, the maturity of cyber risk management at the enterprise level is uneven across sectors. In February 2014, the National Institute of Standards and Technology (NIST) released a Cybersecurity Framework highlighting best practices and standards across the categories of identify, protect, detect, respond, and recover so that organizations can better manage cyber risk

[8] CyberCon 1, referred to as Mobilization, is the highest tier of "response." The term "mobilize" implies Government direction and/or prioritization in the implementation of industry response and is defined as "to organize or adapt (industries, transportation facilities, etc.) for service to the government."

to critical infrastructure. Within the five Framework categories, however, the practices associated with the category of "respond" are even less developed.[9] With this in mind, the NSTAC set out to assess current operational gaps in the context of the varying collaboration levels.

3.1.1 GREEN, BLUE, and YELLOW Levels

At this time, the ability to correlate cyber events within all sector ISACs is limited. While some sector ISACs have strong capabilities to correlate, collaborate, and coordinate sector-level events, as well as maintain mechanisms to cross-correlate and coordinate between ISACs through the National Council of ISACs, the ability to quickly assess and identify potential cyber impacts within all sectors is still not fully developed.

While there is active participation and robust productivity between individual enterprises and various ISACs/trust groups, comparable participation in these types of forums is still limited in some sectors.[10] Liability concerns associated with information sharing are still frequently cited as a limitation impeding enhanced participation in these forums. The NSTAC has previously examined these issues, including in the 2003 *Legislative and Regulatory Task Force Report: Barriers to Information Sharing*.[11]

Previous NSTAC Review: Information Sharing[1]

In 2003, the NSTAC recommended that the President direct the appropriate departments and agencies, in coordination with industry to:

- Develop a process to resolve multi-jurisdictional (Federal, State, and local) conflicts within the appropriate boundaries of Federalism and national, homeland, and economic security;
- Work with Congress to modify the CII Act so that DHS is the clearinghouse and sole dispenser of CII information;
- Encourage Congress to extend the protections of the CII Act to cover departments and agencies other than DHS and, if other agencies should be designated as such, the NSTAC recommends that they adopt the same rules and procedures as DHS for handling CII; and
- Work diligently with Congress to ensure the CII Act's provisions remain intact.

[1]*Please refer to Appendix F, Previous NSTAC Recommendations, for further details regarding the NSTAC recommendations.*

[9] Ponemon Institute, "Cyber Security Incident Response: Are we as prepared as we think?" January 2014.

[10] DHS recognizes these limitations and has developed programs such as the Cyber Information Sharing Collaboration Program (CISCP) to afford enterprises the opportunity to share information not with DHS and supplement other existing sharing mechanisms. CISCP shares cyber threat, incident, and vulnerability information in near-real time, and enhances collaboration to better understand the threat and improve network defense for the entire community.

[11] NSTAC "Legislative and Regulatory Task Force Report: Barriers to Information Sharing" September 2003. Available at: https://www.dhs.gov/sites/default/files/publications/LRTF%20Information%20Sharing%20Report%20%28Sept%202003%29_0.pdf

The capability for cross-correlation of cyber incidents or coordination between ISACs is even more limited. Again, there are exceptions as reflected by the strong inter-ISAC relations between the Financial Services Sector, the Communications Sector, the Defense Industrial Base Sector, and the IT Sector. Nonetheless, limited cross-sector correlation limits early detection and notification of multi-sector impacts, reducing the opportunity to assess the threat and potential national impact, as well as mitigate consequences in a timely manner.

The continued adoption of automated information sharing tools, such as Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) protocols for reporting cyber threat indicators within sectors, coupled with higher-level tools that support aggregated correlation analysis, will support and enhance these capabilities over time. Nonetheless, in the absence of strong cross-sector cyber correlation experience, the goal of a joint, integrated, and cross-sector information sharing and analysis capability to produce timely, reliable, and actionable situational awareness remains elusive and needs to be enhanced. An additional gap identified is the Government's continuing "need to know" approach to sharing timely, reliable, and actionable threat intelligence and information. Much of the information that would be important to making informed risk management decisions is classified, and even the process of creating timely and actionable tear-line products has been challenging. It is incumbent to move to a "need to share" approach, leveraging access to those in the private sector that have necessary clearances. It is also necessary to refine a process, including tear-lines where appropriate, to provide information about tactics, techniques, and procedures—not sources and methods—that would help inform risk management decision-making and incident response.

The NSTAC continues to affirm the development of capabilities associated with enterprise participation in ISACs and other appropriate trust groups. Government and industry should continue to nurture and support these environments and the successes they have demonstrated through sharing cyber threat indicators between peers and Government.

3.1.2 Operational Gaps: Moving from YELLOW to ORANGE

Despite the challenges highlighted above, the ability to disseminate mitigation and recovery options to cyber threats has improved greatly at both the industry and ISAC level, as well as at the DHS NCCIC. Further, there is increased experience in coordinating larger-scale mitigations with law enforcement activities. While some of the larger-scale initiatives have been initiated by law enforcement, others have been at the request of industry. This collaboration has led to enhanced experience in developing a coordinated operational response between Government and a number of industry entities. These initiatives have been successful due to clearly-stated operational objectives, having time to plan the response, and limiting the numbers of parties engaged in the response planning. Additionally, law enforcement was able to leverage existing authorities in achieving the operational response objectives.

It is clear that an ORANGE stage response would require a shift in industry engagement from current DHS and law enforcement protocols. ORANGE is defined as that level where industry can develop the response and implement the mitigations to contain the threat or stop escalation, with additional authorities granted by Government. These new authorities may take any of several forms, such as waivers, indemnifications, and/or access to specific sensitive information

sources. The premise is that because the Government and industry would have mutually agreed that the incident has risen to level ORANGE, such powers and authorities would be extended as a condition of that development. The precise nature and extent of these powers must be negotiated and mechanisms put in place so that different Government entities (e.g., Department of Justice [DOJ] and Department of State) can provide the necessary legal or diplomatic support to react and respond quickly. It is also clear that advanced analysis of the legal authorities needed to support the larger, more comprehensive cyber response capabilities within or across the cyber ecosystem for an ORANGE level incident will be necessary.

Previous NSTAC Review: Cybersecurity Collaboration

The NSTAC's 2009 *Cybersecurity Collaboration Report to the President* recommended that the Government establish a Joint Coordinating Center for public and private sector representatives from various critical infrastructures and key resources sectors to focus on robust information sharing among each other on cyber incident detection, prevention, mitigation, and response. Several of the 2009 NSTAC report findings continue to apply today, including:

- Planning and execution of national cyber incident detection, prevention, mitigation, and response capability requires joint participation of many domestic public and private sector organizations, as well as international entities. Presently, organizations involved in cyber incident efforts are physically separated, functionally disjointed, and lack efficient communications capabilities. Combining all stakeholders into a single Government funded/equipped physical location, with the capability for virtual participation, is necessary for full cybersecurity planning and execution;
- Government and private sector subject matter experts recognize the urgent need for and value of a 24/7 public-private sector collaborative cyber incident detection, prevention, mitigation, and response capability. A phased implementation approach will allow enhanced capabilities to be implemented in an affordable and efficient manner; and
- There is an urgent need to improve upon coordination of existing U.S. and international cyber incident capabilities in both public and private sectors. The need for this capability is growing over time.

Finding: The ORANGE level represents the domain of extensive coordination and collaboration between Government and industry in terms of dynamic protocols and procedures. At lower levels, current practiced behavior should be sufficient to maintain stability and flow in 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. It will be important to thoughtfully 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.

3.1.3 Operational Gaps: RED Stage

As noted in the foundational findings, there 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. While current U.S. priority programs (e.g., telecommunications service priority [TSP]) create a partial policy umbrella for this issue, the TSP program is wholly insufficient for purposes of dealing with RED-level crisis. 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. Since the RED stage of cyber emergency is intended to describe the truly severe degradation of the national ICT base, the expectation is that, at that level, if it is ever achieved, the Nation would essentially be operating on a catastrophic or continuity-of-government footing. Accordingly, at that point, industry would seek to support Government initiatives to defend and preserve the Nation.

Finding: The RED level conceptually represents a cyber emergency of the severest nature and greatest potential impact. At this level, the total commitment of industry to sustain network and system operations will be insufficient to meet the national need. Accordingly, 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.

4.0 ANALYSIS: FOCUS ON "CAPABILITIES"

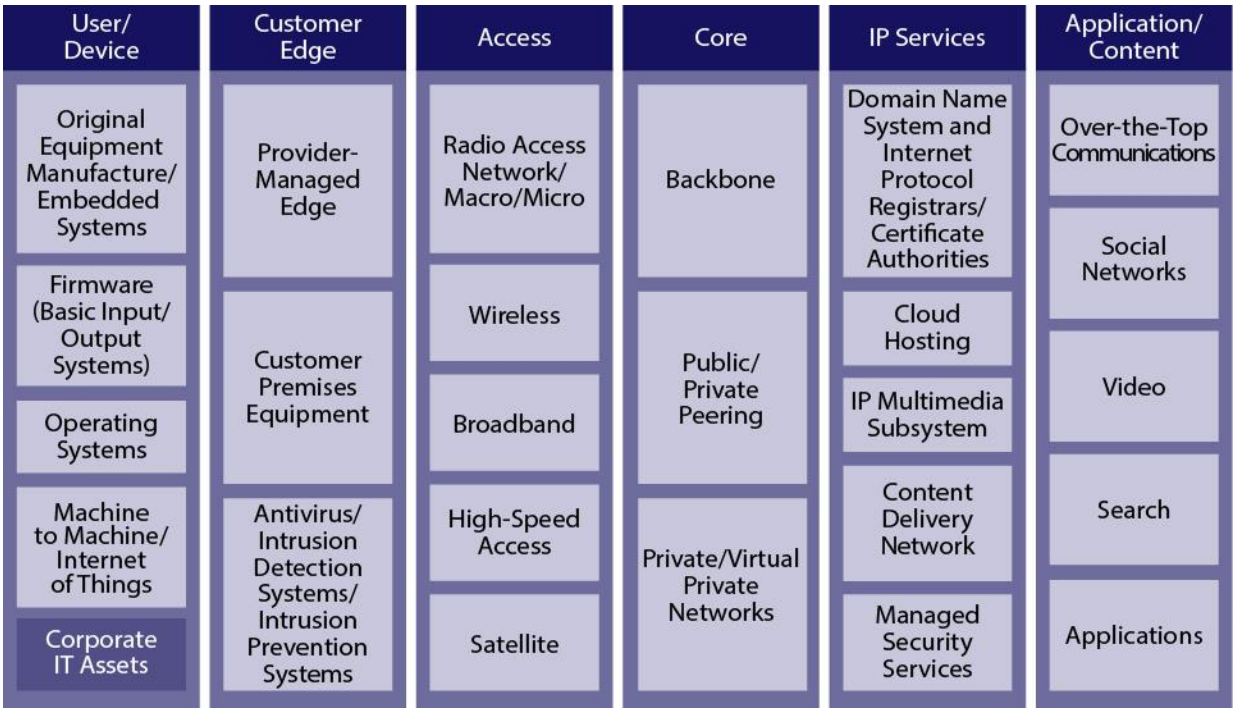
Listed in Section 1.1, this section addresses the NSTAC's "Research and [recommendations for] a methodology by which Government and industry can identify critical commercial assets, functions, and/or capabilities that, if operationally coordinated, would be helpful or are necessary to respond to a cyber-related event of national significance."

The NSTAC applied the same incident reviews used for the trigger/threshold/situation analysis to conduct a review of which entities were impacted, which entities contributed to finding the solution, and who or what operational mechanism entities were used to respond to those incidents. While these historical incidents did not rise to a level of national significance, the NSTAC reviewed additional scenarios that could conceivably escalate to such a level. Both sets of scenarios were used to assess which commercial functions and capabilities were helpful or might be helpful to respond to these events. While the victim(s) changed with each incident or scenario reviewed, the NSTAC found that certain ICT functions were consistently part of creating the solution or were leveraged to assist in implementing the solution. While no single function was common to all scenarios, certain functions occurred enough so as to generate a map of the capabilities that might need to be mobilized to effectively respond to the scenarios examined.

From this review, the NSTAC developed a working model of the functional capabilities (in six categories) associated with the broader global cyber ecosystem. With the exception of the corporate IT assets function, which most closely aligns with enterprise/entity networks, the balance of the ecosystem functionalities are best characterized as services and operations shared and used throughout the global ecosystem. The functions represented in Figure 4, below, enable the cyber ecosystem and are provided by ICT companies.[12] Many of the functionalities are represented, in part, by U.S.-based NSTAC-represented organizations. The entities that provide these functions will, in this report, be referred to as ICT enablers.

[12] Please refer to Appendix C, Glossary, for a definition of the terms contained in this chart.

Figure 4: Cyber Ecosystem Key Players



4.1 Nature of ICT Enablers

The functions that ICT enablers provide are foundational to the global cyber ecosystem. From operating systems to anti-virus an intrusion detection or prevention, local/backbone core transport, certificate authorities, content delivery, and applications, all functions work together to support the global cyber environment. With the exception of some local transport functions, the providers of these functions are multi-national and their products and services are used throughout the world.

Providing these globally-shared functions and services is a large responsibility and, collectively, these enablers act in a fiduciary role for all users of the cyber ecosystem globally. These enablers typically have broad visibility of the global environment, deep technical expertise within their functional space, as well as an understanding of the roles and functions of the numerous enablers within the community. The enablers' global customer base drives their activities towards ensuring that all customers have full access to the capabilities and services they provide, and they take significant care to ensure even-handed treatment of their global customer base. Given the variance in non-disclosure and privacy laws throughout the world, these enablers also generally choose to operate under stricter non-disclosure and privacy environments than entities operating within only one national border.

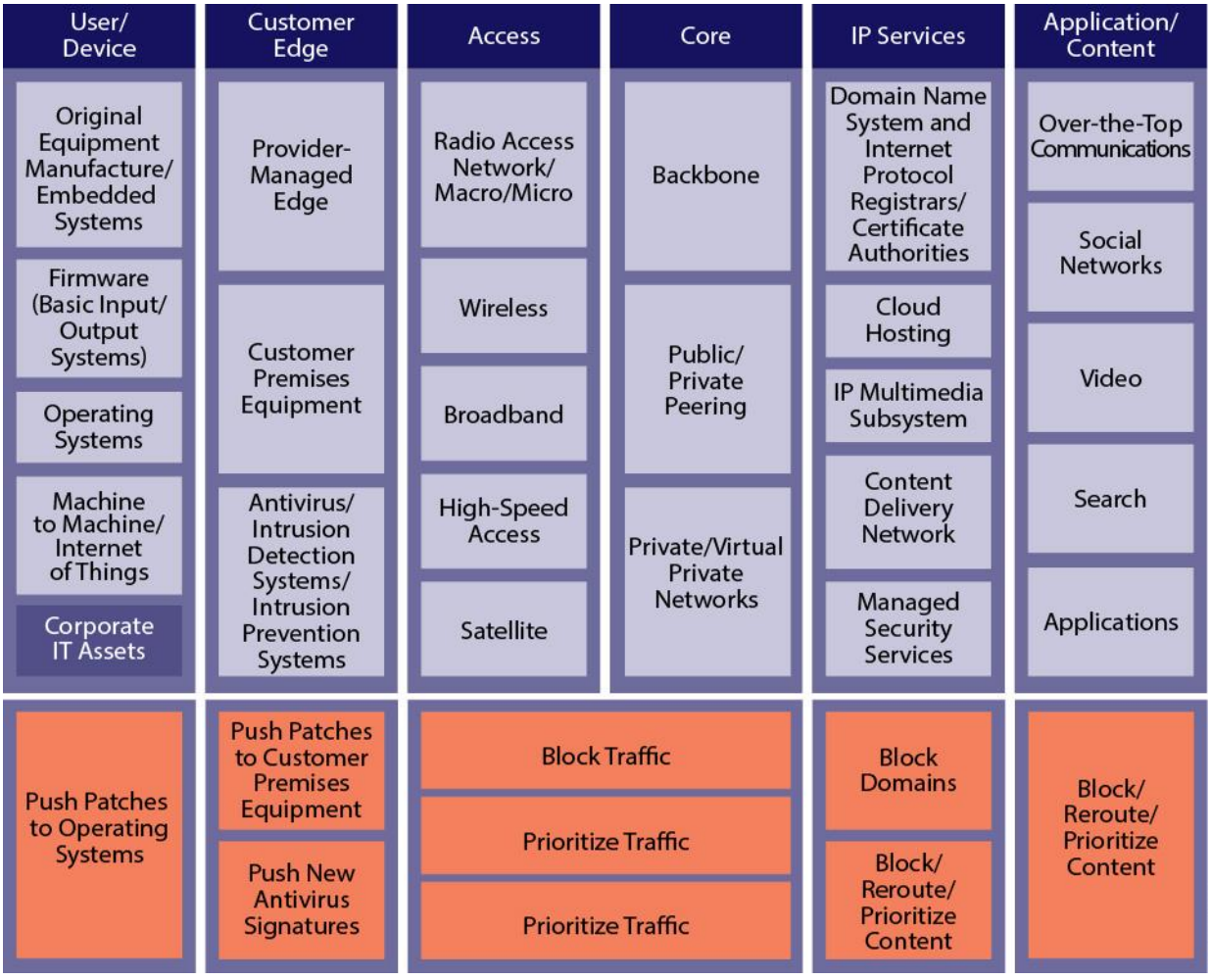
While an attack against enterprise networks generally has a localized impact, a cyber attack against ICT enablers has the potential for far-reaching consequences to the ecosystem. Given the interconnectedness of the gross functional capabilities within the ICT enabler ecosystem, if any two ICT enablers independently identify or are experiencing an incident or incidents, it is

reasonable to more closely examine if those incidents together give rise to systemic consequences. In such cases, the incident should be treated as an event of sufficient magnitude that requires a concerted response beyond a single enterprise or sector.

If there is a major impact to any one of these functions, the ripples will be felt across the globe. As a consequence, the ICT enablers employ extraordinary levels of security to ensure these functions are not compromised, and they have developed incident response capabilities to match. While all enablers have computer security incident response teams (CSIRT), most enablers also have dedicated security incident response teams (SIRT) for product-lines or commercial networks to ensure continuity of the global services they offer. While many of these U.S.-based ICT enablers belong to ISACs for sharing enterprise-related issues, the sharing of information associated with their global products and services is generally conducted in tightly controlled private sector trust groups.

Finally, while incident response at the enterprise level generally has enterprise impact, the reach of incident response by the ICT enablers can have a broad and systematic impact throughout the ecosystem. Figure 5, below, shows a representative example of the gross capabilities of the ICT enablers.

Figure 5: Notional Representation of Gross Functional Capabilities of ICT Enablers



For example, within the access and core categories, there exists the broad capability to block, prioritize, or re-route traffic. While this reach may be necessary to mitigate a major cyber event, these same mitigations could also lead to unintended consequences on end users. These large-scale actions may mitigate the immediate concern at hand; however, legitimate traffic may also be impacted, disturbing the free-flow of information throughout the ecosystem. In the specific case of the ISPs, large-scale blocking, prioritizing, or re-routing of traffic is counter to their global practices (as well as, arguably, to U.S. or global laws and policies) and would undoubtedly have service-level repercussions on customers who rely upon these services to operate. To that end, any response actions taken to address cyber threats must be in proportion to the threat being mitigated, and large-scale response actions will likely require authorities in some form by Government. Comparable arguments can be made for large-scale mitigations taken by any of the ICT enabling functions.

Upon the NSTAC's review of the scenarios that could potentially lead to an event of national significance, the incident management capabilities associated with enterprises or ISACs were not those capabilities necessary to address the systemic issues. Instead, the scenarios that led to such an event potentially implicated multiple ICT enabling functions. The combined mitigation efforts of more than one ICT enabler could have even larger unintended consequences. To the extent that events of national or global significance warrant the mitigation efforts of more than two of the ICT enabler functions, it would be necessary to ensure that potential consequences are contemplated in the development of mitigation strategies and then authorized in some form by Government.

Finding: The response capabilities inherent within enterprises or their ISACs will not likely be the capabilities necessary to address the circumstances in an event of national significance.

Finding: ICT enablers represent the functionalities foundational to the global cyber ecosystem and are most capable to address the threats, develop mitigation strategies, and/or implement systemic remediation.

Finding: The NSTAC believes that ICT enablers likely represent the commercial assets, functions, and/or capabilities that, if operationally coordinated, would be helpful or necessary to respond to a cyber-related event of national significance.

Finding: Coordinated incident response by ICT enablers at ORANGE- or RED-level events may necessitate Government authorities despite the potential for positive impact, as there may be accompanying unintended consequences of such action.

Finding: Properly addressing events of national significance, warranting the mitigation efforts of multiple ICT enablers, will require ensuring that any mitigation strategies developed consider all potential consequences—as well as impacts on all potentially impacted stakeholders, including global Internet users—and are fully authorized by requisite legal and Government authorities in the United States and other relevant jurisdictions.

Finding: Since the global cyber ecosystem is foundationally civilian, the U.S. Government should continue its dialogue to establish global norms for national cyber response and incorporate industry in those discussions to the maximum extent possible.

Unique Challenges of the ICT Enabler Community

Despite the many capabilities associated with this community, there are a number of concerns unique to the ICT enablers that the global community must address over time.

Cyberconflict Issues: Industry (in particular, ICT enablers) will undoubtedly be impacted in the event of cyber conflicts globally. Unlike previous conflicts supported by a defense-specific, industrial base, most of the cyber ecosystem is owned, operated, and powered by civilians. This same ecosystem is used globally by citizens and Governments. Therefore, it is inevitable that the assets of these ICT enablers (products, personnel, equipment, facilities, and networks) will be used in some form or fashion during a cyber conflict. This brings a new factor to the corporate risk profile, for these corporations could arguably be considered "civilians directly participating in hostilities" and become a legitimate target according to the legal definitions of the Geneva Convention.[1]

Government use of these corporate, enabling assets becomes even more problematic if use of those assets in a cyber conflict (even without corporate foreknowledge) is sufficient for the corporate assets to become a legitimate target of war,

> *"…many of the victims of cyberattack—as well as its accomplices—are increasingly likely to be large-scale, private entities playing on the world stage, rather than just nation-states. Accordingly, future (sic. Government) planning needs to account for the Googles, the Microsofts, the Facebooks, the Twitters, and other big players appearing on the scene. A responsible nation needs to decide if it can justifiably use, say, Google services for its own military ends. (And Google will presumably seek to find a way to keep itself from becoming the mere puppet of some irresponsible nation seeking to co-opt it.) These companies will need to carefully consider their roles, knowing that their actions might put their own workers at risk by making them "civilians directly participating in hostilities"—in other words, legitimate targets, okay to hit according to the legal framework of the Geneva Conventions (or at least logical military targets, whether legal or not). Policymakers also must consider whether these companies are entitled to act on their own: If they are the victim of a foreign cyberattack, are they morally or legally permitted to respond aggressively—especially if no state response seems forthcoming? What limits can a hosting government place on the actions of companies located or listed in their territory?"*[2]

The NSTAC acknowledges that these are all questions and considerations that the U.S. Government, in collaboration with other Governments, must address through diplomacy and statecraft. Since the global cyber ecosystem is foundationally civilian, the U.S. Government should continue its dialogue to establish global norms for national cyber response and incorporate industry in those discussions to the maximum extent possible.

[1] Bulletin of Atomic Scientists, "Cyberwarfare ethics, or how Facebook could accidentally make its engineers into targets," http://thebulletin.org/cyberwarfare-ethics-or-how-facebook-could-accidentally-make-its-engineers-targets7404.
[2] *Ibid.*

5.0 ANALYSIS: FOCUS ON OPERATIONAL FRAMEWORKS

Listed in Section 1.1, this section addresses the NSTAC's "Research and [recommendation of] an operational framework that: (1) allows for agile, effective, and distributed implementation across numerous stakeholders, resulting in a coherent, unified, and dynamic national response;

and (2) guides, informs, and prioritizes response across the full spectrum of NS/EP events with cyber implications."

If the ICT enablers would likely need to coordinate an operational response during an event of national or global significance, then determining the means to coordinate these capabilities may address the current operational gap in incident response. The next phase of the NSTAC review focused on leveraging the capabilities of the incident response teams that support the diversity of globally shared products and services.

While the NSTAC review of historical cyber incidents found no cyber event of national significance, a review of those same high-profile events uncovered a number of past scenarios where industry leveraged the combined capabilities of ICT enablers. Common operating characteristics of past mitigation successes included the following:

- Trusted Collaboration: Mitigations were often developed within trusted communities of interest.
- Focused Technical Resources: Participants were limited to technically proficient individuals with relevant skills and/or entities in a position to effect positive change.
- Flexibility: Participants or community members could leverage extended resources, where necessary, outside the core trusted community of interest. For example, a vulnerability in a widely adopted protocol such as Secure Sockets Layer may require several trusted communities to work together to mitigate.
- Corporate Commitment: In some cases, corporate executive officers or other high-level executives are committed to fixing the problem, thus ensuring the appropriate risk acceptance and adequate resourcing. Oftentimes, this commitment is not immediately apparent to incident managers and response leaders.

The NSTAC further found that, with the exception of coordinated law enforcement activities, private sector entities have driven most historical mitigation events; therefore the NSTAC sought to identify and develop an operational framework that would be private sector-driven and meet the privacy, security, and trust concerns of those entities.

The NSTAC reviewed best-in-class practices for incident response at both the enterprise and ISAC level. While the reviewed incident response practices were exemplary for their purposes, they did not adequately address how to coordinate or align the diversity of functional capabilities that might be necessary to address incidents across the global cyber ecosystem. In its continued research, the NSTAC reviewed a multi-enabler protocol developed by the Industry Consortium for Advancement of Security on the Internet (ICASI) called the *Unified Security Incident Response Plan* (USIRP).[13] There are a number of elements that suggest the USIRP might be an appropriate template to coordinate the widely diverse capabilities reflected among the ICT enablers:

[13] ICASI is a virtual organization that uses a common protocol for global incident response by leveraging bilateral or multilateral response experts to manage complex issues and protect the Internet ecosystem.

- The USIRP protocol is triggered when an incident impacts two or more of the members. Since the ICASI members are global enablers of key cyber functions, this trigger closely aligns with the ORANGE and RED stages on the CyberCon (when higher industry collaboration and potential interaction with Government would be necessary).
- The USIRP process is designed to facilitate joint collaboration amongst entities' product or service SIRTs during events of significance. The USIRP is not meant to replace members' individual SIRTs, but rather provide a trusted process that enables members to effectively address a range of multi-sector threats and that runs in parallel and overlays current ICASI member response processes.
- The USIRP complements existing industry response entities including ISACs and enterprise CSIRTS. Further, implementation of any USIRP-developed courses of action (COA) can be amplified and broadly disseminated through the ICASI customer base, as well as their membership and participation in industry forums such as ISACs, trust groups, and standards bodies.

The USIRP process is activated when two or more members believe there is an issue that must be addressed. Given the interconnectedness of the gross functional capabilities of the ICT enabler ecosystem, when any two ICT enablers independently identify or are experiencing an incident or incidents, it is reasonable to more closely examine whether those incidents together give rise to systemic consequences. In such cases, the incident should be treated as one of sufficient magnitude to require a concerted response beyond a single enterprise or sector.

The NSTAC has developed a notional draft for a collaborative ICT enabler protocol based on the ICASI USIRP. The notional collaboration and response process identified three broad phases of the incident response lifecycle as it might apply when leveraging the ICT enablers:

- Open, investigate, and scope problem (Triage);
- Engage and resolve problem (Develop mitigations or fixes); and
- Deploy mitigations, fixes, and incident close (Deploy).[14]

In this model, there are specific touch-points with Government during both the initial triage phase of an incident and during the development phase. This draft process envisages an industry-driven dialogue with Government to identify appropriate and relevant resources for assistance. In addition, the model proposes a unity-of-effort across industry and Government to respond to significant national incidents. During the development phase of the response, individual member organizations would leverage their existing CSIRT processes in coordination with other industry and Government CSIRTs. As the operational framework moves to deployment or implementation phase, the model may identify additional touch-points between industry and Government.

Finding: The ICASI USIRP process framework leverages existing industry best practices and offers a unified incident response template to provide for an "agile, effective, and distributed

[14] Please refer to Appendix E, ICASI Background, to view the notional ICT Unified Security Incident Response Team Process.

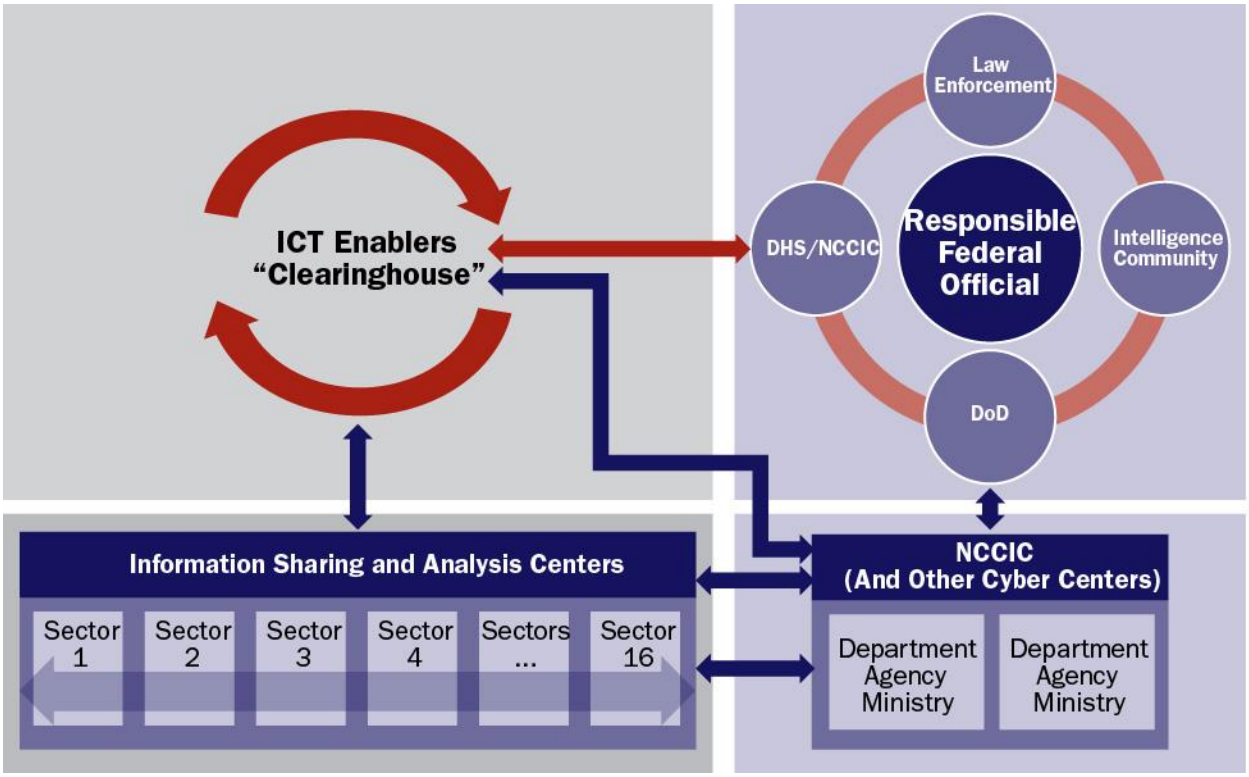
implementation across numerous stakeholders, resulting in a coherent, unified, and dynamic national response."[15]

5.1 Filling the Gap in Incident Management: Leveraging ICT Enabler Capabilities

While NSTAC affirms the continuing development of capabilities associated with enterprise participation in ISACs, as well as inter-ISAC and Government coordination and collaboration, the capabilities inherent within enterprises or their ISACs will likely not be the capabilities necessary to address the circumstances in ORANGE- or RED-level scenarios. Leveraging a unified incident response protocol similar to the ICASI USIRP may be a means to access the ICT enabler capabilities and address the current gap in national coordinated incident management capabilities.

Given the private sector-focused nature of the NSTAC's recommendations in this report, the process flow necessarily focuses on private sector actions, while recognizing that there are critical touch-points and engagements between industry and Government during response. Figure 6, below, highlights a notional, high-level flow chart reflecting how the ICT enabler capabilities could be integrated into existing processes.

Figure 6: Notional Insertion of ICT Enablers into Current Response Framework



[15] *NSTAC Information Technology Mobilization Scoping Report*. May 2014. Available at: https://www.dhs.gov/sites/default/files/publications/Final%20NSTAC%20Information%20Technology%20Mobilization%20Scoping%20Report.pdf

Event Origination and Escalation: At a high level, this process depicts how event information originates at the enterprise level (corporate IT assets) and then, through various information sharing agreements or mechanisms, enters an ISAC. Theoretically, ISACs analyze information across the sector for trends and then have the capability, through their own sharing agreements and mechanisms, to share that information with other ISACs or with the NCCIC. This ISAC-to-ISAC sharing allows for cross-sector aggregation and analysis. At this level, trust groups also play a role in aggregating information and coordinating responses to the level they are capable. However, the NSTAC presumes that under these circumstances ISACs and trust groups are limited in scope and scale and are unable to effectively manage the incident at the scale contemplated in this report.

ICT Enabler Activation and Execution: Should the analysis suggest a widespread (e.g., complete infiltration of a sector or substantial foothold across two or more sectors) or particularly grave event (e.g., a critical dependency is completely overwhelmed and request for resources exceeds available capabilities), the ICT enablers would activate to assess the information. Following initial notification, the relevant members would self-select into the response, providing resources as necessary. Participation in response activities would be virtual, with designated points of contact from each organization or their designees contributing from their respective locations. This process was outlined earlier and a flow chart can be found in Appendix E.

It is important to note that the confederation of ICT enablers would not exist to direct or manage organizational resources; rather, expanding on the concept of trust groups, it would serve as a broader, cross-ecosystem platform to coordinate information sharing, vet incident impact assessments, collaborate on the development and coordination of COAs, and share status of available capabilities. To the extent possible, through pre-planning activities designed to identify possible scenarios (outlined in Path Forward section below) and the relevant stakeholders, many of the mitigation strategies would be pre-scripted, with playbooks available to guide response actions. Accordingly, during incident management, ICT enablers would continually assess the incident, drawing on information from their own sources as well as through ISACs and the NCCIC.

Government Engagement and Authority: Throughout event escalation, activation, and response, the NSTAC anticipates that ICT enablers will regularly coordinate bilaterally with Government to share information on the state of response as well as convey priorities and technical advice. It is in this body that the enablers are able to function in a clearinghouse role, *inter alia*, reviewing Government recommendations or requests for action or technically vetting the feasibility or effectiveness of an action. Similarly, the enablers are able to develop their own COAs, some of which may require Government assistance or sanction, which they will pass to the Government for review and consideration.

At the ORANGE or RED levels, the NSTAC considers it essential that for any coordination or communication with the Federal Government, the Government liaison to the ICT Confederation be empowered to make decisions and clearly and confidently commit resources or actions. The engaging Federal official may vary depending on the nature of the incident and could be from DHS, DOD, the Federal Bureau of Investigation/DOJ, or the White House. In any case, the Federal official would speak on behalf of and, to the extent constitutionally permitted, with the

authority of the Cabinet-level official they are representing. This authority is critical to ensure timely, effective response and the commitment of resources and other assistance.

Consequence Management vs. Incident Management: Throughout these activities, there is an important distinction between incident management and consequence management. Incident management refers to the set of actions intended to address the root cause of the incident at hand, whether that be a software or hardware vulnerability, a network compromise, or other incident. Consequence management refers to the set of actions intended to address the manifestations of the root cause, typically at the enterprise level, identify whether it is cyber or physical in nature, and to protect operations while incident management creates the solution. Accordingly, the activities undertaken by the ICT enablers in this proposed approach would focus exclusively on incident management actions in support of the cyber ecosystem. The corresponding implementation of mitigation actions (e.g., patching systems, replacing hardware, etc.) would flow to the enterprise level via the ISACs or other information sharing mechanisms, as appropriate. While the ICT enablers will themselves implement the COA developed to the degree appropriate, it is important to note that the enterprise or sector(s) must also be prepared to implement the solutions to manage the consequences within their specific environment.

The NSTAC has outlined a means by which widely varying ICT enablers can collaborate together and has also proposed a means to integrate that ICT collaboration into current cyber incident protocols. Together, these processes create a framework that could potentially support agile, effective, and distributed implementation across numerous stakeholders, resulting in a coherent, unified, and dynamic national response.

Throughout this process it has become clear that at lower levels of threat, which is most of the time, current processes are evolving to meet the need and will improve as intra- and inter-sector correlation processes improve. While routine information sharing and collaboration across the national cybersecurity enterprise remains unfinished, this was not the NSTAC's focus. The remaining need—and the gap the NSTAC was specifically asked to address—concerns Government-industry collaboration at the highest levels of threat and national emergency, which the NSTAC has characterized as an ORANGE/RED-level event. While the NSTAC readily acknowledges that an event or events at the highest level of this scale are of lower frequency than events in the BLUE/GREEN/YELLOW levels, additional analysis of the issues related to these levels is outlined below.

6.0 ANALYSIS: FOCUS ON COORDINATED THRESHOLD ROLES

Listed in Section 1.1, this section addresses the NSTAC's "[Recommendation of] an operational framework that… guides, informs, and prioritizes response across the full spectrum of NS/EP events with cyber implications; and [identification] of an operational structure or construct to coordinate assets at each threshold considered, detailing which entities would exercise what roles, as well as suggested approaches for training, and exercises of such contingencies."

Industry has experience in convening to address high-profile cyber issues with and without Government support. The NSTAC anticipates that these types of incidents will continue, and that industry's ability to recognize and mitigate these issues will improve with time. Nonetheless, there are a number of scenarios that could potentially rise to a level where mitigation would require stronger actions concurrent with increased Government support.

The NSTAC discussed a number of scenarios that might be characterized as pre-impact, ORANGE level:

- Cascading Cyber Effects: Enterprises, ISACs, or ICT enablers have communicated a series of "footholds" that threat actors have gained across critical infrastructure sectors and cyber ecosystem components (e.g., operating systems and applications). Collaborative and iterative use of the unified risk assessment approach by Government and ICT enabler teams could enhance correlation of disparate information to determine if the progression of cyber exploitation has reached a threshold necessitating a request for incremental Government support of industry mitigations.
- Low-Probability, High-Impact Cyber Exploitations: Under this scenario, an exploit of a zero-day vulnerability has occurred, evading the industry filters meant to stop this type of attack and prompting ICT enablers to convene. If there is credible information to suggest the means, intent, or ability to engage in disruptive, corruptive, and destructive action at a national scale, the ICT enablers would assess potential impacts, develop mitigations, assess the need for Government support, and make the necessary requests for that support.

Finding: In these pre-impact ORANGE-level scenarios, the protocols for how industry can request and receive incremental Government information or authorities are not well understood. This understanding is necessary, particularly for an environment where fast industry response may be essential for mitigation or containment.

The NSTAC also discussed scenarios that could be characterized at the RED level:

- Government Forewarning of Cyber Activity to Enhance Defensive Posture**:** North Atlantic Treaty Organization Article 5 of the *Washington Treaty* or other "red line" circumstances could prompt cyber retaliation in response to a Government kinetic or cyber attack. Proactive mobilization of ICT enablers could help minimize disruption through enhanced protections, containment strategies, or prioritized reconstitution.
- Post-Incident Prioritized Cyber Restoration and Recovery: In the event a cyber incident of national or global significance has occurred, key resources across the cyber ecosystem would need to be engaged to contain and/or reconstitute national and international capabilities or functions.

Finding: At the RED level, there is little industry understanding regarding Government goals or priorities for pre-impact protection or post-impact recovery; however, this is precisely the assessment and understanding that industry must gain.

In order to determine protection and prioritization efforts at the RED level, it is necessary to identify assets, capabilities, and functions which must be protected and sustained in the event of a cyber incident of national consequence. This critical needs assessment should occur during industry-Government collaborative efforts, utilizing cyber attack scenarios as case studies. Additionally, it is also important to identify which assets, capabilities, and functions must be prioritized for recovery and restoration, which would occur during a post-cyber incident restoration and recovery scenario. This dialogue is consistent with sustainment activities

associated in the DOD computer network defense framework, or alternatively as a broad extension of the concepts reflected in the TSP program.[16, 17]

Understanding what must be protected or recovered during a RED-level cyber event will provide the basis to understand which industry and Government capabilities are needed and the legal authorities required to protect, mitigate, prioritize, and reconstitute those identified assets. A better mutual understanding of *in extremis* needs, priorities, capabilities and authorities at the RED level can also provide greater clarity for more effective ORANGE level response. Industry should identify its intermediate response capabilities, meaning the range of capabilities between current BAU and RED activities, and conduct a mutual assessment to determine if different (i.e., lesser) authorities would suffice for those intermediate steps. With this understanding, industry and Government should agree on standard protocols for requesting and extending legal support, relief, or indemnification to those engaged in protection, sustainment, or defensive activities.

Concurrent with the discussions outlined above, significant discussion and analysis will be required to fully assess the scope of current legal and policy authorities and, more specifically, to explore the potential gaps in such authorities and achieve the mutual goals for protection of the cyber ecosystem. Additionally, it is important to determine if, and to what extent, legal or policy change may be necessary to implement the recommendations in this report; however, the NSTAC is confident that, as with other former and current national security planning and policy regimes, the specifics of details can be protected within a visible umbrella of public policy and creation of global norms.

The scenarios highlighted above are predicated on the foundation of collaboration among industry and between industry and Government for the preservation, protection, sustainment or defense of the global cyber ecosystem. If industry and Government conduct the assessments proposed above, there may be significant enhancements gained in protecting the Nation's domestic, cyber-reliant assets and operations (e.g., water, power, and transportation). These assessments would also assist in expediting requests for incremental legal authorities under less-extreme circumstances (i.e., YELLOW/ORANGE levels). Finally, these discussions appear consistent with capability sustainment activities, or those activities an entity must perform to ensure services continue to be provided at an acceptable level of quality.[18]

While an event or events of this level happen less frequently, it is important that joint industry and Government planning occurs to ensure a national readiness for such a life-threatening eventuality. Such readiness activities would include the joint creation of response plans, frequent exercises to test readiness, and the development of procedures and training of personnel.

To further this understanding, it is necessary for industry and Government to engage in a much deeper level of dialogue and mutual understanding of respective capabilities and domestic NS/EP needs. The NSTAC acknowledges that the assessments outlined above are considered sensitive

[16] Software Engineering Institute, *Incident Management Capability Metrics*, April 2007. Pp A7-A9. Available at: http://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14873.pdf.

[17] TSP Policy. Available at: http://www.ecfr.gov/cgi-bin/text-idx?SID=94cf45bc0802a55b9eb327654afe511d&node=ap47.3.64_16060.a&rgn=div9.

[18] Software Engineering Institute, *Incident Management Capability Metrics Version 0.1*.

work and must be conducted by experts fully versed in their respective company's cyber capabilities, risk management, and continuity planning. Government counterparts to industry must be equally equipped.[19]

Finding: The NSTAC believes there are sufficient U.S.-based entities performing ICT enabler roles to engage in this necessary dialogue and will suggest a path forward for accomplishing these goals.

7.0 FINDINGS DERIVED FROM NSTAC ANALYSIS

The NSTAC analyzed the following areas pertinent to its tasking:

- Identifying thresholds that might require increased operational coordination;
- Identifying commercial assets that would be necessary to respond to a cyber-related event of national significance; and
- Proposing an operational framework that would allow for agile, effective, and distributed implementation, resulting in a coherent, unified, and dynamic national response.

The analytic findings associated with these areas of analysis are re-stated below to serve as a foundation for Section 8, *Path Forward*.

- The unified risk assessment of potential or actual impact provides an indicator of whether an issue should escalate or de-escalate. It is a function of three criteria/parameters: event characteristics, intelligence sources, and capability to respond.
- The ORANGE level represents the domain of extensive coordination and collaboration between Government and industry in terms of dynamic protocols and procedures. At lower levels, current practiced behavior should be sufficient to maintain stability and flow in response to cyber incidents. However, much changes in the Government-industry relationship as industry moves from utilizing existing authorities within YELLOW to requesting incremental Government authorities in ORANGE. It will be important to thoughtfully 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.
- The RED level conceptually represents a cyber emergency of the severest nature and greatest potential impact. At this level, the total commitment of industry to sustain network/system operations will be insufficient to meet the national need. Accordingly, Government will be expected to convey priorities and industry will do all that is possible to support national survival, under Government direction, within a comprehensive, legal, and operational framework to be developed.
- The response capabilities inherent within enterprises or their ISACs will not likely be the capabilities necessary to address the circumstances in an event of national significance.

[19] Roles and responsibilities of Cyber UCG Government officials are outlined in the Cyber UCG Charter, dated June 1, 2014.

- ICT enablers represent the functionalities foundational to the global cyber ecosystem and are most capable to address the threats, develop mitigation strategies, and and/or implement systemic remediation.
- The NSTAC believes that ICT enablers likely represent the commercial assets, functions, and/or capabilities that, if operationally coordinated, would be helpful or necessary to respond to a cyber-related event of national significance.
- Coordinated incident response by ICT enablers at ORANGE/RED-level events may necessitate Government authorities despite the potential for positive impact, as there may be accompanying unintended consequences of such action.
- Properly addressing events of national significance warranting the mitigation efforts of multiple ICT enablers will require ensuring that any mitigation strategies developed consider all potential consequences—as well as impacts on all potentially impacted stakeholders, including global Internet users—and are fully authorized by requisite legal and Government authorities in the United States and other relevant jurisdictions.
- Since the global cyber ecosystem is foundationally civilian, the U.S. Government should continue its dialogue to establish global norms for national cyber response and incorporate industry in those discussions to the greatest extent possible.
- The ICASI USIRP process framework leverages existing industry best practices and offers a potential unified incident response model to provide for an agile, effective, and distributed implementation across numerous stakeholders, resulting in a coherent, unified, and dynamic national response.
- In pre-impact ORANGE-level scenarios, the protocols for how industry can request and receive incremental Governmental information, capabilities, or authorities are not well understood. This understanding is necessary, particularly for an environment when fast industry response is essential for mitigation or containment.
- At the RED level, there is little industry understanding regarding Government priorities for pre-impact protection or post-impact recovery.
- The NSTAC believes there are sufficient U.S.-based entities performing ICT enabler roles to begin this necessary dialogue.

8.0 PATH FORWARD

An effective national ICT mobilization process will involve coordinating across many industry and Government stakeholder communities to respond to significant impacts in a highly interconnected global cyber ecosystem. A first step in this process is gaining an understanding as to what must be prioritized for protective or recovery measures. Due to the complexity and multi-faceted nature of the problem, the NSTAC recommends a phased approach to identifying and addressing cyber-related NS/EP readiness gaps.

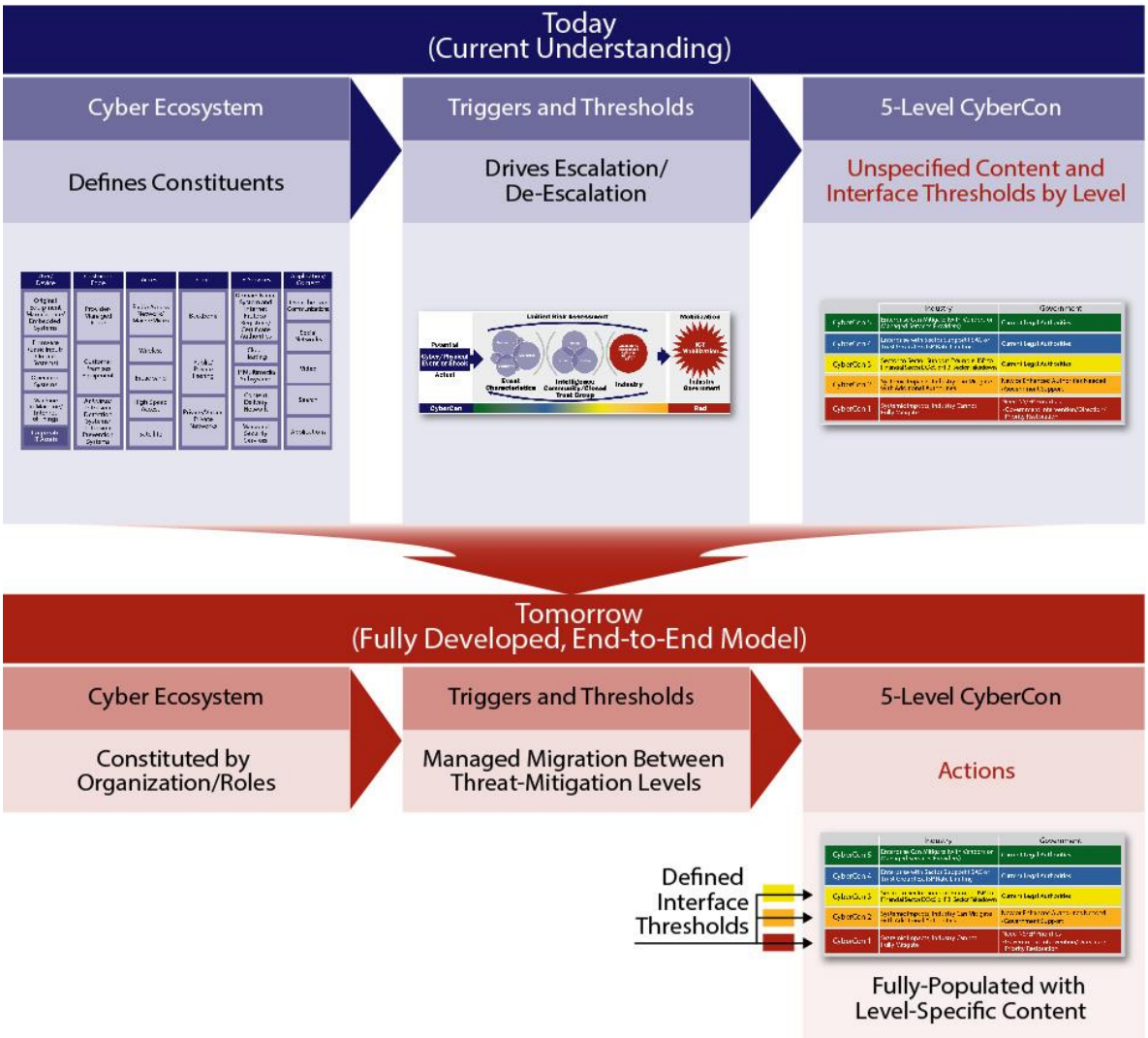
- Design Framework: The NSTAC has outlined a unified risk assessment approach that suggests when increased operational coordination within industry, as well as between industry and Government, might be required; it also highlights the nature of the support and collaboration in a five-level CyberCon graphic. The NSTAC finds that providers of certain ICT functionalities (i.e., ICT enablers) would likely be the entities most necessary to support

incident management for large-scale cyber events. The NSTAC further provides potential templates for how the ICT enablers could collaborate within their community, as well as how support from the ICT enablers might be integrated into current national cyber incident response plans. The NSTAC believes the components within this report collectively provide a design framework to build the requested capabilities.

- Build Capability: The next step toward this capability is to build out the operational framework. The process to undertake this work is outlined below.
- Implement the Capability: Finally, industry and Government stakeholders must incorporate the operations framework developed into response policies and mechanisms, train personnel in its use, and exercise frequently to ensure a quick and agile response.

Figure 7, below, depicts the current NSTAC design elements and identifies outstanding actions to complete the build-out of the recommended national capability.

Figure 7: ICTMS Vision – Now and Future



The top of Figure 7 depicts the current situation. As noted, the NSTAC has identified the ICT functionalities most likely necessary to support incident management for large-scale cyber events. It then outlined a unified risk assessment approach that suggests when an incident might require increased operational coordination between industry and Government and highlights the nature of the support and collaboration in a five-level CyberCon graphic. However, at present, the precise character and content of the actions to be taken cannot be fully populated for levels YELLOW through RED.

In order to be effective, the total national ICT mobilization effort will require clear, mutual understanding of the national needs, priorities, authorities, and capabilities of all partnering participants in both Government and industry. Information flow must conform to clearly-understood guidelines, reinforced through exercise and experience, to ensure complete and efficient situational awareness to the extent needed by all. To accomplish this goal, the NSTAC envisions a greater level of mutual understanding of priorities, response capabilities, and authorities on both sides. To some extent, any plans or protective capabilities developed to meet the Nation's NS/EP goals may require new authorities commensurate with those goals. Equally important will be a mutual understanding of what protection capabilities current laws can accord to industry. These discussions are intended to streamline processes and permit positive actions by all, in proportion to the immediate threat as it evolves.

These understandings define the remaining work, but here the NSTAC recognizes certain limitations in its own ability to progress beyond this design phase. Principal among these limitations is the type of discussions, both in terms of participants and content, which will require great sensitivity. A trusted framework is clearly needed to ensure these discussions can be both candid and safe.

Furthermore, there is the question of who would participate in such discussions. The NSTAC believes that on the industry side, the answer is embedded in the elements of the ICT enablers and their professional and technical equities. This industry group would need to be matched by government experts and organizational representatives from across the national security domain, some of whom may have been involved in the current effort to date. Of note, this would take the form of a working group, with representatives chosen for their domain knowledge and expertise; these representatives would be authorized to represent the views of their organization and operational actions, as well as capable of articulating the full range of relevant authorities and capabilities of the organization, such that these discussions could become codified in NS/EP plans and procedures.[20]

Figure 8, below, depicts these initial discussions in three steps.

[20] *Cyber Unified Coordination Group Charter*, June 2014.

Figure 8: ICTMS Vision – Next Steps

As depicted in Figure 8, the NSTAC envisions three steps required to turn the "design" in this report into a "built-out" operational capability:

1. Identify Industry Constituents and U.S. Government Counterparts: As discussed, the NSTAC proposes the ICT enablers as the basis for identification of industry participants. At the same time, the Government would need to identify counterparts to ensure representation of all aspects of the total national security community.
2. Define Government/Industry Group Priorities and Capabilities Content, by Level: This report recommends that the President convene the group defined above, with a suitable Federal official/organization appointed as the coordinator for the group's activities as they build out the plan. The group would meet in a presumably trusted setting, be granted access to necessary and appropriate information, and commence work.
   - The President should charge the group to mutually outline national priorities and goals for cyber protection, prioritization, and/or recovery, and to identify the likely ICT enablers that would best support those protection goals under varying scenarios.
   - The group should address capabilities to protect, prioritize, and/or recover in terms of the enabler's capacity to act, which is a purely mechanical ability to perform activities relevant to cyber protection.
   - Those potential actions will in turn be evaluated in terms of the enabler's willingness to conduct or perform them. There are numerous reasons why an organization might not currently be willing to take an action it is otherwise capable of performing. These could include impacts to the ecosystem, liability concerns, uncertain legalities, risk to reputation and/or foreign reaction, anti-trust considerations, or others.
   - The group will then review authorities to act and thereby possibly explore and identify mitigations, waivers, or related indemnifications that would ameliorate stakeholders' potential lack of willingness to take some possible action.

- — This process should be iterated, through capacity-willingness-authority-revise authority-feedback and review, until the range of options is exhausted. To the extent current law does not provide the sufficient authorities to meet all the NS/EP goals identified in the discussions outlined above, this gap should be captured for future review in a different environment.
- — The group should establish the specific events, conditions, circumstances, and/or actions which will serve to trigger and invoke the protections defined above.

3. Define Level-Crossing Criteria: At this point the group, comprised of both industry and Government, has identified and specified a number of response options and capabilities, many of which are expected to be conditional on having risen to some high level of crisis. Accordingly, the various actions, new authorities, waivers, and other considerations will have been mapped to specific levels of the CyberCon. What remains is to determine any specific circumstances, observable conditions, or events that might serve to clearly define progression across levels, escalation or de-escalation, as crises evolve. Should these interface specifications be clearly defined, they can be codified for implementation, along with suitable details regarding action options by level.

8.1 Implementing Operational Capabilities

The NSTAC expects that many details related to the internal content of the CyberCon model, once populated, will remain very sensitive and in all likelihood will never be broadly promulgated. However, the NSTAC is confident that, just as with other national security planning and policy regimes of the past and present (such as the TSP program, among others), such details can be protected within a visible umbrella of public policy. For example, to the extent current law does not provide sufficient authorities to meet all the NS/EP goals identified in the discussions outlined above, this information should provide a visible path forward for Government to seek the changes in law it deems necessary.

The visible aspect of the national approach to ICT mobilization could and should also include efforts to incorporate or modify existing incident response plans, programs and policies, as appropriate, as well as incorporate these mobilization capabilities into progressive training and exercises up to the level of National-Level Exercises. In this and all other cases, there should be deliberate attention, especially initially, to establish accountability for capturing lessons learned and operational feedback to refine procedures and plans, which will build confidence and understanding on the part of all participants. While a portion of the initial discussions may be conducted in a trusted environment, the NSTAC believes that most of the implementation, training, and exercise activities can be accomplished within a transparent, partnership environment.

9.0 CONCLUSION

In this report, the NSTAC outlines a unified risk assessment approach that suggests when increased operational coordination within industry, as well as between industry and Government, might be required, and then highlights the level of support and collaboration in a five-level CyberCon graphic. The NSTAC finds that providers of certain ICT functionalities, referred to as ICT enablers, would most likely be the entities most necessary to support incident management for large-scale cyber events. The NSTAC further provides potential templates for how the ICT

enablers could collaborate within that community, as well as how support from the ICT enablers might be integrated into current national cyber incident response plans and response bodies. The NSTAC further outlines some of the challenges facing the ICT enablers in the global economy.

This analysis directly addresses a portion of the original NSTAC tasking, specifically the following:

- Research and identify conditions, triggers, thresholds, and situations that might require increased operational coordination across industry, as well as between industry and Government;
- Research and recommend a methodology by which Government and industry can identify critical commercial assets, functions, and/or capabilities that, if operationally coordinated, would be helpful or are necessary to respond to a cyber-related event of national significance; and
- Research and recommend an operational framework that: (1) allows for agile, effective, and distributed implementation across numerous stakeholders, resulting in a coherent, unified, and dynamic national response.

The analysis addressing these three topics within this report provides a framework design and a strategic vision for industry-Government collaboration in the case of a serious cyber incident. This report then recommends additional follow-on steps to facilitate the completion of this framework and build the ICT mobilization capability.

The NSTAC believes that the findings in this report and recommendations outlined in Section 10 will lead to a national ICT mobilization capability that will support prioritized response across the full spectrum of NS/EP events with cyber implications.

10.0 RECOMMENDATIONS

Developing a national ICT mobilization capability will require a clear understanding of the mutual national needs, priorities, authorities, and capabilities of all partnering participants in both Government and industry. Based on the authorities and responsibilities established by EO 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, the NSTAC recommends the President take the following actions to ensure the Nation is prepared to manage a cyber-related event of national significance:

- Identify and convene a representative group of organizational representatives reflecting the defined ICT functions as described herein and national security organizations of Government.
  - — Appoint a suitable Federal official to coordinate and facilitate the work of this group.
  - — Charge the group to describe mutual national priorities and objectives for protection, prioritization, and/or recovery, and to define in actionable detail the actions, options, authorities, statutory provisions, indemnifications, information flow, waivers, and other processes specific to requesting resources from both Government and industry for those circumstances.

  - — Having defined the national priorities and objectives, identify the key functions and related stakeholders necessary to support them, and the specific events, conditions, circumstances and/or actions which will serve to trigger and invoke the protections defined above.
  - — Conduct an analysis of current NS/EP legal and policy authorities implicated by the identified national priorities and associated actions as identified above. To the extent current legal frameworks do not provide sufficient authorities to meet NS/EP goals, identify the maximum capabilities currently supported by law, thus establishing current operational boundaries, and produce a report, identifying changes in current laws that would facilitate the level of coordinated protections desired.
  - — Examine existing response frameworks, mechanisms, bodies, and constituencies, and adapt, expand, or revise them, as appropriate, to meet recommended ICT response capabilities.

- Create a comprehensive training, education, and exercise regime designed to enhance and maintain readiness by all Government and industry participants in this program.
  - — Develop a timeline for introduction and testing of these procedures in progressively-complex and large-scale exercises, leading to involvement in the National Exercise Program and National-Level Exercises as soon as practicable.
  - — Provide processes to examine feedback and exercise lessons learned, in order to revise and refine procedures as appropriate and as threat conditions evolve.
  - — Establish accountability and ownership across the Federal Government for follow-up on lessons learned and identified gaps to produce an improvement plan, a plan of action, and milestones, and to create a methodology for testing those improvements in succeeding exercises.
- Develop global norms for national cyber response in partnership with industry, incorporating industry expertise and experience to the maximum extent possible.

APPENDIX A: MEMBERSHIP

SUBCOMMITTEE MEMBERS

Ms. Renée James, Co-Chair
Mr. Glen Post, Co-Chair

Ms. Kathryn Condello, ICTMS Working Group Co-Chair
Mr. Patrick Flynn, ICTMS Working Group Co-Chair

Akamai Technologies, Incorporated	Mr. David Belson
AT&T, Incorporated	Mr. Brooks Fitzsimmons
Avaya, Incorporated	Mr. Tony Anastasio
CenturyLink, Incorporated	Mr. David Aschkinasi Mr. Michael Glenn Ms. Sara Roper Mr. Wray Varley
Communication Technologies, Incorporated	Mr. Milan Vlajnic
Department of Homeland Security	Mr. Adam Bulava Mr. John O'Conner
Ericsson, S.A.	Ms. Louise Tucker
FireEye, Incorporated	Mr. Richard Bejtlich
Frontier Communications Corporation	Mr. Michael Saperstein Mr. Erwin Wardojo
Financial Services Information Sharing and Analysis Center	Ms. Denise Anderson
Intel Corporation	Mr. Kent Landfield Mr. John Miller Mr. Brian Willis
Intelsat General	Mr. Timothy Turk
Isis Defense	Mr. Ed Willhide
Juniper Networks, Incorporated	Mr. Robert Dix Mr. Sampak Garg
Microsoft Corporation	Mr. Chris Krebs
National Security Council, Executive Office of the President (EOP)	Mr. Steve Kelly
Neustar, Incorporated	Mr. Rodney Joffe

Office of Science & Technology Policy, EOP	Dr. Michael Johnson
Palo Alto Networks	Mr. William Gravell
Raytheon Company	Mr. William Russ
Sprint Corporation	Mr. Chuck Brownawell
tw telecom	Mr. Colin Gosnell Mr. Henry Yu
Verizon Communications, Incorporated	Mr. Marcus Sachs
Vonage Holdings Corporation	Mr. Venkat Pakeeru

OTHER PARTICIPANTS

AT&T, Incorporated	Ms. Rosemary Leffler
Aveshka, Incorporated	Ms. Lisa Beury-Russo
CSC	Mr. Guy Copeland
Department of Homeland Security	Ms. Jennine Gilbeau Mr. Neil Jenkins

BRIEFERS – SUBJECT MATTER EXPERTS

Atlantic Council	Mr. Jason Healey Mr. Frank Kramer
Department of Defense	Lt. Col David Halla Mr. Guy Walsh
Department of Homeland Security	Mr. Brandon Wales Ms. Bridgette Walsh Mr. Larry Zelvin
IBM	Mr. Peter Allor
Intel Corporation (McAfee)	Mr. Brent Conran
National Cybersecurity Center–Finland	Mr. Kauto Huopio Mr. Jarkko Saarimaki

SUBCOMMITTEE MANAGEMENT

Designated Federal Officer, NSTAC	Ms. Helen Jackson
Alternate Designated Federal Officer, NSTAC	Ms. Suzanne Daage
Triumph Enterprises, Incorporated	Ms. Emily Morin

APPENDIX B: ACRONYMS

BAU	Business as Usual
COA	Course of Action
CIR	Cyber Incident Response
CSIRT	Computer Security Incident Response Team
CyberCon	Cyber Condition
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
EO	Executive Order
ICASI	Industry Consortium for Advancement of Security on the Internet
ICT	Information and Communications Technology
ISAC	Information Sharing and Analysis Center
ISP	Internet Service Provider
IT	Information Technology
NCCIC	National Cybersecurity and Communications Integration Center
NCIRP	Interim Draft National Cyber Incident Response Plan
NIST	National Institute for Standards and Technology
NSTAC	President's National Security Telecommunications Advisory Committee
SIRT	Security Incident Response Team
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Indicator Information
TSP	Telecommunications Service Priority
UCG	Unified Coordination Group (Cyber)
USIRP	Unified Security Incident Response Plan

APPENDIX C: GLOSSARY

Catastrophic Incident: Any natural or manmade incident, including terrorism, which results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. (Catastrophic Incident Annex to the *National Response Framework*)

Certificate Authority: A trusted entity that issues and revokes public key certificates. (National Institute of Standards and Technology [NIST] Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Commercial Asset: A blend of assets, capabilities, and functions. (Defined by the Information Technology [IT] Mobilization Scoping Subcommittee, May 27, 2014)

Consequence Management: Refers to the set of actions intended to address the manifestations of the root cause of an issue (whether cyber or physical in nature), including the implementation of mitigations, until a completion resolution can be effected.

Computer Security Incident Response Team: A service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporate, governmental, or educational organization; a region or country; a research network; or a paid client. (Software Engineering Institute)

Containment: Continuous analysis of the threat/response environment through security management to prevent malware, external attacks, or an insider threat from roaming through interconnected networks. (Adapted from the President's National Security Telecommunications Advisory Committee's [NSTAC] *NSTAC Secure Government Communications Report*, August 20, 2013)

Critical Cyber System/Asset/Function: An asset, system, or function that, if affected by a physical or cyber incident that impacted its confidentiality, integrity, and availability, would have significant negative impact on the national security, economic stability, public confidence, public health or safety of the United States. (Multi-State Information Sharing and Analysis Center)

Critical Infrastructure: Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction. (*National Infrastructure Protection Plan*)

Defense Support of Civil Authorities: Support provided by U.S. Federal military forces, Department of Defense (DOD) civilians, DOD contract personnel, DOD component assets, and National Guard forces (when the Secretary of Defense, in coordination with the Governors of the affected States, elects and requests to use those forces in title 32, U.S.C., status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support,

and other domestic activities, or from qualifying entities for special events. (Also known as civil support.) (Office of the Assistant Secretary of Defense for Homeland Defense)

Distributed Denial of Service Attacks: A denial of service technique that uses numerous hosts to perform the attack and prevents the authorized access to resources or delays time-critical operations. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Domain Name Services (DNS): A mechanism used in the internet and on private intranets for translating names of host computers into addresses. DNS allows host computers not directly on the Internet to have registered names in the same style. (Newton's Telecom Dictionary)

Incident Management: Refers to the set of actions intended to address the root cause of the incident at hand (e.g., software or hardware vulnerability, a network compromise, etc.).

Information Sharing and Analysis Center (ISAC): Trusted entities established by Critical Infrastructure Key Resource (CI/KR) owners and operators to provide comprehensive sector analysis, which is shared within the sector, with other sectors, and with Government. ISACs take an all-hazards approach and have strong reach into their respective sectors, with many reaching over 90 percent penetration. Services provided by ISACs include risk mitigation, incident response, and alert and information sharing. (National Council of ISACs, http://www.isaccouncil.org/aboutus.html)

Information Technology: Equipment, processes, procedures, and systems used to provide and support information systems (computerized and manual) within an organization and those reaching out to customers and suppliers. (Newton's Telecom Dictionary)

Internet of Things: The total interconnected collection of device networks. (Newton's Telecom Dictionary)

Internet Protocol (IP): Part of the Transmission Control Protocol/IP (TCP/IP) family of protocols describing software that tracks the Internet address of nodes, routes outgoing messages, and recognizes incoming messages; used in gateways to connect networks at Open Systems Interconnection network Level 3 and above. (Newton's Telecom Dictionary)

IP Multimedia System: An open Next Generation Networking (NGN) multi-media architecture for mobile and fixed IP services. It is used by telecom operators of NGN, which combine voice and data in a single packet switched network, to offer network-controlled multimedia services. (Newton's Telecom Dictionary)

Intrusion Prevention System: System(s) which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Intrusion Detection Systems: Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse

(attacks from within the organizations.) (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Large-Scale Cyber Attack: See "significant cyber incident."

Machine to Machine (M2M): Technologies that enable computers, embedded processors, smart sensors, actuators, and mobile devices to communicate with one another, take measurements, and make decisions, often without human intervention. (M2M Technology in Demand Responsive Commercial Buildings)

Maximum Segment Size: A parameter of a TCP protocol that specifies the maximum amount of data that can be received through the specific connection at that time. (Internet Engineering Task Force)

Mitigations: The actions of reducing the severity, seriousness, or painfulness of something.

National Security/Emergency Preparedness (NS/EP) Communications: Telecommunication services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States (47 Code of Federal Regulations Chapter II, § 201.2(g)). Also, NS/EP communications also include primarily those technical capabilities supported by policies and programs that enable the Executive Branch to communicate at all times and under all circumstances to carry out its mission essential functions and to respond to any event or crisis (local, national, or international), to include communicating with itself; the Legislative and Judicial branches; State, territorial, tribal and local governments; private sector entities; as well as the public, allies, and other nations. NS/EP communications further include those systems and capabilities at all levels of government and the private sector that are necessary to ensure national security and to effectively manage incidents and emergencies. (NS/EP Communications Executive Committee definition based on Executive Order 13618)

Networks: Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Operating System: A software program which manages the basic operations of a computer system. (Newton's Telecom Dictionary)

Over-the-Top Communications: The ability to deliver real-time communication services and applications across IP networks. (Oracle)

Patch: An update to an operating system, application, or other software issued specifically to correct particular problems with the software. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Protocol: A set of rules and formats, semantic and syntactic, permitting information systems to exchange information. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Radio Access Network: Controls the transmission and reception of radio signals across cellular networks.

Significant Cyber Incident: A severe or critical incident on the Cyber Risk Alert Level System. A significant cyber incident is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks.

A significant cyber incident may destroy, degrade, or disrupt the cyber infrastructure and/or the integrity of the information that supports the private and public sectors. Complications from a significant cyber incident may threaten public health or safety, undermine public confidence, have a debilitating effect on the national economy, or diminish the security posture of the Nation. A significant cyber incident may adversely affect the Nation's ability to project force and may have implications on the Nation's strategic deterrence capability. (Draft Cyber Capabilities Planning Framework)

Structured Threat Information Expression (STIX): A collaborative community-driven effort to define and develop a standardized language to represent structured cyber threat information. The STIX language intends to convey the full range of potential cyber threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible. All interested parties are welcome to participate in evolving STIX as part of its open, collaborative community. TAXII is the main transport mechanism for cyber threat information represented as STIX. Through the use of TAXII services, organizations can share cyber threat information in a secure and automated manner. (http://stix.mitre.org/)

Sustainability: The ability to maintain the necessary level and duration of operational activity to achieve military objectives. Sustainability is a function of providing for and maintaining those levels of ready forces, materiel, and consumables necessary to support military effort. (*Joint Capabilities Integration and Development System [JCIDS] Manual*)

Sustainment Activities: The provision of personnel, training, logistics, and other support required to maintain and prolong operations or combat until successful accomplishment or revision of the mission or of the national objective. (*JCIDS Manual*).

Telecommunications Service Priority (TSP): A regulatory, administrative, and operational system authorizing and providing for priority treatment (i.e., provisioning and restoration) of NS/EP telecommunications services. (http://www.dhs.gov/telecommunications-service-priority-tsp)

TSP Policy: Establishes the framework for telecommunication service vendors to provision, restore, or otherwise act on a priority basis to ensure effective NS/EP telecommunications services. The NS/EP TSP System allows the assignment of priority levels to any NS/EP service

across three time periods, or stress conditions: Peacetime/Crisis/Mobilizations, Attack/War, and Post-Attack/Recovery." (Electronic Code of Federal Regulation – Appendix A to Part 64)

TSP - Control Services and Orderwires: The NS/EP TSP System and procedures are not applicable to control services or orderwires owned by a service vendor and needed for provisioning, restoration, or maintenance of other services owned by that service vendor. Such control services and orderwires have priority provisioning and restoration over all other telecommunications services (including NS/EP services) and are be exempt from preemption. (Electronic Code of Federal Regulation – Appendix A to Part 64*)*

Threat: Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (NIST Special Publication 800-53, CNSS Instruction (CNSSI) 4009, Adapted)

Trusted Automated Exchange of Indicator Information (TAXII): Defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries. TAXII, through its member specifications, defines concepts, protocols, and message exchanges to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats. TAXII is not a specific information sharing initiative or application and does not attempt to define trust agreements, governance, or other non-technical aspects of cyber threat information sharing. Instead, TAXII empowers organizations to achieve improved situational awareness about emerging threats, enabling organizations to share the information they choose with the partners they choose. TAXII is the preferred method of exchanging information represented using the Structured Threat Information Expression (STIX) language, enabling organizations to share structured cyber threat information in a secure and automated manner. (http://taxii.mitre.org/)

Unauthorized Result: An unauthorized result is one that includes: 1) Increased access; 2) Disclosure of information; 3) Corruption of information; 4) Denial of service; or 5) Theft of resources. ("A Common Language for Computer Security Incidents" by John D. Howard and Thomas A. Longstaff; Sandia National Laboratories [Sandia Report: SAND98-8667])

Virtual Private Network: A virtual network, built on top of existing physical networks that provides a secure communications tunnel for data and other information transmitted between networks. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

APPENDIX D: LIST OF HISTORICAL EVENTS

Name of Incident	Type of Incident	Date
Robert Tappen Morris/The Morris Worm	Worm	1988
Kevin Mitnick and Kevin Poulsen Computer and Phone Hacking	Computer and phone hacking	1992 – 1995
Solar Sunrise, Moonlight Maze, Titan Rain, Buckshot Yankee	Probing/hacking of military networks	1998 – 2004
Melissa, ILoveYou, Code Red, Slammer, Sasser	Computer viruses; worms	1999 – 2004
MafiaBoy	Distributed denial of service (DDoS) attacks	2000
DNS Root Server Attacks	DDoS attacks	2002, 2007
Internet Routing Attacks	Border Gateway Protocol attacks originating overseas	2004, 2008, 2010, 2013
Estonia and Georgia Cyber Attacks	DDoS attacks; website defacements	2007, 2008
Heartland, Hannaford, TJX, Epsilon, Sony, RSA, Target, others	Data breaches; malware; spear phishing	2007 – 2013
Conficker, Zeus, Mariposa	Worms; malware; botnets	2008 – 2014
Anonymous and Lulzsec	Targeted ideological hacking; data breaches	2011 – 2012
Flame, Stuxnet, Shamoon	Cyber espionage; malware targeting internal computer systems	2012
Saudi Aramco Cyber Attack	Spear phishing; malware	2012
RasGas Cyber Attack	Spear phishing; malware	2012
Finance and Banking Industry Cyber Attacks	DDoS attacks	2012 – 2013
Heartbleed, Shellshock	Security vulnerability in OpenSSL	2014
Dragonfly	Malware targeting industrial control systems	2014

APPENDIX E: ICASI BACKGROUND

The Industry Consortium for Advancement of Security on the Internet (ICASI) was founded in 2008 in Washington, D.C. by Cisco, IBM, Intel, Juniper, and Microsoft. In addition to the founding organizations, the general membership currently includes Amazon, Oracle, and RIM. The purpose of ICASI is to: proactively collaborate in a trusted environment; analyze, mitigate, and manage multi-vendor security challenges; innovate the processes and practices needed to enhance the global security landscape; and protect the cyber ecosystem.[21]

These ICASI members are leading global information technology (IT) companies that are dedicated to: (1) increasing the speed and effectiveness of multi-vendor, cross-product, and cross-border security response; (2) developing a common operational response protocol; (3) sharing knowledge of current and future threats; and (4) providing industry expertise on emerging global threats, security response planning, and security engineering innovation.[22] ICASI has an opportunity to protect its customer base and advance Internet security. In order to do this, industry vendors look beyond their individual response processes and collaborate to obtain more agile and innovative cybersecurity approaches.

There are six stages to responding to cross product and border security challenges, including: (1) analysis; (2) containment; (3) remediation; (4) mitigation/protection; (5) coordination; and (6) recovery. ICASI's unified response process addresses four of these stages, including: (1) analysis; (2) remediation; (3) mitigation/protection; and (4) coordination. If there is a vulnerability in a system, many researchers do not fully understand the threat; therefore, ICASI conducts an in-depth analysis to determine what the threat is and the potential impact it could have on the ecosystem. Containment occurs on an individual organizational level and is the purview of a Computer Security Incident Response Team and vendors.

ICASI has several standing working groups, including the Common Vulnerability Reporting Framework (CVRF), the Coordination Working Group, and the *Unified Security Incident Response Plan* (USIRP). ICASI developed the CVRF as a framework to explain how to exchange data about vulnerabilities based on an XML-based language; while the coordination working group determines how ICASI establishes and promotes best practices around multifaceted vulnerability disclosure coordination. ICASI's USIRP allows member companies' Security Incident Response Teams (SIRT) to work together to effectively respond to and resolve complex, multi-vendor Internet security issues. The ICASI USIRP includes three major categories: (1) vulnerabilities (may take weeks to months to resolve); (2) incidents that impact three or more members (urgent/emergent); and (3) strategic response (persistent ongoing or long-term problems).[23] Anyone can trigger a USIRP and entities may use the USIRP mailing list to ask for help on compelling cybersecurity issues. Once contacted, incident response experts from member companies meet in a trusted forum to triage the issue and discuss impacts and

[21] ICASI, "Beyond Response: Advancing Internet Security Global Multi-Vendor Incident Response," briefing to the NSTAC. (ICASI briefing to the NSTAC)
[22] ICASI briefing to the NSTAC.
[23] ICASI briefing to the NSTAC.

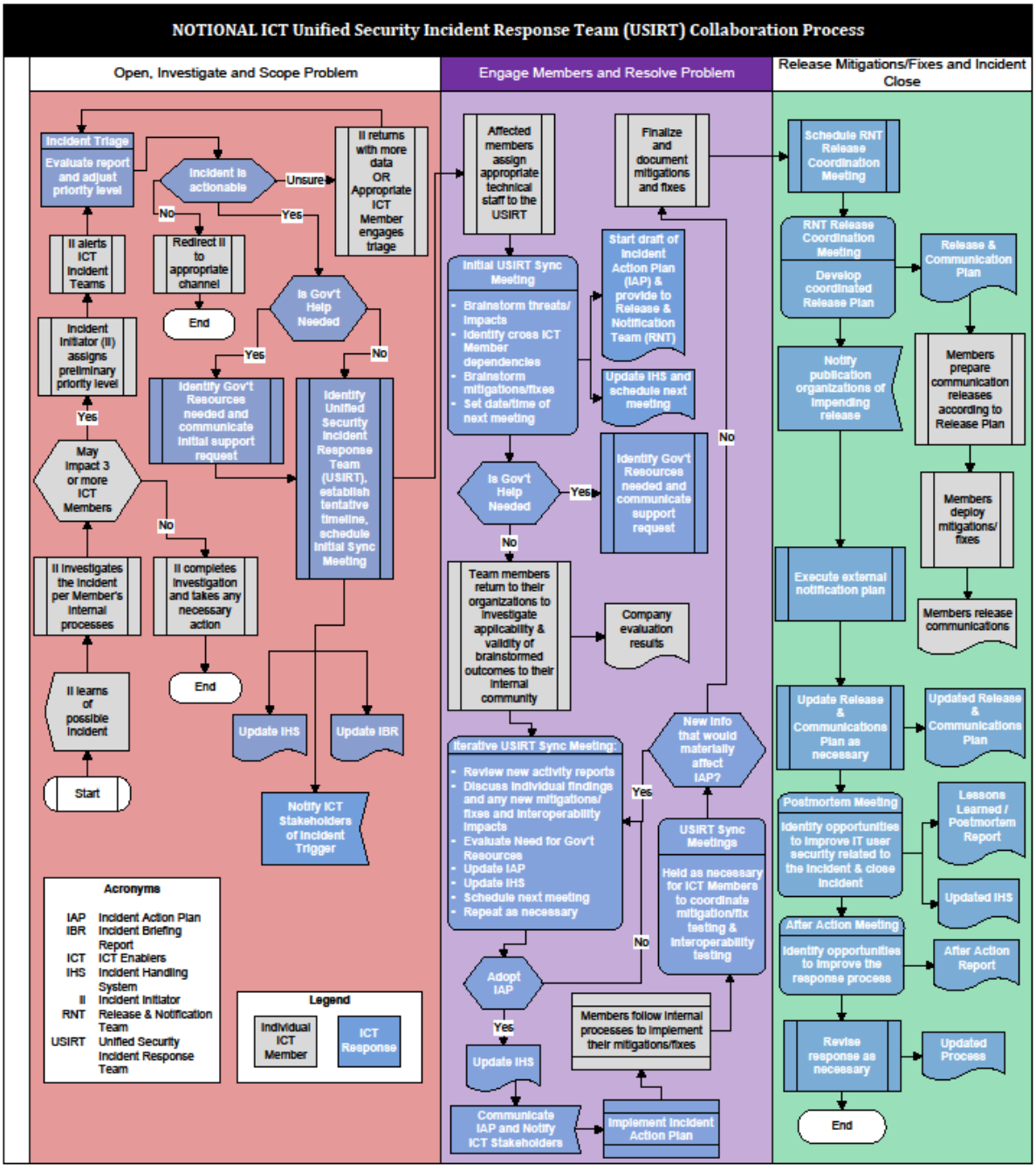
consequences as well as key stakeholders needed to help mitigate the issue. If the incident is being handled by another part of the cyber ecosystem, ICASI will determine how it can best use its expertise and trusted forum to help mitigate the problem, leveraging its ability to reach beyond members to a wider community for expertise.

ICASI's current unified process reflects decision and coordination checkpoints between members' existing SIRT processes. The unified response process includes coordination points between member, legal, corporate communications, government affairs, and incident response Teams. Key USIRP capabilities include:

- Secure collaboration for members;
- Common structured process to follow;
- Ability to reach beyond members to wider community;
- Quick reaction and triage;
- Deep and broad technical resources of members;
- Leverages community of world class responders; and
- Members bring visibility into vulnerability and threats across hardware and software stacks.[24]

[24] ICASI briefing to the NSTAC.

Figure 9: ICTC Unified Security Incident Response Team Collaboration Process



APPENDIX F: PREVIOUS NSTAC RECOMMENDATIONS

In 2003, the NSTAC's Legislative and Regulatory Task Force (LRTF) was tasked with analyzing the information sharing environment since the enactment of the *Critical Infrastructure Information (CII) Act* to determine whether barriers to information sharing still exist between industry and the Federal Government. The LRTF determined that Government and industry share information, and that the CII Act and the final Department of Homeland Security (DHS) information sharing rules are essential for the success of future information sharing.

The LRTF found that the disclosure of information and liability concerns remains a significant issue due to certain conditions under the CII Act. Since DHS is the only Federal agency covered under the CII Act, critical infrastructure data could have potentially been disclosed under the Freedom of Information Act (FOIA) to other Federal agencies or industry groups. Additionally, private industry has concerns with sharing information and participating in Information Sharing and Analysis Centers (ISAC) because they want to protect their primary business interests (e.g., their customers and stakeholders), and it is also very costly to share information with the Government. The LRTF determined that certain liability still existed in information sharing; however, developing strong trust between Government and industry is essential in the establishment of an information sharing program. The NSTAC recommended that the President direct the appropriate departments and agencies, in coordination with industry to:

- Develop a process to resolve multi-jurisdictional (Federal, State, and local) conflicts within the appropriate boundaries of Federalism and national, homeland, and economic security;
- Work with Congress to modify the CII Act so that DHS is the clearinghouse and sole dispenser of CII information;
- Encourage Congress to extend the protections of the CII Act to cover departments and agencies other than DHS and, if other agencies should be designated as such, the NSTAC recommends that they adopt the same rules and procedures as DHS for handling CII; and
- Work diligently with Congress to ensure the CII Act's provisions remain intact.

Following this NSTAC report, DHS developed and initiated the Protected Critical Infrastructure Information (PCII) program, which acted as a clearinghouse and disseminator of CII information. Additionally, the Executive Office of the President was asked to convene a meeting to review recommendations in the NSTAC's policy conflict letter and "analyze their impact to national security and emergency preparedness communications."

The NSTAC anticipates that the recommendations and findings established in the LRTF report will be reviewed and utilized to provide additional insights and knowledge during the suggested Phase Two effort.

APPENDIX G: FINDINGS

Finding	Report Section	Page Number
The unified risk assessment of a potential or actual impact provided an indicator of whether an issue should escalate or de-escalate. The assessment is a function of three criteria/parameters, including: • Event Characteristics: Does the potential or actual event (or series of events) manifest characteristics that could result in substantive disruption, corruption, or destruction of critical infrastructure, EO 13636 Section 9 entities, and sector resources? • Intelligence Sources: Do the perpetrators (i.e., threat actor[s]) have the means, intent, or ability to escalate the potential or actual event to an event of national significance? • Capability to Respond: Based upon prior knowledge, does industry have the capability to respond and address the incident, without changes in legal authority, rules of engagement, or operating framework?	**3.0**	**7**
The ORANGE level represents the domain of extensive coordination and collaboration between Government and industry in terms of dynamic protocols and procedures. At lower levels, current practiced behavior should be sufficient to maintain stability and flow in 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. It will be important to thoughtfully 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.	**3.1.2**	**12**
The RED level conceptually represents a cyber emergency of the severest nature and greatest potential impact. At this level, the total commitment of industry to sustain network and system operations will be insufficient to meet the national need. Accordingly, 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.	**3.1.3**	**13**
The response capabilities inherent within enterprises or their ISACs will not likely be the capabilities necessary to address the circumstances in an event of national significance.	**4.1**	**16**

ICT enablers represent the functionalities foundational to the global cyber ecosystem and are most capable to address the threats, develop mitigation strategies, and/or implement systemic remediation.	**4.1**	**16**
The NSTAC believes that ICT enablers likely represent the commercial assets, functions, and/or capabilities that, if operationally coordinated, would be helpful or necessary to respond to a cyber-related event of national significance.	**4.1**	**16**
Coordinated incident response by ICT enablers at ORANGE/RED-level events may necessitate Government authorities despite the potential for positive impact, as there may be accompanying unintended consequences of such action.	**4.1**	**16**
Properly addressing events of national significance, warranting the mitigation efforts of multiple ICT enablers, will require ensuring that any mitigation strategies developed consider all potential consequences—as well as impacts on all potentially impacted stakeholders, including global Internet users—and are fully authorized by requisite legal and Government authorities in the United States and other relevant jurisdictions.	**4.1**	**16**
Since the global cyber ecosystem is foundationally civilian, the U.S. Government should continue its dialogue to establish global norms for national cyber response and incorporate industry in those discussions to the maximum extent possible.	**4.1**	**17**
The ICASI USIRP process framework leverages existing industry best practices and offers a potential unified incident response model to provide for an "agile, effective, and distributed implementation across numerous stakeholders, resulting in a coherent, unified, and dynamic national response."	**5.0**	**19**
In pre-impact ORANGE-level scenarios, the protocols for how industry can request and receive incremental Governmental information, capabilities, or authorities are not well understood. This understanding is necessary, particularly for an environment when fast industry response is essential for mitigation or containment.	**6.0**	**23**
At the RED level, there is little industry understanding regarding Government goals or priorities for pre-impact protection or post-impact recovery; however, this is precisely the assessment and understanding that industry must gain.	**6.0**	**23**
The NSTAC believes there are sufficient U.S.-based entities performing ICT enabler roles to engage in this necessary dialogue and will suggest a path forward for accomplishing these goals.	**6.0**	**25**

APPENDIX H: BIBLIOGRAPHY

Anonymous. "Emerging Threat: Dragonfly / Energetic Bear – APT Group." Symantec, July 8, 2014. Available: http://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group.

Anonymous. Presentation: "Netwreck: A practical discussion about Internet disruption." Netwreck, June 10, 2010.

Cebula, James J. and Young, Lisa R., "Taxonomy of Operational Cyber Security Risks." Software Engineering Institute, December 2010. Available: http://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15200.pdf.

Cichonski, Paul, Tom Millar, Tim Grance and Karen Scarfone. "Computer Security Incident Handling Guide." National Institute of Standards and Technology, August 2012. Available: http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf.

Conficker Working Group. "Conficker Working Group Lessons Learned." June 2010. Available: http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf.

Department of Homeland Security. *Homeland Security Presidential Directive-5*. February 28, 2003. Available: http://www.dhs.gov/sites/default/files/publications/Homeland%20Security%20Presidential%20Directive%205.pdf.

Department of Homeland Security. *An Analysis of the Primary Authorities Supporting and Governing the Efforts of the Department of Homeland Security to Secure the Cyberspace of the United States*. May 24, 2011. Available: http://www.homelandsecurity.org/docs/reports/MHF-and-EG-Analysis-of-authorities-supporting-efforts-of-DHS-to-secure-cyberspace-2011.pdf.

Department of Homeland Security, Federal Emergency Management Agency. Cyber Incident Annex. December 2004. Available: http://www.fema.gov/media-library-data/20130726-1825-25045-8307/cyber_incident_annex_2004.pdf.

Department of Homeland Security, Federal Emergency Management Agency. Emergency Support Function #2 – Communications Annex. January 2008. Available: http://www.fema.gov/media-library-data/20130726-1825-25045-1540/emergency_support_function_2_communications_annex_2008.pdf.

Department of Homeland Security, Federal Emergency Management Agency. National Incident Management System. Available: http://www.fema.gov/national-incident-management-system

Department of Homeland Security, Federal Emergency Management Agency. National Preparedness Goal. Available: http://www.fema.gov/national-preparedness-goal.

Department of Homeland Security, Federal Emergency Management Agency. National Response Framework. Available: http://www.fema.gov/national-response-framework.

Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). STUXNET Malware Capabilities. December 6, 2010.

Department of Homeland Security, National Protection and Programs Directorate. *National Cyber Incident Response Plan*. September 2010. Available: http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf.

Department of Homeland Security, National Protection and Programs Directorate. *Enabling Distributed Security in Cyberspace*. March 2011. Available: http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

Dorofee, Audrey, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. "Incident Management Capability Metrics Version 0.1." Software Engineering Institute, April 2007. Available: http://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14873.pdf.

Finnish Communications Regulatory Authority. "Regulation 9 on obligation to notify of violations of information security in public telecommunications". January 1, 2010. Available: https://www.viestintavirasto.fi/en/steeringandsupervision/legislation/regulations/regulation9onobligationtonotifyofviolationsofinformationsecurityinpublictelecommunications.html.

Finnish Communications Regulatory Authority. "Regulation 57 on the maintenance of communications networks and communications services, procedures and notifications in the event of faults and disturbances." January 02, 2012. Available: https://www.viestintavirasto.fi/en/steeringandsupervision/legislation/regulations/regulation57onthemaintenanceofcommunicationsnetworksandcommunicationsservicesproceduresandnotificationsintheeventoffaultsanddisturbances.html.

Gurses, Seda. "An Ontology for Multilateral Privacy Requirements Engineering." NYU, May 2010. Available: https://www.cosic.esat.kuleuven.be/publications/thesis-177.pdf.

Harris, Shane. "The Worm that Turned." Government Executive, February 1, 2003. Available: http://www.govexec.com/magazine/2003/02/the-worm-that-turned/13332/.

Irrera, Anna. "The Bank of England Goes to Cyber War." The Wall Street Journal, June 10, 2014. Available: blogs.wsj.com/digits/2014/06/10/the-bank-of-england-goes-to-cyber-war.

Kramer, Franklin D., "Achieving International Cyber Stability." Atlantic Council, September 2012. Available: http://www.atlanticcouncil.org/images/files/publication_pdfs/403/kramer_cyber_final.pdf.

Kramer, Franklin D., "Cybersecurity and Tailored Deterrence." Atlantic Council, December 2013. Available: www.atlanticcouncil.org/images/publications/Cybersecurity_and_Tailored_Deterrence.pdf.

Dr. Levasseur, Robert, Dr. Bethe Hagens and Dr. Anne Hacker. Presentation to the NSTAC: "Information Technology Security and Human Risk: Exploring Factors of Unintended Insider Threat and Organizational Resilience." December 10, 2013.

Lewis, James A. and Timlin, Katrina. "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization." Center for Strategic and International Studies, 2011. Available: http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.

Lynch, Sarah N., "U.S. SEC Official Urges Broader Cyber-Attack Disclosure." Reuters, June 10, 2014. Available: http://uk.reuters.com/article/2014/06/10/sec-cybersecurity-aguilar-idUKL2N0OR13U20140610.

Meyer, David. "DARPA: Without Better Security, the Internet of Things Will be Messy." Gigaom, June 19, 2014. Available: https://gigaom.com/2014/06/19/darpa-without-better-security-the-internet-of-things-will-be-messy/.

O'Connor, Sarah. "Data Sharing Deal with US Referred to EU's Top Court." Reuters, June 18, 2014. Available: http://www.reuters.com/article/2014/06/18/us-facebook-privacy-idUSKBN0ET11X20140618.

Ponemon Institute, LLC. "Cyber Security Incident Response: Are we as prepared as we think." Lancope, 2014. Available: http://www.lancope.com/ponemon-incident-response/.

Prince, Brian. "Code Hosting Service Shuts Down After Cyber Attack." Information Week, June 20, 2014. Available: http://www.darkreading.com/attacks-breaches/code-hosting-service-shuts-down-after-cyber-attack/d/d-id/1278743?_mc=NL_DR_EDT_DR_daily_20140623&cid=NL_DR_EDT_DR_daily_20140623&elq=627ec0c4a5f64f7b8994cc4505677719&elqCampaignId=5255.

The White House, Office of the Secretary. "Statement by the President on the Cybersecurity Framework." February 12, 2012. Available: www.whitehouse.gov/the-press-office/2014/02/12/statement-president-cybersecurity-framework.

Thompson, Amy and Rahn, Cornelius. "Russian Hackers Threat Power Companies, Researchers Say." Bloomberg, July 1, 2014. Available: http://www.bloomberg.com/news/2014-06-30/symantec-warns-energetic-bear-hackers-threaten-energy-firms.html.

Tothova- Jordan, Klara. "Reexamining Article 5: NATO's Collective Defense in Times of Cyber Threats." The Huffington Post, August 13, 2014. Available: http://www.huffingtonpost.com/klara-tothova-jordan/reexamining-article-5-nat_b_5491577.html.