Homeland Security

National Infrastructure Advisory Council (NIAC)

The National Infrastructure Advisory Council (NIAC) provides the President of the United States, through the Secretary of Homeland Security, with advice on the security and resilience of critical infrastructure sectors and their functional systems, physical assets, and cyber networks. The NIAC is charged to improve the cooperation and partnership between the public and private sectors. It also has the authority to provide advice directly to the heads of other agencies that have shared responsibility for critical infrastructure protection. It advises on policies and strategies that range from risk assessment and management to information sharing to protective strategies and clarification on roles and responsibilities between public and private sectors.

Background

The NIAC was created by Executive Order 13231 of October 16, 2001 and continued by Executive Order 13286 of February 28, 2003; Executive Order 13385 of September 29, 2005; Executive Order 13446 of September 28, 2007; Executive Order 13511 of September 29, 2009; Executive Order 13585 of September 30, 2011; and Executive Order 13652 of September 30, 2013. The Council is composed of not more than 30 members, appointed by the President, who are selected from the private sector, academia, and State and local government, representing senior executive leadership expertise from the critical infrastructure sectors as delineated in Presidential Policy Directive 21.Be disclosed through a Freedom of Information Act (FOIA) request or through a request under a similar State, local, tribal, or territorial disclosure law;

This fact sheet is dated. Executive Order 13708 is the latest continuation that expires on Sep. 30, 2017.

Leadership

The position of NIAC Chair and Vice Chair are named by the President. Currently the NIAC Chair and Vice Chair positions are held by Ms. Constance Lau, President and CEO, Hawaiian Electric Industries, Inc.; and Dr. Beverly Scott, CEO, Beverly Scott Associates, LLC, serves as the Vice Chair.

NIAC Operations

The NIAC meets publicly four times each year. Meetings generally are hosted in Washington, D.C. in a venue open to the public and members who want to attend in person. The Council uses its public meetings as working meetings, focused on progress reports from its working groups and on deliberations to produce useful and actionable recommendations in a timely manner. The Council is very active, with high performance goals of delivering quality, well-researched reports between 6-12 months from the inception of the selected studies. Its reports have drawn public and private sector interest with regular requests from congressional committees for copies. The White House monitors the progress of the Council's studies on a regular basis between meetings through a liaison in the National Security Council staff.

Reports Delivered to the President

- Water Sector Resilience, 2016
- Transportation Sector Resilience, 2015
- Executive Collaboration for the Nation's Strategic Infrastructure, 2015
- Critical Infrastructure Security and Resilience National Research and Development Plan, 2014
- Implementation of EO 13636 and PPD- 21, December, 2013
- Strengthening Regional Resilience, November, 2013
- Intelligence Information Sharing Study, 2012
- A Framework for Establishing Critical Infrastructure Resilience Goals, 2010
- Optimization of Resources for Mitigating Infrastructure Disruptions, 2010
- Critical Infrastructure Resilience, 2009
- Framework for Dealing with Disasters and Related Interdependencies, 2009
- Critical Infrastructure Partnership Strategic Assessment, 2008
- The Insider Threat to Critical Infrastructures, 2008
- Chemical, Biological, and Radiological Events and the Critical Infrastructure Workforce, 2008
- The Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States, 2007
- Convergence of Physical and Cyber Technologies and Related Security Management Challenges, 2007
- Public-Private Sector Intelligence Coordination, 2006
- Workforce Preparation, Education and Research, 2006
- Sector Partnership Model Implementation, 2005
- Risk Management Approaches to Protection, 2005
- Common Vulnerability Scoring System, 2004
- Hardening the Internet, 2004
- Prioritizing Cyber Vulnerabilities, 2004
- Evaluation and Enhancement of Information Sharing Analysis, 2004
- Best Practices for Government to Enhance the Security of National Critical Infrastructures, 2004
- Cross Sector Interdependencies and Risk Assessment Guidance, 2004
- Vulnerability Disclosure Framework, 2004

January 2017