Solicited Comments to the Draft Agency White Paper on the Sound Practices to Strengthen the Resilience of the U.S. Financial U.S. System

Fed Docket # R-1128
OCC Docket #02-13
SEC Release #34-46432; File # S7-32-02

October 21, 2002

By Peter Vinella
PVA International, Inc

To Whom It May Concern:

Regulators have often played key roles at critical times in preserving the integrity of the U.S. financial system from a variety of structural vulnerabilities. Regulators, by definition, must protect the essential strengths of the U.S. financial system, its unparalleled transparency, liquidity, depth, safety, solvency, and freedom.

The recent agency white paper, however, clearly demonstrates that governmental and industry regulators have failed -- and continue to fail -- to provide the necessary leadership to establish effective business continuity planning (BCP) in the financial services industry. While some in the industry have argued that no additional regulations are necessary, successful coordination of industry-wide initiatives, such as Y2K, require a high level of regulatory supervision and leadership.

The report recommends that regulators act as removed, inert observers, whose sole duty is to review the mechanics of private sector business continuity planning. There is no mention of the regulators' fundamental responsibility to actively safeguard the U.S. financial system.

The report, in fact, has very little to do with the new realities of the threat of directed terrorist attacks. The authors avoid a discussion of the possibility of a directed terrorist attack altogether. Instead, they focus entirely on the mundane aspects of BCP: the controlled recovery of technical functions in the event of unspecified outages. Many of these stated private-sector BCP goals should already be in place, since they constitute general good-business practice that applies equally to natural or man-made disruptions. The authors even refrain from suggesting, much less mandating, specific private-sector BCP capabilities, or when such capabilities must be in place.

The report also falls far short of the recommendations of the President's Committee for Critical Infrastructure Protection (PCCIP) report released in 1997 in both its assessment of the current situation and its recommendations to mitigate the numerous obvious vulnerabilities in the U.S. financial system. It offers neither long-term solutions nor ways to meet the near-term threat.

The report stresses the positive aspects of the post-September 11th recovery effort. It suggests that the industry has BCP well in hand, that no new regulations are required at this time, and that there is no need for the special involvement of regulators. It also implies that industry BCP performed so well during the days immediately after September 11, that the authors needed only to investigate what worked during the recovery that followed, not lessons regarding how close the industry came to a major stoppage.

The authors, however, ignore the key responsibility of financial regulatory institutions: to maintain the integrity of the U.S. financial system. The report, which was based on numerous interviews with industry participants, presents the self-serving point of view of the private sector: that industry BCP should guarantee only that all obligations owed to individual firms can be met.

Sadly, the report does not even mention the need to maintain public trust in the system, which is paramount in preserving the value and strength of the U.S. financial system.

The authors also ignore what we have learned about potential vulnerabilities to a terrorist attack and how to mitigate them. They miss the most important and successful aspect of the post-September recovery: the ad-hoc crisis management command and control efforts of governmental, industry, and public utility representatives. They also disregard the common lesson of the October 1987 stock market crash and the September 11th attack. It was not industry foresight and preparedness that prevented a major liquidity crisis from occurring, but quick and decisive action by the Fed.

Rather than considering the U.S. financial system in its entirety, the report mysteriously limits its attention to what it terms critical markets: Fed funds, foreign exchange, commercial paper, U.S. government securities, corporate bonds, and mortgage-backed securities. The report ignores such critical markets as the U.S. listed and OTC equity and derivative markets.

In justifying this limitation, the report defines critical markets as those that provide means for banks, securities firms, and other financial institutions to adjust the key cash and securities positions and those of the customers in order to manage significant liquidity, market, and other risks to their organizations.

While the above markets are unquestionably important in maintaining adequate liquidity in the system, this limitation flies in the face of nearly every important industry report since the October 1987 crash, which has stressed important vulnerabilities due to the integration of the global financial markets. Quite simply, the report addresses only those markets which caused the largest players in the private sector the most liquidity problems following the attack and ignores the inherent and systemic problems of a free market economy.

Additionally, the report concentrates only on business functions and processes associated with critical processes, which it defines as cash and securities settlement. However, due to technology and business practice innovation, settlement processes are no longer separable and isolated but integrated fully with nearly all industry business activities. It provides no concrete definition of what exactly these critical processes are. In fact, the report leaves it up to each individual firm to determine these activities for themselves and, incredibly, how best to back them up. Clearly, this does little to protect an individual firm much less the U.S. financial system from an industry-wide crisis.

The report does not identify what types of private-sector firms represent significant risk to the U.S. financial system. Moreover, it provides only a vague reference to what type of firms these may be. The report does not analyze the industry impact if one or more of these institutions should fail. Clearly, the technical problems at just one clearing bank, BoNY, nearly brought the U.S. government securities and mortgage-backed securities market down for weeks.

The reports focuses attention on well-known financial institutions and industry utilities but ignores other potentially significant vulnerabilities, which can have an enormous impact on the U.S. financial system and the country as a whole. There is no mention, for instance, of vulnerable strategic financial services targets such as the USAA, a member-owned, Fortune 500, financial services association serving active U.S. military personnel and reservists worldwide. As USAA heavily relies on Internet technologies, placing false information or infecting their site could cause a major disruption to the U.S. Armed Forces for weeks or even months. This is especially concerning given the extent of our presence in Afghanistan and the growing conflict with Iraq.

The report's recommendations were equally disappointing.

Like most industry responses since September 11th, the report emphasizes the need for technology redundancy and geographic diversification. These are shortsighted, expensive solutions that only address problems associated with collateral damage from a major disruption, not a directed attack. They cannot be viewed as true business continuity solutions because they can't be relied upon to maintain true business value.

For example, the report recommends locating redundant operational and technical staff at remote backup sites to reduce exposure to one geographic location. This will require that firms acquire and operate multiple sites at less than 100 percent capacity. This solution will entail substantial upfront costs and will have a permanent impact on each firm's bottom line.

While the report suggests that these costs can be mitigated through automation and the cross training of staff in multiple disciplines, it ignores the fact that traders and portfolio managers are the only employees allowed by regulation to commit a firm's capital. Although it may be possible to move back-office staff out of metropolitan New York, there is little chance of locating senior business managers to remote secondary locations in South Dakota.

The report also ignores the fact that business in the financial industry is conducted by and between people. Although automated processing may lessen the industry's dependency on people, the financial system will grind to a halt if enough critical people are incapacitated, or worse, killed. This was proven conclusively on September 11. Although increased automated processes may reduce human risk, they increase technology risk proportionately. Risk is simply transferred or transformed, not entirely eliminated. This situation is analogous to pilots and warplanes. While the cost of the aircraft may be quite high, the military is most concerned with the loss of a pilot, which is the most valuable and least replaceable asset.

The report suggests that remote locations can be manned by experienced out-of-region staff, which can be cross-trained to perform numerous duties. It ignores the fact that it is almost impossible to find trained staff out of the major U.S. financial centers. The industry's current operational staff, moreover, does not have extra cycles to perform numerous concurrent duties. This is especially true in times of crisis.

The report's recommendations for technology redundancy and geographic diversification address only collateral damage, not a directed attack. If Al Qaida could hijack several airliners and fly them simultaneously into both the World Trade Center towers and the Pentagon, a terrorist attack could easily target a financial institution's primary and secondary site.

Other recommendations contained in the report are equally flawed. The report stresses the use of alternative communication, but it does not provide any insight into what form this should take. On September 11th, both traditional and cellular telephone service was significantly disrupted. Moreover, dedicated voice and data communications lines from both AT&T and Verizon, including high-speed Internet access, were destroyed. While ConEd, New York City's principal energy utility, offers alternative local phone service, the physical copper and fiber entering specific buildings and running under the streets of New York represents a significant single point of failure and provides the only practical, cost effective means of telecommunication at this time.

The report calls for extremely ambitious and unrealistic recovery times for critical industry services -- in some cases, as short as four hours and less. Clearly, this was impossible on September 11th given the extent of physical and psychological damage. Reopening of the markets before the participants were adequately prepared could have been devastating to the U.S. financial system if things had not gone as smoothly as they did. A more rational approach would be to accept the reality that we cannot foresee all possible threats. Instead of advocating a rapid recovery of critical services, we need to advocate an orderly recovery. There may be situations where the most prudent course of action is to close the markets rather than try to recover before all the necessary safeguards are in place.

The report correctly points out the weaknesses of industry-wide testing and business continuity planning in general. It also points out the difficulty of performing these tests at individual sites and on an industry-wide basis. But the authors make the ludicrous suggestion that the best way to overcome this problem is to perform a series of limited, staged tests until industry-wide end-to-end tests could be organized.

The report makes recommendations that would represent fundamental changes to core industry operations without taking into account their practicality. The cost and time required to build and operate redundant, hot backup facilities, complete with the necessary redundant operations and redundant communications between primary and secondary sites, would be prohibitive.

The amount of business reengineering necessary to meet the recovery and resumption times stated in the report would require an initiative comparable only to the industry's aborted effort to move to T+1 settlement. The cost of that move was estimated at $8 billion and would take up to five years to implement.

The report does not provide a roadmap on how this enormous project would be accomplished. The report naively argues that this project will be completed because the private sector is committed to creating business continuity plans that will improve the resilience of the U.S. financial system. Protecting the U.S. financial system, however, is the role of the regulators, not private-sector firms who should be concerned with safeguarding their franchise and preserving shareholder value.

Conclusion

The industry's existing business continuity planning is woefully inadequate to meet the threats of the 21st Century. This report does little or nothing to change this fact. While there seems little doubt that terrorists are targeting the U.S. financial system and future attacks will likely occur, the lack of leadership from the regulators as demonstrated in this whitepaper is almost deafening.

To be sure, there have been numerous distractions since September 11. The bear market, a fragile U.S. economy, accounting scandals, and high-profile bankruptcies all have taken the spotlight away from BCP. And yet, sound BCP is just as important to building long-term confidence in the U.S. financial system as sound accounting practices.

Regulators and the private sector need to quickly address the following essential issues:

1. Preventing a terrorist attack from occurring. The industry must adopt the same attitude towards the threat of terrorism as it does to crime and theft. This requires a fundamental shift in the industry's mindset, which will lead to an equally fundamental rearchitecting of its core business practices and processes. Given the industry's primal fear of both of these requirements, this will only come about through the strong and determined leadership and pressure from governmental regulators

2. Lessening the impact from terrorist attack: While some of the suggestions put forth by regulators and the private sector address physical, collateral damage, we need to consider terrorism in a bigger, long-term perspective. This effort should take into account the full context of the U.S. economy and U.S. financial system. Technology redundancy and geographic diversification are simply not enough

3. Meet the near-term threat: Any meaningful measures to prevent future attacks and lessen their impact will take considerable time and money to formulate and implement. In the meantime, the U.S. financial system is vulnerable -- arguably more vulnerable now than prior to September 11th. Accepting this reality, we need to quickly develop and deploy a cohesive strategy to effectively deal with events like September 11th, ones that do not

require significant time and monetary investments. We need to formalize the informal emergency command and control mechanisms that were erected in the hours after the September 11th attack, and which were largely responsible for getting the markets open in a relatively rapid and orderly way.

What is urgently missing is vision and leadership. Instead of simply thinking in terms of collateral damage, we must start to think in terms of attacks targeted specifically at crippling the U.S. financial system. While the industry has a right to be proud of its response immediately following the attack, the attack did not target the U.S. financial system, but only the World Trade Centers, a mere icon of American power. Critical industry utilities such as payment systems, exchanges, depositories were able to quickly recover because they were not targeted and received only collateral, albeit heavy, damage. The industry recovered in spite of the lack of sound BCP and security, not because of it. Today we are no more prepared to face a near-term crisis than we were on September 11th.

In the face of new terrorist threats, we must all recognize that substantive regulations are needed to protect the integrity of the U.S. financial system and the trust placed in it. This is not a free market issue. It is simply accepting the reality that in times of a major crisis, significant controls and coordination are needed to protect the system, not free markets.

While we are highly critical of the interagency report, our comments are not meant to be a general indictment of all industry regulators. PVA has been involved in several regulatory audits and, in every case, the regulators have been highly skilled, dedicated professionals who diligently carried out their assignments, often in difficult situations. Moreover, in many occasions in the past, the authors of the interagency report, the Federal Reserve Bank, the Securities and Exchange Commission, and the Office of the Comptroller of the Currency, have provided important leadership on numerous issues, notably, risk management. Hopefully, these prestigious agencies will reexamine the work contained in this interagency report and put forth a document more in line with their normally high standards.

As regulators, however, the authors of this report have forsaken their solemn duty to protect the public's interests in favor of pleasing the industry that they are charged with regulating. The report should be simply discarded because it is impractical, lacking in substance, soft on the industry, and provides no value in safeguarding the U.S. financial system from terrorist attack.