Review of NGAC-GOADS,

INCITS Project CS1/2195-D, Rev. 1.3, 11 April 2014

From: Hilary H. Hosmer, President of Data Security Inc. Bedford, MA

Date: June 20, 2014

I have read NGAC-GOADS 2195, now in public review. I glanced at the mathematical sections.

Here are a few points. I hope you find them constructive.

1. The Abstract needs editing. Since this is the only part of the document that most people read, it should be clear and interesting. Except for sentence 1, the abstract is dense and wordy.

   Revised sentences 2 and 3: NGAC's flexible infrastructure controls access to different types of resources by different types of applications and users. It supports different types of policies simultaneously, is scalable, and stays manageable in the face of change.

2. Scope is very good!
   a. Para 2: grammar change: "A wide variety of policy types."
   b. Para 3 and 4 describe Hosmer and Bell's 1990's multipolicy work (see point 7. bibliography expansion recommended)

3. Definitions in 3.1 need some work. For example:
   a. "Access right" includes reference to PIP, not yet defined. I suggest "permission to perform operations on information resources, including data objects and the policy information database."

   b. "Access request" definition is too computer-oriented.
      On behalf of a user, a process provides the information necessary to accomplish a desired operation such as read, write, delete, or add. The user's access rights, the object desired, and the operation wanted are provided as a series of arguments in the request.

3.3 grammar: “keywords that indicates”

4. Basic elements 4.2 need illustrative examples, because their definitions include themselves. For example, user attributes could be clearance level (Top Secret), role (Doctor), limitations (no access after 5 p.m. and before 7 a.m.).

5. Assignment 4.2.2
The English explanation preceding the equations is good. Make it easier to understand the math. Mention the existence of the notation on page 50. Consider including the mathematical names in the explanations. For example:

U = union of sets
“The policy element set PE of all users U, all user attributes UA, all object attributes OA (which includes objects O), and all policy classes PC is defined mathematically as follows:

PE = **U** U UA **U** OA **U** PC

This means that all the users, user attributes, objects and other object attributes and policy classes are in the policy element set and can be used for defining access control policy.

[Question: Aren’t there other parts of a policy in the policy element set besides policy classes? See Hosmer Metapolicies II, NCSC 1992.]

6. How do multiple policies interact? Does each have veto power over the others as in previous versions?

7. The Bibliography at the end has only three references, and omits many of the researchers who have contributed to multiple policies development. This standard is built upon 20 years of work by leading researchers, and we should be proud of it! Expand the bibliography!

Necessary inclusions to the bibliography:

a. Hilary H. Hosmer "The Multipolicy Paradigm," NCSC/NIST, 1992.

[Reason: I originated the multipolicy machine concept in 1990, first presented it at ACSAC 1990 and then introduced the ideas at NIST in 1991. "The Multipolicy Paradigm", a consolidation of two years of work inspired a number of research projects, including NIST's Policy Machine and NGAC.]

b. David Bell "Modeling the Multipolicy Machine" (NSPW 1994),

Appropriate inclusions:

1. Other key multiple policy researchers include: Sushil Jagodia, Pierangelo Samarati, E. Bertino, D. Ferraiolo and the NIST team, and others.

I suggest grouping the authors by category (e.g. access control, multiple policies, NIST), rather than just alphabetical order.

Suggestion to make expansion easy:

2. Pablo Galiasso, who earned his Ph.D. at Tulsa U. in 2001 with a thesis on "A Policy Mediation Architecture for Multi-enterprise Environments" did a thorough literature search which is included in the paper "Policy Mediation for Multi-enterprise Systems" coauthored with Vincent Hu and David Ferraiolo in 2000. Although his bibliography was not included in subsequent Policy Machine or NGAC work, it is very good and would, with permission and some updating from 2000, facilitate expanding the NGAC-GOADS bibliography.