NIAC The President's National Infrastructure Advisory Council

September 1, 2017

The Honorable Donald J. Trump
President of the United States
The White House
1600 Pennsylvania Avenue, N.W.
Washington, DC

Dear Mr. President,

At the request of the National Security Council, the President's National Infrastructure Advisory Council (NIAC)—your CEO-level council for critical infrastructure insight and perspective—examined how federal authorities and capabilities can best be applied to improve cybersecurity of the most critical infrastructure assets.

Our nation needs direction and senior leadership to dramatically reduce cyber risks. **Our recommendations call upon the Homeland Security Advisor to convene agency heads and industry executives to take rapid action**. To start, we recommend convening senior administration officials and executives in the electricity, finance, and communications sectors, where cyber risks are clear and present, and where executive engagement is high.

The NIAC's 11 recommendations present near-term, top-priority solutions these leaders can direct action on. Three recommendations are highlighted here, and the study contains several more:

- Establish **SEPARATE, SECURE COMMUNICATIONS NETWORKS** specifically designated for the most critical cyber networks, including "dark fiber" networks for critical control system traffic and reserved spectrum for backup communications during emergencies.
- Identify best-in-class **SCANNING TOOLS AND ASSESSMENT PRACTICES**, and work with owners and operators of the most critical networks to scan and sanitize their systems on a voluntary basis.
- **USE THE NATIONAL-LEVEL GRIDEX IV EXERCISE (NOVEMBER 2017) TO TEST** the detailed execution of Federal authorities and capabilities during a cyber incident, and identify and assign agency-specific recommendations to coordinate and clarify the federal government's response actions.

Our study found that the substantial cyber capabilities among Federal agencies are divided, uncoordinated, and often duplicative—making them insufficient to address sophisticated cyber threats today. A nation-state cyber attack on U.S. infrastructure also places private companies on the front line. This presents a national security challenge unlike any other. Industry access to federal resources is often hindered by multiple technical, legal, liability, and information sharing constraints. Our recommendations aim to address these and other challenges.

As a nation, we need to move past simply studying our cybersecurity challenges and take meaningful steps to prevent a major and debilitating cyber attack. The time to act is now.

On behalf of our fellow NIAC members, we thank you for the opportunity to serve our country through participation in this Council.

Sincerely,

Constance Lau

President and CEO
Hawaiian Electric Industries, Inc.
NIAC Chair

Dr. Beverly Scott

CEO
Beverly Scott Associates, LLC
NIAC Co-Chair