Introduction

On February 12, 2013, the White House announced the "Improving Critical Infrastructure Cybersecurity" Executive Order [1]. Subsequently, on February 26, 2013, the National Institute of Standards and Technology (NIST) published in the Federal Register a Request For Information (RFI) [6]. Therein, the RFI requests comments to specific questions in three sections:

- Current Risk Management Practices
- Use of Frameworks, Standards, Guidelines, and Best Practices
- Specific Industry Practices

This document is submitted to the attention of Ms. Diane Honeycutt, National Institute of Standards and Technology, located at 100 Bureau Drive, in Gaithersburg, Maryland, on behalf of Tripwire, Inc., headquartered in Portland, Oregon.

About Tripwire

Since, 1987, Tripwire has focused on solutions relating to the automation of continuous monitoring. Tripwire is a recognized thought leader in the area of secure continuous monitoring and information security risk mitigation.

In the period since Tripwire's inception, we have worked with over 7,000 customers in both the public and private sectors, and have gained first-hand knowledge of the challenges these organizations face trying to keep systems secure and compliant.

We also face these challenges ourselves. As a medium-sized, private company, we are similar in scope to many other organizations that face the struggles of being secure and compliant efficiently.

The Tripwire toolset is designed to connect security to the organization's mission, by providing robust and flexible tools that automate security configuration management against most of the frameworks being used today. Tripwire's tools analyze, identify, prioritize, and remediate security risks due to non-compliant network devices, servers, workstations and applications.

Response Overview

Tripwire's perspective is such that four general truths exist in our common industry:

1. **Threat agents have evolved:** The people behind today's breaches are no longer simply making statements; they're stealing intellectual property or money.
2. **Systems complexity continues to increase over time:** Not five years ago the "cloud" was just forming, and not two years ago "BYOD" wasn't a really big deal.
3. **Dynamism of situational awareness is increasing:** Motivated and resourceful threat agents take advantage of systems complexity and change tactics often. We must defend against many attacks, when the threat agent need only realize one. This makes situational awareness more fluid than it used to be.
4. **Our qualified resources are scarce:** We simply do not have enough qualified information security resources to combat our collective adversary.

Consequently, we believe that the strategy and tactics we use as defenders must necessarily focus on operational loss minimization using processes that rely on tools that:

- **Act as force multipliers:** Enable information security personnel to act as more than one.
- **Embed information security domain knowledge:** Let a few do common work, then put that knowledge into the tools to be leveraged appropriately
- **Automated:** Wherever possible, automation must be used to decrease our reaction time and the adversary's window of opportunity
- **Share information:** Tools should interoperate and cooperate as much as possible out of the box, and they should be configured to share information with partners and appropriate authorities (i.e. ISAC, CERT, CSIRT, a user community).

Present Control Frameworks are incapable of supporting our evolved needs. Therefore, Tripwire proposes that the current Framework model evolve into one that focuses on three main concepts.

1. **Persona Definition:** A *persona* provides a "face" to your users beyond role and responsibility. From *Agile Software Requirements:* "user personas provide a means of further refining the approach to the user to make sure that the needs of different types of users are met" [7].

   Given a specific business process, who interacts with this process? Who are the stakeholders? What roles do they play? What are their personal and professional goals and aspirations? From this information a *primary* persona can be discovered along with *secondary* personas [7]. These personas inform the Control Framework in terms of what it needs to deliver.

2. **Business Process Identification and Description:** Current Control Frameworks take a "security objective" perspective, such as "maintain the confidentiality of information," but what is needed is a statement of "how confidentiality is achieved in operational terms, such as physical and logical access control, user enrolment, and audit trail" [8]. Put another way, Control Frameworks should increase their focus on business processes.

3. **Controls Overlay:** Given that the appropriate business processes have been defined in step two, then each process can be examined for control applicability.

   Does a given control apply to the business process? How? What steps in the process need to be changed? What tools might be required? How can the process be measured? How can the process be made efficient?

We have been slicing the bread the same way we always have – vertically. To get real value from Control Frameworks, we should start slicing the bread horizontally as well, so we can see how each control relates to existing business processes. B seeking out these business processes, enumerating them, diagramming them, and identifying the boundaries where they work together, we can then lay control objectives on top to provide more meaningful guidance to organizations of all sizes.

Why is this important? Because business processes can be described visually and, in some cases, translated directly into an executable language. Points of clarification can be made in succinct prose. Abstract business processes can be provided to be adapted. Patterns of adaptation could be returned to the community. Once these are done, checklists can be created and segmented for varying degrees of enterprise resilience.

It is time to abandon Control Frameworks as we know them and move forward to a more effective, pragmatic, and efficient future and it is Tripwire's hope that NIST agrees and is able to navigate the tumultuous waters of change over the course of these next several months