A. Background and Context

Thank you for the opportunity to comment to "Views on the Framework for Improving Critical Infrastructure Cybersecurity," Docket Number: 151103999-5999-01, Document Number: 2015-31217, December 11, 2015.

At the outset, I would like to acknowledge the efforts of NIST and its stakeholders in developing the initial version of the framework. The production of the initial version of the framework is significant in that it provides organizations with an explicitly articulated, formalized baseline for managing cyber security risk in the context of critical infrastructure, a baseline whose components and related attributes – for e.g., core functions (Identify, Protect, Detect, Respond, Recover), and implementation tiers (Partial, Risk Informed, Repeatable, Adaptive) - remained implicit, and unexpressed, until its development. The transition from anectodal references about critical infrastructure protection to authoritative, corporate intelligence through the publication of the framework is, in and of itself, a seminal achievement and, as such, worthy of recognition and acknowledgement.

It is worth noting that, while the framework establishes formalisms for components and related attributes, the matter of framework utility is otherwise discretionary, subject to an organization's situational analysis of need. In this regard, Section 3.0 of the framework itemizes the following five (5) possibilities for framework use:

a. as the basis for an organization's review of its cybersecurity practices
b. as the basis for an organization's establishment, or improvement, of its cybersecurity program
c. as the basis for an organization to communicate its cybersecurity requirements to its stakeholders
d. as the basis for an organization to identify opportunities for new or revised informative references
e. as the basis for an organization's methodology to protect privacy and civil liberties

NIST's non-prescriptive approach to framework use allows organizations to assess how to best leverage framework content – the formalisms - to address their own topical, local, and entity-specific, ends in the critical infrastructure context. Framework utility, then, is a function of organizational context, and not a directive of the document itself.

B. Recommendation and Rationale

Given NIST's open approach to organizational use and adoption of the framework, the purpose of this submission is to recommend that the next iteration of the framework be used to inform the development of critical infrastructure architecture.

Rationale for this recommendation is based on the uses of the framework described in the current version, all of which emphasize operational considerations as their discrete scopes of interest. While legitimate and defensible as objectives, these scopes of interest do not address the discipline of architecture, and the pivotal role that architecture plays in describing critical infrastructure at a level of detail that authoritatively informs its design, and subsequent deployment, and implementation, into a steady state operational environment. As such, the next iteration of the framework would include the following use statement fragment:

"... as the basis for an organization's description of its critical infrastructure architecture."

Figure 1 depicts both current, and recommended, scopes of interest of the framework on a temporal continuum that begins with architecture and ends with operations.

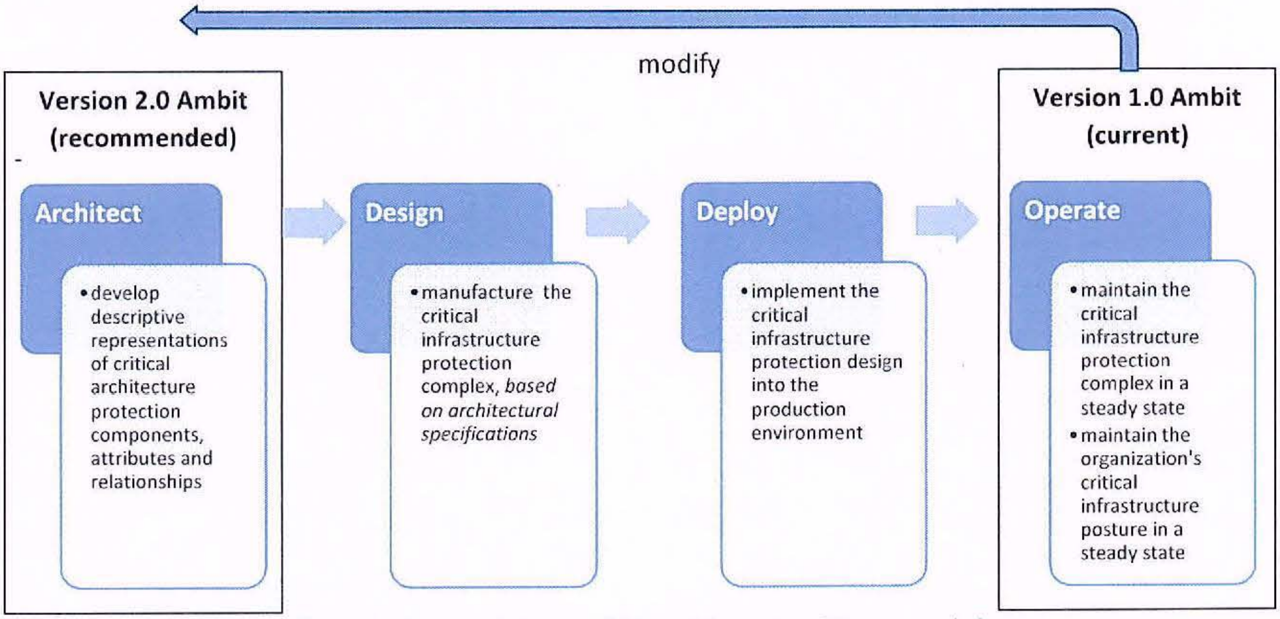
modify
Version 2.0 Ambit (recommended)
Architect
• develop descriptive representations of critical architecture protection components, attributes and relationships
Design
• manufacture the critical infrastructure protection complex, *based on architectural specifications*
Deploy
• implement the critical infrastructure protection design into the production environment
Version 1.0 Ambit (current)
Operate
• maintain the critical infrastructure protection complex in a steady state
• maintain the organization's critical infrastructure posture in a steady state

Figure 1 – Framework Scopes of Interest: Current and Recommended

C. Employing Architecture

The NIST framework focus is the protection of critical infrastructure proper based on a five-stage approach, beginning with breach identification and ending with recovery to steady-state operations. What the framework does *not* contemplate, and therefore does not represent, is the contextualization of the approach within a larger, more comprehensive, and generally accepted, architectural ambit that consists of the following views:

1. Set the boundary/limits of the scope of interest.
2. Develop the semantic structures, meaning, concepts for the scope of interest.
3. Develop the as-designed, design logic for affected systems/automation targets.
4. Develop the as-planned technology required to operate systems/automation targets.
5. Develop the tooling configuration required to operate the as-planned technology components.
6. Operate the instantiation.

The foregoing six (6) views form part of the Zachman Framework for Enterprise Architecture, and inform the manufacture of composite models, while the six (6) verticals, each of which addresses a particular interrogative - what, how, where, who, when and why – inform the engineering of primitive, one-dimensional models. The use of the Zachman Framework as the point of departure for contextualizing the NIST framework is, in the opinion of the writer, critical. Without the application of architectural rigour that the Zachman Framework affords, it will be difficult for organizations to use the NIST framework as-is as no architectural baseline will have been established (a) to contextualize the contents of the NIST framework, and (b) through which critical infrastructure design is subsequently informed.

Murray Rosenthal, CISA, CRISC
Senior Policy Analyst (Security)
Risk Management and Information Security
Strategic Planning and Architecture
Information & Technology Division
City of Toronto
55 John Street, 17th Floor
Toronto, Ontario Canada
M5V 3C6

v: 416.392.8447
f: 416.696.3714
e:mrosent@toronto.ca