NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

PUBLIC MEETING AGENDA
September 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 *William F. Flynn*, Deputy Assistant Secretary for Infrastructure Protection, DHS *Robert Kolasky*, Director, Task Force for the Implementation of Executive Order 13636 and Presidential Policy Directive 21, DHS (invited) *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**	*Robert Kolasky*, Director, Task Force for the Implementation of Executive Order 13636 and Presidential Policy Directive 21, DHS (invited)
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 *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 *William F. Flynn*, Deputy Assistant Secretary for Infrastructure Protection, DHS *Robert Kolasky,* Director, Task Force for the Implementation of Executive Order 13636 and Presidential Policy Directive 21, DHS (invited) *Nitin Natarajan,* Director, Critical Infrastructure Policy, National Security Staff

MINUTES

NIAC MEMBERS PRESENT IN ARLINGTON, VA:

NIAC MEMBERS ATTENDING VIA CONFERENCE CALL:
Mr. Jack Baylis; Mr. Glenn Gerstell; Ms. Peg Grayson; Mr. David Kepler; Ms. Constance Lau; Mr. Bruce Rohde; Mr. Michael Wallace

MEMBERS ABSENT:
Mr. David Bronczek; Mr. Gilbert Gallegos; Mr. David Grain; Mr. Philip Heasley: Commissioner Raymond Kelly; Mr. Donald Knauss; Mr. James Nicholson; Mr. Gregory Peters; Mr. James Reid; Dr. Beverley Scott; Mr. Greg Wells

SUBSTANTIVE POINTS OF CONTACT ATTENDING VIA CONFERENCE CALL:
Mr. Ted Basta (for Dr. Beverly Scott); Ms. Joan Gehrke (for Mr. James Nicholson); Naureen Khabir (for Commissioner Raymond Kelly)

OTHER DIGNITARIES PRESENT:
Mr. William F. Flynn, Deputy Assistant Secretary, IP, DHS; Mr. Chris Anderson, IP, DHS; Mr. Kevin Stine, NIST; 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

Chris Anderson, Speaking for the 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. She explained that this meeting is the third 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. Flynn thanked the Council for inviting him to participate in the discussion, as well as for its work to help build a more resilient national infrastructure program that secures physical assets and enhances cybersecurity through a whole-of-community approach. He noted that in the two previous meetings, the NIAC has provided valuable insight and recommendations on what incentives could be leveraged to encourage adoption of the voluntary cybersecurity framework, as well as on methods of enhancing information sharing. NIAC member comments were integral in constructing deliverables for both the EO and PPD-21. Mr. Flynn also thanked the NIAC and the Integrated Task Force (ITF) for their work within the public-private partnership, and extended his condolences to victims of the recent Navy Yard shooting in Washington, D.C.

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 security and resilience (CISR) 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.

Mr. Anderson, who replaced Mr. Robert Kolasky role in the meeting, echoed Mr. Flynn and Mr. Natarajan's comments, and also thanked the Council for its participation, constructive feedback, and flexible recommendations on the complex challenges the Nation faces in enhancing the security and resilience of critical infrastructure. He acknowledged that the ITF has pushed an aggressive timetable that the NIAC has consistently met. Mr. Anderson also noted that the NIPP rewrite is continuing at an equally aggressive pace. The day for comments will be September 20, followed by a two-day public session on September 27and 28.

NIAC members then approved the meeting minutes from the July 17 Public Meeting.

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

Kevin Stine, Manager of Security Outreach and Implementation in the Computer Security Division of the National Institute of Standards and Technology (NIST)

Mr. Kevin Stine, who represented the National Institute of Standards and Technology (NIST), who led the ITF working group to develop the Cyber Security Framework, explained that he is responsible for constructing the voluntary cybersecurity framework mandated by the EO, and would be sharing a brief status report on NIST implementation plan and activities to date.

There are three specific requirements NIST is trying to achieve in collaboration with critical infrastructure owners and operators to develop the voluntary cybersecurity framework: 1) developing a set of existing standards, guidelines, best practices and methodologies to promote the protection of critical infrastructure; 2) providing an approach that can help owners and operators of critical infrastructure and identify ways to manage cybersecurity risk; and 3) identifying areas for improvement that need to be addressed through future collaborations, either with standards and development organizations or with particular sectors moving forward. NIST has obtained significant feedback from industry and other stakeholders through an open and transparent process to help shape the framework. When the EO was issued in February, NIST began gathering input from industry on the types of practices, standards, and guidelines used today that are particularly effective in helping manage cybersecurity risk within the context of organizations and critical infrastructure sectors. NIST has also solicited feedback from many associations and government agencies.

Mr. Stine also mentioned that NIST has been engaging in a series of open and public workshops since the release of the EO. The purpose of these workshops is to engage in-person representatives of critical infrastructure organizations and sectors. Workshops were held at the Department of Commerce in Washington, D.C., in April; at Carnegie Mellon University in Pittsburgh in May; at the University of California, San Diego, in July; and at the University of Texas in Dallas in September.

Mr. Stine noted that a preliminary cybersecurity framework will be released October 10, with 45 days allotted for public comment. This will be announced in the Federal Register. Comments will be adjudicated, along with those already received, to address differing models for framework management and evolution of the framework beyond the February 2014 final issue date.

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

Ms. Lau then introduced Mr. Kepler, and thanked him for his 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 the voluntary cybersecurity framework.

Mr. Kepler began by noting the positive observations expressed by Working Group members on the voluntary cybersecurity framework.

Overall, the framework presents a coherent and practical approach to cybersecurity that effectively coordinates the experience, standards, and practices already in use. Mr. Kepler noted that the care in emphasizing the voluntary nature of the framework will help attract members of the private sector. The risk-based approach the framework uses — which highlights the differences among industries and sectors — is likely to increase adoption and compliance as well. Mr. Kepler also noted that the tier-structure of the framework being used to assess implementation and performance standards is familiar to the private sector, and the Information Technology (IT) industry in particular. The framework's commitment to timely and actionable

guidance for future collaboration and continued development is also appealing to the private sector.

To improve the framework, Mr. Kepler reiterated the Working Group's earlier recommendation for a stronger focus on process- and outcome-based metrics as a means for assessing the effectiveness of applying the framework. Mr. Kepler cited "Metrics for Measuring Efficient Effectiveness of Critical infrastructure Cybersecurity Information Sharing Efforts," a report commissioned by DHS, as the basis for this recommendation. Similar benchmarks and processes for information sharing and the gathering of intelligence should be established in the framework as well.

Mr. Kepler also recommended that ownership and responsibility for continued development of the framework remain with the private sector, most likely in a university setting, which is a proven model that can be easily funded by critical infrastructure sectors and companies. He cited the success of the Mary Kay O'Connor Process Safety Center at Texas A&M University as an example of a sustainable and continuously improving model.

Mr. Kepler then pointed out that while the EO excluded consumer-based IT products, it did not exclude all IT products. He explained that the Working Group thinks there is a need to emphasize securing standards for IT products in all critical infrastructure sectors, with the lifeline sectors — Water, Electricity, Transportation, and Communications — as the first priority. The standards that exist with the International Society of Automation (ISA) and Information Sharing Environment (ISE) would likely contribute to addressing this concern.

Mr. Kepler then discussed recommendations for maximum adoption of the voluntary cybersecurity framework that are aligned with the critical purpose outlined in the EO: the national and economic security of the United States depends on the reliable functioning of critical infrastructure in the face of cyber threats.

The first key principle to securing maximum adoption of the voluntary cybersecurity framework is securing the lifeline sectors and their interdependencies . The lifeline sectors constitute the backbone of the country and help facilitate the other twelve critical infrastructure sectors.

The second key principle is to engage the IT sector to have strong and secure products that support the cyber needs of the lifeline sectors, which support directly the first principle. Strong linkages exist between government agencies, financial sectors, and other networks that must be designed in an integrated approach to make sure the lifeline sectors are secured.

The third key principle is to use an outcome-based process in the framework. The EO requires the cybersecurity framework to identify and understand related risks and ensure that the associated programs are aligned with mitigating those risks and enhance preparedness.

The fourth key principle concerns the need for timely, accurate, and actionable information sharing between Federal Government and private sector participants and their peers. In addition, there is a need for adequate protection to ensure the information is used for intended purposes.

Mr. Kepler then shifted his presentation to the primary incentives Working Group members have identified in order to encourage the private sector to adopt and utilize the voluntary cybersecurity framework.

The strongest incentive to adoption is confidence that the framework will be effective in improving a company or sector's security posture in a cost-effective manner, through clear, outcome-focused goals and objectives for providing critical infrastructure security and resilience.

Transparency, like confidence, is also a primary incentive for adoption of the framework. Timely, accurate, relevant, and actionable information sharing between the Federal Government and private sector is critical, particularly with regard to high-priority threats. But information must also be shared whenever possible with the general public to sustain motivation for action. Mr. Kepler explained that while the private sector is attracted to clear outcome-focused goals and objectives, it is equally attracted to clear and effective implementation plans that have milestones and are transparent to members of the general public, primarily their shareholders.

Mr. Kepler then noted that companies should have assurances of limited protection for liability, antitrust protection, and limited Federal Government access for unrelated agencies. When companies act in good faith by volunteering their information for security purposes only, they should be assured that their information will not be misused. Private sector partners often feel volunteering their information to the Federal Government opens them up to a wider probe of their business practices. Mr. Kepler stressed again that assuring the private sector that their information will be used only for intended purposes is likely to encourage more companies to adopt the framework.

Duplication in existing laws and regulations is another area of concern for the private sector. To match the timeliness and flexibility of the private sector, the Federal Government needs to streamline and simplify processes that frequently create duplication. Mr. Kepler noted that this is a recurring recommendation of the private sector, and speaks to the importance of preparing for known threats, fixing existing problems, and responding to attacks and incidents in a timely manner.

Mr. Kepler concluded his presentation by emphasizing the need for a national unity of effort based in broad participation, collaboration, and trust. Incorporation of the above outlined key principles in an outcome-based approach is highly likely to result in widespread adoption of the voluntary cybersecurity framework.

Discussion then shifted to comments and clarifying questions from NIAC and Administration members.

Mr. Flynn thanked the Working Group for their efforts and noted that their presentation and work thus far has been clear, insightful, and actionable for the Federal Government. He also agreed with the Working Group's call for an outcome-based process and explained that this is a key priority moving forward.

Mr. Gerstell then pointed out that the Working Group's recommendations are of even greater importance for smaller owners and operators. Larger owners and operators are more likely to have sophisticated internal security operations that can bypass public-private partnership challenges; smaller owners and operators, on the other hand, are very careful when partnering with the Federal Government out of fear of greater intervention than intended.

Mr. Natarajan agreed with Mr. Gerstell and noted that this idea is a central focus of the National Security Staff's (NSS) efforts. He explained that NSS is trying to identify contracts and subcontracts and generate mechanisms to spread synergies across sectors while securing interdependencies with other sectors. Mr. Natarajan used the example of a smaller owner or operator being penetrated by a hacker, with that first company used as a means to get to larger owners or operators, causing greater damage to an entire sector.

Mr. Kepler agreed with Mr. Natarajan's assessment and noted that companies need to make good decisions and enforce strict standards up and down their supply chain and within their sector to benefit all involved and the public-private partnership as a whole.

Ms. Grayson also supported Mr. Natarajan's assessment and suggested that a possible recommendation be for Fortune 1000 companies to mentor smaller companies in their supply chain or within their industry in general to extend best practices and the framework for wider adoption. Mr. Kepler then explained that this can be accomplished through a simple structure, and simplified standards that are mutually beneficial to both larger and smaller owners and operators and lower national and company risk.

Mr. Wallace also noted the need to consider vulnerability, risk, and impact for a company, as well as its risk profile, assets, and its stakeholders. He explained that it is important to get companies of all sizes to think in terms of the former, more national lens, as well as their individual vulnerability, risk and impact.

NIAC Members then affirmed the Working Group's recommendations.

VI. PUBLIC COMMENT: DISCUSSION LIMITED TO MEETING AGENDA ITEMS — *Nancy J. Wong*, DFO, NIAC, DHS

No public comments were registered.

VII. CLOSING REMARKS

Constance H. Lau, NIAC Chair

William F. Flynn, Assistant Secretary for Infrastructure Protection, DHS

Chris Anderson, Speaking for the 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. Flynn thanked the NIAC for the opportunity to engage them on the voluntary cybersecurity framework and for their continued input on the EO, PPD-21, and NIPP rewrite. He noted that the NIAC's recommendations have mirrored much of what they've been hearing from other sources but come from a unique perspective. Mr. Flynn also emphasized that all parties — whether as part of government, or as private sector owners and operators — have a vested interest in making the policies of the EO and PPD-21 timely and actionable to all stakeholders.

Mr. Natarajan thanked the NIAC for their continued hard work and in-depth analysis. He again noted the NIAC's unique insight and perspective the Council's feedback offers through precise, concise, and actionable recommendations to make tangible changes with clear goals in mind. Mr. Natarajan also noted the struggle to implement outcome-based metrics across all critical infrastructure sectors. He explained that this will be a key initiative moving forward, along with the protection of propriety information by using it for its intended purposes.

Mr. Anderson thanked the NIAC and the EO-PPD Working Group for its presentation and thoughtful recommendations. He commented that the Working Group has given him and his team a lot to consider going forward and that he looks forward to the final report.

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)

September 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

Approval of Minutes

UPDATE AND DISCUSSION ON IMPLEMENTATION PLAN FOR EXECUTIVE ORDER 13636 AND PRESIDENTIAL POLICY DIRECTIVE 21

Kevin Stine
Manager, Security Outreach and Integration Computer Security Division, National Institute of Standards and Technology (NIST)

PRESENTATION AND DISCUSSION ON COUNCIL RECOMMENDATIONS FOR THE 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)

September 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 on the Cybersecurity Framework
- Positive Working Group Member Observations on the Cybersecurity Framework
- Working Group Member Recommendations on Areas For Future Improvement Concerning the Cybersecurity Framework
- Working Group Recommendations for Maximum Adoption of the Cybersecurity Framework
- Appendix

Framing Questions

On the Cybersecurity Framework

Framing Questions

- What necessary elements must be in the Framework in order to facilitate broadest adoption by owners and operators?
- What might be the most efficient and effective processes facilitating adoption, and what can the government do to facilitate?
- What is the best way for the Government to measure usefulness and adoption of the Framework?

Framing Questions Continued

- What are the obstacles preventing adoption, particularly for those organizations outside the Fortune 1000?
- What do you recommend as the target audience(s) and the message to facilitate adoption?
- What issues may exist requiring alignment across Federal agencies, regulatory and non-regulatory, and with other levels of government? What would you recommend addressing these issues?

Positive Observations

From the Working Group on the Cybersecurity Framework

Positive Observations

- Care has been taken throughout the development process to stress that use of the Framework is voluntary.

- The Function, Category and Subcategory hierarchy in the Framework core are very similar to those hierarchies included in Quality Management Systems plans.
  - This allows for flexibility in application.
  - The concept of "tiers" is similar to levels typically seen in IT Industry capability maturity models.

Positive Observations Continued

- There is specific and actionable guidance on how to apply the Framework (Section 2.4), including some practical examples.
- Partnership between government and the private sector is emphasized, not only in the development of the Framework, but in its continued application.
- A risk-based approach is used, acknowledging that there are differences by industry or sector; cyber risk management should be integrated with existing processes, and is not something separate.

Working Group Recommendations

On Areas For Continued Improvement

Working Group Recommendations on Areas For Continued Improvement

- A focus on both process and outcome-based metrics as a means of assessing effectiveness in applying the Framework.
  - See "Metrics for Measuring the Efficacy of Critical Infrastructure Cybersecurity Information Sharing Efforts," by Flemming/Goldstein (2012)

Working Group Recommendations on Areas For Continued Improvement

- More specifics are needed regarding who will have ownership of and responsibility for the continued development of this Framework once released.
  - We agree with the stated goal for this to be in the private sector.
  - We would recommend housing it at a university, with base funding coming from critical infrastructure companies.

- The Framework should include sections on information sharing and benchmarking to ensure that companies establish processes to gather cyber intelligence and to assess cyber programs versus industry trends and practices.

Working Group Recommendations on Areas For Continued Improvement

- Details should be developed about the mechanisms that will be used to improve and develop this model, and to coordinate its application for the purpose of sharing of experiences.

- Additional basis for, and emphasis on, security standards for IT products is required (i.e., "Secure by Design" concept).
  - This is a critical foundational element of the framework. For industrial control systems, the ISA/IEC 62443 series addresses this specifically.

Working Group Recommendations on Areas For Continued Improvement

- Given the focus on lifeline sectors (Energy, Water, Transportation and Telecommunications) and their interdependencies, more emphasis on Process Control Systems and the specific or unique characteristics or constraints is required.
  - (Private sector is continuing to address this through collaboration between ISA, the Automation Federation and the developers of the Framework.)
  - For example, the precedence of Confidentiality over Integrity and Availability that is typical for information systems changes to a preference for Availability and Integrity over Confidentiality for industrial systems design.

Working Group Recommendations

For Maximum Adoption of the Cybersecurity Framework

Critical Purpose: National and Economic Security from Cyber Threats

- This Critical Purpose is clearly outlined by the President in Executive Order 13636 (EO):
  - "Repeated cyber intrusions into critical infrastructure demonstrate the need for improved Cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats."

Key Principles

- Focusing first on securing the lifeline sectors (Energy, Water, Transportation, and Telecommunications) and their interdependencies.

- Engaging participation of the IT Sector in the recognition that improving quality and security of IT products and services are required to protect the cyber backbone of the lifeline sectors.
  - In addition, government agencies and the financial sector and their networks are a foundation to these lifeline sectors, and will need a high-priority focus.

Key Principles Continued

- Using an outcome-based process in identifying significant risks and their mitigations, including response preparedness.

- Sharing of relevant and actionable information between the government, private sector participants and their peers, with adequate protection to ensure the information is used for the Critical Purpose.

Key Principles Continued

- Leveraging and aligning existing standards, management systems and regulations that are demonstrated to work towards achieving the Critical Purpose.

- Pursuing and prosecuting those participating in cyber criminal and espionage acts.

Primary Incentives

- Confidence that the framework will be effective in improving security posture, in a cost-effective manner:
  - There are clear outcome-focused objectives and goals in securing CIKRs
  - There is transparency and focus on the high-priority threats.
  - National Cybersecurity program and framework have clear and effective implementation plans

Primary Incentives Continued

- Information that is shared in addressing cybersecurity is used for security purposes only.
  - These include limited protection for liability, antitrust, and limit to government access for other use when a company acts in good faith.
- Streamline and removal of duplication within existing regulations.
  - Develop a cybersecurity risk framework that leverages or gives credit for the compliance with existing regulations (SoX, HIPAA, CFATS, etc.) and avoids duplication of effort, including elimination of compliance with multiple standards.
- There are clear, outcome-based metrics (see appendix), with commitments to improve these requirements.

Conclusion

- Having national unity of effort to strengthen and maintain a secure, functioning, and resilient infrastructure requires broad participation, collaboration, and trust.
  - The probability of success will be improved by incorporating the key principles and outcome-based deliverables stated above in all aspects of EO 13636 & PPD 21.
- The NIAC working group will re-frame its previous responses in the context of these principles, and will provide future responses in this context as well.
- It is recommended that the President factor these principles into the development of the Cybersecurity Framework.

Appendix

Table ES1. Metrics for Measuring the Performance of Critical–Infrastructure–Centric Cybersecurity Information Sharing

Inputs	Processes	Outputs	Outcomes
Shared information comprises both data and meaning: ▪ % of participating entities reporting that shared information received in a given time period contains both data and meaning ▪ % of submitted information and analytic products (based upon a random sample) that contain both data and meaning **Shared information is relevant:** ▪ % of participating entities reporting that the shared information they receive in a given time period informs decisions that reduce cyber risks to critical infrastructure ▪ % of participating entities reporting that the shared information they receive in a given time period contains new data, new meaning, or both ▪ % of *specific* information submissions or analytic products released in a given time period that inform decisions, and contain new data, new meaning, or both ▪ Number of instances in a given time period that *specific* submissions or products that were not yet known about led to the discovery of a previously unknown cyber incident, once deployed	**The goal is specified:** ▪ % of participating entities reporting that the goal has been developed, issued, and disseminated by a coordinating body **The goal is agreed upon:** ▪ % of participating entities providing express or implied concurrence with goal **Participating entities are appropriate:** ▪ % of participating entities who meet specified criteria ▪ % of participating entities who report that they can generate, analyze, or use information to achieve the goal **Entities are participating:** ▪ % of entities logging on to the information sharing website at least once in a given time period ▪ % of entities sending information to the website at least once in a given time period ▪ % of entities receiving information from the website at least once in a given time period ▪ % of entities participating in scheduled collaborative exchanges in a given time period ▪ % of entities with at least one person on the NCCIC floor at least once in a given time period ▪ % of entities who report independent collaboration with other entities in a given time period ▪ % of entities responding to RFIs in a given time period	**Information is used for tactical and strategic purposes:** ▪ % of participating entities reporting use of shared information to improve or implement security controls in a given time period (tactical use) ▪ % of participating entities reporting use of shared information to inform resource allocation decisions in a given time period (strategic use) ▪ % of received (i.e., accessed) information used to improve or implement security controls in a given time period (tactical use) ▪ % of received (i.e., accessed) information used to inform resource allocation decisions (strategic use)	**Goal is achieved** (all in a given time period): ▪ Number of incidents causing unavailability of critical services and estimated associated costs of damage ▪ Number of incidents causing the loss of critical data and estimated costs of damage ▪ Number of detected incidents, both prevented and successful, and estimated costs of damage ▪ Unplanned downtime ▪ Mean time to incident detection ▪ Mean time to incident remediation ▪ Mean time to incident recovery ▪ Mean time between failures

Working Group Members

WG 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, *Senior Advisor, Center for Strategic and International Studies (CSIS), Director, Nuclear Energy Program*	Electricity, Nuclear
Constance H. Lau, *President and CEO, Hawaiian Electric Industries, Inc.*	Electricity

Public Comment

Nancy Wong
Designated Federal Officer, NIAC

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

Constance Lau
NIAC Chair

Closing Remarks

Adjournment

Constance Lau
NIAC Chair