**THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE**

Information Technology Mobilization Scoping Report

May 21, 2014

President's National Security Telecommunications Advisory Committee's Information Technology Mobilization Scoping Report

I. Overview and Background:

In 2014, the Director of National Intelligence issued a statement to the United States Senate Select Committee on Intelligence, identifying cyber attacks as the top threat to our Nation's security for the second consecutive year.[1] Additionally, many experts in both Government and industry recognize that our Nation's dependence on cyber systems increases our vulnerability to this threat.

To bolster our Nation's cybersecurity posture, Government and industry have developed, or are currently developing, programs, policies, and methodologies to help manage cyber risks to their respective infrastructures and exchange threat information. For example, under Presidential Policy Directive 8, *National Preparedness,* the Federal Government has developed capabilities-based decision making tools to help strengthen "the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber attacks, pandemics, and catastrophic natural disasters."[2] The Government has also sponsored a series of cyber-focused exercises, including National Level Exercise 2012 and the Cyber Storm Exercise series, to test these programs, policies, and methodologies. Collectively, these initiatives are part of an ongoing effort to improve the understanding of respective capabilities of the public and private sectors and improve coordination—within Government and between Government and industry—during a cyber-related event.

Despite this progress, there is not yet an effective methodology in place to coordinate Government and industry's operational response capabilities across the full spectrum of national security and emergency preparedness (NS/EP) events with cyber implications. Cyber exercises have consistently demonstrated a need to better understand the resources and capabilities necessary to respond; develop the means to coordinate relevant assets; and clarify the roles and authorities of industry and Government partners before, during, and after a response. Furthermore, policy and doctrine needed to manage cyber responses to events of national significance are incomplete, and are also complicated since many of the Nation's established response resources are jurisdictionally-organized, while cyber events do not unfold within those geographic boundaries.

As a result, the Executive Office of the President requested that the President's National Security Telecommunications Advisory Committee (NSTAC) conduct a study of this issue. Accordingly, in February 2014, the NSTAC's Designated Federal Officer (DFO) established the Information Technology Mobilization Scoping Subcommittee.

[1] Clapper, James R. "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community, U.S. Senate Select Committee on Intelligence." January 29, 2014. Available at: http://www.dni.gov/index.php/newsroom/testimonies/203-congressional-testimonies-2014/1005-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community

[2] Executive Office of the President. Presidential Policy Directive 8, *National Preparedness*. March 30, 2011. Available at: https://www.dhs.gov/presidential-policy-directive-8-national-preparedness

II. Estimated Time Frame and Priority:

The NSTAC would complete its final report by November 2014.

III. Value in Researching Issue:

The ability of the private and public sectors to respond effectively to low-probability, high-impact, cyber-related events of national significance is a key element of resiliency and assuring national security and public safety. Exercises have demonstrated that current, prevention, protection, mitigation, response, and recovery efforts may not be sufficient for a large-scale cyber-related event. Determining the appropriate range of industry-Government relationships, coordination mechanisms, and, as necessary, building the capabilities needed to respond to a cyber-related crisis will require a high degree of partnership between the Government and industry.[3] Once determined, the proposed framework will serve as the new foundation for a shared risk management posture.

IV. Approach:

The NSTAC will examine the implications of operational coordination of critical commercial assets or capabilities to facilitate a response to a cyber-related event of national significance. This examination will focus on three fundamental areas: (1) a methodology and process for identifying assets, functions and/or capabilities; (2) the conditions, triggers, and thresholds for increased coordination across industries, as well as between industry and Government; and (3) an operational framework and operational structure for this coordination effort. Specifically, the NSTAC will:

- 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 identify conditions, triggers, thresholds, and situations that might require increased operational coordination across industry, as well as between industry and Government;
- Research and recommend an operational framework that: (1) guides, informs, and prioritizes response across the full spectrum of NS/EP events with cyber implications; and (2) allows for agile, effective, and distributed implementation across numerous stakeholders, resulting in a coherent, unified, and dynamic national response; 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.

To perform the research and develop recommendations to the President, the NSTAC will:

- Receive briefings from key experts in Government, industry, and academia who can provide insight on past and present mobilization plans and policies, cyber-related event thresholds, and related activities;

[3] Daniel, Michael. November 20, 2013, NSTAC Meeting Remarks. November 20, 2013.

- Identify authoritative definitions for terms used, such as “mobilization” and “critical commercial assets” to ensure a common lexicon between private and public sector partners;
- Identify case studies or other scenarios (both cyber and physical) as examples to determine appropriate response and coordination strategies;
- Examine how to ensure unity of effort across industry and Government when responding to a major cyber-related event of national significance;
- Research industry’s existing response capabilities and those actions industry may take independently or collectively without legal restrictions or Government involvement, and identify criteria for when, and to what degree, Government involvement may be requested or required;
- Explore and analyze international concerns or issues that may enhance or hinder national response coordination;
- Analyze related response policies and operational methodologies intended to help coordinate resources and capabilities, and their applicability to the information and communications technology (ICT) industries; and
- Study and recommend revisions to Federal Government-centric capabilities, planning frameworks, and prioritization schemas to align commercial planning efforts and determine appropriate response and operational coordination points.

V. Proposal:

The NSTAC’s members represent the Nation’s most sophisticated ICT organizations, making the committee well suited to examine industry-Government ICT response coordination. The NSTAC recommends the establishment of a subcommittee to study ICT response coordination for managing a cyber-related event of national significance. If approved, the NSTAC will produce a report to the President that will describe the **needs, benefits, and operational efficacy of a national ICT response coordination capability.**

VI. Schedule

- May 2014: Present final scoping report for members’ deliberation and vote.
- May 2014: Hold the first research subcommittee meeting.
- June - August 2014: Identify and invite relevant subject matter experts to brief the subcommittee; begin writing the draft report.
- August 2014: Provide an update to the NSTAC members during the member conference call.
- September - October 2014: Finalize the draft report.
- November 2014: Present final report to members for deliberation and vote.