THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

Industrial Internet Scoping Report

FEBRUARY 19, 2014

PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE
INDUSTRIAL INTERNET SCOPING REPORT

I. Overview and Background:

Global communications networks that intersect with physical infrastructure underpin almost every facet of American society. This includes systems that provide critical support to public infrastructure, social interaction, and the country's national and economic security. Unfortunately, this increasing interdependency of the physical and cyber domains is accompanied by a corresponding growth in threats and vulnerabilities, creating a challenge in balancing the benefits and the risks of this evolving interconnection.

Industry and the Federal Government have initiated several programs designed to enhance the security of the Internet as it supports national security and emergency preparedness (NS/EP) functions; however, technological innovation continues to advance ahead of security solutions to protect applications and interconnections. An example of this is the rapid proliferation of interconnected physical devices and their inclusion into systems supporting critical infrastructure is the Industrial Internet, more commonly referred to as the Internet of Things (IoT).

In addition to the phrase Industrial Internet, the IoT is referred to by several terms, including machine-to-machine (M2M) communications, Internet of everything, and cyber physical systems (CPS).[1] Broadly speaking, the IoT is an expansion of the global infrastructure through existing and evolving interoperable information and communication technologies. It incorporates the interconnection of physical and virtual systems to enable new and autonomous capabilities. For the purposes of this research effort, IoT-enabled consumer products and services will be included only to the extent that they interact with NS/EP systems. The IoT is characterized by four main attributes:

- Time Scale: Automated systems that operate in the physical world and engage in analysis and action faster than humans can comprehend, participate in, or supervise.
- Interdependence: Actions and consequences, some unanticipated, that can result from the interactions between systems.
- Prediction/Learning: Systems that are constantly evolving through experiences and additional data.
- System Management and Control: Emerging networked technologies that may not conform to older, established models.

Current projections indicate that the IoT will impact and influence an ever-broadening scope, ranging from national systems and policies to personal life and social interactions; despite this, many questions regarding the impact of this rapidly-growing medium on NS/EP remain unaddressed. As a result, the Executive Office of the President (National Security Council) requested that the President's National Security Telecommunications Advisory Committee (NSTAC) conduct a study of this issue. Accordingly, in October 2013, the NSTAC's Alternate

[1] In the absence of authoritative definitions of the Industrial Internet, IoT, and related phrases, the NSTAC will continue to use the term IoT throughout the scoping and research phases.

Designated Federal Official established an Industrial Internet Scoping Subcommittee to examine the cybersecurity implications of the IoT and further refine the issue to be studied.

II. Estimated Time Frame and Priority:

The NSTAC plans to complete its final report by November 2014.

III. Value in Researching Issue:

The adoption of the IoT is creating a dramatic increase in the number of sensors and devices that can autonomously communicate, thus creating massive new data sources and increasing automation that is often far removed from any human interaction. Potential benefits include the development of innovative services and, in many cases, more efficient use of infrastructure. However, the security risks resulting from an exponential expansion in attack surfaces, a changing threat landscape, privacy concerns, an increased potential for kinetic-focused cyber-attacks, and changes to the hardware lifecycle must also be considered. These benefits and risks are already being recognized in the early deployment of IoT, necessitating a better understanding of the technology, the implications of existing and new policy structures, and the impacts on critical infrastructure security and resilience.

IV. Approach:

The NSTAC will examine the cybersecurity implications of the IoT, within the context of NS/EP, by focusing on four areas: **security, operations, design, and policy**. The NSTAC will explore questions in these areas, including, but not limited to:

- In what ways do the deployment of IoT capabilities and technologies impact existing cybersecurity risk management processes and procedures for both industry and Government?
- How can legacy systems be effectively and safely integrated with current and emerging networks and IoT services and applications?
- What defensive and protective capabilities should be developed to mitigate risks created by the IoT?
- How should Government policy adapt to address issues such as IoT application security, potential network performance issues, privacy impacts, and economic factors?
- What uses, if any, of IoT capabilities for NS/EP applications should be researched, developed, and deployed?
- How does the IoT create an opportunity to develop a more robust and secure underlying network that build upon the past several decades of Internet research?

Some questions may not be relevant in all four areas. The subcommittee anticipates that, because the IoT is an emerging topic advanced by rapid innovation, new questions may arise during the research phase.

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

- Identify three to five case studies to be used as examples in determining NS/EP risk management issues resulting from implications of the IoT. Case studies will be chosen from the 16 critical infrastructure sectors defined in Presidential Policy Directive/PPD 21, *Critical Infrastructure Security and Resilience*.

- Receive briefings from key experts in Government, industry, and academia who are engaged with the issue and can provide insight on applicable technical issues, intelligence threat information, and general lessons learned, best practices, and/or research activities. At a minimum, briefers should include representatives from leading organizations and projects from Government, industry, and academia (e.g., the Defense Advanced Research Projects Agency, National Security Agency, European Network and Information Security Agency, the National Institute of Standards and Technology, Cyber Security Research Alliance, and smart grid developers).
- Review current Government efforts and policy documents, as well as NSTAC reports, for applicability.
- Review academic literature and current research on the topic.

V. Proposal to NSTAC:

Recommend that the NSTAC commission a subcommittee to study the cybersecurity implications of the IoT, within the context of NS/EP.

VI. Schedule

- February 19, 2014: NSTAC members deliberate and vote on the NSTAC Industrial Internet Scoping Report to create an NSTAC subcommittee to examine the NS/EP cybersecurity implications of the IoT.
- March 2014: Hold the first subcommittee meeting.
- April 2014: Identify and invite relevant subject matter experts to brief the subcommittee
- May 21, 2014: Provide an update to the NSTAC members at 2014 NSTAC Meeting.
- August 2014: Provide an update to the NSTAC members during the member conference call.
- August 29, 2014: Continue developing draft report.
- September 2014: Discuss the draft report with NSTAC members.
- November 2014: Present final report at the November 2014 NSTAC member meeting for deliberation and vote.