NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

PUBLIC MEETING AGENDA

August 14, 2013
4:00 p.m. – 5:30 p.m. EDT
National Intellectual Property Rights Coordination Center Auditorium
2451 Crystal Drive, Suite 150, Arlington, VA 22202

I.	**OPENING OF MEETING**	*Nancy J. Wong,* Designated Federal Officer (DFO), National Infrastructure Advisory Council (NIAC), Department of Homeland Security (DHS)
II.	**ROLL CALL OF MEMBERS**	*Nancy J. Wong,* DFO, NIAC, DHS
III.	**OPENING REMARKS AND INTRODUCTIONS**	*Constance H. Lau,* NIAC Chair *William F. Flynn,* Deputy Assistant Secretary for Infrastructure Protection, DHS *(invited)* *Jeanette Manfra,* Deputy Director, Task Force for the Implementation of Executive Order 13636 and Presidential Policy Directive 21, DHS *Nitin Natarajan,* Director, Critical Infrastructure Policy, National Security Staff
IV.	**UPDATE AND DISCUSSION ON IMPLEMENTATION PLAN FOR EXECUTIVE ORDER 13636 AND PRESIDENTIAL POLICY DIRECTIVE 21 BY THE DEPARTMENT OF HOMELAND SECURITY**	*Jeanette Manfra,* Deputy Director, Task Force for the Implementation of Executive Order 13636 and Presidential Policy Directive 21, DHS
V.	**PUBLIC COMMENT: DISCUSSION LIMITED TO MEETING AGENDA ITEMS**	*Nancy J. Wong,* DFO, NIAC, DHS

VI.	**DISCUSSION AND DELIBERATION ON COUNCIL RECOMMENDATION FOR IMPLEMENTATION PLAN FOR EXECUTIVE ORDER 13636 AND PRESIDENTIAL POLICY DIRECTIVE 21**	*David Kepler,* NIAC Working Group Co-Chair *Philip Heasley,* NIAC Working Group Co-Chair
VII.	**CLOSING REMARKS**	*Constance H. Lau,* NIAC Chair *William F. Flynn*, Deputy Assistant Secretary for Infrastructure Protection, DHS *(invited)* *Jeanette Manfra,* Deputy Director, Task Force for the Implementation of Executive Order 13636 and Presidential Policy Directive 21, DHS *Nitin Natarajan,* Director, Critical Infrastructure Policy, National Security Staff

MINUTES

NIAC MEMBERS PRESENT IN ARLINGTON, VA:

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:
Gen. Albert Edmunds (Ret.); Ms. Peg Grayson; Mr. Phil Heasley; Mr. David Kepler; Mr. Donald Knauss; Ms. Constance Lau; Mr. James Reid; Mr. Bruce Rohde

MEMBERS ABSENT:
Mr. David Bronczek; Mr. Jack Baylis; Mr. Gilbert Gallegos; Mr. Glenn Gerstell; Mr. David Grain; Mr. Philip Heasley; Commissioner Raymond Kelly; Mr. James Nicholson; Mr. Thomas Noonan; Mr. Gregory Peters; Mr. Gregory Wells; Dr. Beverley Scott; Mr. Michael Wallace

SUBSTANTIVE POINTS OF CONTACT ATTENDING VIA CONFERENCE CALL:
Ryan Beck (for Commissioner Raymond Kelly); Ms. Joan Gehrke (for Mr. James Nicholson); Frances Paulson (for Mr. David Bronczek)

OTHER DIGNITARIES PRESENT:
Mr. William F. Flynn, Deputy Assistant Secretary, IP, DHS; Ms. Jeanette Manfra, IP, DHS; Mr. Nitin Natarajan, NSS; and Ms. Nancy Wong, DFO, NIAC, DHS

I, II. OPENING OF MEETING, ROLL CALL *Nancy J. Wong*, DFO, NIAC, DHS

Nancy Wong opened the meeting and called the roll. She then turned the meeting over to Constance Lau, NIAC Chair.

III. OPENING REMARKS AND INTRODUCTIONS

Constance H. Lau, NIAC Chair

William F. Flynn, Deputy Assistant Secretary for Infrastructure Protection, DHS *(invited)*

Jeanette Manfra, Deputy Director, Task Force for the Implementation of Executive Order 13636 and Presidential Policy Directive 21, DHS

Nitin Natarajan, Director, Critical Infrastructure Policy, National Security Staff

Ms. Lau welcomed NIAC members and Federal Government representatives, and provided an overview of the meeting. Topics included a status report and discussion on the implementation plan for Executive Order 13636 (EO) and Presidential Policy Directive 21 (PPD-21) by the Department of Homeland Security (DHS), as well as discussion and deliberation on Council recommendations for the implementation of the EO and PPD-21 with regard to information sharing. She explained that this meeting is the second of three special meetings the Council is holding to comment and make recommendations on the implementation of the EO and PPD-21, as well as the revision of the National Infrastructure Protection Plan (NIPP). Ms. Lau then opened the floor for opening remarks from Administration officials.

Mr. Natarajan thanked members for the opportunity to speak and hear the Council's input on information sharing and the implementation of the goals laid out in the EO and PPD-21. He noted that the Administration has outlined a holistic approach in the two documents, expanding the critical infrastructure mission to include a focus on resilience and all-hazards preparation, as well as emphasizing cyber resilience and security issues underpinning all sectors. Mr. Natarajan restated his thanks for the NIAC's unique perspective and continued input towards making the EO and PPD-21 actionable and deployable at all levels of the public-private partnership.

Ms. Manfra echoed Mr. Natarajan's comments, and also thanked the Council for its participation, constructive feedback, and recommendations on information sharing and the other complex critical infrastructure security and resilience challenges the Nation faces. She

emphasized that the Council's work is fundamental to the Integrated Task Force's (ITF) mission of successfully implementing the EO and PPD-21 throughout the public-private partnership.

IV.	**UPDATE AND DISCUSSION ON IMPLEMENTATION PLAN FOR EXECUTIVE ORDER 13636 AND PRESIDENTIAL POLICY DIRECTIVE 21 BY THE DEPARTMENT OF HOMELAND SECURITY**	*Jeanette Manfra,* Deputy Director, Task Force for the Implementation of Executive Order 13636 and Presidential Policy Directive 21, DHS

Ms. Manfra began by giving an overview of the sources consulted for the ITF's work on enhancing information sharing. She explained that the ITF is attempting to address a broad range of information sharing challenges and generate a strong, comprehensive statement through the rewrite of the National Infrastructure Protection Plan (NIPP) that also address the deliverables of the EO and PPD-21. To address this, the ITF established two working groups, the Information Sharing Working Group and the Situational Awareness/Information Exchange Working Group, as a joint effort to codify cyber and physical protection and resilience linkages.

Ms. Manfra explained that there is a great need to enhance Federal Government coordination and information sharing by targeting both internal government entities and external private sector partners. To address this, the working groups are developing a shared concept of operations, discrete set of metrics to measure disposition of threat reporting, as well as a number of initiatives that improve policies and processes.

Currently, there are roughly 400 products that are shared either internally or externally, that relate to threats, vulnerability, and situational awareness. These are being shared with partners through meetings and other data exchanges Ms. Manfra noted that by studying the distribution cycle for these processes, the ITF will be able to identify the strongest baseline data exchange practices.

The ITF has learned a lot about timely and actionable information sharing from reviewing recent counterterrorism policies as part of the NIPP revision. Adopting similar frameworks will help the Federal Government expand consistent best practices into the cybersecurity realm, mature the public-private partnership, reinforce the need for a cultural change within the Federal Government to appreciate the information requirements of private sector partners, and help prevent events with better notifications.

Ms. Manfra introduced her DHS colleagues present in the room: Mr. David McAuley of DHS' Office of Intelligence and Analysis, as well as Preston Wertz and Anne Sorroco who have been leading the Situational Awareness and Information Exchange Working Group.

V.	**DISCUSSION AND DELIBERATION ON COUNCIL RECOMMENDATIONS FOR IMPLEMENTATION PLAN FOR EXECUTIVE ORDER 13636 AND PRESIDENTIAL POLICY DIRECTIVE 21**	*Dave Kepler, NIAC Working Group Co-Chair* *Philip Heasley, NIAC Working Group Co-Chair*

Ms. Lau then introduced Mr. Kepler, Co-Chair of the NIAC EO-PPD Working Group, and thanked him for his leadership and dedicated service.

Mr. Kepler began by endorsing efforts to align the cybersecurity information sharing framework with the private sector's need for timely, specific, and actionable information. He explained that it is important that the framework establishes a safe harbor for information sharing that benefits all critical infrastructure sectors. Within the safe harbor there would be recognition that proprietary information will only be used for its intended purposes, limited anti-trust regulations will be enforced, and privacy will be maintained. Mr. Kepler noted that Federal Government and private sector partners working together in good faith will encourage greater private sector participation in the information sharing program.

Mr. Kepler then explained that the most significant incentive for private sector partners to engage in the cybersecurity information sharing framework is the opportunity to receive timely, specific, and actionable information. Additional incentives could include technical guidelines, as well as support and sharing of cybersecurity best practices between DHS, the National Security Agency (NSA), and the private sector.

Effective mechanisms for attracting and retaining private sector partners would likely include easy access for those partners to threat indicators through a portal similar to the Homeland Security Information Network (HSIN) or the United States Computer Emergency Readiness Team (US-CERT). Mr. Kepler explained that ideally, information would be displayed in a format that can be used by each company to search their own security logs, against known issues including IP addresses, domains, and malware hashes.

Another effective mechanism to engage private sector partners would come from sharing the specific vulnerabilities, threats, methods, and motivations of attackers. Mr. Kepler noted that this level of detail is invaluable to a company and would build on other effective mechanisms for improving information sharing: simple processes, eliminating redundancy, and maintaining multiple lines of communication, especially informal, that are transparent.

Mr. Kepler discussed the need to balance the classification of information with the ability to communicate that information up and down an organization. He stressed that implementing cybersecuirty solutions is different than implementing physical security solutions; cybersecurity

solutions often require more flexibility and timeliness through strategic and tactical operational-level information sharing regardless of an individual's security clearance level, and that when processing classified information and information needed for implementation, there is frequently overlap. To address this overlap, information that does not need to be classified, should be segmented from data that does need to be classified to the greatest extent possible and so it is framed to make it actionable for broad implementation actions.

In addition to expedited security clearances for certain individuals, Mr. Kepler also outlined that there needs to be more clarity on how classified information can be used within a company whose monitoring systems are not certified for classified information. If action is to be taken, information needs to be declassified for deeper and broader communication within a company or industry. Mr. Kepler emphasized that broader dissemination for cybersecurity information is a specific direction from the EO.

The need for a safe harbor structure for cybersecurity information sharing cannot be understated. It is essential for the Federal Government to recognize that the concerns of the private sector in sharing information may inhibit sharing at desired levels. Federal Government adoption of policies that specifically address concerns that information sharing could lead to governmental inquiries and regulation beyond the original and intended purpose for which the information was offered, is the most likely means to addressing these concerns.

Mr. Kepler also suggested that leveraging existing programs, specifically DHS' Protected Critical Infrastructure Information (PCII) program would help address private sector information sharing concerns. He explained that both private sector and government users have confidence in this program, making it a prime resource for implementing the deliverables of the EO and PPD-21, as well as the updates to the NIPP. Generating mechanisms to ensure that proprietary information remains confidential and is not disseminated within the government, except where there are legitimate and compelling reasons to do so, is also likely to help address information sharing concerns.

Finally, Mr. Kepler addressed metrics for the information sharing framework. On behalf of the working group, Mr. Kepler cited and recommended a document to the ITF from the Homeland Security Studies and Analysis Institute (HSSAI), a non-profit, Federally funded research and development center operated by Analytic Services Inc. on behalf of DHS, has created a document entitled "Metrics for Measuring the Efficacy of Critical Infrastructure-Centric Cybersecurity Information Sharing Efforts." This document details options for metrics which include the attributes of effective information sharing (i.e. relevance, timeliness, accuracy, etc.) and the outcome based goal of information sharing which is primarily 'no loss of control'.

Members of the NIAC and Federal Government officials were then asked to voice any clarifying questions they had.

Ms. Manfra asked Mr. Kepler to elaborate on his comments about DHS' PCII program, in particular the ways in which PCII and other existing programs can be leveraged and any additional information sharing programs and principles NIAC Members have used successfully in the past. She also noted that she is aware of previous NIAC recommendations in this area of the last few years.

Mr. Kepler emphasized the importance of diverse network-based relationships. Speaking from his experience in the chemical sector, Mr. Kepler described the value of informal networking with other companies up and down the value chain. He explained that informal relationships with industry partners not only made information more timely and actionable, but it also makes sector-wide executive engagement on more formal topics more likely because of the familiarity, rapport, and trust that have been established. Mr. Kepler then reiterated the Working Group's support for PCII because of its ability to create trusted relationships and maintain a safe harbor for member's proprietary information.

Mr. Natarajan then asked Mr. Kepler to expand on the Working Group's recommendations regarding anti-trust concerns and regulation, including how constraints can be alleviated for the private sector. He asked if there were any deeper recommendations to address more specific issues that are preventing bigger goals from being achieved.

Mr. Kepler explained that many concerns about anti-trust regulation can be addressed by determining potential issues beforehand. These areas include information that when shared may be perceived on its own as antitrust, but during an emergency event need to be managed and distributed in a timely and actionable manner.

Ms. Wong suggested that a future report by the Working Group would help to clarify the issue of antitrust and other processes that are not perceived as being as efficient as they should be from the end-user perspective.

Mr. Kepler agreed to take up the report on behalf of the Working Group and explained that the key will be distinguishing between tactical-operational information sharing and strategic information sharing that secure propriety information whenever possible, but also reflect the nuances within and among sectors that need to be shared in a timely and actionable manner. Mr. Kepler also noted that developing proper metrics for these types of information is even more important and will likely require input from DHS and other sector-specific agencies (SSAs).

Ms. Manfra then asked Mr. Kepler to elaborate further on the types of information the private sector wants shared, as well as more details on specific individuals or entities who should be involved, to help the Federal Government create a more robust information sharing model that incorporates all levels of the public-private partnership.

Mr. Kepler reiterated the need to predetermine how the classification of information is structured. He explained that it is not necessarily that more people need to have clearances, but rather that they are able to obtain the right level of detail in the reports they receive so that both private sector executives and their employees can be timely in their response to emergency events.

High-level strategic information sharing, as it was discussed, can be less specific and less subject to higher classifications, while more operational-tactical information will likely need to be more specific. It was noted that physical security concerns can often be addressed by raising the level of security at a site broadly without sharing confidential information. Cybersecurity concerns however often demand more intimate details and will require more sharing of classified information due to their various forms and global origins.

Ms. Lau then suggested to Mr. Kepler that the Working Group, in the preparation of their final report, ask the Federal Government to identify organizations that are meeting on a regular basis within the sectors. Identifying and engaging these groups would likely help build relationships across the public-private partnership.

The Council then affirmed the Working Group recommendations as the consensus of the Council.

VI. PUBLIC COMMENT: DISCUSSION LIMITED TO MEETING AGENDA ITEMS

Nancy J. Wong, DFO, NIAC, DHS

No comments were registered by members of the public.

VII. CLOSING REMARKS

Constance H. Lau, NIAC Chair

William F. Flynn, Deputy Assistant Secretary for Infrastructure Protection, DHS *(invited)*

Jeanette Manfra, Deputy Director, Task Force for the Implementation of Executive Order 13636 and Presidential Policy Directive 21, DHS

Nitin Natarajan, Director, Critical Infrastructure Policy, National Security Staff

Mr. Natarajan thanked the NIAC for their continued hard work, and again noted the NIAC's unique insight and perspective the Council's feedback offers. He also noted that improved information sharing is an ongoing process within the Federal Government that has not been fully accomplished but has made a lot of progress. Mr. Natarajan illustrated the progress the public-private partnership has made by pointing out that higher level questions are being asked today that were not even considered five years ago.

Ms. Lau then reminded all in attendance that the third meeting special meeting the Council is holding to comment and make recommendations on the implementation of the EO and PPD-21, as well as the revision of the National Infrastructure Protection Plan (NIPP) will be held on September 17th. She also noted that the October 7th NIAC Quarterly Business Meeting has been rescheduled for November 21st.

VIII. ADJOURNMENT

Constance H. Lau, NIAC Chair

Ms. Lau thanked all in attendance and adjourned the meeting.

I hereby certify the foregoing minutes accurately represent the discussion and events that transpired at the meeting held on the date first noted above.

By: _____ Date: _____
Constance H. Lau, Chair, NIAC

National Infrastructure Advisory Council (NIAC)

August 14, 2013

National Intellectual Property Rights Coordination Center Auditorium

Opening of Meeting

Nancy Wong
Designated Federal Officer, NIAC

Roll Call of Members

Nancy Wong
Designated Federal Officer, NIAC

Roll Call – NIAC Meeting Attendance

NIAC Member	Present	Telecon	POC
Jack Baylis			
David J. Bronczek			
Albert J. Edmonds			
Glenn Gerstell			
David Grain			
Margaret Grayson			
Philip Heasley			
Raymond Kelly			
David Kepler			
Donald Knauss			
Constance Lau			

NIAC Member	Present	Telecon	POC
James B. Nicholson			
Thomas E. Noonan			
Gregory A. Peters			
James A. Reid			
Bruce Rohde			
Dr. Beverly Scott			
Michael Wallace			

Opening Remarks and Introduction

Constance Lau
NIAC Chair

Opening Remarks and Introduction

UPDATE AND DISCUSSION ON IMPLEMENTATION PLAN FOR EXECUTIVE ORDER 13636 AND PRESIDENTIAL POLICY DIRECTIVE 21 BY THE DEPARTMENT OF HOMELAND SECURITY

Jeanette Manfra
Deputy Director, Task Force for the Implementation of Executive Order 13636 and Presidential Policy Directive 21, DHS

PRESENTATION AND DISCUSSION ON COUNCIL RECOMMENDATIONS FOR IMPLEMENTATION PLAN FOR EXECUTIVE ORDER 13636 AND PRESIDENTIAL POLICY DIRECTIVE 21

David E. Kepler
NIAC Working Group Co-Chair

Philip Heasley
NIAC Working Group Co-Chair

National Infrastructure Advisory Council (NIAC)

Executive Order-Presidential Policy Directive Working Group (EO-PPD WG)

August 14, 2013

David E. Kepler
Executive Vice President/ Chief Sustainability Officer, Chief Information Officer
The Dow Chemical Company
Co-Chair

Philip Heasley
President and CEO
ACI Worldwide
Co-Chair

Agenda

- Framing Questions for Information Sharing
- Working Group Recommendations on Cybersecurity Information Sharing
- Appendix

Framing Questions On Information Sharing

- What obstacles do you see in the current information sharing environment with the Federal government and with the state and local government? What do your employees see when they try to obtain or send information to the Federal government? What causes the most heartburn and inefficiencies that demotivate sharing of information with the Federal government or with the SLTT?
- What are incentives to increased information exchange?
- What are the most effective mechanisms/processes that you have seen?
- What are the unique aspects of cyber information sharing that might differ from physical information sharing? Is the right information reaching the right people to take the action that is needed? If not, how can this be addressed specifically for cyber information sharing?

Framing Questions On Information Sharing

- What principles or actions that can be taken to be most likely to encourage voluntary information sharing? Least likely?
- What is the core value proposition for two-way cyber related information sharing?
- How should the Federal Government and private sector owners and operators track metrics for timely and coordinated sharing of cyber threat information and situational awareness at appropriate classifications? What might be the metrics for effective information sharing in both cyber and physical/operational dimensions?

Working Group Recommendations

On Cybersecurity Information Sharing

The EO-PPD Information Sharing Framework

- Aligned with the private sector's need for sharing timely and actionable information
- Can benefit all critical infrastructure sectors
- A significant challenge is to share information in a timely, specific and actionable way between the Government and private sector
- Creation of a "safe harbor"
- A recognition that information will only be used for intended purposes combined with limited anti-trust and privacy regulation protection, when acting in good faith, will encourage greater private sector participation in the information sharing program.

Incentives

- The opportunity to receive timely and actionable information, by itself, is a significant incentive for companies to opt into the information sharing program
- Additional incentives could include technical guidelines, support and sharing of cyber security practices between DHS/NSA and the private sector.

Effective Mechanisms

- The private sector needs easy access to indicators via a portal similar to those used by HSIN and US-CERT. Information must be in a format and specificity that can be used by each company to search their own security logs (i.e. IP addresses, domains, malware hashes, etc.).
- Sharing specific vulnerabilities, threats, methods and motivations of attackers will also help private sectors make more accurate and effective use of resources to improve cybersecurity postures.

Effective Mechanisms Continued

- All current Federal mechanisms for Information Sharing (one-on-one, US-CERT, Intelligence briefings,…) should be reviewed with the goal of simplifying processes, eliminate redundancy , improve coordination among different Federal agencies and ensure consistency of information delivered as suggested by the NIAC in 2012.
- DHS should collaborate with the private sector on information sharing work process definition, to ensure that procedures are effective and efficient for exchanging information between the owners and operators and government at all levels.

Classification of information in the management of Cybersecurity

- Another significant barrier to an effective information sharing program is the structure in how information is classified.
- Information needs to be more finely divided, so that as much of what is shared as possible can be declassified. That will allow more information to be disseminated among the private sector to resources that can take specific actions.

Classification of information in the management of Cybersecurity Continued

- Although DHS plans to expedite clearances, there needs to be more clarity on how classified information can be used within a company whose monitoring systems will not be certified for classified information. If action is to be taken, information needs to be declassified for deeper and broader communication within a company or industry.
- Execution of cyber security does not just fall within the CISO or CIO. Unlike some information that could be actionable despite being highly compartmentalized, because of the use and implementation of Information Technology systems and controls across entire facilities and organizations, there is a need for cybersecurity information to be disseminated more broadly. This direction has been provided for in the new Executive Order.

Principles to encourage information sharing

- Recognizing that the concerns of the private sector in sharing information may inhibit the desired level of this sharing, the Federal government should adopt a policy that specifically addresses concerns that information sharing could lead to governmental inquiries and regulation beyond the original particular purpose for which information may have been offered.
- DHS PCII (Protect Critical Infrastructure Information) is a good example of a program that can be leveraged in other sectors to address this concern.

Principles to encourage information sharing Continued

- To allay such concerns, and in appreciation of the greater benefits that may arise from encouraged information sharing by the private sector to the public authorities, the Federal government could, for example, provide mechanisms to assure that information will remain confidential and not disseminated within the government except where there are legitimate and compelling reasons to do so.
- To further illustrate, such mechanisms might range from the designation of particular means and channels of communication to assure confidentiality, to the creation of "safe harbors" whereby private sector entities could have limited anti-trust protection, the ability to divulge information free of civil or criminal liability under privacy protection laws, and to the establishment of exceptions for disclosure regarding cyber incidents by SEC public reporting companies under limited conditions.

Metrics

- As stated in the National Infrastructure Protection Plan, information sharing is a means to an end, not an end itself.
- An information sharing effort should recognize, understand, and concur with a common goal. The Homeland Security Studies and Analysis Institute (HSSAI), a non-profit federally funded research and development center operated by Analytic Services Inc. on behalf of the DHS has created document entitled "Metrics for Measuring the Efficacy of Critical Infrastructure-Centric Cybersecurity Information Sharing Efforts. This document details options for metrics which include the attributes of effective information sharing (i.e. relevance, timeliness, accuracy, etc.) and the outcome based goal of information sharing which is primarily 'no loss of control'.
- We recommend that, if the Integrated Task Force is not leveraging this document, that it serve as the framework for the development of the metrics.

Appendix

Working Group Members

WG Member	Sector Expertise
David E. Kepler, *Executive Vice President/ Chief Sustainability Officer, Chief Information Officer, The Dow Chemical Company,* Co-Chair	Chemical
Philip Heasley, *President and CEO, ACI Worldwide,* Co-Chair	Telecommunications
Glenn S. Gerstell, *Managing Partner, Milbank, Tweed, Hadley, & McCloy LLP*	Water, Telecommunications
Michael J. Wallace, *Former Vice Chairman and COO, Constellation Energy*	Electricity, Nuclear

Public Comment

Nancy Wong
Designated Federal Officer, NIAC

DISCUSSION AND DELIBERATION ON COUNCIL RECOMMENDATIONS FOR IMPLEMENTATION PLAN FOR EXECUTIVE ORDER 13636 AND PRESIDENTIAL POLICY DIRECTIVE 21

Constance Lau
NIAC Chair

Closing Remarks

Adjournment

Constance Lau
NIAC Chair