HRAC RFP Submission: Outstanding Issues

Title	**Dropping the requirement for defining a policy object interface**
ID	46
Priority	2
Description	Issue #1 Choosing not to address this requirement results in almost all of the rest of my objections. It seems to me that the goal of the RFP is to create a standard interface for the evaluation of a security policy. Necessitated by that is the standardization of a policy object interface. Please note that I am NOT proposing the standardization of policy CONTENT! Clearly, that would be impossible. However, the interface should be definable, and the capabilities that can be defined/controlled within a policy should be definable. As a result of not defining this policy interface, you've instead had to define a lot of pieces of what ought to be implementation details, and proposed that the industry should standardize on the mechanism for evaluating policy.
Date Issued	1/21/99
Depends on Issues	No dependencies
Pointed by	Kurt Schurenberg
Related Refs	No additional references
To propose a resolution	Bob Blakley
Proposed Resolution	Bob will respond to this issue.

Title	**The lack of a Context Sensitive ACL makes the submission ineffective**
ID	47
Priority	2
Description	Issue 2. The lack of a Context Sensitive ACL makes the submission ineffective. (It's a weakness of the RFP that Context-Sensitive ACL is optional, IMHO.) Context Sensitive ACL is an optional requirement which appears to be unaddressed as a result of the decision to not support the required requirement for policy interface definition. If the submission dealt with objects as objects, then the policy interface could allow decisions based on the contents of the object being evaluated. Since the submission has moved instead to controlling access to named strings, there is no option except to evaluate each attribute of an object which might be sensitive or policy-driving as a separate named resource. This creates more load on a system which appears to be likely to have performance implications already. Imagine a system which allows retrieval of patient records from a variety of "publishers" (like hospitals, clinics, practices, etc.) A policy may allow a user to see any patient record published by a hospital or clinic with which the user is associated, unless the diagnosis of the record has to do with AIDS, mental health, or alcoholism. By it's very nature, the evaluation is done after data has been retrieved (but before it is shown to the user), so the filtering cannot be applied on the front end (by modifying the query, for example). Thus, you must look inside the contents of the object on which policy is being evaluated to find data relevant to the decision being made. The Dynamic attributes do not provide a method for defining this, and since the object itself is not available, there's no way to make decisions based on this. If it's thought that you can define the interface to hand in this "sensitive" data, configured somehow as a security attribute, this means that the policy must be embedded in the code which queries the system for authorization. That would be an expensive and difficult system to maintain.
Date Issued	1/21/99
Depends on Issues	No dependencies
Pointed by	Kurt Schurenberg
Related Refs	No additional references
To propose a resolution	Bob Blakley
Proposed Resolution	This issue is incoherent.

Title	**Use cases for the proposed interfaces**
ID	25
Priority	3
Description	The submission needs use cases to: 1. To see if the proposed design will satisfy most of the cases of the facility use, 2. To show how the proposed facility should be used. It would be nice to do a use case from COAS
Date Issued	9/11/98
Depends on Issues	No dependencies
Pointed by	
Related Refs	No additional references
To propose a resolution	John Barkley and Konstantin
Proposed Resolution	John will review and modify introductory text If by the due time editor does not get updated use cases, they will be taken out of the text.

Title	**ASTM Access Control Matrix security standard**
ID	26
Priority	3
Description	"Has anyone looked at the ASTM standard? It would be most PC to include a reference...if it applies."
Date Issued	10/ 6/98
Depends on Issues	No dependencies
Pointed by	Mary Kratz
Related Refs	E-mail message from Mary Kratz to the submission list on 10/1/98
To propose a resolution	Konstantin
Proposed Resolution	Konstantin will contact Mary Kratz to get a copy for review. ASTM have not published the text yet.