The September 11 attacks severely disrupted U.S. financial markets, resulting in the longest closure of the stock markets since the 1930s and severe settlement difficulties in the government securities market. While exchange and clearing organization facilities were largely undamaged, critical broker–dealers and bank participants had facilities and telecommunications connections damaged or destroyed. These firms and infrastructure providers made heroic and sometimes ad hoc and innovative efforts to restore operations. However, the attacks revealed that many of these organizations’ business continuity plans (BCP) had not been designed to address wide-scale events.

GAO reviewed 15 organizations that perform trading or clearing and found that since the attacks, these organizations had improved their physical and information security measures and BCPs to reduce the risk of disruption from future attacks. However, many of the organizations still had limitations in their preparedness that increased their risk of being disrupted. For example, 9 organizations had not developed BCP procedures to ensure that staff capable of conducting their critical operations would be available if an attack incapacitated personnel at their primary sites. Ten were also at greater risk for being disrupted by wide-scale events because 4 organizations had no backup facilities and 6 had facilities located between 2 to 10 miles from their primary sites.

The financial regulators have begun to jointly develop recovery goals and business continuity practices for organizations important for clearing; however, regulatory efforts to improve preparedness and oversight of market participants’ risk reduction efforts.

What GAO Found
The September 11 attacks severely disrupted U.S. financial markets, resulting in the longest closure of the stock markets since the 1930s and severe settlement difficulties in the government securities market. While exchange and clearing organization facilities were largely undamaged, critical broker–dealers and bank participants had facilities and telecommunications connections damaged or destroyed. These firms and infrastructure providers made heroic and sometimes ad hoc and innovative efforts to restore operations. However, the attacks revealed that many of these organizations’ business continuity plans (BCP) had not been designed to address wide-scale events.

GAO reviewed 15 organizations that perform trading or clearing and found that since the attacks, these organizations had improved their physical and information security measures and BCPs to reduce the risk of disruption from future attacks. However, many of the organizations still had limitations in their preparedness that increased their risk of being disrupted. For example, 9 organizations had not developed BCP procedures to ensure that staff capable of conducting their critical operations would be available if an attack incapacitated personnel at their primary sites. Ten were also at greater risk for being disrupted by wide-scale events because 4 organizations had no backup facilities and 6 had facilities located between 2 to 10 miles from their primary sites.

The financial regulators have begun to jointly develop recovery goals and business continuity practices for organizations important for clearing; however, regulatory efforts to improve preparedness and oversight of market participants’ risk reduction efforts.

What GAO Recommends
GAO recommends that the Chairman, SEC, work with industry to
- develop goals and strategies to resume trading in securities markets,
- determine sound business continuity practices needed to meet these goals,
- identify organizations critical to market operations and ensure they implement sound business continuity practices, and
- test strategies to resume trading.

In addition, the report contains recommendations to improve SEC’s oversight of information technology issues.