MICHAEL M. HONDA
17TH DISTRICT, CALIFORNIA

WASHINGTON OFFICE
1713 LONGWORTH BUILDING
WASHINGTON, DC 20515
PHONE: (202) 225-2631
FAX (202) 225-2699

DISTRICT OFFICE
2001 GATEWAY PLAZA
SUITE 670W
SAN JOSE, CA 95110
PHONE: (408) 436-2720
FAX (408) 436-2721

HTTP://HONDA.HOUSE.GOV/

Congress of the United States
House of Representatives

COMMITTEE ON APPROPRIATIONS
SUBCOMMITTEES:
COMMERCE, JUSTICE, SCIENCE
LABOR, HEALTH AND HUMAN SERVICES, EDUCATION

SENIOR DEMOCRATIC WHIP

CONGRESSIONAL ASIAN PACIFIC
AMERICAN CAUCUS, *CHAIR EMERITUS*

SUSTAINABLE ENERGY AND ENVIRONMENT COALITION,
VICE CHAIR

LGBT EQUALITY CAUCUS, *VICE CHAIR*

December 10, 2013

Mr. Patrick D. Gallagher
Director
National Institute of Standards and Technology
United States Department of Commerce
100 Bureau Drive, Stop 1000
Gaithersburg, MD 20899-1000

Director Gallagher:

I commend NIST's excellent work in partnering with industry to develop the preliminary Cybersecurity Framework, which will enhance the cybersecurity of our nation's critical infrastructure. I am concerned, however, that as currently constructed, the Framework will not stop attacks by advanced threat actors using sophisticated tactics such as exploiting previously unknown vulnerabilities (zero-day attacks) or using never seen before malware. Addressing these threats is critical, as advanced cyber adversaries are targeting critical infrastructure companies to the detriment of U.S. economic and national security.

Emerging best practices use behavioral and virtualization techniques to identify and block sophisticated threats. For example, the recently-released NIST *Special Publication 800.53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organization*, describes the use of detonation chambers to quickly find malicious code (SC-44, found in Appendix F-SC, page F-214):

> Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator (URL) requests in the safety of an isolated environment or virtualized sandbox. These protected and isolated execution environments provide a means of determining whether the associated attachments/applications contain malicious code. While related to the concept of deception nets, the control is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, it is intended to quickly identify malicious code and reduce the likelihood that the code is propagated to user environments of operation (or prevent such propagation completely).

Despite of the widespread adoption of SC-44 across the Fortune 500, NIST's preliminary Cybersecurity Framework does not point to SC 44 as an informative reference. This is a serious

oversight that will leave critical infrastructure vulnerable to advanced cyber threats even after they spend resources adopting and implementing the Framework.

In order to mitigate risk from zero-day and other sophisticated attacks, I recommend that NIST add SC-44 into the Framework as an informative reference to some or all of the following subcategories:

a) DE.AE-2 Detected Events are analyzed to understand attack targets and methods
b) DE.CM-4. Malicious Code is detected
c) DE.CM-5 Unauthorized mobile code is detected
d) RS.AN-1 Notifications from the detection system are investigated
e) RS.AN-2 Understand the impact of the incident
f) RS.AN-3 Forensics are performed
g) RS.MI-1 Incidents are contained
h) RS.MI-2 Incidents are eradicated

Thank you for work on this important subject that is vital to national security. I believe the incorporation of the state-of-art best practice SC-44 will enable critical infrastructure companies to move to a proactive security posture that will identify and block sophisticated cyber threats intent on stealing U.S. intellectual property and disrupting our nation's critical infrastructure. Please feel free to contact Dr. Eric Werwa of my staff at eric.werwa@mail.house.gov or (202) 225-2631 if you have any questions.

Sincerely,

Michael M. Honda
Member of Congress