9110-9P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2013-0074]

Review and Revision of the National Critical Infrastructure Security and Resilience (NCISR) Research and Development (R&D) Plan Outline and Specific Questions Regarding the Content

AGENCY: National Protection and Programs Directorate, Department of Homeland Security (DHS).

ACTION: Notice and request for comments and answers to specific questions.

SUMMARY: This Request for Information (RFI) notice informs the public that the Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) is currently developing a National Critical Infrastructure Security and Resilience Research and Development Plan (NCISR R&D Plan) to conform to the requirements of Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience.* As part of a comprehensive national review process, DHS solicits public comment on issues or language in the NCISR R&D Plan that need to be included. Critical infrastructure includes both cyber and physical components, systems, and networks for the sixteen established "critical infrastructures".

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 NCISR R&D Plan should be forwarded to Kristin Wyckoff, DHS/S&T/RSD, 445 Murray Lane, SW, Mail Stop 0208, Washington, DC 20528-0208. 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-2013-0074" and may be submitted by one of the following methods:

- **Federal eRulemaking Portal:** http://www.regulations.gov.
- **E-mail:** R&DWG@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 "FOR FURTHER INFORMATION CONTACT" 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. Please limit submissions to a maximum of 10 pages of text if possible. 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.

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

FOR FURTHER INFORMATION CONTACT: Kristin Wyckoff, DHS/S&T/RSD, 445 Murray Lane, SW, Mail Stop 0208, Washington, DC 20528-0208.

SUPPLEMENTARY INFORMATION:

I. Public Participation

The Department of Homeland Security (DHS) invites interested persons to contribute highly relevant content for consideration in the development the National Critical Infrastructure Security and Resilience Research and Development (NCISR R&D) Plan. Content can include, but is not limited to, published information and data, technical views, and/or ideas on research and development priorities, unsatisfied requirements or unmet capabilities, and/or current and long-term issues for critical infrastructure. Input is welcome from stakeholder groups, private and public entities, and individuals on content to be included to best fulfill the intended purpose of the plan. Comments that will provide the most assistance to DHS in writing the NCISR R&D Plan will include the reason for the recommended information or topic along with supplemental data, information, or authority that supports such recommendation.

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

[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

state, local, tribal, and territorial entities to enhance the security and resilience of critical infrastructure.

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 actions is to develop a National Critical Infrastructure Security and Resilience R&D Plan. This is to be done within two years of the date of the directive, or by February 12, 2015, with the Secretary of Homeland Security working in coordination with the Office of Science and Technology Policy (OSTP), the Sector Specific Agencies (SSAs), Department of Commerce (DOC), and other Federal departments and agencies. The plan is to take into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide research and development requirements and investments. The plan shall be issued every four years after its initial delivery with interim updates as needed. The plan will provide input to align Federal and Federally-funded research and development activities seeking to strengthen the security and resilience of the Nation's critical infrastructure.

III. Initial List of Issues To Be Updated in the NCISR R&D Plan

PPD-21 specifies the following elements shall be included in the NCISR R&D Plan:

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

1. Promote research and development to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology;
2. Enhance modeling capabilities to determine potential impact on critical infrastructure of an incident or threat scenario as well as cascading effects on other sectors;
3. Means to facilitate initiatives to incentivize cybersecurity investments and the adoption of critical infrastructure design features that strengthen all-hazards security and resilience; and
4. Prioritize efforts to support the strategic guidance issued by the Secretary of Homeland.

The NCISR R&D Plan will be written by coordinating with the full range of critical infrastructure partners and other stakeholders. This notice extends an invitation to the broader public to provide input on the technical content and foci for the NCISR R&D Plan needed to best achieve the goals established in the Presidential Executive Orders and Directives. To assist the reviewer, DHS has developed a proposed structure and outline for the NCISR R&D Plan which is included with this notice. The purpose of this notice is to request public comment on this draft outline indicating priority topics or ideas they believe should be included and why that are listed or not listed. These comments and inputs would help to ensure the NCISR R&D Plan mandated by PPD-21 is relevant and useful, guiding research and development that will strengthen the security and resilience of the Nation's critical physical and cyber infrastructure.

IV. NCISR R&D Plan Outline

Below is the list of the topic areas proposed for the NCISR R&D. This request for information solicits feedback on the proposed content, foci, and relevant high-priority subtopics. Recommendations on changes, additions or deletions to the proposed list are also encouraged. Justification for inclusion is requested to strengthen the value of the input received.

- Background and Problem
- Challenges and Milestones
- Future State and Vision
- Objectives
- Cyber-Physical Systems
- Interdependencies
- Operations, Modeling & Simulation
- Human Systems Elements
- Education
- Public/Private/Local Partnerships
- R&D Transition to Use
- Multi-domain R&D
- National R&D and Incentives
- Science Challenges
- Key Elements for Sector R&D Planning
- Execution and Coordination Strategy
- Tools and Methodologies
- Standards and Regulations

- Means to achieve R&D Objectives
- Priorities and Metrics
- Emerging Threats

Additional feedback on the document structure, priority topics, technical or discipline emphasis, and/or method of prioritization of research and development topics are welcomed.

V. Specific Questions

Answers to the below specific questions are desired to ensure the NCISR R&D Plan best addresses and covers what is needed to fulfill its intention and purpose:

1. What types of sector interdependencies of critical infrastructure entities and sectors are important to be included in the NCISR R&D Plan? How well do current analysis methods appropriately address the full operational impacts and complexities of sector interdependencies and the effects of cascading failures for individual assets and/or infrastructure sectors?

2. This is a national research and development plan. What are the highest priority regional, state, local, tribal or territorial issues and concerns that should be included or addressed through a comprehensive research and development agenda? Who are the key players and beneficiaries for such a research and development agenda? How should this research agenda be implemented so to solicit innovative solutions that are broadly accepted by the stakeholder community?

3. How should prioritization of research and development areas be best accomplished? What specific selection and performance criteria should be used to prioritize research and development topics within and between sectors?

4. What is a topic area or issue that you feel is essential to be included in a national NCISR R&D Plan?

Dated: November 27, 2013.

Robert Kolasky,

Director,

Integrated Task Force,

Cyber EO and PPD-21 Implementation,

Office of Infrastructure Protection,

National Protection and Programs Directorate,

Department of Homeland Security.

[FR Doc. 2013-29039 Filed 12/04/2013 at 8:45 am; Publication Date: 12/05/2013]