Honeywell

Incentives to Adopt Improved Cybersecurity Practices

Response to Notice of Inquiry

Docket Number 130206115-3115-01

April 29, 2013

Submitted to:
Office of Policy Analysis and Development
National Telecommunications and Information Administration
ATTN: Alfred Lee
1401 Constitution Ave NW, Room 4725
Washington, DC 20230

Submitted by:
Honeywell International Inc.
Honeywell Global Security
101 Columbia Road
Morristown, NJ 07962
ATTN: Steve Kostiw
Global.Security@Honeywell.com

INCENTIVES TO IMPROVE CYBERSECURITY PRACTICES

Honeywell International Inc. (Honeywell), through its Global Security division, is pleased to respond to the National Telecommunications and Information Administration's inquiry regarding Incentives to Adopt Improved Cybersecurity Practices (Docket Number 130206115-3115-01). We understand this inquiry supports the evaluation of the benefits and relative effectiveness of incentives to adopt the Cybersecurity Framework currently being developed by the National Institute of Standards and Technology (NIST).

Executive Order 13636 Improving Critical Infrastructure Cybersecurity requires the Secretaries of Homeland Security, Treasury and Commerce to make recommendations related to incentives that would support the adoption by owners and operators of critical infrastructure of the Cybersecurity Framework currently under development by NIST. Through its services division, Honeywell Technology Solutions Inc., Honeywell was pleased to respond to the recent NIST Request for Information (Docket Number 130208119-3119-01). We are also actively partnering with NIST as a founding member of the Cyber Security Research Alliance.

As documented in our response to NIST, Honeywell believes that the proposed NIST Framework should be risk-based to permit industry to respond quickly to rapidly evolving threats. Government should advocate but not mandate good security practices, and promote sector-specific plans and investment in more proactive, preventive, and predictive capabilities for cyber defense. A framework should advocate more predictive (as opposed to reactive) cybersecurity processes. Several core Honeywell themes referenced in our NIST response are:

- A "one size fits all" approach is not effective. Critical infrastructure is diverse; the threats and their solutions vary. We recommend tailoring for each critical infrastructure sector.
- Standards must be risk-based, flexible, and capable of keeping pace with evolving threats. They should promote the value of meeting objectives and should not directly prescribe the means of compliance. We do not support standards that require "check the box" assessments and/or static control frameworks.
- We encourage NIST to harmonize and synchronize the new framework with existing standards and/or policies to avoid duplication, inconsistency and regulatory confusion.

We understand the NIST Framework will not be published in its final form until February 2014. The absence of a published framework makes it difficult to assess the specific types of investments required by companies to be compliant. Given this lack of data, Honeywell is unable to provide specific endorsements or critiques of incentives. Instead, we will provide general comments about core principles that we believe should be included in a Government incentive program.

Honeywell supports U.S. Government efforts to improve cybersecurity for critical infrastructure by implementing an incentives program that promotes effective security and also provides companies the opportunity to realize a business advantage over organizations that maintain less than adequate security programs. Ultimately, the success of an incentive program will require compliance with the NIST Framework. We believe the evaluation of compliance should not solely be accomplished by U.S. Government audits. Compliance should also be evaluated using

internal security certification processes, internal organization self assessments and vulnerability assessments governed by widely accepted industry standards.

Information sharing between the Government and the private sector should focus on threat indicators, threat assessments, and countermeasures and support stated data privacy restrictions. Companies that participate in good faith in cyber threat sharing activities should be provided liability protection. For instance, Honeywell would welcome liability protection for acting in good faith on Government furnished threat information. Such liability protection should include immunity from private causes of action based on a company's use or disclosure of cyber threat information, as well as any act or omission following the lawful receipt of cyber threat information.

Additionally, Honeywell would seek anti-trust protection as an incentive to work with other companies across sectors to share threat information and cybersecurity best practices.

Protection should also be provided against Freedom of Information Act (FOIA) disclosures of threat information shared with the Government, especially when that information is attributed to specific companies.

As an additional incentive, the Government should expedite security clearances to appropriate personnel employed by critical infrastructure owners and operators to enable sharing of sensitive threat information.

Owners and operators who adopt the framework should receive prioritized cybersecurity technical assistance e.g., Industrial Control Systems-Computer Emergency Response Team (ICS-CERT), as well as incident response support. In addition, protocols need to be developed to allow these owners and operators access to priority Internet service during major incidents complicated by periods of severe network congestion or disruption.

When evaluating contract proposals, the U.S. Government should consider preferential evaluation for companies that employ agreed upon standards, or propose to improve cybersecurity measures.

Honeywell encourages U.S. Government funds be directed to cybersecurity research grants and for other investments in cybersecurity products and services for framework owners and operators. Alternatively, the Government could tie existing grants to the adoption of the cybersecurity framework.

Cybersecurity insurance, if more broadly promoted and adopted, could be a source of encouragement to companies to implement constantly improving standards as a condition to obtain insurance at reasonable rates. In addition, federal reinsurance programs should be considered to help underwrite the development of cybersecurity insurance programs.

The U.S. Government should encourage private industry and/or standards bodies, to create an award for companies that adopt cybersecurity practices; customers may be more likely to purchase products and services from companies that have achieved the award or designation.

The Honeywell mission to "build a world that is safer and more secure" extends to cyberspace and we value action that seeks to safeguard the United States as well as our own business assets. Thank you for the opportunity to participate and contribute on this important issue.