



NSTAC Meeting Discussion Aid

November 20, 2013

Agenda Item: Industrial Internet Scoping Subcommittee Update

Time: 9:25 a.m. – 9:35 a.m.

Participants: Mr. Steve Bennett, Symantec, and Mr. William Swanson, Raytheon
Co-chairs, Industrial Internet Scoping Subcommittee

Background

In August 2013, the National Security Staff requested that the NSTAC examine possible cybersecurity implications of the Industrial Internet. As a result, the NSTAC established the Industrial Internet Scoping Subcommittee (IISS) in October 2013. The IISS is co-chaired by Mr. William Swanson, Raytheon, and Mr. Steve Bennett, Symantec.

Approach

- The IISS is examining the way in which speed and emerging technologies have presented new cybersecurity implications and are creating exponential risks for both national and economic security.
- To inform its scoping effort, the IISS will continue to meet with subject matter experts and industry leaders working within the Industrial Internet space. It will also perform research and analysis on related efforts occurring across government.

Current Progress

- The IISS held its kickoff meeting on October 29, 2013. The purpose of the meeting was to discuss the scoping approach and methodology, refine the issues for examination, and begin exploring questions that the NSTAC should address during its examination.
- The IISS received a technical briefing on the Industrial Internet from Mr. John Pescatore, a recognized cyber expert and the Director of Emerging Security Trends at the SANS Institute. His presentation provided a brief history of the Industrial Internet and discussion around evolving critical security controls to accommodate the Industrial Internet.

Next Steps

- Based on discussions at its initial meetings, the IISS will:
 - Select and arrange for subject matter experts to brief on topics relative to the Industrial Internet at future meetings;
 - Define a common taxonomy of the Industrial Internet and differentiate it from the terms Internet of Things and cyber physical systems;
 - Determine to what extent international issues should be examined given the global parameters and implications of the Industrial Internet;
 - Consider conducting a risk analysis and create a risk register to better inform the effort; and
 - Continue to examine complimentary efforts across other Federal departments and agencies.
- The IISS will continue to meet weekly until the conclusion of the scoping effort in February 2014.



NSTAC Meeting Discussion Aid

November 20, 2013

Agenda Item: Information Technology Mobilization Study

Time: 9:45 a.m. – 10:15 a.m.

Participants: Mr. Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator, National Security Staff (NSS); and NSTAC Members

Background

Government and industry have developed or are currently developing programs, practices, and methodologies to sharing threat information. There are also existing processes in place or being developed to identify critical infrastructure. Despite this progress, there is no methodology in place to allow for the mobilization of critical assets in the commercial sector that could be coordinated to respond to a large-scale, determined cyber attack that would rise to a high national security concern.

Purpose

During this session the National Security Staff will present this next tasking to the NSTAC members and provide an opportunity for discussion on the tasking's scope.

Questions for the NSTAC to Address

In the proposed study, the NSTAC would seek to:

- A. Identify the critical commercial assets that would be helpful, if operationally coordinated, to defend against or thwart a massive cybersecurity attack against the nation;
- B. Determine the criteria or situations which might require such infrastructure to be mobilized;
- C. Determine the operational methodology in which such assets could be mobilized to present a coordinated response for a determined amount of time; and
- D. Identify the operational structure to coordinate such assets, including which Government entities would exercise what roles, as well as preparation and training for, and exercise of such contingencies.

Deliverable

The NSTAC will produce a report to the President that will describe the needs, benefits, and operational efficacy of a national information technology mobilization capability. In so doing, the NSTAC will provide its analysis of the questions above, as well as its initial consideration of the authority or authorities under which such a plan could be implemented. A detailed analysis of the authorities may be considered separately, outside the scope of this initial study, as determining the operational efficacy would be a pre-requisite to an examination of legal authority.



NSTAC Meeting Discussion Aid

November 20, 2013

Agenda Item: Roundtable Discussion: Cybersecurity Framework

Time: 12:00 p.m. – 1:00 p.m.

Participants: The Honorable Patrick Gallagher, Director, National Institute of Standards and Technology (NIST) and Under Secretary of Commerce for Standards and Technology;
Ms. Suzanne Spaulding, Acting Under Secretary for National Protection and Programs Directorate;
Dr. Phyllis Schneck, Deputy Under Secretary for Cybersecurity;
Mr. Daniel; and
NSTAC Members

Background

In February 2013, the President released Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*. The EO directs NIST to work with stakeholders and lead the development of a voluntary framework to reduce cyber risks to critical infrastructure. According to the EO, the Cybersecurity Framework should include “standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.” The framework’s intent is to assist critical infrastructure owners and operators in managing cyber risks in a way that is prioritized, flexible, repeatable, and cost-effective. NIST is expected to release the final Cybersecurity Framework in February 2014.

Purpose

The purpose of this agenda topic is to engage NSTAC members and Government stakeholders in a discussion on the NIST Cybersecurity Framework. Following a brief presentation by NIST, the NSTAC members will have an opportunity to ask questions and provide feedback regarding the Framework’s adoption, including adoption incentives. As representatives from major communications, information technology, and defense companies, the NSTAC members can provide a unique perspective to NIST to assist in NIST’s implementation of the framework.

Discussion

Dr. Gallagher will begin the discussion by providing:

- A brief overview of the Cybersecurity Framework;
- The process and approach under which NIST collected input for the Framework; and
- A discussion on whether the input received helped address NIST’s goals.

Following Dr. Gallagher’s remarks, NSTAC members will have the opportunity to provide an industry perspective on how to incentivize other organizations to adopt the Framework and how to measure the successes of adoption. Additional discussion questions/topics may include:

1. Many large companies, such as those represented on the NSTAC, already implement rigorous cybersecurity regimes across their organization. How can smaller organizations be incentivized to use the Framework?
2. How can NIST measure the Framework’s success once released?