Strategy & Policy, Infrastructure Protection
National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528

Joint National Priorities (JNP) Refresh Questionnaire

This questionnaire is designed to gather insights into the current usage of the Priorities and how they can and should be used going forward. Your inputs will be used to help structure the first session around commonly identified themes and are not intended to be representative of the comprehensive opinions of the partnership regarding potential updates. Thank you in advance for your completion and return of the questionnaire by **Friday, August 25th**.

Utility of JNP

Did your organization use the JNP as a guiding principle, as an impetus for change or collaboration, a combination of the above, or were the JNP not specific or measurable enough to be useful?	Any additional details you would like to add regarding the utility of the JNP.
Combination	***CSCC Response: The Comm Sector reviews all major priority and threat assessments in the development of its' work plan in major CSCC Venues (NSTAC, CSCC, Comm-ISAC) to ensure issues are being addressed and are in alignment with NS/EP needs. In that respect the JNP (as well as other USG documents) acts as guiding principles as well as ongoing impetus for collaboration.***

Review of JNP

Joint National Priority	Description	Keep, Modify, Discard	Recommended Changes
Strengthen the Management of Cyber and Physical Risks to Critical Infrastructure	Strengthening risk management of cyber and physical threats and hazards is a national priority, as articulated in PPD-21 and Executive Order (EO) 13636. NIPP 2013 promotes an integrated, holistic approach to address the increasing reliance of critical infrastructure assets on information and communications technology (ICT) systems and networks. Critical infrastructure partners should use the Framework for Improving Critical Infrastructure Cybersecurity (www.nist.gov/cyberframework) within their organizations and promote its use across sectors and stakeholders. In addition, the critical infrastructure community should explore technological, behavioral, and organizational solutions for managing cyber and physical risks to critical infrastructure.	Keep	
Build Capabilities and Coordination for Enhanced Incident Response and Recovery	The critical infrastructure community should share timely and relevant information during and following incidents to support the rapid restoration of lifeline functions. Critical infrastructure partners should prepare and maintain integrated cyber response and recovery plans to help their organizations manage cyber incidents efficiently and effectively. The critical infrastructure community should improve the tracking and implementation of corrective actions identified through incidents and exercises to inform future planning and response efforts.	Keep	
Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines	Public-private partnerships are the primary mechanism for coordinating and integrating individual partner efforts to manage critical infrastructure risk and share information. A particular priority in the future is to leverage existing national and international partnerships and expand a network of regional and State, local, tribal, and territorial coalitions to strengthen national capacity.	Modify	*The "particular priority in the future" appears to focus solely on expanding the Public participants in the Public-Private partnership. This does not necessarily achieve the goal of strengthening collaboration across sectors, jurisdictions and disciplines. We have seen that other sectors remain ill-informed of the best ways to collaborate with the Communications Sector and the NCC. Perhaps the focus for the next iteration here is to identify improvements in Cross Sector sharing.*
Enhance Effectiveness in Resilience Decision-Making	There is broad recognition across the critical infrastructure community of the need to strengthen infrastructure resilience — particularly for infrastructure providing lifeline functions — to increase its ability to withstand and rapidly recover from all hazards under evolving conditions. Effective planning requires evaluation of long-term trends affecting infrastructure risk, such as climate change and increasing reliance on information and communications technology systems. Critical infrastructure partners should consider resilience at each stage of the supply chain and infrastructure lifecycle, including research and development, design, investment, construction, operation, maintenance, repair, and disposal, destruction, or decommissioning. This includes identifying and exploring innovative financing mechanisms to encourage investments that enhance all-hazard resilience.	Modify	*There was substantive effort within the Sector (2015-2016) to work with NIST in the development and release of their Community Resilience Framework. However, there was a presumption of grant money (financing mechanisms) being made available to Communities that has not materialized. In the absence of funding it's not clear significant resources will be applied moving forward. In the absence of funding (or some other instigator) to support Communities undertaking this resilience planning, it is not clear that these efforts will remain a priority for the Comms Sector.*
Share Information To Improve Prevention, Protection, Mitigation, Response, and Recovery Activities	Sharing timely, relevant information and intelligence promotes awareness of threats and hazards, enabling the implementation of measures to mitigate risk. Collaborative efforts in government and industry focus on determining priorities for analysis in the context of the critical infrastructure operating environment, establishing and using reliable and appropriate means of dissemination across and within sectors, and providing feedback for continuous improvement. The overall goal of these efforts is an information-sharing culture based on the "need to share" and "responsibility to provide."	Modify	*Two unresolved issues that impact information sharing are: 1) classification of information, and 2)fear of retribution for sharing information in the absence of legal testing. With respect to 1: The classification issue remains as a constant barrier when known threats are NOT shared with CI/KR due to the level of classification. Ironically, the vast majority of actionable information is not subject to classification in and of itself. The time to de-classify remains long, and this situation is further exacerbated by the amount of time it takes for USG to process clearances for Industry. As a consequence, Comms believes that many critical infrastructure owner/operators remain vulnerable to known threats. With respect to 2: While CISA provides protections, and Comms is leveraging these protections, the language is focused on "Enterprise" information sharing and does not directly address an entity such as an ISP that has higher level situational awareness. Further CISA has not been fully tested in the courts. These concerns are exacerbated when certain USG entities continue to demonstrate a willingness to search for any failings that led to a security breach, and then to prosecute those that suffered the loss.*

Are there any strategic threats not accounted for in the JNP?

Yes or No	If yes, please describe the threat(s)
Yes	***USG Mitigation Strategies to address EMP and GPS Vulnerabilities have not been developed. These are long-standing, known vulnerabilities. Further, Vulnerabilities associated with Under Sea Cable assets are also known. A number of joint analyses to prepare for under-sea mitigation support have been recommended by Industry, but to date, no action has been taken.***

Additional Suggested JNP (if any)

Joint Priority	Description

Any Other Suggested Improvements or Modifications Regarding JNP

Your Role (Optional)

Open Response:

Please return questionnaire to CIPAC@HQ.DHS.GOV.