# DEPARTMENT OF COMMERCE NOTICE OF INQUIRY TEMPLATE

September 10, 2010

VIA ELECTRONIC FILING

The Honorable Gary Locke
Secretary
United States Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

RE: *Cybersecurity, Innovation and the Internet Economy, Docket No. 100721305-0305-01*

Dear Secretary Locke:

Attached for electronic filing in the above-referenced proceeding, please find the *Initial Comments of Honeywell, Inc. on the Cybersecurity, Innovation and the Internet Economy, Docket No. 100721305-0305-01.*

Should you have any questions or need further information regarding this filing, please contact us.

Sincerely,

/s/

**Amy Chiang**
Director, Government Relations
Honeywell International
(202) 662 2638
amy.chiang@honeywell.com

**UNITED STATES OF AMERICA**
**BEFORE THE**
**UNITED STATES DEPARTMENT OF COMMERCE**

| | | |
|---|---|---|
| | **)** | |
| **Cybersecurity, Innovation and the** | **)** | **Docket No.** 100721305-0305-01 |
| **Internet Economy** | **)** | |
| | **)** | |

# INITIAL COMMENTS OF HONEYWELL, INC. ON CYBERSECURITY, INNOVATION AND THE INTERNET ECONOMY

Pursuant to the July 28, 2010 Notice of Inquiry ("NOI") of the Department of Commerce, the National Institute of Standards and Technology ("NIST"), and National Telecommunications and Information Administration ("NTIA"), in the above-referenced proceeding,[1] Honeywell, Inc. ("Honeywell") respectfully submits these comments on the Department of Commerce's NOI on Cybersecurity, Innovation and the Internet Economy ("CIIE"). Honeywell appreciates the opportunity to comment on measures to improve cybersecurity while sustaining innovation, as part of the Department's Internet Policy Task Force's comprehensive review of the nexus between cybersecurity challenges in the commercial sector and innovation in the Internet economy.

Honeywell respectfully submits our perspective on policy issues that need to be considered, and on implementation challenges and opportunities critical to enhancing innovation while ensuring cyber security. We base our views on Honeywell's market-

[1] *Cybersecurity, Innovation and the Internet Economy*, Notice of Inquiry, 75 FERC ¶ 44216 ("NOI").

leading position in authentication (including biometrics), facility access control systems, and information and security management for critical infrastructures.

## I. COMMUNICATIONS

All correspondence, communications, pleadings, and other documents relating to this proceeding should be served upon the following persons:

**Amy Chiang**
Director, Government Relations

Honeywell International
101, Constitution Ave. NW, #500W
Washington DC 20001

**Telephone:** (202) 662 2638
**Fax:** 202-662-2675
**Email:** amy.chiang@honeywell.com

**Dr. Sanjay Parthasarathy**
Director, Technology Strategy

Honeywell International
101, Constitution Ave. NW, #500W
Washington DC 20001

**Telephone:** (612) 356 3512
**Fax:** 202-662-2675
**Email:**
sanjay.parthasarathy@honeywell.com

## II. BACKGROUND AND EXECUTIVE SUMMARY

Honeywell is a global provider of software and hardware solutions and services that run industries, secure buildings and protect critical infrastructure. Secure information access, data integrity, and privacy are the underlying tenets in Honeywell’s development methodologies. We share our perspective on innovation and cyber security, based on our expertise in providing enterprise authentication and access control systems, biometrics, and, our participation in cyber programs (both classified and unclassified).

Strong authentication is a critical enabler for the internet economy to flourish. It:

- Provides a more secure Internet environment, which promotes innovation while reducing risk
- Promotes the adoption of electronic delivery of services (e.g., patient records) by enhancing both security and efficiency
- Facilitates the secure use of smart mobile devices to conduct business

We outline three areas where we believe the government needs to act, along with public-private organizations, to sustain innovation in the internet economy while ensuring cyber security. As explained below, these include adopting appropriate policies, implementing cyber secure technologies, and providing incentives for the private sector to do likewise.

### A. Policy issues:

Honeywell encourages the administration to adopt policy that supports the development and deployment of strong individual and machine authentication mechanisms. The mechanisms could be used to strongly authenticate email, access to web pages, Internet based transactions, remote control functions (e.g. smart grid enabled energy management), electronic medical records and many interactions between citizens and the Government.

### B. Implementation:

Honeywell strongly advocates the deployment of cyber security technologies that can be used for enhancing both cyber and physical authentication. This implies funding for research to address outstanding issues in identification, authentication, privacy, traceability and forensics. Governmental organizations need to drive standards for strong authentication and authorization, for example, iris template representation and public key certificate formats.

### C. Incentives:

Finally, the administration should structure the delivery of Government services and commercial incentives to promote the adoption and enhancement of services delivered via strong authentication.

This viewpoint illustrates the challenges and benefits in a few key areas. However, the ideas presented here are broadly applicable to other application areas involving finance and e-government.

## III. COMMENTS

### A. Overview

US companies, consumers and the overall economy would benefit from the improved efficiency and reduced losses enabled by strong authentication. The administration should adopt policies which support the development and deployment of strong authentication mechanisms for email, access to web pages, audio, video and software. The anticipated benefits of a strong identification and authentication infrastructure include:

- ***Reduced SPAM, Phishing and malware:*** If the true source of email was strongly authenticated, then consumers and business could better protect themselves from unwanted mail. Likewise, strong authentication, even from a compromised PC, would make it easier for administrators or law enforcement to track down the source of unwanted mail.

- ***Enables innovation and online services***: Strong authentication mechanisms reduce risk of fraud and therefore allow more information and more types of transactions to take place online. Reducing the security risk then stimulates innovation. It allows both Government services and private sector entities to offer new services that are not acceptable in the current risk environment. New infrastructure, such as the smart grid, has the potential to provide significant energy savings. However, it cannot be secured unless home owners, utilities and other energy related service providers can be strongly authenticated. Authentication adds another layer of protection for businesses against piracy and industrial cyber-espionage.
- ***Reduce password risk:*** Passwords are inexpensive, easy to change and hard to remember. More importantly they are growing less secure each year. The ability of humans to memorize passwords has remained constant for the last 25 years, and it will remain constant in the future. However, computing power has increased significantly in the last 25 years, and it will continue to increase. This leads to an environment in which passwords which were considered strong in 1990 are now easily cracked by modern computers. The problem will only get worse as computing power increases.
- ***Reduced identity theft:*** The social security number amounts to a fixed password which US citizens are forced to share with many organizations

## B. Policy Creation and Adoption

Emerging policy should provide the structure and incentives for creating a strong identity infrastructure without favoring any particular technology. Viable approaches could include biometrics, token based authentication (e.g. embedded in a cell phone or Smart card based driver's license) and could be provided by the Government (similar to the passport process) or by private industry. The policy issues which the Government can influence include:

1. **Organizational support and structure**: The Government includes organizations which are in a position to support change. NIST has both the computer security expertise and the charter to create standards related to strong authentication. The Social Security Administration has the ability to be an early adopter of strong authentication or they could become an impediment by continuing to use a social security number/authentication system based upon the same technology that was used in 1936. The IRS, Veterans Administration and DoD have the ability to modernize and streamline Government. However these groups must work together with commercial entities to establish one common standard and compatible policy.

2. **Registration**: The Government is the de-facto organization for providing identification credentials. Birth certificates, Social Security Numbers, driver's licenses and passports are all forms of government issued identification. However, the system is fragmented. The Government has the opportunity to harmonize these different forms of identification and create electronic credentials usable over the internet.

3. **Use**: The Government is in a position to establish guidelines for the use of strong authentication credentials. Today, policy requires the use of the social security number for financial transactions (opening a bank account, paying taxes, etc.). The Government has an opportunity to encourage the use of strong authentication by adopting it themselves and providing the support infrastructure for banks and other organizations to share in the benefits of a strong authentication credential.

4. **Liability**: The Government needs to develop policy addressing the liability associated with use, acceptance and potential compromise of strong authentication. The Government has protected its citizens via laws providing information privacy and establishing liability for

## C. Implementation of Technologies and Standards

### 1. Technologies

There have been numerous advances in technology since the Social Security Number was first implemented in 1936. The technology available today to support strong authentication include:

- ***Biometrics***: Iris recognition is recognized as one of the most stable and accurate biometric technologies. It changes very little with age, is difficult to forge and has very low error rates. The biometric template of an iris may be encoded in a memory device such as a smart card.

- ***Smart cards***: Contactless smart cards are widely used for access to secure buildings. The world is adopting RFID/Smart Card technology for passports. The DoD Common Access Card (CAC) serves as a proof of the capability and security of smart card technology. Advances in technology have reduced the cost of smart cards while improving their reliability and capability.

- ***Public Key Cryptography***: This technology provides the means to apply and verify digital signatures on identification documents, emails, tax forms, medical information and anything else that may be transferred over the internet. Fast, secure cryptography is enabled by modern microprocessors. It has been studied and approved by cryptographers within NIST and the National Security Agency.

- ***Federated and cooperative authentication***: In today's internet connected world we are all forced into multiple authentications as we traverse from company to company across the internet. Technologies exist which allow environments in which an individual authenticates once and is then provided with a secure token that identifies who we are to the various systems and data that we are requesting access to. Those systems and data will allow access based on the secure token contents meeting specific gating functions into the data. Similar technology allows for delegation of access rights so that a user can provide a third party temporary rights to access the user's data.

## 2. Standards

NIST has established standards for public key cryptography and related cryptographic functions such as the Advanced Encryption Standard (AES) and Secure Hash Functions (e.g. SHA-2). Additional standards would need to be developed relating to iris template representation, public key certificate formats and other aspects of the strong identification/

authentication system. NIST would certainly play a role in establishing standards to support secure protocols for digital exchange of information. The standardization of electronic passport information serves as a starting point for establishing the standards which will allow nation wide (and cyber space) validation of strong authentication.

## IV. Conclusion

The technology available for authenticating individuals and protecting sensitive authentication information has changed dramatically since 1936 when Social Security Numbers were first issued. The growth of the internet has heightened the need for strong authentication in order to support innovative services and reduce the drag on the economy due to weak and inefficient authentication mechanisms. The technologies available today include biometrics, public key cryptography and contactless smart cards.

The US Government is in a position to stimulate innovation by:

1. Establishing policy supporting strong authentication mechanisms
2. Moving Government issued identification information (SSN, Driver’s license, etc.) to modern technology which protects from identity theft and provides strong authentication.
3. Ensuring Government organizations (SSA, IRS, etc.) are early adopters of strong authentication to drive user education and market acceptance.

WHEREFORE, Honeywell requests that the Department of Commerce's Internet Policy Task Force consider policy and implementation issues together in determining the future of the internet economy. The Task Force should put in place an appropriate incentive structure that promotes collaboration across and within private and public sector enterprises.

Respectfully submitted,

______/s/____________

**Amy Chiang**
Director, Government Relations

Honeywell International
101, Constitution Ave. NW, #500W
Washington DC 20001

**Telephone**: (202) 662 2638
**Fax**: 202-662-2675
**Email**: amy.chiang@honeywell.com

Dated:  September 10, 2010