Information Technology
Industry Council

August 19, 2013

Bob Kolasky
Director, Integrated Task Force, Cyber Executive Order and PPD 21 Implementation
Senior Advisor to the Assistant Secretary Office of Infrastructure Protection
Department of Homeland Security

RE: Comments on the Draft Revised National Infrastructure Protection Plan (NIPP)

Dear Mr. Kolasky:

The Information Technology Industry Council (ITI) appreciates the opportunity to comment on the revised draft National Infrastructure Protection Plan (NIPP), released August 12.

ITI is the premier voice, advocate, and thought leader in the United States for the information and communications technology (ICT) industry. ITI's members[1] comprise the world's leading technology companies, with headquarters worldwide. Cybersecurity is rightly a priority for all governments. We share the goal with governments of improving cybersecurity and therefore our interests are fundamentally aligned. As both producers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy. In the United States, ITI is a member of the IT Sector Coordinating Council (SCC), and many of our companies are members of the IT and/or Communications Sector Coordinating Councils. Through the SCCs and other bodies and avenues we take seriously our responsibility in the public-private partnership to improve cybersecurity.

ITI supports the review and revision of the NIPP to ensure that it remains relevant to the critical infrastructure (CI) mission over time. However, while we appreciate that the Department is working within the deadline established in PPD-21, we are very concerned that the short time frame (one week) for stakeholder review and comment on this draft does not afford adequate opportunity for us or other stakeholders to provide the substantive, thoughtful feedback required. Thus, while we provide preliminary comments in this letter and the attached comment form, we also respectfully suggest that the Department request an extension for the update of the NIPP beyond the October 8, 2013 deadline. An extension is key to allow for greater collaboration and deliberation in the update process. In fact, we understand that the IT SCC has alerted DHS that, due to the compressed time frame, the IT SCC will not be commenting during this review cycle on the update to the NIPP. As an IT SCC member, ITI supports its concerns and decision.

General Substantive Comments: Below are our comments on the document's major substantive issues.

- ***Contradictory definitions of critical infrastructure (CI).*** The document contains confusing/contradictory definitions of CI. All references must be consistent with each other and with current law/policies. See ITI's red flag/critical comments #s 1, 2, and 3.
- ***Information sharing.*** The document refers to mandatory information-sharing, including of vulnerabilities. The former contradicts the current voluntary approach preferred by

[1] See attached ITI member list.

industry and the latter contradicts best practices. In addition, the document should explore in greater detail the current perceived barriers (legal and otherwise) to greater voluntary multidirectional information sharing and what role, if any, the NIPP has in identifying and overcoming them. There needs to be greater clarity in the document as to those information sharing mechanisms and channels to be used. See ITI's red flag/critical comments #s 4 and 5 and substantive comments #11.

- ***References to design and supply chain regarding ICT systems and products.*** There are numerous references to the roles sector-specific agencies (SSAs) and local and municipal governments should play in ensuring that security and resilience are designed into CI. There also are statements that the NIPP is responsible for supply chain security. At the same time, there is no acknowledgement of what the ICT industry is doing to address these concerns and how the NIPP can or should support industry efforts. See ITI's red flag comments #s 6 and 7.
- ***References to Cybersecurity Framework.*** The document contains many cross-references to the NIST Cybersecurity Framework that does not yet exist. We suggest removal of these references. See ITI's red flag comments # 8.
- ***References to outcomes and measurements.*** Numerous references are seemingly tied to regulations. While we agree that outcomes and measurements are important, the emphasis on them lends the document a regulatory tone. Further, industry's role in the creation of these metrics is not clear. See ITI's red flag comments # 9.
- ***Lack of articulation of roles of state and local governments.*** The document emphasizes these entities' participation in the CI risk equation without clearly describing their roles and responsibilities. See ITI's red flag comments # 10.
- ***Contradictory risk assessment approaches.*** The document outlines two different risk management programs that are based on different methodologies. See ITI's substantive comment #12.

Detailed Comments: See attached matrix.

ITI would like to thank DHS for its industry outreach regarding revision of the NIPP. We hope that our input is helpful and will receive due consideration. We are available at any time to elaborate on our comments and suggestions. ITI and its members look forward to continuing to work with DHS and the Administration generally to improve America's cybersecurity posture. Please continue to consider ITI a resource on cybersecurity issues moving forward and contact me with any questions at dkriz@itic.org or 202-626-5731.

Sincerely,

Danielle Kriz
Director, Global Cybersecurity Policy

CC: J. Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator

Attachments: ITI comment matrix and list of ITI member companies

Document Clearance Comment Form

Title or Description of Document: Comments on Draft NIPP Rewrite	**For Internal DHS Use: Lead Action Officer Name and Component:**
Comments provided by: Information Technology Industry Council (ITI)	**Date: August 19, 2013**

INSTRUCTIONS: The reference column is where you will type the document line numbers you are commenting on.
The Comment columns are where you will type your comment.

#		
#	**Reference**	**RED FLAG / CRITICAL COMMENTS**
1.	833, 855, 861, 864, 949, 1143, 1150, 1170, 1175, 1188, 1358, 1443	The draft repeatedly identifies “assets, systems, and networks” as critical infrastructure that should be reviewed and secured. This is inconsistent with the definition used in the Homeland Security Act and the Executive Order, neither of which specifically discuss “networks.”
2.	62-64; 347-354; 860-864; 1187-1188	The NIPP redraft confuses the definition of “Critical infrastructure” (CI) and creates significant ambiguity by: stating the communications and energy sectors are “uniquely critical”; stating that the statutory CI definition is “not the last word,” and suggesting that State, tribal, territorial, local and community level entities should designate CI; and referring to “nationally critical” assets. Perhaps more importantly, there is no discussion of the heightened CI category of “Critical Infrastructure at Greatest Risk” as envisioned in President Obama’s Cybersecurity Executive Order, EO 13636 (EO), or the significant activities of the CDIIWG to identify such critical assets and systems. Taken together, these varying definitions and the absence of any discussion of “at greatest risk” CI creates a great deal of confusion and uncertainty for all CI sectors and participating entities regarding important questions regarding the scope of CI.
3.	41, 74	At the same time, the NIPP references “cyber critical infrastructure”, which the document states is derived from EO 13636 and PPD-21. However, this term does not exist in either document
4.	89-92; 1106-1108; 1587-1592, etc.	The NIPP redraft has numerous references to information sharing, and particularly to the importance of achieving “situational awareness,” and providing “near-real-time (24/7)” threat and incident reporting, etc. While there is some acknowledgment of the various legal and other “barriers to multi-directional sharing” (including liability considerations, classified/sensitive information, use of vulnerability info by regulators, and laws and policies that restrict information dissemination) that might need to be “removed or minimized” to attain the NIPP’s situational awareness and other information sharing goals, there is almost zero effort in the NIPP to substantively identify those barriers, nor any discussion in the NIPP of a plan to remove or minimize such barriers, nor any discussion of what role if any the NIPP should play, vis-à-vis other stakeholders, in identifying, removing, or overcoming such perceived barriers.
5.	1174-1179, etc.	The NIPP redraft contains references to mandatory information sharing, such as the comment ‘*“To establish this situational awareness, those who obtain information relevant to critical infrastructure threats, vulnerabilities, consequences, and the operating environment* ***must*** *share information with the decision-makers across the partnership.*” References such as this contradict the existing voluntary sharing model supported by industry. Such references to

Document Clearance Comment Form	
Title or Description of Document: Comments on Draft NIPP Rewrite	**For Internal DHS Use: Lead Action Officer Name and Component:**
Comments provided by: Information Technology Industry Council (ITI)	**Date: August 19, 2013**

INSTRUCTIONS: The reference column is where you will type the document line numbers you are commenting on.
The Comment columns are where you will type your comment.

#		
		mandatory sharing are particularly troubling in the context of the contemplated sharing of vulnerabilities as articulated in the NIPP redraft, and do not align with current industry best practice related to vulnerability disclosure.
6.	206-208; 817-820; 937-1052	There are several references in the NIPP redraft to the roles SSAs should play in ensuring that CI has security and resilience designed in and that supply chains are in scope of concern/responsibility for the NIPP. While security by design and supply chain security are certainly important concepts, there is no acknowledgment in the redraft of what the IT industry is currently doing in these areas, and very little indication that industry input has even been solicited on how best to approach these complex subjects. Rather, the redraft contains conclusory comments such as - '*Often, however, security and resilience considerations are not factored into the decision-making process, particularly when the infrastructure is being designed, constructed, and updated'* (940-942) suggesting that industry is not proactively addressing security risk in the design of products and services. This broad and overly simplistic statement is misleading at best, and provides a clear indication of why industry input should have been solicited much earlier in the drafting process. Additionally, statements such as - '*The role of the critical infrastructure partnership at the national level is to build the conditions through which security and resilience considerations can influence decisions during the "design" phase, and to help promote the business case for such investment*" carve out a role for the NIPP which seems questionable and unprecedented - is the proper role of the NIPP to intersect/influence ICT system design decisions, and to help provide the business case justification for such decisions?
7.	242-243; 870-876; 952-963; 1019-1028	There are multiple references in the NIPP redraft encouraging federal, local, and municipal government entities to develop or strengthen laws, regulations and rules to address the design, construction and updating of critical infrastructure systems for security, including ICT system design, and to promote increased investment in security. We do not believe it is prudent to involve regulatory entities at any level in ICT system design or business investment decisions.
8.	66-72; 732-733; 1010-1014; 1727-1732	The NIPP redraft contains multiple references to the Cybersecurity Framework being developed by NIST pursuant to the EO. While we are supporting NIST's efforts to develop a Framework of cybersecurity standards and best practices, we do not support codifying a Framework that doesn't yet exist in laws, regulations, or policy documents such as the NIPP. We believe it is premature for the NIPP redraft to reference the Cybersecurity Framework.
9.	234-249; 695-701; 780-782; 1641-1651; 1686-1744, etc.	The draft NIPP focuses on outcomes and measurement throughout the document. While agreeing with the notion of outcomes and measurements to performance, the emphasis on measurements lends an overall regulatory tone to the document. While there are numerous references to the role of SSAs in creating measurements and reporting performance to these measurements, the redraft leaves unclear industry's role in the creation of metrics, and the extent to which new regulatory activities will be used to manage to these metrics. There are references to SSAs gaining 'firsthand knowledge' about CI-related risk (e.g., 248),

Document Clearance Comment Form

Title or Description of Document: Comments on Draft NIPP Rewrite	**For Internal DHS Use: Lead Action Officer Name and Component:**
Comments provided by: Information Technology Industry Council (ITI)	**Date: August 19, 2013**

```
INSTRUCTIONS:  The reference column is where you will type the document line
               numbers you are commenting on.
               The Comment columns are where you will type your comment.
```

#		
		implying an undefined audit or oversight role for SSAs. Overall, the regulatory tone of the draft creates an unnecessarily adversarial relationship in what is intended to be a partnership. In addition, the document mandates the creation of multi-year national priorities for the NIPP established annually, and that the SSAs will monitor and report progress to those national priorities. The role of industry in that process, as well as the industry burden to support the monitoring and reporting associated with such process, is left unclear by the redraft.
10	308-312; 355-373; 455-461; 878-883; 885-888; 908-914; 1022-1024; 1113-1115; 1207-1209	Throughout the document there is an emphasis on the importance of State and Local participation in the CI risk equation. We agree that State and Local Authorities and Responders play an important role in the overall protection of CI - however the document does not clearly articulate the roles and responsibilities and relationships between National, State and Local governments, and Industry Owners and Operators in the Partnership Model. Without defining clear lines of engagement and an overarching prioritization process, it will be difficult for the various stakeholders to understand how to engage, when to engage and where to apply resources to meet priorities. The lack of clarity on this point in the NIPP redraft could lead to a proliferation and balkanization of CI related activities across state, regional and national environments.
#	**Reference**	**SUBSTANTIVE COMMENTS**
11	Passim	Despite multiple references in the NIPP redraft to improving information sharing, the document leaves it unclear what specific information sharing mechanisms are to be used to effectuate its information sharing goals. The NIPP should clarify information sharing channels and reinforce existing sharing constructs (such as the ISACs) explicitly in the document to ensure clarity in the partnership model for critical information sharing capabilities. Such clarity should reinforce existing sharing channels while not impacting the flexible nature of the NIPP to enable new sharing mechanisms as they emerge.
12	792-935	There are several questions/concerns regarding the risk management approach outlined in the NIPP redraft. The document outlines two risk management programs – the Strategic National Risk Assessment (SNRA) and Threat and Hazard Identification and Risk Assessment (THIRA). As described, the SNRA process appears to be an asset-based risk assessment methodology. This does not reflect current best practices supporting function-based assessments, such as described in DHS's own CARMA methodology, and used in the IT Sector Risk Assessment produced by the IT-SCC/GCC partnership as directed by the NIPP. Regarding the overall assessment system, and how it is implemented, distributed and used, it remains unclear and raises several important questions: • How does the SNRA process align with the recent work done by the Critical Infrastructure Identification Work Group (CDIIWG) and, as mentioned above, the CARMA Methodology? • Is the SNRA intended to be a national assessment or a sectorial one? In either case, how are sectorial assessments incorporated into a

Document Clearance Comment Form	
Title or Description of Document: Comments on Draft NIPP Rewrite	**For Internal DHS Use: Lead Action Officer Name and Component:**
Comments provided by: Information Technology Industry Council (ITI)	**Date: August 19, 2013**

INSTRUCTIONS: The reference column is where you will type the document line numbers you are commenting on.
The Comment columns are where you will type your comment.

#		
		proportionally weighted national assessment? • Who owns and conducts the THIRA assessments, and how do they inform the SNRA? Are they conducted with the same process as the SNRA? Are they conducted in conjunction with the appropriate SSA? • How will the SNRA leverage the multitude of assessments already being conducted by SLTT entities as part of their normal operation?
13		The draft NIPP does not include any mention of the NCIPP or nomination guidance for critical infrastructure. The plan should include some language on sharing of the nomination lists with the sector coordinating councils, during the annual approval process.
14		The draft NIPP fails to include any aggregate reporting of cyber incidents that are triaged and resolved by the information sharing (HITRAC, US-CERT etc.) and fusion centers. Aggregate statistics of threats should be published at the sector level on a quarterly basis as an interactive public map (e.g. National Broadband Map) and a machine-readable data set, in compliance with the administration's Open Data Policy.

Innovation.
Insight.
Influence.

ITI member companies

accenture

Adobe

Agilent Technologies

Alcatel·Lucent

ALTERA

AMD

Aol.

Apple Inc.

APPLIED MATERIALS

Autodesk

BlackBerry

BROADCOM

Canon

ca technologies

Cognizant

CORNING

DELL

ebay

EMC²

EPSON

ERICSSON

facebook

FUJITSU

Google

hp

htc

IBM

intel

intuit

Kodak

lenovo

LEXMARK

Micron

Microsoft

monster

MOTOROLA SOLUTIONS

NCR

NOKIA

ORACLE

Panasonic

QUALCOMM

RICOH

SAMSUNG

SAP

Schneider Electric

SONY

Symantec.

SYNOPSYS

TERADATA
Raising Intelligence

Texas Instruments

VERISIGN

vmware