**CCEVS Policy Letter #15**

8 September 2008

SUBJECT: Mandatory Inclusion of Audit Generation Functionality in TOEs

POLICY: Every TOE must provide the capability to generate audit records for all security events associated with security relevant actions whose result depends upon user input, or that are the result of an access decision made by the TOE.

FAU_GEN need not be claimed in cases where there is no decision-making made by the TOE, or where audit generation can be performed in the environment (see EXCEPTIONS, below). Any such cases must be justified.

With respect to auditing of access decisions, the level of detail depends on the specified audit level. At the Basic level of audit, only access failures are auditable. At the Detailed level, all access decisions are auditable.

RATIONALE: The purpose of audit functionality is to detect attempts to gain forbidden access to resources. Because attempts at access and verification of permission involve decision-making, the general rule is that auditing is required at all points at which a decision is being made.

The mandate for audit generation capabilities stems from the presumption that the detection of security events can take place only where those events occur. That is, the part of the TOE (code) that creates the event has the sole ability to be aware that the event has occurred and, therefore the sole ability to create the audit record. This is in contrast to other security functions (audit collection or identity authentication, for example that can conceivably be expected to be performed in the environment).

OBJECTIVE: This need for the audit record generation is based upon the fact that it is imperative that security events are capable of being detected and associated with users that create them. These events can likely be detected only by those portions of the TSF that provide the associated security functionality.

EFFECT: This policy adds only the requirement for audit generation capabilities. These generated audit records must either be stored within the TOE (FAU_STG is also claimed in the ST), or must be off-loaded into the environment. If audit storage and protection is to be provided by the environment, this must be described in the ST under the Assumptions made by the TOE and in the Environment Description (in terms of Objectives for the Environment, and - if present - SFRs for the Environment).



9800 Savage Road, Suite 6757, Ft. Meade, MD 20755-6757
Phone: (410) 854-4458 Fax: (410) 854-6615
E-mail: scheme-comments@missi.ncsc.mil Web: http://www.niap-ccevs.org/cc-scheme

RELATED POLICIES: Policy 13 provides instruction on what services must be included within the scope of an evaluation, based upon the technology type. This policy augments Policy 13 by identifying audit generation as a service reasonably expected in TOEs.

EXCEPTIONS: (1) If a TOE performs no decision-making at all, FAU_GEN need not be claimed. For example, a KVM switch performs no decision-making; it merely transports electrical signals from the selected input connection to the output connection. For this exception to be allowed, its description must be accepted by CCEVS.

(2) There might be a situation wherein security events within the TOE can legitimately be detected in the environment and this remains a possibility that CCEVS is willing to consider. For this exception to be allowed, its description must be accepted by CCEVS and a description of the situation within the ST would have to clearly describe how the TOE environment is expected to fulfill this responsibility so that no security events could occur undetected.

EFFECTIVE DATE: This policy addendum takes effect immediately for all EAPs submitted to CCEVS.

**Original Signed By**

AUDREY M. DALE
Director



9800 Savage Road, Suite 6740, Ft. Meade, MD 20755-6740
Phone: (410) 854-4458 Fax: (410) 854-6615 E-mail: ccevs-comments@missi.ncsc.mil
Web: http://www.niap-ccevs.org/cc-scheme