# LIVEWIRE – AFTER ACTION REPORT

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgements</td>
<td>3</td>
</tr>
<tr>
<td>I. Executive Summary</td>
<td>4</td>
</tr>
<tr>
<td>II. Preface</td>
<td>7</td>
</tr>
<tr>
<td>III. Background</td>
<td>9</td>
</tr>
<tr>
<td>IV. Observations</td>
<td>13</td>
</tr>
<tr>
<td>V. Policy Issues and Related Questions</td>
<td>24</td>
</tr>
<tr>
<td>VI. Recommendations</td>
<td>27</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Acronyms</td>
<td>30</td>
</tr>
</tbody>
</table>
ACKNOWLEDGEMENTS

The Exercise and Scenario Development (ESD) Group at Dartmouth’s Institute for Security Technology Studies sincerely appreciates the commitment of resources on the part of many stakeholders to make Livewire possible. The Department of Homeland Security (DHS) devoted an extraordinary level of personnel resources to maximize the value of their participation in the exercise. Likewise the Emergency Planning and Response Directorate (FEMA) within DHS strongly advocated and participated in Livewire. At DHS request the National Security Agency committed exceptionally professional and knowledgeable personnel to the Livewire project, without whose strong support Livewire would have been impossible to implement. We are grateful for the backing of Paul Kurtz and Greg Rattray on the HSC and NSC staffs, respectively.

Livewire was useful primarily due to the strong participation of industry and state/local government organizations. The ISTS is truly grateful for the dedication of time and resources by stakeholders in private industry, as well as state and local government, and hope that each organization received the desired level of return from its valuable contribution.

We also wish to thank The MITRE Corporation, The National Center for the Study of Counter-Terrorism and Cyber-Crime at Norwich University, The Wargaming Center at the Naval War College, the New England Information Operations Center of the U.S. Army Reserve, and the Critical Infrastructure Protection Project at George Mason University School of Law’s National Center for Technology and Law for the resources and expertise each provided. Within Dartmouth, we wish to acknowledge the strong support of the Office of the Provost, the Grants and Contracts Office, the Thayer School of Engineering, the Tuck School of Business, Sociology faculty at the school of Arts and Sciences, the staff of the Public Key Infrastructure (PKI) lab, and the Kiewit Computation Center.
SECTION 1 – EXECUTIVE SUMMARY

Purpose: This report summarizes activity and observations from the Livewire exercise. It is intended for a primary audience of policy-level decision-makers within participating organizations, with emphasis on lessons for federal authorities.

Livewire Background

Purpose of Livewire Exercise: Livewire was a large-scale cyber-focused communications exercise engaging private and public-sector decision-makers. It was the first in what is intended to be a series of three exercises designed to substantially contribute to the design and implementation of the National Cyber Security Response System (NCSRS) as called for in The National Strategy to Secure Cyberspace.

Scenario: Livewire posited a scenario, in which a nation-state launches a campaign-level, well-coordinated cyber attack against a diverse target set of key infrastructure nodes within the United States. The aggressor’s aim is to apply pressure on the U.S. economy sufficient to force the U.S. to change its foreign policy. The scenario included attacks aimed at disrupting key nodes within the telecommunications (Internet), energy, and finance sectors, also attempts through cyber means to disrupt federal, state, and local government response and recovery. The hypothesis behind the selection of this scenario was that response mechanisms appear stove-piped, ad-hoc, and uncoordinated across sectors and between levels of government and potentially not sufficient to handle a well-coordinated, campaign-level cyber attack lasting weeks to months and targeted across sectors.

Public Sector Objectives: Through the Livewire series of exercises, federal stakeholders seek to understand which elements of the current cyber-focused ad-hoc response mechanisms might perform well against a concerted threat, and which need to be strengthened; what coordinated decision-making mechanisms exist and where there are gaps; where actors are likely to work at cross-purposes without better coordination; and the extent of information-sharing seams between organizations. Objectives further include practicing of coordinated responses, sorting of roles and responsibilities, exercising policies and procedures, and decision-making relative to continuity of operations and resource allocation under conditions of uncertainty and stress.

Participants: Over 50 organizations and 300 people participated in Livewire from many venues around the country:
1. Federal government: (acronyms in appendix A) Department of Homeland Security (IAIP, EP&R, TTIC); (White House: NSC, HSC, OMB, OSTP); Department of Commerce, Department of Defense (JTF-CNO, NORTHCOM, DIA); Department of Energy; Treasury; Department of Justice (FBI Cyber Crimes Division, Computer Crime and Intellectual Property Section (CCIPS)).
2. State and local government: Two major cities and their associated state governments.
3. Finance and Multi-State Information Sharing and Analysis Centers (ISAC’s).
4. A range of private enterprises including telecommunications firms, hardware and software manufacturers, internet service providers (ISP’s), a large energy provider, and large financial
institutions, including a major national bank, a securities exchange, a securities clearing utility, and a large agency clearing firm.

**Executive Agent:** Dartmouth’s Institute for Security Technology Studies (ISTS) was the Executive Agent for the exercise and was supported by a wide range of subject matter experts from the public and private sectors.

**Key Observations (Prioritized):**

- **Who is in charge?** Many policy issues remain open relative to transitioning of authority, roles, and responsibility between agencies as a cyber event escalates from an enterprise problem, to a law enforcement issue, to a homeland or national security event (Refer to Section 5).
- **Some participants assumed that federal authorities will be able to anticipate a widespread cyber attack, and will be the initial and continuing source of situational awareness for state and local decision-makers or private industry. Livewire brings these assumptions into question. All stakeholders should realize that timely attribution of the source of an attack may not exist. The indications of a sophisticated and coordinated cyber attack may not be initially visible to the cadre of technicians monitoring Internet health or assessing now familiar patterns of vulnerability exploits. Private industry will be an integral component in the Indications and Warning process; it must provide timely indications of cyber attack and other information needed to gain and maintain situational awareness.**
- **A “large scale” cyber attack as envisioned in the Livewire scenario would have activated established emergency response communications. However, these mechanisms are not sufficient to ensure necessary situational awareness between private industry and government authorities in the case of a large-scale cyber attack that crosses sectors, industries, and/or levels of government, particularly in the critical early stages of that attack.**
- **Current means of predicting the economic impact of potential cyber attacks and response options are inadequate.**

**Key Recommendations (Prioritized):**

- **A National Cyberspace Security Response system must be capable of dealing with infrequent strategic and wide-scale cyber attacks, not just the more common set of criminal and/or nuisance cyber events. This plan should clearly delineate authority, roles, and responsibilities across a range of escalation thresholds.**
- **All levels of government and industry should be involved in developing viable response options to mitigate the effects of a cyber attack that uses the Internet as a conduit for putting critical infrastructure at risk.**
- **On a sector, regional, and individual enterprise basis, identify and promulgate the specific information gathering and sharing requirements needed to gain situational awareness under the conditions of a cyber attack. Ensure these information requirements directly support the timely selection and implementation of effective response options. Ensure all**
participants in a national cyber response system understand the technical and situational types of information that must be shared; the processes for sharing it, and who the recipients should be under different threshold conditions. Pay particular attention to thresholds that may not have been crossed yet in the real world, i.e. when a cyber problem transitions from that which should be addressed by law enforcement to that which falls under the authority of homeland or national security authorities. Discover the legal, cultural, and organizational hurdles for sharing critical information, and take the necessary steps now to overcome these hurdles.

• Consider the extent to which the Homeland Security Advisory System should be sensitive to non-physical threats and to geographic and sector variations.

• Develop a means of institutionalized authentication between decision-makers in government at all levels and critical infrastructure nodes within private industry.

Relation to the Department of Homeland Security

Livewire presented the first opportunity for the DHS Interagency Incident Management Group to come together as a response group. It did so for three full days, during which it:

• Coordinated efforts to pull information from private and public sector players;
• Analyzed scenario-based events and determined that seemingly disparate cyber attacks against various enterprises in different sectors amounted to a coordinated attack requiring that the national alert level be upgraded from yellow to orange;
• Discussed the need for a separate “cyber” alert condition (“cyber orange, cyber red”); and
• Anticipated that the degradation of national information infrastructure through cyber attacks might severely undermine effective implementation of physical security measures as the traditional color alert system moved from yellow to orange to red.

Livewire helped the National Cyber Security Division (NCSD) of DHS evolve quickly. It offered the NCSD a timely opportunity to immerse itself in a challenging cyber response problem and apply lessons learned from that opportunity toward creation of documented processes for responding to cyber events. It also presented a valuable opportunity for the merged NCSD elements (National Communications System, Federal Computer Incident Response Center, and the National Infrastructure Protection Center) to practice a range of complex coordination processes as a cohesive unit.

The EP&R Directorate gained needed insight into the potential for disruption of its assigned tasks if there is a loss of Internet Protocol (IP) –based communications systems.

Livewire introduced key people across the federal government, from various ISACs, state and local governments, and within a purposely-restricted segment of industry to one another.
A top priority of the 2003 *National Strategy to Secure Cyberspace* is the creation of a National Cyberspace Security Response System. The *Strategy* intends that this system provide similar capability vis-à-vis strategic cyber attacks as does the North American air defense system against aerospace threats. An effective cyber response system ultimately will extend into the private sector and across international boundaries and must harness the participation of a broad constituency whose only common ground is its information interconnectivity. The major elements of the national aerospace defense system include people, organizational structure, processes, technologies, and training. The same elements of a cyber response system must reflect a diversity of organizational cultures, risk and threat assessments, missions, communication processes, and technological capabilities. Each constituent organization must be engaged on its own terms. In the absence of mandated participation each must perceive value to participate voluntarily in a coordinated response system.

As *Livewire* showed, the indications of a sophisticated and coordinated cyber attack may not be initially visible to the cadre of technicians monitoring Internet health or assessing now familiar patterns of vulnerability exploits. Rather than disrupt telecommunications networks, sophisticated attackers may use these networks as conduits of cyber attack. Such indications may only be manifested in disrupted business processes, unusual societal effects, or as technical anomalies at the edges (end users) of the Internet. Widely distributed across sectors, many indicators might never be noticed before an attack vector is publicly visible. If noticed at all, they may appear to enterprise-level decision-makers as discrete events, not worth communicating to those with responsibility for piecing together an all-source cyber picture. If communicated at all, knowledge of any single indicator may remain within a small network of trusted professional or personal acquaintances. If communicated to public authorities, there remain additional hurdles for the sharing of valuable indicators between different state, local, and federal authorities.

Once a strategic and coordinated cyber attack is underway, actual or perceived disruption of communication networks may make it difficult for federal authorities to gain and maintain situational awareness of key infrastructure capability around the country.

With few exceptions it is the responsibility of private industry to recognize and address a significant anomaly to its “normal” state of business or network health. This dependence on the private sector suggests how integral a component private industry will be in a national cyber response system. This component must help to provide decision-makers with timely indications of cyber attack and other information needed to gain and maintain situational awareness. This component may also be required to implement carefully coordinated defensive measures in concert with organizations beyond their normal business environment.

An often-voiced theme from *Livewire* is that private industry will only share information desired by the federal government (i.e., will only participate in a coordinated response system) if there is perceived value in doing so. Public agencies must reciprocate by sharing valuable information on a timely basis with industry. By collaborating with CERT/CC to establish the US-CERT as a central national authority for addressing cyber threats, DHS has taken effective
advantage of nationally-recognized expertise within that organization and the trusted
relationships it has with many in private industry and government to set a standard for providing
value to the private sector. CERT/CC has demonstrated its value to a variety of constituents by
providing tactically useful information. To the extent that the US-CERT continues to extend its
utility in collecting, analyzing, and sharing tactically-relevant information it will enhance the
capability of the National Cyberspace Security Response System.

Yet as challenging as it is to engage the voluntary participation of a diverse constituency
in sharing of tactically useful information relative to common cyber incidents, it will be even
more difficult to engage the involvement of that same constituency in a response system capable
of addressing infrequent strategic cyber threats. There are several reasons for this: economic,
cultural, political, and technical. Many factors combine, perhaps, to create complacency in the
public mind toward the possibility of a strategic cyber attack that differs greatly from the routine
in signature, focus, duration, magnitude, and effect. Relatively low-level cyber incidents have
become routine. Some Chief Information (Security) Officers are quite confident of their ability to
secure their enterprise fortress, yet their control ends at their gates. A central purpose of
Livewire, and arguably its chief value, was in sensitizing decision-makers to the possibility of a
strategic cyber attack. Certainly Livewire substantially increased the number of individuals who
have considered the implications of a strategic cyber attack on the U.S.

The possibility of a debilitating strategic cyber attack is quite difficult to comprehend due
to a lack of prior experience. Strategic attacks are by nature much less likely to occur than
criminal or terrorist incidents. It took Sputnik and the Cold War to galvanize public support for
strategic aerospace defense capability. Sputnik was publicly visible. Its cyber equivalent may
not be as evident. Some well-informed officials wonder if that equivalent hasn’t already
streaked across cyberspace (9 of 13 Domain Name Servers affected by a single attack in 2003;
known compromise of over 100,000 machines world-wide for Distributed Denial of Service
attack purposes). Others publicly question any possibility of effective cyber attacks by terrorist
groups or nation states.

It may be that a strategic cyber attack cannot be defended by traditional military actions,
and therefore must be met through the coordinated efforts of a broad coalition in industry and
government. Cyber-defensive assistance from either the military or Department of Homeland
Security is not yet sufficiently defined to meet these circumstances.

To the extent that national and homeland security officials believe that such a threat now
or may in the future exist, practiced response to that threat is critical. It is best to work through
the many challenging issues facing improved coordination between private- and public-sector
stakeholders in an exercise environment rather than during a real-world crisis.
SECTION 3 – BACKGROUND

Livewire engaged many decision-makers from federal, state, and local governments, along with their private-sector counterparts, in a week-long cyber “discovery” exercise to practice response to a complex cyber attack by a capable adversary. The purpose of this effort was to help illuminate the coordination processes, communications paths, and other architectural elements required of a National Cyber Security Response System as called for in The President’s National Strategy to Secure Cyberspace (http://www.securecyberspace.gov/).

The National Strategy identifies eight major actions and initiatives for cyberspace security response:

- Establish a public-private architecture for responding to national-level cyber incidents;
- Provide for the development of tactical and strategic analysis of cyber attacks and vulnerability assessments;
- Encourage the development of a private sector capability to share a synoptic view of the health of cyberspace;
- Expand the Cyber Warning and Information Network to support the role of DHS in coordinating crisis management for cyberspace security;
- Improve national incident management;
- Coordinate processes for voluntary participation in the development of national public-private continuity and contingency plans;
- Exercise cyber security continuity plans for federal systems; and
- Improve and enhance public-private information sharing involving cyber attacks, threats, and vulnerabilities.

The National Cyberspace Security Response System (NCSRS) is envisioned to be a public-private architecture, coordinated by the Department of Homeland Security and intended for:

- Analyzing and warning
- Managing incidents of national significance
- Promoting continuity in government systems and private sector infrastructures
- Increasing information sharing across and between organizations to improve cyberspace security.

The NCSRS will include governmental entities and nongovernmental entities, such as private sector information sharing and analysis centers (ISACs).

Objectives: Exercise objectives included:

- Examine the decision making systems from enterprises and state and local government up to and including the national government while practicing a coordinated response to a concerted cyber threat;
- Examine the roles and responsibilities and internal and cross organizational procedures required to defend against a sustained attack on and through the Internet; and
- Foster relationships between public and private sector organizations.

Included in these objectives was a desire to understand which elements of the current ad hoc cyber-response mechanisms might perform well against a concerted threat, and which
mechanisms need to be strengthened; what coordinated decision-making mechanisms exist, and where additional mechanisms are needed; where agencies are likely to work at cross-purposes without better coordination; and the extent of information-sharing gaps between organizations. The exercise further allowed practicing of coordinated responses, sorting of roles and responsibilities, exercising policies and procedures, and decision-making relative to continuity of operations and resource allocation under conditions of uncertainty and stress. Federal, state and local government agencies and private sector enterprise participants also desired to enhance in-house cyber security and apply lessons learned as a result of their exposure to Livewire.

**Scenario:** *Livewire* simulated a scenario in which a capable adversary launched a month-long, well-coordinated cyber attack against a diverse target set of key infrastructure nodes (energy, telecommunications, finance, and state/local governments) within the United States. The aggressor’s aim was to apply pressure on the U.S. economy sufficient to force the U.S. to change its foreign policy. The scenario assumed a technically capable and well-funded adversary and a campaign planning and preparation period of over three years. Given these assumptions, a cyber attack of this nature was considered by a range of technical experts in both private industry and government to be technically feasible.

The exercise, which occurred within a simulated network environment, was conducted for five days representing the initial 30 days of this scenario in compressed time with roughly six days of events happening every day of exercise play. The event started from a normal state of network health and progressed slowly toward a sustained cyber campaign attacking financial, energy, telecom and state and local government sectors. The cyber campaign scenario simulated attacks on and through the Internet. Within this scenario, e-mail and other Web-based services became unreliable, information systems and databases connected to the Internet became inaccessible, content was corrupted, and back-up systems including manual alternatives to automated systems became overloaded. Control systems for critical infrastructure such as energy distribution were disrupted.

**Exercise Structure:** *Livewire* engaged decision-makers within most participating organizations at three different levels: strategic leadership, continuity of operations, and the network operations center. The federal sector participation took place only at the first two levels because federal systems were not attacked in the *Livewire* scenario. Three coordinated exercise drivers generated the exercise activities:

- A network simulation representing generic versions of sector-level enterprise networks displayed the effects of various attacks, allowed the network operations centers to conduct defensive operations, and presented the results to network managers. There were 20 networks and about 750 nodes in the simulation.
- A detailed event list of over 2,000 discrete events which we call “injects” supported by dynamic scripting provided the collateral effects of the attack to decision-makers in a fully interactive exercise environment. (Typical inject syntax: Router DoS attack from Internet against Firewall, Firewall_3, IP 43.10.0.5, from ISP_SouthC (via router Pub_Internet))
- A simulated 'Virtual News Network (VNN)-type' news feed provided most participants with a general picture of critical events as they took place to insure that the federal sector
had the visibility on the societal consequences of the attacks that they would have in the real world.

**Rules of Engagement:** The exercise did not include attacks on or through real-world networks. Attacks and remediation occurred within a secure, distributed, and controlled Web-based exercise simulation environment. The one-sided scenario injects to force decision-making were scripted. The exercise was played at the unclassified level to ensure maximum participation by the private sector. Private and public sector organizations participated voluntarily. The identities of private-sector organizations playing in *Livewire* are not for attribution. All participants are self-evaluating their performance; this assessment by the ISTS team focuses on coordination between organizations.

**Sequence of Major Activities:** The following events were part of the design and implementation of *Livewire*:

- Initial Planning Conference (April 2003) – bring together stakeholder representatives and exercise designers to explain the exercise and development process
- Mid-Term Planning Conference (June 2003) – to gain buy-in of the scenario and understanding of objectives
- Dry-Run (September 2003) – to shake down the software and communications
- Final Planning Conference (September 2003) – review final scenarios for conflicts
- Exercise (October 27-31 2003)
- After-Action Conference (December 10 2003) – stakeholders sit around the table with government agency personnel to talk about issues raised
- Policy Seminar (December 15, 2003) – engage high level government officials to address key questions about role and response

**Participants:** Over 50 organizations and 300 people participated from many venues around the country:

- Federal government: (White House: NSC, HSC, OMB, OSTP); Department of Homeland Security (DHS) units such as the Interagency Incident Management Group (IIMG), elements of Information Analysis and Infrastructure Protection (IAIP) and Emergency Preparedness & Response (EP&R - FEMA) including Homeland Security Operations Center, National Cyber Security Division, National Communication System, U.S. Secret Service, National Coordination Center, Infrastructure Coordination Division, Information Management & Requirements Division, Risk Assessment Division, Protective Services Division, FEMA Regions I and X, and EP&R headquarters elements); DoD (JTF-CNO, NORTHCOM, Intelligence Community); Department of State (Policy, Plans, and Analysis); CIA; DOE; Commerce; Treasury; the Federal Reserve, the Securities and Exchange Commission; and DOJ (FBI Cyber Crimes Division, U.S. Attorney’s Office).
- State and local governments: Two major cities and their associated states; another six states participated through the Multi-State ISAC.
- Finance, telecommunications sectors, and Multi-State ISACs
A range of private enterprises including telecommunications firms and Internet Service Providers (ISPs), software and hardware providers, large financial institutions, and a multinational energy provider.

Exercise Scope: *Livewire* did not include any of the following due to resource and time constraints:

- Inter-sector interdependencies (i.e., a participant from the finance sector was not required to respond to disruptions in the energy sector, or vice-versa). The only interdependencies examined were reliance on telecommunications and IT infrastructure, as well as reliance on the federal government to respond to issues of homeland and/or national security).
- There was no attempt to include more than a handful of participants from the banking and finance, energy, IT and telecommunications sectors.
- Federal participants were not required to “play” their own dependencies on IT infrastructure; rather their participation was limited to responding to problems raised in the various infrastructure sectors and by state and local governments.
- The scope of the *Livewire* scenario was limited almost exclusively to cyber events.
- The scenario was one-sided, that is events were driven by opponent activities and there was limited “free play.”
At the time that Livewire was conducted, efforts to create a National Cyberspace Security Response System were basically at the “blank slate” stage. The Bush Administration published the National Strategy calling for the creation of a Response System early in 2003. The National Cyber Security Division (NCSD) within DHS, charged with executing the Strategy, did not formally “stand up” until just prior to Livewire. To their credit, the NCSD and its parent organization, the Information Analysis and Infrastructure Protection (IAIP) Directorate, used Livewire as a timely opportunity to baseline processes, establish organizational relationships, and collaborate with stakeholders in industry and across government to define, in some measure, the operational requirements for such a system. Livewire forced NCSD to start off at a sprint. The ISTS believes the NCSD performed well under the circumstances.

At the request of federal authorities Livewire examined a strategic cyber attack scenario. Those authorities shared with the ISTS their concern for a future in which information warfare presents a far more robust set of cyber “attack vectors” than those posed by current viruses, worms, and distributed denial of service attacks. Without comment on the validity of that view of the future of information warfare, the ISTS was strongly influenced by its interactions with a range of stakeholders during the last year toward the conclusion that the nation is a long way from a system capable of dealing with strategic cyber threats. We saw little evidence of a set of cohesive processes or system components capable of providing detailed situational awareness from private industry and state/local authorities to federal authorities in the event of a large-scale cyber attack that crosses sectors, industries, and/or levels of government.

Judging by the Livewire scenario, crafted by subject-matter experts from industry and government, the indications of a sophisticated and coordinated cyber attack may not be initially visible to the cadre of technicians monitoring Internet health or assessing now familiar patterns of vulnerability exploits. Private industry will be an integral component in the Indications and Warning process; as such it must help to provide decision-makers with timely indications of cyber attack and other information needed to gain and maintain situational awareness in an event that might evolve to risk significant portions of U.S. society, economy, and government.

It is intuitively obvious that telecommunications carriers will be central to a response system capable of dealing with strategic cyber threats. They own the pipes through which an adversary could theoretically launch attacks at critical end-user targets. The ISTS was surprised by the degree to which many of the telecommunications firms, which the ISTS attempted to engage in Livewire, declined to participate, even while acknowledging the potential value of the exercise to their organizations. It seems likely that many firms were concerned that Livewire might show that ad-hoc mechanisms for addressing today’s cyber threats must not be relied upon to thwart a sophisticated and wide-spread attack by a capable and determined adversary, and that this conclusion might lead to unwanted regulation. As a “first of breed” exercise, Livewire was not sufficiently sophisticated to reveal the extent to which the ad-hoc “first responder” community of Internet technicians may or may not be able to mitigate a strategic cyber threat.

It was not a surprise to see the extent to which many policy issues remain open relative to transitioning of authority, roles, and responsibility between agencies as a widespread cyber event
escalates. The thought of dealing with a strategic cyber attack is new to many in industry and state/local governments, and probably also to many in law enforcement. Federal roles and responsibilities are obviously in a state of change and evolving rapidly. The ISTS hopes many of the policy questions raised in this report can be addressed to some extent by relevant authorities within the next year. We advocate evaluating the merits of these decisions in a future exercise, perhaps as early as April ’05.

The ISTS believes the following subjective observations are relevant to the creation of a National Cyberspace Security Response System. They reflect participant and/or observer lessons learned. Each represents an informed, thoughtful, and professional opinion resulting directly from an immersive experience in Livewire. They are loosely grouped into the following categories: Crisis Response Planning; Situation Awareness; Coordination and Communication; Response and Mitigation; Roles and Responsibilities; Regulation; and Future Exercises.

(Note: Parentheses indicate the primary source of the observation. “ISTS Team” indicates the observation is made by the Institute for Security Technology Studies at Dartmouth College and/or the subject-matter experts or observers it hired for the exercise. “S&LG” indicates the primary source of the observation is from a participant from one or more of the participating State and Local Governments. Other names are self-explanatory.)

**Crisis Response Planning**

1. (ISTS Team) Drawing from its experience during both the design and implementation of the exercise, the ISTS found that challenges leading to confident and informed national-level decision-making in the event of such a crisis include:
   a. Building trust relationships and ensuring trusted communications,
   b. Addressing enterprise concerns about disclosure risks and unwanted regulation,
   c. Establishing and practicing effective cross-sector coordination processes, and
   d. Understanding the potential economic, diplomatic, and national-security implications of various response options.

2. (ISTS Team) The issues of government functions relative to public safety and health are vital, however, political concerns will, in many cases, drive public information policy and mass communications.

3. (S&LG) State and local government participants found that cyber disruptions, at the level experienced in this exercise, threaten the ability of the government to exercise its primary responsibility to assure the health and safety of its citizens. As a public safety issue, a wide range of consequences must be anticipated and traditional responses may not be appropriate.

4. (S&LG) State and local government participants found that there is a need for authoritative threat and event-level response guidelines that include prioritization of (or restoration of) service, delineation of changes to roles, responsibilities, and jurisdictions between federal, state, and local governments and the private sector.
5. (S&LG) State and local officials, in after-action review of their participation and lessons learned from Livewire, concluded that the relationship between the cyber world and the public safety world needs to be clarified and documented. Cyber threats pose real public safety and security challenges. The exercise demonstrated the need for constant communication between the two worlds. Physical protection of critical state information technology infrastructure and services, as well as the state’s Chief Information Officer and other senior technical staff (city, state and public safety) became an issue that needs to be further explored. Perhaps adopting traditional public safety incident command methodology within the cyber world might be discussed and, conversely, public safety officials might include cyber threats as a legitimate threat to the state’s infrastructure.

6. (Federal Energy) Drawing from response to scenario-based events during the exercise, federal participants from the energy sector question how long the electric power industry can operate/run the electric grid in manual mode. They have concern that people and skills necessary for manual operations have migrated away from the industry and/or atrophied as it has evolved to Internet-based market matching (producers to distributors) and IT-dependent control systems.

7. (ISTS Team) The cyber-protection requirements and expectations associated with the establishment of Homeland Security Advisory System Threat Condition Orange were unclear to many participants. Are there circumstances under which an increased threat condition might be declared based on cyber threats alone?

8. (S&LG) State officials concluded that access to systems and locations also become an issue. From a state perspective, how do we manage systems remotely? Although individual entities may have current reaction plans, how do we approach this as an enterprise (state)? What impact does a biological or chemical attack or accident have on access to systems? Credentialing of public safety and law enforcement personnel is being discussed at the state Executive Office of Public Safety level, but are we considering designating certain Information Technology personnel as a part of the public safety world?

9. (S&LG) The exercise confirmed the need to establish a strategy from the political and media world. Who presents the message to the public in such an event? Is it the local official, such as the Mayor, or at the state level, the Governor? What about the national message? Do we have a strategy in dealing with the media? All of these questions arose within Livewire.

10. (S&LG) As part of the wrap-up process subsequent to their participation in the exercise, the ISTS team asked state and local government officials to use their best judgment to define disruption in the event of loss of access to Data/Network Operations Centers. They did so in duration-dependent terms:

   a. One Day: “minimal disruptions,” “inconvenience” are key descriptors.
      1) Critical public safety systems immediately operate from back-up locations.
2) Some critical operational systems may be operated in “old” manual modes.

b. One Week: “major” or “significant” disruptions are key descriptors.

1) Mid-term (or long-term depending on circumstances) disruption affects services to citizens and to government employees.

2) Also affects city/state financial and revenue services.

3) Public reaction (pressure and panic) would also be a major factor.

c. One Month: “disastrous” or “non-functioning” are potential descriptors if the nature of the event prevents employment of Continuity of Operations or Disaster Recovery plans.

Network restoration priorities would be public safety (police/fire/emergency management services/health) dispatch and communications systems, and systems supporting communication between public officials and citizens.

11. (Finance) Finance sector participants found during the exercise that notwithstanding their sophisticated risk management and mitigation processes, in a time of crisis Finance and Banking sector enterprises would prefer to behave as a system rather than a collection of independent companies each making decisions independently. This culture drives the need at each enterprise for early recognition by federal or sector-level authorities regarding the scope of an untoward event, as well as the desire for informative, sector-wide information during a wide-spread crisis.

12. (Finance) Finance sector participants found during the exercise that their sector will require frequent and intense interaction between financial firms, the FSSCC, regulators, and DHS to meet a wide-scale crisis. Opportunities are needed for key FSSCC members to work with and clarify how they communicate with DHS.

### Situation Awareness

13. (ISTS Team) Creating common situational awareness within the federal government, much less across multiple sectors and multiple levels, is a critical, yet challenging, problem given the speed and potential breadth of a cyber attack.

14. (ISTS Team) In the event of a widespread cyber attack, communications with unfamiliar and untrusted sources will be necessary. Established networks of personal relationships may not be extensive enough to cover communication requirements in the event of a broad cross-sector crisis.

15. (ISTS Team) Determining that an increase in cyber activity is a focused attack and then attributing that attack to a source may be a lengthy and challenging task, inhibiting actions to mitigate the attack. However,

   a. the federal Interagency Incident Management Group decided that available response options (i.e. somehow segmenting the network) might cause more harm, economic or otherwise, than allowing the attacks to continue;
b. purely defensive measures only mitigated the consequences; they did not prevent nor end the attack;

c. defensive solutions may require 'quarantining' a large segment of the cyber infrastructure to contain a cyber attack vector and reduce the likelihood of re-infection with significant economic consequences; and

d. if major sector or cross-sector solutions of this nature are required, they must be coordinated at the Federal level, creating a significant public-private relationship issue.

16. (ISTS Team) National information collection, analysis, dissemination and sharing were fragmented and incomplete, resulting in slow recognition that an attack was taking place and incomplete situational awareness throughout the exercise. A federal player goal was to discriminate between normal activity and coordinated attacks. Challenges to meeting this goal included:

a. Lack of a clear definition of the responsibilities of public and private organizations including the ISACs for information gathering, analysis and dissemination; i.e., define what the federal government is responsible for and what is the ISAC responsible for;

b. Lack of defined essential elements of information and common information collection processes that were understood and accepted across public and private sectors. This results in multiple organizations all collecting similar information from the same places;

c. There was little push of information - virtually all information had to be pulled from organizations experiencing problems;

d. In many cases organizations experiencing problems lacked a clear understanding to whom or when they must report problems;

e. Policy conflicts confounded information sharing between private and federal sectors other than where required by regulatory requirements; and

f. Some members of the private sector see communication with the federal government as principally one-way, with very limited payback, while potentially damaging in a highly regulated industry.

17. (ISTS Team) It might be difficult to determine whether seemingly isolated attacks in fact represent a strategic and coordinated threat. A sophisticated attack may not be visible to telecommunications network operators, but rather might only manifest itself later with harmful effects on a societal level, possibly well after the attack occurs. An effective intelligence Indications and Warning component of a cyber response system must:

a. Recognize (among other tactical intelligence indicators) the possibility of both technical and societal indications of an attack, or the presence of only technical or societal indications, and

b. Maintain a relevant picture of the national status of key infrastructures, across all sectors.
c. Operate in a degraded communications environment, including that in which the potential for misinformation is a concern.

18. (ISTS Team) Members of the Intelligence Community (IC) believe attribution of cyber attacks may not be possible or not timely enough in many circumstances. While this assessment did not originate with Livewire, the exercise did reinforce that a lack of attribution negatively impacts ability to perform Indications and Warning and respond effectively.

19. (Intelligence Community) IC representatives believe there is a need for the IC to better understand what are considered “normal state” business processes, so as to better gauge anomalies as potential early indicators. This might include building business process models for individual sectors and across all sectors.

20. (S&LG) Reporting thresholds were not clear to state and local government participants, who found that there is no simple and effective reporting structure for cyber disruptions between local and state governments, nor between local/state governments and their federal counterparts.

21. (Finance) Participants in this sector found during the exercise that the Financial Services ISAC (FS/ISAC) will likely be a key node for crisis communications, information-sharing, analysis and widespread dissemination of periodic situation reports and crisis action messages. Participants expected and needed specific, timely analysis of technical and non-technical information. Participants from the finance industry believe that in the event of a wide-scale cyber attack, the FS/ISAC will require a more robust information-sharing capability than it currently has. The Next Generation FS/ISAC is expected to take this role. (Note: ISAC play in Livewire was limited to the Finance sector and the Multi-State ISAC. The ISTS team believes the conclusions drawn for the FS/ISAC above most likely pertain to other ISACs as well, given that the FS/ISAC is currently one of the most capable ISACs).

22. (Finance) As one participant expressed it, “How can we better assess scope/scale/effects of opponent’s cyber operations?” Within the constraints of the exercise, the finance sector did not have a centralized information processing center. Participants mentioned the Y2K center as a successful model; it would be worthwhile to review the mechanisms that were established for Y2K. Note: The Financial and Banking Information Infrastructure Committee (FBIIC) Communications Center did not participate in Livewire; the ISTS cannot comment on its utility as a centralized processing center. Federal finance officials believe it would contribute significantly to situational awareness within the sector, even within the Livewire scenario.

23. (Finance) Within the exercise, some information from DHS—such as changes to alert levels—reached finance sector participants through the FS/ISAC, other information did not. Participants believe that information from the DHS daily intelligence summary or other finished analytical products might have aided the finance sector to better defend itself. As one private-sector participant summarized, “Status reports on scale of attack from the Federal entities would have been helpful.” Note: the ISTS team questions whether daily summaries would be sufficient to address a rapidly evolving cyber attack.
24. (Dept of Commerce) The threshold for convening the federal Interagency Incident Management Group (IIMG) was set artificially low for Livewire, so that the newly-organized group could maximize its learning opportunity. The threshold for convening the IIMG should remain relatively low in order to foster similar processes and expectations between federal agencies and get them thinking along the same lines.

**Communication and Coordination**

1. (ISTS Team) There is a requirement for coordinating both sector and national responses to such events and closing the gaps that exist between sector-level response activities, law enforcement, and national/homeland security functions in a cyber operations environment.

2. (ISTS Team) Some participants observed that the rapid transition of voice telephony to ‘voice over IP’ (VoIP) places both of the primary communications systems used by the private sector at risk under a cyber campaign. Note: The Livewire scenario did not include any VoIP attack events; this observation was made in general terms in after-action discussions.

3. (ISTS Team) Participants from the Finance and Energy sectors stated that they could not operate selected primary or back-up systems if both voice and Internet communications were unavailable. However, the private networks owned by major corporations in many cases do provide robust internal communications.

4. (ISTS Team) Backup communications capabilities and/or processes may be needed to support the widely diverse and distributed range of private-sector stakeholders needed to guarantee “Continuity of Society”, “Continuity of Economy”, and “Continuity of Operations (COOP) in the event of national-level disruption of critical infrastructure, just as they now exist for Continuity of Government. Although some private-sector participants had robust backup communications capabilities for business-to-business processes, these capabilities do not necessarily ensure crisis communication between industry and government, or between industries or sectors.

5. (Dept of Commerce) Out-of-band communications that can cross sectors should be developed. This includes federal, state, local, and private sectors, including those not currently included in the ISAC framework.

6. (Telecommunications / IT) Participants from the telecommunications and IT services sectors believe the following key questions were highlighted during Livewire; the answers will help to focus development of a National Cyberspace Security Response System.
   a. Who do I first notify concerning cyber attacks?
   b. What do I tell them?
   c. What should I expect in response?
   d. When do I need to make a report?

7. (S&LG) During the exercise, officials noted much more “bubble-up” coordination and communication at the enterprise- and sector- levels than was observed through active,
decisive coordination by Federal entities such as DHS or the FBI. Lack of information from federal authorities about what was happening nationally was an impediment to state and local decision-making. These officials desire the establishment of clear lines of communication and coordination from the Federal government to the states and municipalities as well as to the various business sectors to achieve a systematic and effective approach to coordinated response.

8. (ISACs) The Multi-State ISAC desires an established communications protocol for interfacing with federal agencies, the US-CERT, and other ISACs. It also needs a protocol and strategy for accessing the technical resources of major hardware and software vendors, and redundant communications (fax, non-IP communications, etc.) in anticipation that Internet traffic will be impacted under some scenarios.

9. (Finance) Livewire demonstrated that private-sector enterprises in the Finance Sector desire to communicate freely with other enterprises, industry associations and regulators during a crisis. In a crisis, senior decision-makers rely on shared awareness and the consensus that results. Given the constrained number and type of participants in this first nationally-scoped cyber exercise, Livewire did not effectively validate whether or not that this type of shared communication and awareness is possible under the circumstances of a wide-spread cyber attack.

10. (Finance) Participants in a finance sector seminar (part of Livewire) found that while each of the industry’s crisis management groups has its own mechanism for initial discussion of critical issues, there is no similar, formal mechanism for coordination between groups. Such a group needs to include individuals from each organization that commits to “meet” (on a virtual basis) on short notice to discuss unfolding events and decide whether a sector crisis is likely.

11. (Finance) Once the nature and scope of the crisis was apparent, private- and public-sector participants were eager to share and cooperate provided the mechanisms to do so are available. One such mechanism, audio conferences, was not well represented in the exercise. Such measures have been very successful at responding to widespread crises and are expected to play a central role in the future.

12. (Finance) Interagency coordination within the government can be confusing during a crisis, especially one that affects multiple sectors. Livewire helped agencies practice coordination and learn about one another’s missions, but more work is needed, particularly regarding the role of financial regulators vis-à-vis DHS and Intelligence staffs.

13. (Finance) Livewire did not alter a going-in assessment on the part of federal regulators that the existing communication architecture works well across government and with depository institutions.

14. (Finance) Sector-level enterprises desire timely reporting from DHS on the nature and scope of a perceived coordinated cyber attack.

15. (Finance) Some participants assessed that no formal communication paths seem to exist for communication between DHS and private enterprises.

16. (ISTS Team) The DHS Interagency Incident Management Group determined that it needs to have representatives from both the Finance and Energy sectors as members of its group
in the event of a real-world cyber attack. The telecommunications ISAC is normally represented by a National Coordinating Center representative at the IIMG.

17. (Finance) Some private-sector participants requested to be more aware of communications between their federal counterparts. Just knowing that the “people up there” are talking with one another gives the private sector more of a sense that they are not alone during a crisis.

Response and Mitigation

1. (Federal, State and Local Government) A broad-based cyber threat could rapidly risk loss of public confidence in availability of basic services or credibility of important business transactions. The public information aspect of response planning is vital at all levels (enterprise, sector, government). Traditional public communication avenues may be disrupted; alternate means of addressing public concern must be planned and practiced.

2. (ISTS Team) Cross-company emergency response teams, perhaps coordinated by US-CERT or the IT/ISAC, will likely fill an important niche during a strategic cyber attack. While companies within the information technology industry have considerable experience responding to problems with their own products, there is comparably little practice organizing a coordinated response to widespread, coordinated attacks across many technologies.

3. (ISTS Team) The private sector has never had to deal with extensive attacks requiring forensics at many places in separate industries. Forensic teams will need to coordinate actions during a large-scale crisis.

4. (S&LG) As part of the exercise, state and local government officials were asked to consider the potential impact of loss of a local “carrier hotel” (a building housing both telecommunications and Internet Service Provider equipment and cabling). They offered two observations:

a. Participants assessed that regional impact of the loss of Internet was significant, but not all-inclusive. City officials quickly identified an alternate ISP provider to restore some lost services. In addition, state emergency management officials worked with FEMA to arrange for communications capabilities from regions out of the area. Although the state eventually declared a statewide emergency, FEMA agreed to dispatch these units early in anticipation of that declaration.

b. The length of time required to restore connectivity, affects the ability of state and local governments to provide essential services. A disruption of short duration would have minimal impact. In most instances where the loss of connectivity continued for more than one week, consequences increase and more comprehensive actions would be necessary. In some situations “BI” practices (before the Internet), such as operating many systems in manual modes, might have to be temporarily re-instituted. While the effect on government efficiency could not be clearly detailed, there could be detrimental consequences in some services, most notably those involved in public safety. Presently many organizations’ plans for BI-type operations are not exercised or do not exist and there is a need to update these plans.
Roles and Responsibilities

1. (ISTS Team) The Office of Science Technology Policy used the Livewire exercise to examine the roles and mission of OSTP in different scenario situations. While OSTP has clear authority in specific situations (such as a declared state of war), an unattributed large-scale cyber attack will likely cloud lines of authority and responsibility.

2. (ISTS Team) Cyber attacks will likely not respect geographic, political, and sector boundaries. However, traditional response resources, decision-making authority, and trust relationships typically do respect these boundaries. A national cyber response system must build upon, but not necessarily be limited by, established relationships and structure including existing federal response mechanisms.

3. (Federal Energy) Federal sector participants from this sector found that communications between the federal government and companies in the oil and gas industry have the potential to be problematic given the lack of experience between the federal sector and the Energy ISAC. There needs to be more trust building activities between the federal government and the Energy ISAC so they can both provide and receive critical information about threats to or conditions in the industry during a crisis.

4. (ISTS Team) The cyber-specific roles and responsibilities of the Department of Homeland Security were unclear to participants from state and local governments, as well as to some participants from private industry. State and local government participants stated that they are unsure of the “rules of engagement” with DHS. They also desire to know initial points-of-contact for reporting under different circumstances. State and local incident managers, and their private-sector counterparts, desire to know the kind of information DHS desires and is prepared to provide, and how best to initially engage in two-way communications with DHS.

5. (S&LG) The exercise confirmed that each participant agency’s responsibilities are different and their priorities are also different. Thus it is not surprising that in some instances they may compete. Recognition and responses to events differed widely, often exposing unfamiliarity with established protocols or reinforcing the need to develop an awareness tool. It became clear early that individuals interpret events differently and reaction to certain activities may not be adequate. Without guidelines all levels of staff are faced with making decisions or not reacting at all.

6. (ISACs) It is questionable today whether most ISACs can or must provide effective Incident Command and Control. As next-generation ISAC capability matures, this question may resolve in favor of at least select ISACs taking on that role.

7. (ISACs) The role and responsibilities of the Multi-State ISAC are unclear to State and local governments, as are rules of engagement with the Multi-State ISAC. State and local officials desire to work out points of contact, information sharing requirements, and assurances for protection of shared information.

8. (Finance) Responders at government agencies need to be comfortable with the roles of people at other agencies for smooth crisis response. Established relationships are a key to successful communication. The financial regulators have offered to provide DHS with an overview of the banking and finance system. Some participants from the private sector felt that discussions of procedures need to be capped with additional exercises.
Regulation
1. (ISTS Team) Participants in other sectors opined that a lack of Telecom performance regulation places other critical infrastructures at risk. (Note: it may be that Telecom performance regulations are adequate, but that infrastructure owners in other sectors, almost all of whom have clear and direct dependencies on Telecom performance, should be made more aware of them).

2. (Energy) Experienced energy sector observers, having discussed electric energy distribution with industry representatives for several months in preparation for Livewire, noted the following: Notwithstanding the feasibility and supportability of manual operations of the electric grid, immediate regulatory relief of OASIS (Open Access Same-time Information System) requirements would probably be necessary for an Independent System Operator to run a “static” and segmented electric grid.

Future Exercises
1. (ISTS Team) Livewire raised several issues concerning the scope of current missions and responsibilities as a wide-spread cyber attack unfolds. These issues need to be more fully addressed in follow-on analysis and future exercises or seminars, including the following questions.
   a. What scope or level of attack warrants elevating discussions above the individual organization’s area of responsibility and authority? What mechanisms exist to facilitate doing this? Are there constraints inhibiting doing so?
   b. How many sources of information can any one enterprise, or organization such as an industry association, consider?
   c. How can law enforcement authorities (and other government entities) filter important information out of ongoing investigations or intelligence reports to enhance sector awareness?
   d. How effective are the current style of teleconferences? What alternatives to such teleconferences exist, or have been considered?

2. (S&LG) Some participants expressed a desire for legislatively-mandated exercise programs to enhance non-emergency-setting relationships and knowledge transfer, regularly renew long-lasting, process-driven relationships as a means of offsetting staff departures, and foster cross-sector relationship building. Participants stated a desire for scored practice exercises for individual agencies, at the sector level, and across sectors.
SECTION 5 – POLICY ISSUES AND RELATED QUESTIONS

As a result of Livewire, the ISTS Team recommends the following policy-related issues and questions for consideration by relevant agencies. The issues conform to the following scenario sequence:

- **Stage One:** early stages of an attack with focus on the required private sector/public sector partnership
- **Stage Two:** middle stages of an attack with focus on evolving responsibilities to defend and mitigate
- **Stage Three:** later stages of the attack with focus on responding to the attack

1. **Policy issue:** Does a cyber threat of major magnitude require a more structured Public/Private response than a nuisance cyber threat, with a central crisis manager responsible for directing and prioritizing all response activities to mitigate circumstances?
   a. What policies or legislation are needed to define new authorities? What are the policy conflicts?
      1) Does each private sector need to be treated uniquely or will one program fit all?
      2) Are there other sectors that need to be considered in the critical infrastructure, e.g., the retail sector and consumers, and that need to be represented by an Information Sharing and Analysis Center (ISAC)? Would Transportation be a candidate for inclusion?
      3) What new mandated directions and procedures must be established for better information sharing between public and private sectors as well as between public sectors?
   
   b. Are current information sharing systems and relationships adequate or is there a need to establish a formalized reporting process that kicks in at some ‘threshold’?
      1) Is there a difference between highly regulated sectors such as finance and other less regulated sectors? If so, is there a need to establish reporting processes in the less regulated sectors that parallel those that currently exist in regulated sectors?
      2) Are both technology driven and educational approaches needed to assist/encourage the private sector to share more information, with whom they share the information, and in what format?
      3) What are the thresholds/seams in which the Federal government changes its processes for receiving/pushing information from/to the private sector – what is the baseline for defense in each sector?
      4) Can the Federal government win trust with the private sector by showing they are able to provide value and not impede progress as they ask the private sector to share more information with the Federal government?
      5) What types of information need to be distributed to the private sector during a widespread and coordinated cyber attack?

   c. What protocols are needed to get from the day-to-day attack phase (malicious incidents) to a campaign attack (major magnitude) phase?

Dartmouth College Proprietary
LIVEWIRE – AFTER ACTION REPORT

1) Can the Federal government prioritize a more structured yet flexible response system?
2) What is the threshold at which a threat reaches “major magnitude,” and what are the protocols?
3) Is a central manager (Principal Federal Agent) needed – a focal point for coordinating public-private cyber responses?
4) What agency coordinates when cyber activities in one sector impede actions of other sectors?

2. Policy issue: What are the shifting roles and responsibilities of Federal agencies in crisis and consequence management as a cyber attack scenario moves from malicious incident to a national security issue?

a. Which agencies have which responsibilities during which phase? Is there a single agency in charge operationally?
   1) What are the thresholds for various levels of responsibility?
   2) What responsibilities does the federal government have during recovery from a 9/11-like cyber attack given that most of the assets are in the private sector?
   3) Are there responsibilities for which no single agency is, or for which multiple agencies are defined as the lead?

b. What are the authorities?
   1) Does the Cyber Interagency Incident Management Group (CIIMG) have authority to be in charge/coordinate during these shifting phases?
   2) Is a threshold needed to convene a continuous CIIMG?
   3) Have we experienced events that might be illustrative of a set of thresholds we could use to cause the formation of a CIIMG?
   4) Do Homeland Security Presidential Directive (HSPD)-5 mechanisms to manage domestic terrorist incidents apply?

c. How are resources obligated to operational authorities when an attack occurs?
   1) What is the proper mechanism for allocating resources from different agencies to likely response tasks including assessment that an attack is coordinated, determining its magnitude, taking or recommending defenses actions, inter-agency coordination, and attribution?
   2) What type of resources can be expected from the private sector as they respond to a cyber campaign level attack?

3. Policy issue: What is the range of options for responding to a cyber campaign against the Nation’s private and public critical infrastructures? Who is responsible for planning, executing, and assessing this campaign?

a. Which agencies have what responsibilities and authority to respond? Which agency leads the response?
   1) Will DHS (National Cyberspace Security Division) have the lead? If not, who has the lead for information gathering, fusion, analysis, and dissemination?
2) Who has the authority to determine/define that we are under a major cyber attack?
3) Who has responsibility to perform attribution?
4) Who has authority to execute the response?
5) What authorities and/or permissions will be needed to shut down gateways?

b. What are credible response options?
   1) How does “response” need to be defined?
   2) What are the proper procedures and protocols for moving into a “response” mode?
   3) Do cyber incidents need to be prioritized in the same way that Public Safety incidents are prioritized? Would this process help define escalation?
   4) Are there adequate procedures to deal with a major cyber campaign (sustained attack)?
   5) How is a major attack determined?
   6) How might the timeline between attack determination and attribution be shortened?
   7) Are current defensive options adequate? If not, is there a need to expand defensive options available following determination of attack, but prior to attribution?
   8) How must the attribution process be improved?
   9) What are the federal agency priorities during the following attack phases: defend, recover, attribute, and respond?
  10) What cyber responses are needed after attribution is accomplished?
  11) What cyber response options might be appropriate during the period of time it takes to determine that a physical event has a cyber trigger?
  12) What policy guidance is given to the states to establish a cyber defense plan?

c. What is the private sector’s role during a response phase?
   1) Does the private sector want a role in when/where/how to respond?
   2) Is the private sector needed to execute desired response options? If so, what is the authority for its involvement?
   3) Is there a need for private sector relief from regulation in order to participate in desired response options?
   4) What coordination measures can be put in place between public and private sectors to insure the economic effects of desired response options are not worse than the attack itself?
SECTION 6 – RECOMMENDATIONS

Federal Level

1. (ISTS Team) Develop a National Cyber Crisis Response Plan outlining information analysis, assessment and integration capability to respond to wide-spread or strategic cyber attacks against the U.S. This plan must clearly delineate authority, roles, and responsibilities across a range of escalation thresholds. It should include authoritative threat- and event-level response guidelines including prioritization of (or restoration of) service, delineation of changes to roles, responsibilities, and jurisdictions between federal, state, and local governments and the private sector.

2. (ISTS Team) All levels of government, and industry, should be involved in developing viable response options to mitigate the effects of a cyber attack that uses the Internet as a conduit for putting critical infrastructure at risk.

3. (ISTS Team) On a sector, regional, and individual enterprise basis, identify and promulgate the specific information gathering and sharing requirements needed to gain situational awareness under the conditions of a cyber attack. Ensure these information requirements directly support the timely selection and implementation of effective response options. Ensure all participants in a national cyber response system understand the technical and situational types of information that must be shared; the processes for sharing it, and who the recipients should be under different threshold conditions. Pay particular attention to thresholds that may not have been crossed yet in the real world, i.e. when a cyber problem transitions from that which should be addressed by law enforcement to that which falls under the authority of homeland or national security authorities. Discover the legal, cultural, and organizational hurdles for sharing critical information, and take the necessary steps now to overcome these hurdles.

4. (ISTS Team) Consider updating the Homeland Security Advisory System to make it more sensitive to non-physical threats and to geographic and sector variations.

5. (S&LG) Develop baseline IT-focused prescriptive actions for municipal governments to take when the threat level is at yellow, orange, and red.

6. (ISTS Team) Develop a means of institutionalized authentication between decision-makers in government at all levels and critical infrastructure nodes within private industry.

7. (Energy) Study the electric industry’s ability to operate/run the electric grid in manual mode, with specific attention to the possibility that people and skills necessary for manual operations may have migrated away from the industry and/or atrophied as it has evolved to Internet-based market matching (producers to distributors) and IT-dependent control systems.

8. (Energy) Consider regulatory relief from the requirements of OASIS (Open Access Same-time Information System) to allow an Independent System Operator to run a “static” and segmented electric grid when warranted.
9. (Various) Federal authorities, regardless of sector, should leverage the presence of on-site regulators to facilitate information-sharing and coordination between private and public sector authorities, especially during a perceived period of emerging disruptive conditions. (Note: Finance sector regulators act as a first line of communications between public and private sectors; this role should be replicated in other sectors if it does not already exist.)

10. (S&LG) Develop a coordinated media plan between federal, state, and local officials that (a) addresses the circumstances of a cyber attack, and (b) addresses the possibility of cyber disruptions during a physical crisis.

11. (ISTS Team) Take steps to foster and continually reinforce organizational, rather than personal, trust relationships. Develop processes, procedures, and plans to:
   a. Rapidly enable trusted communications, including across sectors,
   b. Allow communications between unknown or newly-introduced individuals and organizations,
   c. Allow communication between organizations outside of normal paths or relationships, and
   d. Protect information.

12. (General) Grant clearances to key private-sector decision-makers and selected staff in order to facilitate information sharing between private industry and the government, including the intelligence community, under crisis conditions.

13. (Federal) Develop a national-level visualization tool that enhances situational awareness by federal crisis managers in the event of a major cyber disruption. Consider test-bed employment at the sector level.

14. (S&LG) Encourage the development and growth of intra-state ISACs with easy-to-follow formulas for states and municipalities.

15. (Finance) Develop options for deployable forensic teams or coordination mechanisms between forensic teams in government, industry, academia, and security companies. (Note: this may be a worthwhile joint project between NCSD, the US-CERT, and DOJ).

16. (S&LG) Schedule Livewire-like exercises on a regular basis throughout the country and for all sectors. Stress inter-sector dialogue during these exercises.

17. (S&LG) Develop local and regional forums for discussing possible IT terrorism scenarios. Include role playing and face-to-face small group, inter-sector discussions. Encourage institutionalized committees that explore solutions to problems uncovered during exercises and discussions.
State Level
(Note: all recommendations in this category were self-identified by state and local government participants).

18. Formulate state strategy consistent with Homeland Security initiatives and include protocols up, down, and across.

19. Establish and mandate roles and responsibilities at the state level and organizational level.

20. Develop a “playbook” for senior decision makers for use in case of major cyber events.


22. Integrate cyber experts with public safety experts.

23. Develop education and awareness programs for all governmental entities and include non-governmental entities where appropriate.

24. Support the development of a state ISAC and make use of the Multi-State ISAC.

25. Develop local and state strategy to manage politics and media.

26. Develop internal after action and recommendation report for state and local officials.

27. Expand existing capabilities for mutually independent, but cross-sector capable, secure communications and incident command/site capability including wire-line and wireless, device-agnostic telecommunications, such as the fairly robust capabilities that some agencies such as EP&R (FEMA) now have. Likewise there is a need for secure, physical command centers with the capacity to collect, evaluate, update, and disseminate incident-related information.

Sector Level

28. (Finance) Establish a formal mechanism for coordination between groups and associations within the finance sector.

29. There is a need for sector-level centralized information processing centers with greater analysis capability than exists for some of the current ISACs.
### Appendix A – Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BI</td>
<td>Before the Internet</td>
</tr>
<tr>
<td>CCIPS</td>
<td>Computer Crime and Intellectual Property Section</td>
</tr>
<tr>
<td>CERT</td>
<td>Formerly Computer Emergency Response Team – at Carnegie Mellon</td>
</tr>
<tr>
<td>CIIMG</td>
<td>Cyber Interagency Incident Management Group</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DIA</td>
<td>Defense Intelligence Agency</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Server</td>
</tr>
<tr>
<td>DoD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DOE</td>
<td>Department of Energy</td>
</tr>
<tr>
<td>DOJ</td>
<td>Department of Justice</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>EP&amp;R</td>
<td>Emergency Preparedness and Response – DHS</td>
</tr>
<tr>
<td>FEMA</td>
<td>Federal Emergency Management Agency - DHS</td>
</tr>
<tr>
<td>FBIIC</td>
<td>Financial and Banking Information Infrastructure Committee</td>
</tr>
<tr>
<td>FS/ISAC</td>
<td>Financial Services ISAC</td>
</tr>
<tr>
<td>FSSCC</td>
<td>Financial Services Sector Coordinating Council</td>
</tr>
<tr>
<td>GRID</td>
<td>National Electric Grid</td>
</tr>
<tr>
<td>HSPD</td>
<td>Homeland Security Presidential Directive</td>
</tr>
<tr>
<td>HSC</td>
<td>Homeland Security Council – White House</td>
</tr>
<tr>
<td>I&amp;W</td>
<td>Indications and Warning</td>
</tr>
<tr>
<td>IAIP</td>
<td>Information Analysis and Infrastructure Protection – DHS</td>
</tr>
<tr>
<td>IC</td>
<td>Intelligence Community</td>
</tr>
<tr>
<td>IIMG</td>
<td>Interagency Incident Management Group – DHS</td>
</tr>
<tr>
<td>IMRD</td>
<td>Information Management &amp; Requirements Division – DHS</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISAC</td>
<td>Information Sharing and Analysis Center</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>ISTS</td>
<td>Institute for Security Technology Studies</td>
</tr>
<tr>
<td>IT/ISAC</td>
<td>Information Technology ISAC</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Name</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>JTF-CNO</td>
<td>Joint Task Force – Computer Network Operations (DoD)</td>
</tr>
<tr>
<td>MS/ISAC</td>
<td>Multi-State ISAC</td>
</tr>
<tr>
<td>NCC</td>
<td>National Coordinating Center - NCS</td>
</tr>
<tr>
<td>NCS</td>
<td>National Communications System - DHS</td>
</tr>
<tr>
<td>NCSD</td>
<td>National Cyber Security Division - DHS</td>
</tr>
<tr>
<td>NCSRS</td>
<td>National Cyberspace Security Response System</td>
</tr>
<tr>
<td>NORTHCOM</td>
<td>US Northern Command – DoD</td>
</tr>
<tr>
<td>NSC</td>
<td>National Security Council – White House</td>
</tr>
<tr>
<td>NTSB</td>
<td>National Transportation Safety Board</td>
</tr>
<tr>
<td>OASIS</td>
<td>Open Access Same-time Information System - Electric</td>
</tr>
<tr>
<td>OCC</td>
<td>Office of the Controller of the Currency</td>
</tr>
<tr>
<td>OCS</td>
<td>Office of Cyberspace Security – White House</td>
</tr>
<tr>
<td>OMB</td>
<td>Office of Management and Budget – White House</td>
</tr>
<tr>
<td>OSTP</td>
<td>Office of Science and Technology Policy – White House</td>
</tr>
<tr>
<td>RAD</td>
<td>Risk Assessment Division – DHS</td>
</tr>
<tr>
<td>SEC</td>
<td>Securities and Exchange Commission</td>
</tr>
<tr>
<td>STRATCOM</td>
<td>US Strategic Command</td>
</tr>
<tr>
<td>US-CERT</td>
<td>US Computer Emergency Readiness Team</td>
</tr>
<tr>
<td>USSS</td>
<td>US Secret Service – DHS</td>
</tr>
</tbody>
</table>