UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON. D.C. 20549

DIVISION OF
MARKET REGULATION

June 1, 2001

By Fax at and By Mail

TEMPLATE VERSION

Dear :

In recent months, we have received inquiries seeking clarification on when the ARP desk officers should be notified of systems outages and system changes. Attached is a memorandum providing further guidance on these issues.

Please contact if you have any questions.

Sincerely,

Larry E. Bergmann
Senior Associate Director

TO: SROs and Nasdaq

FROM: Larry E. Bergmann

DATE: June 1, 2001

SUBJECT: Guidance for Systems Outage and System Change Notifications

In recent months, the Automation Review Policy ("ARP") staff has received a number of inquiries seeking clarification on when to notify the ARP desk officers of systems outages and system changes. This memorandum is intended to provide clarification and guidance in these two areas.

1. Systems Outage Notifications.

As explained in the second ARP policy statement,[1] entities covered by ARP should provide ARP staff with immediate notification of significant systems outages ("Systems Outage Notifications"). *See* ARP II at 3 and 7. This memorandum provides guidance regarding when an outage should be considered "significant" and how promptly the outage should be reported to ARP staff.

A. What Constitutes a Significant Outage.

System outages that are significant should be reported to ARP staff. Systems outages are any interruptions or disruptions to trading, information dissemination, clearance, or settlement systems. *See* ARP II at 6. Reportable outages are not limited to breakdowns and system failures, but also include threats or potential threats to operations. The following are non-exclusive examples of situations for which an outage is deemed significant and thus should be reported?

1. Outage resulting in a failure to maintain any service level agreements or constraints;
2. Disruption of normal operations, *e.g.*, switchover to back-up equipment with zero hope of near-term recovery of primary hardware;
3. Loss of use of any system;
4. Loss of transactions;

---

[1] Securities Exchange Act Release No. 29185 (May 9, 1991) [56 FR 22490] ("ARP II"). The first ARP policy statement is Securities Exchange Act Release No. 27445 (November 16, 1989) [54 FR 48703] ("ARP I").

[2] Items 1 – 7 in this list of examples were previously provided to all clearing agencies on June 8, 1994, and to other SROs in a variety of contexts. Items 8 – 10 have been added as a result of more recent experiences with SROs.

5. Outages resulting in excessive back-ups or delays in processing;
6. Loss of ability to disseminate vital information;
7. Outage situation communicated to other external entities;
8. The event was (or will be) reported or referred to the entity's Board of Directors or senior management;
9. The event threatened systems operations even though systems operations were not disrupted; for example, the threat caused the entity to implement a contingency plan;
10. Queuing of data between system components or queuing of messages to or from customers of such duration that a customer's usual and customary service delivery is affected.

Significant outages should be reported immediately even if third parties, natural disasters, or unusual events beyond the control of the reporting entity caused the event. The duration or expected duration of an outage is not determinative of whether the outage is significant, or whether the outage should be reported.

In previous years, outages deemed significant have included a subway fire that caused a power loss and required an entity to switch to full back-up; a cut cable line causing loss of use of systems; brief denial-of-service or other hacker attacks that temporarily disabled systems or caused system slowdowns; and heavy order backlog delays.

Finally, where an entity is uncertain whether an outage is significant, the entity should contact the ARP desk officer. Significant systems outages have the potential to affect market stability, and early detection of possible problems may help us in assessing the potential for harm to investors as well as to the entity itself. *See, e.g.,* Section 11A(a)(1) of the Securities Exchange Act of 1934 ("Exchange Act"); *see also* ARP I (policy issued because of concern regarding the impact that systems failures may have on public investors, broker-dealer risk exposure, and market efficiency).

B. Reporting Outages.

As discussed above, we expect entities to report all significant outages. The length of time that the outage is expected to continue determines when the outage should be reported to ARP staff. If it appears that the outage may extend for thirty (30) minutes or longer, the entity should contact the appropriate ARP staff member immediately. If it appears that the outage will be resolved in less than thirty (30) minutes, the entity should report the outage within a reasonable time after the outage has been resolved. *See* ARP II at 7-8.

Regardless of the duration of the outage, the entity is expected to provide a written description of each significant outage within a reasonable period (within 24 hours) after resolution of the problem. The description should provide details concerning the nature and extent of the problem, including systems affected, effect on the trading community, and the nature of the corrective action. *See* ARP II at 8. The items that

should be reported in each Systems Outage Notification are identified in Attachment A to this memorandum.

2. System Change Notifications.

Entities in the ARP program are also expected to provide advance notice of significant changes to automated systems. *See* ARP II at 1-2; 6-7. System changes include additions, deletions, or other changes to automated trading, information dissemination, clearance, or settlement systems. System changes should be reported to ARP staff on an annual basis (as part of an Annual Report) and an as-needed basis (through System Change Notifications). -*See* ARP II at 3.

A. What Constitutes a Significant System Change.

ARP II provides a non-exclusive list of factors that should be considered in determining whether a system change is significant and should be reported. The list includes a change that: (1) affects existing capacity or security; (2) in itself raises capacity or security issues, even if it does not affect other existing systems; (3) relies upon substantially new or different technology; (4) is designed to provide a new service or function for SRO members or their customers; or (5) otherwise significantly affects the operations of the entity. *See* ARP II at 7.

, The following is a non-exclusive list of examples of system changes that are deemed significant for purposes of ARP: [3]

1. Major systems architectural changes;
2. Reconfigurations of systems that cause a variance greater than five percent (5%) in throughput or storage;
3. Introduction of new business functions or services;
4. Material changes in systems;
5. Changes to external interfaces;
6. Changes that could increase susceptibility to major outages;
7. Changes that could increase risks to data security;
8. The change was (or will be) reported or referred to the entity's Board of Directors or senior management;
9. Changes that may require allocation or use of significant resources (for example, a project that may require 12 or more man-month hours).

As with systems outages, entities should also consider other facts and circumstances regarding each system change in determining whether the change is significant. Entities are encouraged to inform ARP staff of changes that otherwise may not be considered significant in order to keep the Commission informed of system developments at the entity. *See* ARP II at Note 20.

[3] Items 1 – 7 in this list of examples were previously provided to all clearing agencies on June 8, 1994, and to other SROs in a variety of contexts. Items 8 – 9 have been added as a result of more recent experiences with SROs.

System Change Notifications should be made significantly in advance of the planned production date so that the staff can evaluate the adequacy of the capacity estimates and tests, and security measures. The process for advising ARP staff of system changes does not eliminate the need for filing under Section 19(b) when the system change also entails a need for changing an SRO rule. *See* ARP II at 6. A System Change Notification submitted with a rule filing should be a separate document and clearly distinguished as such.

The items that should be reported in each System Change Notification are identified in Attachment B to this memo.

Conclusion

We encourage you to discuss with the ARP staff any questions regarding whether an outage or system change is significant. Since the ARP policy statements were issued, the pace of system changes has significantly increased, and automated systems have far more impact on the markets today than ever before. With this in mind, it is critical to the effectiveness of the ARP program that the ARP desk officers receive timely information regarding significant outages and system changes.

Attachments

Attachment A: Systems Outage Notification Elements.

The following are baseline elements that should be addressed in both written Systems Outage Notifications and in the course of contemporaneous conversations between the entity and ARP staff. You should include as much detail as possible for each element.

1. Identifying Information:
   - o Entity Name
   - o Individual Contact Name(s)
   - o Phone Number(s)

2. Outage Dateffime[sic] Information.

3. Location-specific Information (source and location of problem).

4. System Involved:
   - o System Application Name
   - o Relevant Release, Version, Platform Information

5. Nature of Outage.

6. Suspected Cause of Outage.

7. Brief System Profile:
   - o Batch/Online
   - o Other Characteristics
   - o Functional Synopsis

8. Contingencies Implemented.

9. Effects:
   - o Other Internal Systems
   - o Interaction With Other Markets/Exchanges/Clearing Corporations/SIAC/Customers
   - o Member Firms

10. Established or Projected Delays.

11. Other Businessffrade[sic]-level Impacts.

12. Relation to Any Prior Outage.

13. Corrective Resolution
    - Date/Time Information
    - Resolution Specifics – steps taken and impact of each step

14. Total Downtime.

15. Follow-up/Future Preventative Actions.

Attachment B: System Change Notification Elements.

The following are elements that should be addressed in all System Change Notifications. You should include as much detail as possible for each element.

1. Brief high-level description of the functionality and configuration of the affected system.

2. Description of systems development process.

3. Relationship to other systems: narrative and schematic.

4. Schedule for implementing the system change.

5. Capacity effects ofthe change.

6. Outline and description of test plans with schedules and timeframes.

7. As soon as such results and data are available, description of test results (capacity, stress, performance) with supporting graphical data and statistics.

8. Contingency protocols, *i.e.,* fallback options and disaster recovery measures.

9. Vulnerability assessments, security measures.

10. Has a Rule 19b-4 filing been made in connection with this system change notification?