Honeywell

Preliminary Cybersecurity Framework Comments

Docket Number 130909789-3789-01

December 13, 2013

Submitted to:

Information Technology Laboratory,
ATTN: Adam Sedgewick,
National Institute of Standards and Technology,
100 Bureau Drive, Stop 8930,
Gaithersburg, MD 20899-8930

Submitted by:

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

PRELIMINARY CYBERSECURITY FRAMEWORK COMMENTS

Honeywell is pleased to respond to the National Institute of Standards and Technology's request for comments regarding the Preliminary Cybersecurity Framework, Docket Number 130909789-3789-01 ("the Framework").

Summary

Although the Framework contains risk-based principles that are designed to respond to evolving threats, Honeywell believes that the Framework is just one component of a predictive cyber security process that should also include:

- **Encourage Information Sharing:** Effective information sharing between government and industry partners, including classified information, in real time.
- **Ensure Liability Protection:** Information sharing liability protection to safeguard companies that participate in information sharing activities in good faith.
- **Provide Incentives:** Appropriate incentives for companies to develop proactive, preventive and predictive capabilities for cyber defense.

General Comments

1. **Delineate Responsibilities Clearly:** The Framework should delineate the roles and responsibilities of both critical infrastructure operators and product manufacturers and suppliers, thus emphasizing that cyber security efforts are shared responsibilities.

2. **Employ BSIMM:** The Framework should reference Building Security In Maturity Model (BSIMM) in its informative reference list. It provides a comprehensive list of activities for software assessment and evaluation.

3. **Encourage Continuous Improvement:** The Framework should promote a continuous improvement process. In its current iteration, the Framework does not reference improvement opportunities until the Framework "Respond" and "Recover" phases -- and even then the Framework does not specifically contemplate an explicit lessons learned protocol. Furthermore, the Framework does not establish a protocol for organizational changes like a new acquisition or a material change in assets such that an organization should assess whether the current security posture is still adequate.

4. **Develop Adoption Conformity Guidelines:** The Framework lacks specific adoption/conformity criteria that would otherwise provide an organization with a standard process to assess the maturity of its implementation of the Framework functions and profiles. Although organizations are invited to "self assess" compliance and assign current and target tiers, there are no objective criteria for the assessments, e.g., transitioning from a preventive posture to a predictive or resilient security capability; or conducting vulnerability testing vs. penetration testing, -- thus no common criteria between organizations.

Because supply chain cybersecurity is a growing concern, creating a common set of objective standards/criteria and language for industry would encourage private-public trust.

5. **Enhance Cyber Security Workforce Skills:** The Framework should emphasize the importance of a skilled cyber security workforce to raise the level of technical skills of those who operate critical infrastructure. For example, the Framework should consider including an informative reference list that contains cyber security certifications and corresponding summaries of competencies that each certification provides to help organizations understand their current and future needs.

6. **Outline Global Impact:** The Framework should more clearly articulate a protocol for the mapping and harmonization of global laws and regulations, e.g., reciprocity agreements for global critical infrastructure regulations, to reduce duplication and costs.

7. **Establish Appropriate Privacy Methodology:** Honeywell believes privacy and cybersecurity go hand in hand. Accordingly, Honeywell applauds NIST's willingness to address privacy issues in the NIST Cybersecurity Framework. Although the inclusion of privacy standards in the Framework is important, however, a privacy methodology that includes open-ended and burdensome mandates may discourage organizations from adopting the voluntary Framework. Honeywell urges NIST to review and revise the Framework's privacy methodology (Appendix B) to ensure that the methodology is narrowly focused to reflect private sector practices relating to privacy. By including an appropriately tailored privacy methodology as part of the Framework, NIST will encourage the adoption of the Framework and allow an organization to complement its cybersecurity program with a privacy program that addresses privacy issues directly implicated by the organization's approach to cybersecurity.

Specific Comments

Page	Line	Section	Comments	Suggested Changes
2	118	Overview	The Framework Core is vague on the need for continuous improvement within each of the five functions; threats are dynamic.	
6	243	Identify	Risk Assessment (246) and Risk Management Strategy (246) are both components of the *Risk Management Process*. The *Identify* (243) function provides Risk Assessment (246) and Risk Management Strategy (246) but should precede both tasks with Framing Risk.	NIST SP800-39 states: "Risk framing, as its principal output, produces a risk management strategy that addresses how organizations intend to assess risk, respond to risk, and monitor risk."
6	243	Identify	The value of regular and ongoing assessments in this function should be emphasized.	
7	265	Respond	The *Respond (265)* function includes: "Develop and implement the appropriate activities…" (265). The Risk Management Strategy is the response activities and has already been developed during the *Identify* function.	See NIST SP 800-39 Page 8 Para. 2: "Another primary input to the risk response component is an output from the risk framing component—the risk management strategy that defines how the organization should respond to risk." By moving to the more complete "Risk Management Process" during the *identify* function the entire concept falls in line with, and enhances, NIST Special Publication 800-30 – Guide for Conducting Risk Assessments and NIST Special Publication 800-39 – Managing Information Security Risk.

Page	Line	Section	Comments	Suggested Changes
7	273		One of the aspects of recover should be lessons learned and require modifications to the process to prevent re-occurrence and proactively take steps to avoid exploited risks and continuously improve the process.	
9	318	Info Flow Figure 3	The heading under Risk Management includes "Mission Priority and Risk Appetite and Budget"; Risk Appetite is being used instead of Risk Tolerance.	The term "Risk Tolerance" is used in SP 800-53R4, SP 800-30, SP 800-37 and SP 800-39. Suggest using Risk Tolerance instead of introducing a new term (Risk Appetite).
15	RA	Append A		ID.RA-2 – Additional Informative Reference: NIST SP 800-53 Rev.4: AC-21.
21	PT	Append A		PR.PT-2 – Additional Informative Reference: NIST SP 800-53 Rev.4: AC-20(2).
21	PT	Append A		PR.PT-3 – Additional Informative Reference: NIST SP 800-53 Rev.4: AC-17, AC-18, AC-19, AC-20.
22	PR	Append A	In addition to protection by risk analysis emphasize also to manufacturer's security technical implementation guidelines and that those systems are operating according to governing standards and conform to lifecycle management to maintain system currency.	
22	DE	Append A		DE.CM-1 – Additional Informative Reference: NIST SP 800-53 Rev.4: AU-6(2), AU-6(4.)

Page	Line	Section	Comments	Suggested Changes
24	RS	Append A		RS.PL-1 – Additional Informative Reference: NIST SP 800-53 Rev.4: IR-7, IR-8.
25	RS	Append A		RS.CO-1 – Additional Informative Reference: NIST SP 800-53 Rev.4: PL-4, PS-6, PS-7, SA-9.
27	484	Append A	Analysis should also be included in the recovery function. During the Respond function analysis identifies the event and determining how to respond. After the recovery an Analysis of the current Protections should be done to determine how to improve protections against a similar threat. Follow with further Analysis to determine if the threat could have been detected sooner so it did not become an event. Lastly determine if the Response was sufficient and appropriate as well as was the Recovery function conducted properly.	

Page	Line	Section	Comments	Suggested Changes
		Append A	The "Framework Core" subcategories are very similar to NIST SP 800-53. Between a third and a half of the 800-53 controls considered "suggested" are referenced and virtually every subcategory points to specific 800-53 controls. If the intent is to better align government and industry, it would seem the Cybersecurity Framework controls should use the same controls promulgated to government by NIST.	Instead of an entirely separate framework "core," an additional category for "critical infrastructure" added to 800-53 might make more sense. For critical infrastructure systems, a unique set of 800-53 controls would be used, similar to how we differentiate between controls for say a MAC I Classified and MAC II Sensitive system. Instead, the Cybersecurity Framework seems to just reword and reorganize 800-53 controls that say similar things and this may cause unnecessary confusion.