

requested SSM plan in an electronic format, and any portion of the plan that is claimed to be CBI entitled to protection under CAA section 114(c) or the Trade Secrets Act must be clearly designated in the submission. Moreover, we want to encourage all parties to adopt procedures for providing public access to SSM plans which avoid unnecessary burdens or delays. Therefore, if an owner or operator and a requestor both agree that it would be more expedient or convenient for the requestor to examine the SSM plan (or a portion thereof) at the facility where it is maintained, this approach could be utilized instead of requiring submission of the SSM plan to the permitting authority. This on-site inspection procedure would be most practicable in those instances where the owner or operator has concluded that it is not necessary to redact claimed CBI when the plan is being examined at the facility that maintains it.

We think this approach assures appropriate public access to SSM plans, but dramatically reduces the aggregate expenditure of resources by sources and permitting authorities. We recognize that this approach could result in some additional delay before a member of the public could obtain a copy of the non-confidential portions of an SSM plan. However, we think that requiring routine submission of every SSM plan, without regard for whether any member of the public will ultimately seek access to it, involves a resource burden which is disproportionate to the time which may be saved when a specific plan is actually requested by a member of the public.

As for the concern of some commenters that claimed CBI information might be inadvertently disclosed, we think this is less probable when SSM plans must be submitted only on demand rather than routinely. If a submitter knows that the non-confidential portions of a plan will definitely be disclosed, we believe the submitter will be more likely to do a good job of segregating claimed CBI and preparing to properly substantiate its claim.

Some commenters expressed concern about the Homeland Security implications of public access to SSM plans. It may be that some information in a particular SSM plan could be sensitive from a Homeland Security perspective. In most instances, we think that such sensitive information would also be entitled to confidential treatment under CAA section 114(c). However, we note that the entire Federal government is presently reviewing public access requirements to assure that they are

compatible with Homeland Security, and it is possible that we may in the future propose other changes in public access to SSM plans as part of this important effort.

### 3. Reporting Requirements

During the April 5, 2002, rulemaking concerning revisions to the General Provisions and section 112(j) rules, we received a comment from representatives of the State and local permitting authorities indicating that it would assist them in performing their oversight function if facilities were required to include the number and a description of all malfunctions that occurred during the prior reporting period in the required semiannual report. In response to that comment, we added a new reporting obligation to the language governing periodic SSM reporting in 40 CFR 63.10(d)(5)(i). However, the language we added was not limited to malfunctions and required that the facility report "the number, duration, and a brief description of each startup, shutdown, and malfunction." We later concluded that the inclusion of startups and shutdowns in this reporting requirement was unnecessary and burdensome, and we proposed to delete these events from this provision.

Many commenters supported that proposal. The Sierra Club opposed the deletion of startups and shutdowns from this reporting requirement, arguing that sources might improperly define events as startups and shutdowns. We consider this type of abuse unlikely, and we do not believe in any case that the routine reporting of all startups and shutdowns would be particularly helpful in preventing it.

In some industries, startup and shutdown events are numerous and routine. So long as the provisions of the SSM plan are followed, there does not appear to be any real utility in requiring that each individual startup and shutdown be reported or described. As many commenters noted, in those instances where a startup or shutdown includes actions which do not conform to the SSM plan and the standard is exceeded, the facility is otherwise required to promptly report these deviations from the plan.

Some commenters objected to our retention of the new malfunction reporting requirement. These commenters argue that a requirement to report all malfunctions is duplicative of other requirements, except in those instances where an SSM plan was followed during an event and no excess emissions occurred. We do not agree with these commenters that the

malfunction reporting requirement should be entirely eliminated, but we have concluded that its scope can be narrowed.

With respect to malfunctions, the rule expressly requires that the SSM plan must be revised by the facility if there is an event meeting the characteristics of a malfunction which is not addressed by the plan (40 CFR 63.6(e)(3)(vii)). At the time of proposal, we believed that reporting of all malfunctions is necessary to assure that this requirement is satisfied. However, after reviewing the comments and evaluating this issue in the context of the rule as a whole, we believe that the problem of identifying new kinds of malfunctions which would require revision of the SSM plan is adequately addressed by other provisions in the rule. If a type of malfunction is not addressed by the current SSM plan, we believe that any actions taken during such a malfunction cannot be reasonably construed as actions consistent with the plan and that such actions would otherwise be reportable under § 63.10(d)(5)(i) or § 63.10(d)(5)(ii). We discuss these reporting provisions further below.

However, we also agree with a comment by the Sierra Club that reporting of malfunctions would help permitting authorities determine whether sources are attempting to circumvent the standard by improperly defining events as malfunctions. To prevent this type of potential abuse, we do not think that all malfunctions need to be reported. Rather, we think this problem can be addressed by requiring that the affected source report only those malfunctions which occurred during the reporting period and which caused or may have caused an emission limitation in the relevant standard to be exceeded. Thus, we have decided to retain the requirement that the owner or operator report malfunctions in the periodic report, but to limit its scope to those malfunctions which caused or may have caused an emission limitation in the relevant standard to be exceeded.

Moreover, we stated in the proposal that minor or routine events that do not have a significant impact on the ability of a source to meet the standard need not be classified as a malfunction, addressed by the SSM plan, or included in periodic reports. We think there is no reason to classify an event as a malfunction if it does not cause, or have the potential to cause, the emission limitations in an applicable standard to be exceeded.

A number of commenters requested that we make this policy clear in the regulatory language, rather than only in the preamble. These commenters