9110-9P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2013-0024]

Review and Revision of the National Infrastructure Protection Plan

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: Notice and request for comments.

SUMMARY: This notice informs the public that the Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection (IP) is currently reviewing the National Infrastructure Protection Plan (NIPP) to conform to the requirements of Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, and, as part of a comprehensive national review process, solicits public comment on issues or language in the NIPP that need to be updated.

DATES: Written comments are encouraged and will be accepted until [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Written comments and questions about the NIPP should be forwarded to Lisa Barr, DHS/NPPD/IP/Office of Strategy and Policy, 245 Murray Lane, SW, Mail Stop 8530, Arlington, VA 20598-8530. Written comments should reach the contact person listed no later than [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. Comments must be identified by "DHS-2013-0024" and may be submitted by one of the following methods:

- **Federal eRulemaking Portal:** http://www.regulations.gov.

- **E-mail:** EO-PPDTaskForce@hq.dhs.gov. Include the docket number in the subject line of the message.

Instructions: All submissions received must include the words "Department of Homeland Security" and the docket number for this action. All comments received (via any of the identified methods) will be posted without change to http://www.regulations.gov, including any personal information provided. You may submit your comments and material by one of the methods specified in the **ADDRESSES** section. Please submit your comments and material by only one means to avoid the adjudication of duplicate submissions. If you submit comments by mail, your submission should be an unbound document and no larger than 8.5 by 11 inches to enable copying and electronic document management. If you want DHS to acknowledge receipt of comments by mail, include with your comments a self-addressed, stamped postcard that includes the docket number for this action. We will date your postcard and return it to you via regular mail. For purposes of review, the 2009 NIPP can be found at http://www.dhs.gov/nipp.

Docket: Background documents and comments can be viewed at http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Lisa Barr, DHS/NPPD/IP/Office of Strategy and Policy; 245 Murray Lane, SW, Mail Stop 8530, Washington, DC 20528-8530 or 703-235-9542.

SUPPLEMENTARY INFORMATION:

I. Public Participation

The Department of Homeland Security (DHS) invites interested persons to contribute suggestions and comments for the rewrite of the National Infrastructure Protection Plan (NIPP) by submitting written data, views, or ideas. Comments that will provide the most assistance to DHS in updating the NIPP will explain the reason for any recommended changes to the NIPP and include data, information, or authority that supports such recommended change. Linking changes to specific sections of the NIPP would also be helpful. There will be an opportunity to review a revised document reflecting the various changes sometime this summer.

II. Background

On February 12, 2013, President Obama signed Presidential Policy Directive 21[1] (PPD-21), *Critical Infrastructure Security and Resilience*, which builds on the extensive work done to date to protect and enhance the resilience of the Nation's critical infrastructure. This directive aims to clarify roles and responsibilities across the Federal Government and establish a more effective partnership with owners and operators and state, local, tribal, and territorial entities to enhance the security and resilience of critical infrastructure.

[1] PPD-21 can be found at: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

President Obama also signed Executive Order (EO) 13636[2] on February 12, 2013, entitled *Improving Critical Infrastructure Cybersecurity*. By issuing the EO and PPD together, the Administration is taking an integrated approach to strengthening the security and resilience of critical infrastructure against all hazards, through an updated and overarching national framework that acknowledges the increased role of cybersecurity in securing physical assets.

PPD-21 sets forth several actions that the Secretary of Homeland Security shall take to implement the directive. One of these is to develop a successor to the NIPP to address the implementation of PPD-21; the requirements of Title II of the Homeland Security Act of 2002, as amended; and alignment with the National Preparedness Goal and System required by Presidential Policy Directive 8 (PPD-8).

The 2009 NIPP set forth a comprehensive risk management framework and defined roles and responsibilities for DHS; the Sector-Specific Agencies (SSAs); other Federal departments and agencies; state, local, tribal, and territorial governments; critical infrastructure owners and operators; and other stakeholders in industry, academia, and non-governmental organizations. The NIPP provides a coordinated approach for establishing national priorities, goals, and requirements so that resources can be applied in the most effective manner. The NIPP risk management framework responds to an evolving risk landscape; as such, there will always be changes to the NIPP—from relatively minor to more significant—to ensure it remains relevant to the critical infrastructure mission over time.

III. Initial List of Issues To Be Updated in the NIPP

[2] EO 13636 can be found at: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

PPD-21 specifies the following elements that shall be included in the successor to the NIPP:

- Identification of a risk management framework to be used to strengthen the security and resilience of critical infrastructure;
- Protocols to synchronize communication and actions within the Federal Government; and
- A metrics process to be used to measure the Nation's ability to manage and reduce risks to critical infrastructure.

Some other actions required of the Secretary for Homeland Security under PPD-21 also must be addressed in the successor to the NIPP, including a description of functional relationships within DHS and across the Federal Government related to critical infrastructure security and resilience; and any changes to the sector partnership resulting from the evaluation of the existing public-private partnership model. Finally, the plan must consider sector dependencies on energy and communications systems, and identify pre-event and mitigation measures or alternate capabilities during disruptions to those systems.

The NIPP review will be coordinated with a broad range of critical infrastructure partners and other stakeholders. This notice extends an invitation to the public to provide feedback on the 2009 NIPP and those changes that should or should not be made. To assist the reviewer, DHS has conducted a review of expected changes to the NIPP and an initial list of potential changes is included in this notice. The purpose of this notice is to request public comment on additional changes that would help fulfill the mandate of

PPD-21 to make the successor to the NIPP more relevant and useful in strengthening the security and resilience of the Nation's critical physical and cyber infrastructure.

Some of the known changes that will be addressed in the successor to the NIPP are:

- Changes to the sectors and designated SSAs;
- Changes in terminology based on recent directives;
- Alignment with PPD-8 on National Preparedness;
- Updates to information-sharing tools and mechanisms;
- Critical infrastructure security and resilience regulatory programs;
- Updates on measurement and reporting and risk-informed resource allocation;
- Review and update cycles for the NIPP and Sector-Specific Plans (SSPs);
- Closer integration of physical and cybersecurity, including increased coordination of research and development efforts;
- Review of the risk management approach;
- Sector dependencies on energy and communications systems;
- Increased regional emphasis of critical infrastructure security and resilience; and
- Other issues, such as aging infrastructure and climate change adaptation.

These changes are discussed further below.

IV. Discussion of Issues To Be Addressed in the Successor to the NIPP

Implementing PPD-21 will require DHS to address a number of specific issues in reviewing and updating the NIPP. However, since the NIPP was last issued in 2009, critical infrastructure programs across the Nation have matured and produced lessons learned and best practices from day-to-day operations, exercises, and actual incidents that

should be incorporated in any successor to the plan. The new document must incorporate developments including new laws, EOs, Presidential directives, and regulations, and procedural changes to critical infrastructure security and resilience activities based on real-world events and emerging risks.

Some of the known changes that will be addressed in this review of the NIPP are described below. DHS welcomes comments and ideas on areas that should be updated, expanded, changed, added, or deleted as appropriate.

Changes to the Sectors and SSAs

PPD-21 reduces the number of sectors from 18 to 16 by designating two previously existing sectors as new subsectors. National Monuments and Icons is now a subsector of the Government Facilities Sector and Postal and Shipping is a subsector of the Transportation Systems Sector. In addition, the PPD changed the names of two sectors to better reflect their scope:

- The Banking and Finance Sector is now the Financial Services Sector; and
- The Water Sector is now the Water and Wastewater Systems Sector.

Finally, PPD-21 designates new co-SSAs for two sectors, as follows: the General Services Administration joins DHS as a co-SSA of the Government Facilities Sector and the U.S. Department of Transportation joins DHS as a co-SSA for the Transportation Systems Sector.

Changes in Terminology and Alignment with Presidential Policy Directive 8, National Preparedness

PPD-21 changes the lexicon by using critical infrastructure security and resilience in place of critical infrastructure protection. The new terminology is consistent with the

national preparedness construct established by PPD-8. The five mission areas under PPD-8—prevention, protection, mitigation, response, and recovery—link to the two major outcomes that preparedness seeks to achieve: security, which closely aligns with prevention and protection; and resilience, which more closely aligns with mitigation, response, and recovery. There is overlap among all of the PPD-8 mission areas and between those mission areas and the concepts of security and resilience. The new terminology supports the move toward a more comprehensive approach to overall national preparedness, of which critical infrastructure security and resilience are major components. The use of the term "security" in this context applies to all hazards and not simply threats from terrorism.

Updates to Information-Sharing Tools and Mechanisms

PPD-21 sets forth the following strategic imperative: "A secure, functioning, and resilient critical infrastructure requires the efficient exchange of information, including intelligence, between all levels of government and critical infrastructure owners and operators." To that end, several of the actions required of DHS in the PPD are designed to improve and streamline information sharing between the Federal Government and critical infrastructure partners and stakeholders. DHS requests comments and input on ways that the current NIPP information-sharing approach and mechanisms could be changed and improved.

Critical Infrastructure Security and Resilience Regulatory Programs

Through existing regulations, the Federal Government can mandate security-related activities and protocols, as appropriate and authorized by Congress, to better ensure that a baseline level of security is being maintained at various types of critical infrastructure

facilities. An example of currently existing regulatory regimes that enhance critical infrastructure security and resilience include regulations pursuant to the U.S. Coast Guard's Maritime Transportation Security Act (MTSA), 33 CFR Parts 101-107, which requires certain critical infrastructure located adjacent to a U.S. port or waterway to conduct facility security assessments and develop and implement facility security plans. DHS is not proposing new regulatory authority through this notice, but is requesting input on ways to better integrate existing regulatory programs into the NIPP framework.

Updates on Measurement and Reporting Processes and Risk-Informed Resource Allocation

DHS has been working to improve metrics and reporting processes to assess national critical infrastructure security and resilience efforts and identify opportunities for improvement. Over the last year, DHS and the SSAs have worked to streamline data collection processes, and identify links between the National Preparedness Goal core capabilities and the national critical infrastructure protection outcomes. The successor to the NIPP will reflect the maturation of metrics processes, and efforts to use those metrics to inform resource allocation decisions.

Review and Update Cycles for the NIPP and SSPs

The revision cycle for the SSPs follows the NIPP revision cycle by one year, to ensure that the concepts and strategic direction provided in the NIPP are captured in the next edition of the SSPs. In 2010, government and private sector partners agreed that a four-year review cycle was sufficient to keep the NIPP and SSPs current and would provide better alignment with the Quadrennial Homeland Security Review. This change

took effect in July 2011, placing the next review and rewrite of the NIPP in 2013 and the next reissue of the SSPs in 2014.

Following development of the successor to the NIPP in late 2013, DHS will issue guidance to the SSAs for revising the SSPs. This guidance will cover the major updates and changes to the NIPP to address implementation of PPD-21 so the sectors can incorporate these updates into the SSPs as appropriate.

Closer Integration of Physical and Cyber Security

DHS leads an Interagency Task Force charged with accomplishing the integrated implementation of PPD-21 and EO 13636. The task force includes representatives from DHS, the SSAs, and other Federal departments and agencies with a role in critical infrastructure security and resilience and/or cybersecurity. The task force established various working groups to address the deliverables required for implementation of the EO and PPD. Many of these deliverables will influence and be reflected in the successor to the NIPP and the document will address physical and cybersecurity in a more integrated and holistic manner.

A key part of this approach includes greater integration and coordination of research and development efforts for physical and cybersecurity and strategic planning to support the development and use of incentives to facilitate this integration. DHS requests comments on the timeframe and requirements for research, development, and incentives for increased cyber-physical integration and how the successor to the NIPP can integrate the concepts and implementation of physical and cybersecurity.

Review of the Risk Management Approach

The NIPP's risk management framework establishes an approach for setting goals; identifying infrastructure; combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk; developing security measures and resilience strategies; and measuring effectiveness.

It is designed to respond to an ever-changing risk environment and, as such, it provides an adaptable framework to address evolving and emerging risks to critical infrastructure. DHS is not seeking to make significant changes to the basic structure and concept of the risk management framework but rather to review how PPD-21 and other recent directives and events will influence the context and application of the risk management framework going forward.

Sector Dependencies on Energy and Communications Systems

PPD-21 acknowledges the dependency of all critical infrastructure sectors on energy and communications systems and functions and requires that these dependencies be specifically considered in reviewing the NIPP. The updated document will consider pre-event and mitigation measures or alternate capabilities that communities and critical infrastructure owners and operators may bring to bear during disruptions to those systems and functions. This aligns with implementation of the National Preparedness Goal under PPD-8.

Increased Regional Emphasis

As DHS has sought to improve the efficacy of the delivery of critical infrastructure protection and resilience support and assistance to state, local, tribal, territorial, and private sector partners, it has moved toward a more decentralized regional model that leverages field-based employees. The regional model synchronizes with DHS's effort to

provide more tailored support to specific geographic regions to more closely address their unique challenges, such as region-specific hazards (e.g., earthquakes, hurricanes), and operating environments.

Other Issues – Aging Infrastructure and Climate Change Adaptation

The areas of aging infrastructure and climate change are appreciated as risks of concern to critical infrastructure security and resilience. As a result, these issues will be considered as part of the all-hazards approach in reviewing and rewriting the NIPP.

Dated: May 31, 2013.

Robert Kolasky,

Director for Strategy and Policy,

Office of Infrastructure Protection,

National Protection and Programs Directorate,

Department of Homeland Security.

[FR Doc. 2013-13427 Filed 06/05/2013 at 8:45 am; Publication Date: 06/06/2013]