## NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

### PUBLIC MEETING AGENDA

July 17, 2013
3:00 p.m. – 4:30 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<br>*Nitin Natarajan*, Director, Critical Infrastructure Policy, National Security Staff<br>*Samara Moore*, Director for Cybersecurity and Critical Infrastructure, National Security Staff<br>*Caitlin Durkovich*, Assistant Secretary for Infrastructure Protection, DHS<br>*Robert Kolasky*, Director, Task Force for the Implementation of Executive Order 13636 and Presidential Policy Directive 21, DHS |
| **IV.** | **UPDATE AND DISCUSSION ON IMPLEMENTATION PLAN FOR EXECUTIVE ORDER 13636 AND PRESIDENTIAL POLICY DIRECTIVE 21 BY THE DEPARTMENT OF HOMELAND SECURITY** | *Robert Kolasky*, Director, Task Force for the Implementation of Executive Order 13636 and Presidential Policy Directive 21, DHS |

| | | |
|---|---|---|
| **V.** | **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<br>*Philip Heasley,* NIAC Working Group Co-Chair |
| **VI.** | **Public Comment: Discussion Limited to Meeting Agenda Items** | *Nancy J. Wong,* DFO, NIAC, DHS |
| **VII.** | **Closing Remarks** | *Constance H. Lau,* NIAC Chair<br>*Nitin Natarajan,* Director, Critical Infrastructure Policy, National Security Staff<br>*Samara Moore,* Director for Cybersecurity and Critical Infrastructure, National Security Staff<br>*Caitlin Durkovich,* Assistant Secretary for Infrastructure Protection, DHS<br>*Robert Kolasky,* Director, Task Force for the Implementation of Executive Order 13636 and Presidential Policy Directive 21, DHS |

## MINUTES

### NIAC MEMBERS PRESENT IN ARLINGTON, VA:

### NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:

Mr. Jack Baylis; Mr. Glenn Gerstell; Ms. Peg Grayson; Mr. Phil Heasley; Mr. David Kepler; Ms. Constance Lau; Mr. James Reid; Mr. Bruce Rohde; Mr. Michael Wallace

### MEMBERS ABSENT:

Mr. David Bronczek; Mr. Gilbert Gallegos; Mr. David Grain; Commissioner Raymond Kelly; Mr. Donald Knauss; Mr. James Nicholson; Mr. Gregory Peters; Mr. Greg Wells; Dr. Beverley Scott

### SUBSTANTIVE POINTS OF CONTACT ATTENDING VIA CONFERENCE CALL:

Ryan Beck (for Commissioner Raymond Kelly); Ms. Joan Gehrke (for Mr. James Nicholson)

### OTHER DIGNITARIES PRESENT:

Ms. Caitlin Durkovich, Assistant Secretary, IP, DHS; Mr. Robert Kolasky, IP, DHS; Ms. Samara Moore, NSS; 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

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

*Samara Moore*, Director for Cybersecurity and Critical Infrastructure, National Security Staff

*Caitlin Durkovich*, Assistant Secretary for Infrastructure Protection, DHS

*Robert Kolasky*, Director, Task Force for the Implementation of Executive Order 13636 and Presidential Policy Directive 21, DHS

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. She explained that this meeting is the first 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 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.

Ms. Durkovich thanked the Council for inviting her to participate in the discussion, as well as for its work to help build a more resilient system that secures physical assets and enhances cybersecurity through a whole-of-community approach. Ms. Durkovich also thanked the NIAC and the Integrated Task Force (ITF) for their work within the public-private partnership.

Mr. Kolasky echoed Ms. Durkovich and Mr. Natarajan's comments, and also thanked the Council for its participation, constructive feedback, and flexible recommendations on the complex critical infrastructure security and resilience challenges the Nation faces.

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

*Robert Kolasky*, Director, Task Force for the Implementation of Executive Order 13636 and Presidential Policy Directive 21, DHS

Mr. Kolasky began by giving an update on the reports that Federal agencies have produced regarding incentives that would promote adoption of the cybersecurity framework. The departments of Commerce, Defense, Treasury, and Homeland Security collaborated on potential incentives, followed by the submission of independent reports by each department. Those reports have been sent to the White House, and will be released to the public following review.

Mr. Kolasky noted that the incentives reports are not the end of the ITF's work on incentives. The ITF still requires help in coordinating administrative action concerning what incentives can and should be moved forward from their analytical state to formal policy. DHS has been working with partners across the Federal Government, as well as private sector owners and operators, to develop a voluntary program that will combine incentives with technical assistance and support from the Federal Government.

The ITF delivered an evaluation of the existing public-private partnership model to the White House during the week of July 8. The report, which considers the partnership in the context of the holistic policy approach needed to address the increasingly complex threat environment, details how the existing model has proven effective in enhancing critical infrastructure security and resilience and in increasing the emphasis on the vulnerabilities of aging infrastructure.

## V. DISCUSSION AND DELIBERATION ON COUNCIL RECOMMENDATIONS 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

Ms. Lau then introduced Mr. Kepler and Mr. Heasley, Co-Chairs of the NIAC EO-PPD Working Group, and thanked them for their leadership and dedicated service. Ms. Lau also thanked Mr. Gerstell and Mr. Wallace for their participation in both the EO-PPD Working Group and the Regional Resilience Working Group. Mr. Kepler also thanked Co-Chair Mr. Heasley and fellow Working Group members Mr. Gerstell and Mr. Wallace for their contributions, and began the presentation by discussing Working Group member perspectives on incentives.

Mr. Kepler began by noting the Working Group's first recommendation: Grants are likely to be the most effective means for encouraging adoption of a cybersecurity framework. Grants focused on creating capacities and capabilities to benefit an entire industry encourage companies to participate in the framework, and enhance overall collaboration and support networks. Direct Federal funding and prior knowledge of grant contingencies are also likely to increase framework adoption and compliance. Mr. Kepler noted that Federal funding for grants should be outcome-based, and any penalties for incomplete adoption of the framework should not exceed the value of the original grant. In addition, grants should encourage the creation of capabilities — such as industry training programs, information sharing capabilities, or the establishment of research consortiums — that will benefit an entire sector, rather than a single company.

Mr. Kolasky asked for clarification regarding where Federal grants would be distributed to create this desired effect.

Mr. Kepler noted that many sectors have established industry associations that could be engaged in the program, as those organizations' roles within industries are most likely to encourage collaborative efforts between small and large companies, which benefits the entire industry.

Ms. Lau added that similar research organizations already exist in the Electric Sector, and that peer assistance helps to create synergistic relationships between large and small companies. And, as more companies adopt the framework, well-developed best practices emerge, which can help to spur further adoption in the sector. Mr. Kepler then discussed the working group's second recommendation on incentives: Liability caps are more effective than liability reductions in encouraging adoption of the cybersecurity framework. Caps make participation in planning and preparation for high-impact, low-probability events more attractive to executives, as companies are able to recoup insurance benefits if needed. Mr. Kepler noted that uncapped liabilities present the possibility of underwriters, in effect, setting security policy, by transferring the financial risks entirely to insurance providers — and since the goal of the framework is to lower risk, rather than transfer it, liability caps are more likely to encourage improved security and resilience practices across industries. Working Group members also emphasized the importance of acknowledging good-faith efforts of companies working to adopt the framework; without that acknowledgement, companies could be at greater risk of litigation and antitrust issues.

Mr. Kepler then discussed the Working Group's third recommendation: The Federal Government should require cybersecurity framework compliance on its suppliers, related to critical infrastructure. Procurement, and the Federal Government's purchasing power, could be a means to encourage wider implementation of the cybersecurity framework, Mr. Kepler said. If security and resilience standards require hardware and software suppliers to provide more secure and resilient assets, systems, and tools when selling to the Federal Government, those baked-in standards will be part of the hardware and software sold to private sector owners and operators as well. Much vulnerability associated with critical infrastructure is directly or indirectly related to IT hardware and software, and the private sector uses many of the same tools and systems as the Federal Government does. As a result, the leveraging of Federal purchasing power would lead to enhanced security and resilience overall, Mr. Kepler said.

Mr. Kolasky asked Mr. Kepler whether he thought government-to-business procurement policies would translate into business-to-business relationships.

Mr. Kepler expressed his belief that it would have that effect, as the standards create a base level of trust in the work of suppliers for critical infrastructure owners and operators. That, in turn, allows owners and operators to focus on security and resilience issues unique to their industry.

Ms. Lau noted that concept could be applied to any industry, particularly in regulated industries where there is larger purchasing power. She asked if that was something the Working Group discussed.

Mr. Kepler noted that the program, as a voluntary, standards-based approach, would include certain requirements and practices applicable to almost any critical infrastructure. The Federal Government would essentially accelerate part of the framework adoption process, he added.

Mr. Kepler then discussed the Working Group's fourth recommendation: that the Federal Government should evaluate and leverage existing regulations to determine which policies could be referenced in the proposed framework. The use of policies and practices in the framework that are already regulated allows for their use as a supplement to any standard that is created in a relevant and robust risk management process. This approach will simplify the compliance process and reduce costs, Mr. Kepler said. In addition, the potential consequences of not participating, including harm to value chains, should encourage further participation.

Mr. Kepler then discussed recommendations the Working Group is considering in addition to those based on the scoping questions provided by the ITF:

- There is a need for a robust, dynamic risk identification process
- The Federal Government should ensure the availability of qualified and vetted security professionals
- Private sector participants in the cybersecurity framework should receive limited protection from antitrust regulations

Mr. Kepler noted that the NIAC has previously published two research reports with references to security training and credentialing programs, which may be applicable and transferrable to the cybersecurity framework. The NIAC has also previously published recommendations regarding the need for antitrust vehicles that can provide protection for companies to discuss their private security threat information.

Mr. Kepler transitioned to Working Group member recommendations on the National Infrastructure Protection Plan (NIPP) rewrite.

Members noted the value of senior-level buy-in among owners and operators. Executive-level engagement is likely to encourage private sector adoption of the NIPP, as executives are directly involved in the allocation of company resources. Mr. Kepler added that it would also be beneficial to have executives review and summarize the plan, in order to make clear to other executives the value proposition of the NIPP. Mr. Kepler also noted the Working Group's willingness to provide that input.

The Working Group also highlighted the value of clear and concise communication that makes clear the value of the public-private partnership to private sector owners and operators. Mr. Kepler noted that there are numerous tools and techniques exist, created by both the Federal Government and the private sector, and all those tools and techniques can be leveraged to encourage adoption and compliance with the NIPP.

The Working Group also recommended prioritizing the 4 lifeline sectors — water, electricity, communications, and transportation —because they facilitate the other 12 sectors. Ms. Lau noted that the NIAC Regional Resilience Working Group has also been highlighting the importance of the lifeline sectors and their cascading effects on all sectors.

In addition, Working Group members recommended that development of the implementation plan is a collaborative effort between the public and private sectors. This is likely to be the most effective way to convey stakeholder concerns, as it will not only address the common concerns of both public and private participants, but also do so in language that is accessible and readily readable to senior-level executives.

Mr. Kepler also noted the importance of guiding regulators through the complexities of the public-private partnership. He noted the Working Group's concern that punitive oversight measures could undermine the private sector's involvement in the voluntary structure, and added that the private sector is willing to assist in the development and education of regulators.

The Working Group's final additional recommendation is that the Federal Government should provide services that can be leveraged by the broader owner/operator community. Owners and operators can become overwhelmed by the scope of security options they have to choose from, leading to untimely decisions or no decision at all. The Federal Government and large companies have the opportunity to synthesize complex security and technology standards to enhance sector security postures to become more secure and resilient through well-calibrated systems that are in tune with current and future threat indicators. Mr. Kepler emphasized that while deploying appropriate technology is important, the right kind of product stewardship and follow up is also critical.

Ms. Moore thanked the working group for their timely analysis and recommendations on the EO and PPD-21 as well as the NIPP rewrite.

The Council motioned to approve the recommendations. Ms. Lau then opened the meeting to additional discussion and questions.

Mr. Kolasky noted that the ITF is considering the Council's notion of lifeline sector prioritization in their ongoing deliberations. He asked whether the NIAC was referencing the specific sectors, or the lifeline functions they deliver. He also asked if the Council is recommending that sectors delivering lifeline functions be promoted as first among equals. Mr. Kolasky noted that the ITF is deliberating on whether the lifeline sectors should be singled out as enduring national priorities, or be considered as part of a regulatory prioritization process with strategic policies contained in the NIPP.

Ms. Lau and Ms. Wong said that the Council would take these questions under advisement, and have answers and recommendations by the next Public Meeting on August 14th.

Mr. Natarajan noted the Administration's position that the prioritization of the lifeline sectors be portrayed as having additional emphasis, rather than primacy, in order to continue viewing all 16 sectors as critical. The Administration does not want to suggest, for example, that keeping the power on is more important than public health or food safety.

Mr. Kepler agreed, and explained that the Working Group's assignment of the lifeline sector designation is the result of an analysis that revealed those four lifeline sectors. Those sectors are needed to keep the other 12 sectors functioning.

The Council then approved the recommendations on the EO and PPD-21 and the NIPP revision.

## VI. PUBLIC COMMENT: DISCUSSION LIMITED TO MEETING AGENDA ITEMS

*Nancy J. Wong,* DFO, NIAC, DHS

Ms. Prudence Parks of the Utilities Telecommunications Council thanked DHS and the NIAC, and expressed her gratitude for its participation in framework development. She complimented DHS and the White House for their willingness to engage with the private sector, as well as for the transparency of deliberations.

## VII. CLOSING REMARKS

*Constance H. Lau,* NIAC Chair

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

*Samara Moore,* Director for Cybersecurity and Critical Infrastructure, National Security Staff

*Caitlin Durkovich,* Assistant Secretary for Infrastructure Protection, DHS

*Robert Kolasky,* Director, Task Force for the Implementation of Executive Order 13636 and Presidential Policy Directive 21, DHS

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.

Ms. Moore echoed Mr. Natarajan's comments and thanked the NIAC for the opportunity to engage them on the EO, PPD-21, and the NIPP rewrite. She added that all parties — whether as part of government, or as private sector owners and operators — have a vested interest in making the policies timely and actionable.

Mr. Kolasky thanked the NIAC and the EO-PPD Working Group for its presentation and thoughtful recommendations. He explained that DHS and the Administration realize that if infrastructure owners and operators do not see their perspectives in a critical infrastructure security and resilience plan, then the plan is unlikely to succeed.

## 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)

July 17, 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

**Robert Kolasky**

Executive Director, Integrated Taskforce for the Implementation of EO 13636 and PPD-21, DHS

# 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

**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)

July 17, 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 Recommendations on Incentives
- Working Group Recommendations on Incentives
- Additional Recommendations Generated from Working Group Comments & Discussion
- Framing Questions for  Recommendations on National Infrastructure Protection Plan Revision
- Working Group Recommendations on National Infrastructure Protection Plan Revision
- Appendix

# Framing Questions

For Recommendations on Incentives

# Framing Questions on Incentives

- What incentives are most likely to be adopted voluntarily by owners and operators?

- What incentives are least likely to be adopted voluntarily by owners and operators?

- Executive level engagement with the Federal government helps Executives create priorities, allocate resources, and hold individuals accountable for private sector actions. What steps can be taken to ensure Executives are engaged and driving voluntary incentive adoption?

# Framing Questions on Incentives (cont.)

- □ Executives are cognizant of their fiduciary responsibilities to shareholders. How can the Federal government best reduce risk and uncertainty for Executives and encourage voluntary incentive adoption?

- □ How can incentives best be paired with tools, technology, assets, and processes the government has, in order to encourage voluntary adoption?

- □ How can Executive Summaries on incentive implementation be precisely and concisely written for Executives with little prior knowledge or experience in critical infrastructure security and resilience in order to communicate what happens, how things work, and how their risk and uncertainty are reduced?

# Framing Questions on Incentives (cont.)

- How can the Federal government make all incentives voluntary while balancing regulation and oversight to facilitate a networked-coordination environment?

- How can incentives best target lifeline sectors most critical in an actual emergency?

- How can incentives best be prioritized to coordinate with infrastructures dependent on lifeline sectors that currently lack the resources, strength, or internal capabilities to bring themselves up to the level needed the case of an actual emergency?

# Framing Questions on Incentives (cont.)

- What steps should be taken to ensure that all NIAC members are fully aware of the alignment and structure of all 16 sectors in order to prioritize incentives and their voluntary adoption?

- To what extent should time limits and sunset clauses be incorporated to promote voluntary adoption?

- Are there additional incentive categories that should be considered in addition to the 14 proposed?

- Should any of the 14 proposed incentive categories be broken down further?

- Is their relevant research, literature, or Member experience that the Working Group should consider in either cyber or non-cyber contexts?

# Working Group Recommendations

On Incentives

# Grants are an effective means for encouraging adoption of a cybersecurity framework

- Direct Federal funding for investment in the framework would be beneficial.
- It is important to clearly articulate any contingencies associated with the grants.
- Funding results should be outcome-based, and penalties should not exceed the value of the grant.
- Grants should be focused on creating capability that can benefit an entire industry sector, and not one company.
  - i.e. industry training programs, information sharing capability, research consortium for sector specific technologies, etc.

# Liability caps are more effective than liability reductions

- Security is not improved by simply transferring risk to insurance companies. A more effective strategy for encouraging participation would be to cap the liability associated with compliance with the cybersecurity framework.
- Not capping liability may create an environment in which insurance underwriters dictate security policy.
- Companies acting in good faith should not see additional risk in adoption of the framework.
- A policy similar to the SAFETY Act, which provides liability protection to encourage adoption of the "Cybersecurity Framework" or similar industry standard, should be considered as an option.

# The Federal Government should require cybersecurity framework compliance on its suppliers, related to critical infrastructure

- □ Government procurement power has numerous indirect benefits for the private sector. It incentivizes suppliers to enhance the security of their products and services — which are often the same products and services used in private critical infrastructure.
- □ The Government needs to include hardware and software suppliers in any scope of procurement policy. Reducing the risk associated with hardware and software systems allows owners and operators to redirect their attention to other critical security concerns.
- □ Many risks that CIKR owners/operators face are a direct result of vulnerabilities within purchased IT hardware and software.

# Evaluation and leveraging of existing regulations

- Leveraging of compliance with existing laws into the framework is more effective than introducing new rules that may create conflict.
- Many cybersecurity policy and practices are already regulated.
- Layering additional policies and regulations on top of current regulations will create larger compliance models reducing flexibility, increase costs, and reduce effectiveness.

# Additional Recommendations

Drawn from Working Group Comments & Discussion

# A robust, dynamic risk identification process

□ Compliance with the cybersecurity framework compliance needs to be focused on the major risks in critical infrastructure.

□ Greater credibility will be granted to a program that allows an owner/operator to focus adoption on the major risk areas. It will emphasize protection of vital assets, as well as reducing cost to both industry and the Federal Government.

□ Rate recovery for price regulated industry is an effective incentive; however, keeping the focus on high risks lowers downstream consumer impact.

# Ensuring the availability of qualified, vetted security professionals

- New areas of compliance require additional professionals to ensure compliance, and qualified personnel can be challenging to find.
- Federal assistance with background checks, and leveraging of existing programs could establish a greater reserve of qualified professionals.
- Further information:
  - NIAC 2006 Report on Workforce Preparation, Education and Research
  - NIAC 2008 Report on "The Insider Threat to Critical Infrastructures"

# Anti-trust protection

- The effectiveness of the Executive Order and subsequent PPD relies heavily on the sharing of threat information between the public and private sectors, but also will require sharing amongst private sector companies. Currently this sharing is discouraged due to the concern of violating, or the appearance of violating, of Anti-Trust regulations. Government must provide Limited Anti-Trust vehicles that provide protections for companies that discuss and share cyber threat information.
- The NIAC previously noted the value of limited antitrust protections in its 2009 report, titled “Critical Infrastructure Resilience,” in relation to the Protected Critical Infrastructure Information (PCII) program. In that report, it was noted that the United Kingdom has enhanced risk information sharing among competitors by scrubbing the source of the information, and focusing only on mitigation methods, and that a similar set of rules could dispel fears of using such information against the entity providing it.

# Framing Questions

For Recommendations on National Infrastructure Protection Plan Revision

# Framing Questions on NIPP Revision

- □ How does the Federal government write a short and clear revised plan that is flexible adaptable, and readable to owners and operators outside of the Beltway?
- □ What has to be in the plan for it to be seen as useful and applicable to owners and operators?
- □ How do we incorporate the concepts of how the critical infrastructure mission can operate in a "networked-coordination" environment; but provide enough structure and order that those who are going to be implementing the NIPP can build their own plans, processes, etc.in a measurable way from a national perspective?

# Framing Questions on NIPP Revision (cont.)

- How can the plan focus on critical functions and services (such as the lifeline infrastructures and dependencies by the other sectors) while maintaining appropriate and relevant risk based momentum in the other sectors?

- How can the plan incorporate appropriate support for the 4.8 Million O/O community (baseline) so that they also can benefit from the national programs, capabilities, and lessons learned; that they know what to do and where to go for infrastructure security and resilience information and advice/guidance (given continuous restrained Federal resources)?

# Working Group Recommendations

On National Infrastructure Protection Plan Revision

# Executive-level engagement is vital in any effort to encourage private sector use of the NIPP, and should be embraced in every public-private partnership activity

- Executive-level private sector officials set priorities, direct resources, and can hold others accountable within the corporation. Because of this, the success of any partnership with owners and operators is contingent upon successful engagement with those who have the most ability to direct a company toward a more secure and resilient posture — CEOs and executives with board member oversight.
- The revised NIPP should include a summary for these officials to improve the understanding of the critical infrastructure security and resilience (CISR) mission. The Federal Government should seek input and help from the private sector to develop a communication plan targeted at Senior Business Leaders that may include meetings with senior executives, CEO forums, and executive summaries to further explain the relevance of the NIPP.  This should include sector specific messaging.
- In addition, an advisory panel — with the ability to guide and mold the development of a flexible, adaptable, outcome based plan — should be considered as a means to enhance the value of the document.

# To make the plan useful and valuable to the private sector, clear, concise communication incentivizing the public-private partnership value proposition is needed

- There are numerous tools, technologies, and programs created by the Federal Government and Industry that can assist in risk assessments and risk management. A simple description of how these programs can reduce risk, along with an explanation of the participation process, would better inform senior-level private sector stakeholders on the value of the NIPP framework. For example, the Chemical sector, DHS developed the CFATS program that helps assessing risk and security practices. The National Institute of Standards and technology (NIST) also provides guidance that can be leveraged. Established Industry standards like ISO 27001 and ISA /ISEC 62443 series for Industrial Automation can be used as well during NIPP revision.
- Examples of successful public-private partnership efforts would provide real-life demonstrations of the value drawn from the NIPP, and how a company can collaborate in the networked environment.

# The four "lifeline sectors" – water, electricity, communications and transportation – should be the focus of prioritized efforts to enhance security and resilience, with a recognition of the importance of information technology to those sectors

- Rather than attempting to dedicate equal attention to all 16 critical infrastructure sectors, the effect each sector has on the well-being of the Nation should be taken into consideration. "Lifeline Sectors" — Water, Electricity, Communications, and Transportation — are regarded as central to the Nation; as a result, those sectors should receive the largest share of immediate attention in the effort to increase security and resilience. Limited Federal resources should not be diluted by applying equal immediate effort to each sector; instead, a tiered system should be established to guide prioritization. Of the remaining critical infrastructure sectors, importance will vary among regions but the financial sector stands out as being important to national economic activity.
- Sectors which supply critical IT hardware and software to CIKR sectors also need appropriate attention. All CIKR sectors rely heavily on IT backbone products such as operating systems, network hardware, process control systems, etc. Secure backbone products create resiliency throughout the entire supply chain.

# Development of the implementation plan should be a collaborative effort between the Federal Government and owners and operators

- □ Plans that are considered, developed, and deployed solely by Federal agencies often produce actions only for the Federal Government itself. A high-level public-private partnership planning group — featuring industry executives and practitioners, as well as senior-level Federal officials — could produce a more effective plan by addressing the issues facing all stakeholders in the partnership.

# It is important to have a voluntary structure for private sector participants, and that regulators are guided in the navigation of the public-private partnership.

- The Federal Government should be careful to ensure that regulatory bodies do not attempt to impose their will onto the partnership. Punitive oversight measures would only be counterproductive to efforts to enhance the public-private partnership.
- A commitment to educate regulators is also needed from the Federal Government on evaluation and consideration of those owners and operators collaborating on the CISR mission and partnership.
- The Federal Government should seek the support from the private sector to educate its regulators and Industry on Cyber security practices being implemented in the Industry. Private Sector is willing to help in the development and education of the regulators.
- It is also recommended that those entities in the partnership are granted some protections from regulative bodies as they work to improve security and resilience.

# Providing services which can be leveraged by the broader owner/operator community

- One of the key challenges that NIPP revision will have is to address is incorporating appropriate support for the broader 4.8 Million O/O community.  To address it, The Federal Government can influence the private sector IT companies to play a bigger role in helping to uplift the security posture of the 4.8 million O/O community.  While standards and information sharing will play a big role in this endeavor, Operators are often overwhelmed and under-informed when choosing the right security technology and identify the "threat indicators".  Creating a common national cyber threat database which is populated by both public and private entities and available by subscription to all owner / operators would eliminate some of the barriers in picking the technology and security practices needed by a company to effectively implement a cyber security framework.
- This is an area where grant incentives may be considered.

# Appendix

# Working Group Members

| Working Group Member | Sector Experience |
|---|---|
| **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 |

# Closing Remarks

# Adjournment

**Constance Lau**

NIAC Chair