

Safe, Secure, Setting New

FEBRUARY 2004



Dear Customers:

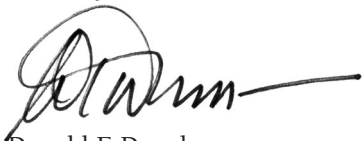
I am pleased to share with you this report on our efforts at DTCC to strengthen our business continuity plans and resources.

We have been working vigorously for several years now to upgrade and fortify our business continuity plans and to implement centers for data processing and operations that are widely dispersed geographically. As I know many of you have done, we have worked especially hard to increase employee safety and security, and to disperse our staff more broadly so that our “knowledge capital” isn’t always in one place. We have done the same at the executive level, while also establishing new crisis command and control processes. We have significantly improved the resiliency of our processes to store and preserve your data, and, as you know, we have been testing to ensure connectivity between your primary and back-up sites and all of our locations.

Given the interdependencies that are so characteristic of our industry, we did not do and could not have done this alone. It was a team effort involving the contributions and collaborative efforts of our own suppliers and other technology companies, of industry groups and individual industry members. It likewise involved consultation with regulatory agency staff and others in government to make sure that the appropriate standards were developed and applied. Together we have dramatically improved the security of the industry’s core clearance and settlement processes.

Let me thank all who contributed to this effort. Let me invite you to offer comments and suggestions. And let me assure you that we will continue to focus on ensuring the safety and resiliency of the industry’s infrastructure.

Sincerely,

A handwritten signature in black ink, appearing to read "Donahue", with a long horizontal flourish extending to the right.

Donald F. Donahue
Chief Operating Officer
The Depository Trust & Clearing Corporation

Safe, Secure, Setting New Standards

A Report to the Industry on Business Continuity Planning

TABLE OF CONTENTS

Executive Summary5

Overview: challenges and responses

- The overriding industry challenge.....7
- The DTCC challenge7
- The DTCC experience: testing plans and validating assumptions.....8

Implementing, advocating and redefining business continuity best practices on multiple fronts

1. Protecting People and Sustaining Business Operations

- Staff decentralization.....11
- Management dispersal and rotation.....11
- Communications.....12
- Priority phone service and emergency access.....12
- Employee safety12
- Physical security12

2. Ensuring Certainty of Data and Systems

- Create multiple, geographically dispersed facilities to ensure system redundancy and data safekeeping

 - Geographically dispersed back-up facilities13
 - Redundant functionality13
 - Two-hour recovery13
 - Moving higher volumes of data over longer distances.....14
 - Assembling high-end, highly responsive data storage systems14

- Sustain a resilient communications network and telecom system

 - The SMART backbone14
 - The SMART role in business continuity15
 - Protecting telecommunications15
 - Expanding the network15
 - Remote command and control.....15
 - Expanded back-up resources for clearing services16
 - Managing cyber-risk vulnerabilities.....16

3. Managing Through a Crisis

- Strengthen DTCC's continuity and control process

 - Executive command team.....17

First-response action teams	17
Core business continuity command groups	17
Crisis command center	18
4. Keeping Customers and Regulators Informed	
Instill confidence during a crisis by providing customers, markets and regulatory authorities the information necessary to assess the situation and make decisions	
Crisis communication.....	18
Communicating with customers.....	18
5. An Operational Risk Management Program Supports Business Continuity Objectives	
Managing operational risk on a daily basis	19
6. Testing Business Continuity Plans	
Conduct rigorous, regular testing of DTCC’s continuity plans and contingencies	
DTCC testing	19
Work with customers to strengthen their business continuity plans and infrastructures	
Ensuring connectivity	20
Connectivity testing	20
Customer recovery planning	20
7. Business Continuity – “Release 3.0”	
Addressing our dependence on cyberspace	21
Addressing our interdependencies.....	22
Straight-through processing.....	22
Coordinating between public and private sectors	23
Coordinating across borders	24

Executive Summary

Since the events of September 11, 2001, the need to protect the global financial system has brought heightened attention to business continuity planning, both in the United States and in markets worldwide. The need is particularly acute for The Depository Trust & Clearing Corporation (DTCC), the largest post-trade financial services infrastructure company in the world. Safeguarding DTCC's ability to support its critical clearing, settlement and asset servicing roles, as well as the highly specialized knowledge of its employees, is acknowledged by the industry and regulators alike to be essential to sustaining the safety and soundness of U.S. financial markets.

Contingency and continuity planning goes back many years at DTCC. Over the past two years, however, DTCC has moved aggressively — as have other companies in the industry — to upgrade its continuity plans and expand its resources in order to strengthen the resiliency of its business operations against the possibility of wide-scale disruption. DTCC continues to be a leader in the securities industry in the efficiency and effectiveness of its business continuity planning and facilities. DTCC's own resiliency, however, is only part of the story. The resiliency of DTCC's industry partners and participants, and of key infrastructures on which all of us rely, is equally important to assuring the ability of the financial markets to continue in the face of extreme events. Recognizing this, we believe it is important to share DTCC's experience and the practical knowledge it has gained from the past two years to encourage wider and more informed discussion and focus on business continuity planning throughout the industry.

The purpose of this report is to contribute to and continue that dialogue by reviewing how DTCC has approached various business continuity issues, what we have learned about them, and how we have modified our plans through these experiences. We hope that this will help our participants and others in the market in their own thinking about these problems. Specifically, this report seeks to:

- Spell out the challenges we anticipate and plan for at DTCC;
- Discuss the reasons we have taken a leadership role in business continuity planning;
- Document the steps DTCC has taken so far to help ensure safety and soundness in U.S. financial markets;
- Assure the financial services industry and government agencies that we intend to maintain our leadership role;
- Alert our customers and participants that we will continue to conduct planning exercises and connectivity tests, and that network changes we are planning to ensure greater centralized control and resiliency may require their participation; and
- Encourage more discussion about continuity planning as a way to help advance the further development of industry best practices.

Building on our existing continuity plans and drawing on our experience and that of the industry during 9/11 and the 2003 blackout in the Midwest and Northeast, we have developed — and tested — action plans for each of the key challenges facing DTCC. We now have plans and resources in place to:

- Achieve recovery, even in the most dire circumstances, within the two-hour window mandated by government agencies, with faster recovery the objective in less extreme situations.
- Increase employee safety and disperse staff across geographically diverse operating facilities in accordance with the recommendations of an interagency government paper.
- Operate multiple back-up data centers linked by our highly resilient network technology.
- Provide tighter emergency command and out-of-region operating control.
- Utilize new technology we developed in conjunction with partners to provide high-volume, high-speed, asynchronous data transfer over distances of 1,000 miles or more.
- Reinforce our processes that mitigate marketplace, operational and cyber-attack risks.
- Test our own continuity plan readiness and connectivity on a regular basis, ensuring that our customers can connect to our primary, remote and alternate sites, and that we can connect to theirs.
- Communicate on an emergency basis with the market, our customers and government agency decision-makers.
- Evaluate, test and utilize best business continuity and resiliency practices.

There are, of course, limits to the information about our plans and facilities that we can share with the public. In fact, some of the information and discussion in this report has been purposely cloaked to maintain security. But we are confident the report can achieve its purpose without disclosing any information that would compromise the security of DTCC's employees, plans or facilities — or those of any other industry participant.

This report is also available on our Web site, www.dtcc.com. Additional copies may be obtained by e-mailing info@dtcc.com or by calling Ms. Lorna Helwig at 212 855-4837. Questions, comments or queries should be directed to Messrs. George Perretti, DTCC Vice President, Corporate Infrastructure Contingency Planning, at 212 855-8176 or gperretti@dtcc.com; or Ken Wright, DTCC Manager, at 212 855-1368 or kwright@dtcc.com. Additional contacts for various specific elements of DTCC's contingency planning are listed in the appropriate sections of this report.

Overview: challenges and responses

THE OVERRIDING INDUSTRY CHALLENGE

One of the most critical challenges facing the global financial services industry is to ensure rock-solid resiliency and sufficient redundancy in the industry's infrastructures to guarantee the continuity of clearance, settlement and asset servicing in the event of a disaster or widespread disruption affecting one or more critical financial markets. In the aftermath of 9/11, for example, the collapse of communication links in sections of New York City impacted a key services provider to the U.S. government securities markets, causing a multibillion-dollar clearing backlog. That, in turn, resulted in severe, although temporary, liquidity problems for a number of market participants. The interdependent nature of financial markets means that, without sufficient resiliency to withstand disruptions, there could be systemic repercussions reverberating across critical market structures — and hence the markets themselves.

In response to this profound systemic issue, U.S. financial regulatory authorities issued an *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*¹ in 2003. The paper identifies three business continuity objectives that have special importance for all financial firms. They are:

1. Rapid recovery and timely resumption of *critical operations* following a wide-scale disruption;
2. Rapid recovery and timely resumption of critical operations following the loss or inaccessibility of *staff* in at least one major operating location; and
3. A high level of confidence, through ongoing use or robust testing, that *critical internal and external continuity arrangements are effective* and compatible.

Papers and documents on business continuity released by other authorities — both regulators and industry groups such as the Group of Thirty (G30)² — all agree on these key objectives.

THE DTCC CHALLENGE

Just how rapid an organization's "recovery and timely resumption of critical operations" should be necessarily depends on the role the organization plays in the financial services industry. For core clearing and settlement organizations such as DTCC, there is general agreement among regulators and industry participants (at least within the United States) that the goal for "within-the-business-day" recovery and timely resumption of critical operations should be no more than two hours from the time of dislocation. DTCC's contingency plans are geared to achieving such a rapid recovery even in the most dire circumstances, with faster recovery the objective in less extreme situations.

DTCC has accepted the challenge of meeting this very rigorous standard for recovery because, as the largest post-trade financial services infrastructure organization in the world, we have a central role in the functioning of the capital markets. Through its subsidiaries DTCC provides clearing, settlement and information services

for virtually all trades in U.S. markets, including trades in equities; corporate, municipal and government bonds; mortgage-backed securities; and the broad array of money market instruments. In 2003, DTCC's subsidiaries cleared or settled transactions valued at USD 923 trillion. In other words, DTCC settles securities transactions roughly the equivalent of the entire U.S. gross domestic product every three days. On average, DTCC's clearing corporation clears 18.9 million equity "sides" a day with a value of more than USD 325 billion. DTCC's depository maintains custody of 2.2 million securities issues, including instruments issued by companies and governments in more than 100 different countries.

An extended delay in carrying out these activities could create operational, financial and structural problems for market participants that would readily spill over into the markets themselves. For example, since DTCC's clearing subsidiaries take on counterparty credit risk in the clearing process for many securities trades, they assume trillions of dollars worth of credit risk on behalf of their participants each day. A failure of clearing corporation operations would, at minimum, introduce unprecedented uncertainty into the markets, if not forcing them to temporarily suspend operations. In the same way, a failure in the data processing or communications systems that DTCC's depository subsidiary uses to settle trades could leave millions of market transactions uncompleted, sowing confusion among market participants and stretching intra-day credit facilities. Events of this magnitude could severely impact investor confidence and, in view of the interdependencies of the world's financial systems, have implications globally. DTCC has no choice but to ensure that its systems and operations meet the highest standards of resiliency.

THE DTCC EXPERIENCE: TESTING PLANS AND VALIDATING ASSUMPTIONS

Along with many other financial services companies, DTCC brings hard-won experience to continuity planning. At DTCC, continuity planning has always been an integral part of our business culture. For more than a decade, DTCC has had in place back-up data processing operations providing for multi-center control of data processing operations and the synchronous replication of critical participant data to multiple sites. For more than a decade, each of the company's operating units has been required to draw up detailed recovery plans and test them regularly. These are some of the key reasons DTCC succeeded in keeping all of its critical services fully operational on 9/11 and in the week that followed, allowing the company to settle outstanding transactions valued at more than USD 1.8 trillion.

The events of September 11th, however, made clear to us and to all in the financial services industry that we were operating under a new paradigm. No longer could we simply plan to maintain business continuity in the face of localized problems such as a severe storm, a fire or a flood. We now had to plan for previously unthinkable or unimaginable scenarios with potential repercussions across an entire region or financial market — or beyond.

Within two weeks of 9/11, DTCC had already begun a rigorous review of its disaster recovery and business continuity plans in order to identify strengths and weaknesses in the context of this new understanding of business continuity and to build on the experience gained. In addition to examining our actions and responses, we

assessed which continuity systems and operating procedures worked well and which did not, the kinds of problems our staff encountered, the various challenges our customers had to cope with, the banking and payment issues that emerged, and the points of vulnerability, such as communications, that became apparent across the market.³ While this analysis identified what had been learned from the actual experiences of the days following the September 11th attacks, its primary focus was on evaluating whether the security and business continuity plans we then had in place would be sufficient to address those new potential vulnerabilities and threats that could play a role in future disruptions. The results of this analysis, and the steps DTCC has taken in response to issues it identified, have been in part shared with the industry over the past two years, and are further described throughout this paper.

Subsequent experience gained in the power blackout of August 14-15, 2003, the most severe in U.S. history, also proved valuable—and affirmed some of the conclusions we had drawn in our immediate post-9/11 analysis. In fact, the blackout afforded a good test of DTCC's new contingency procedures. Again, DTCC remained fully operational, handling normal clearing, settlement and asset servicing activities. We transferred lead responsibility for business operations to one of the company's remote operating locations, while the command center in another of the company's remote facilities—unaffected by the blackout—stepped in to manage data processing operations. As it routinely does in such emergencies, DTCC also began contacting its customers to make sure they would be capable of conducting settlement, while company executives consulted throughout the night with industry, regulatory and government organizations to ensure that preparations were complete to permit smooth clearing and settlement operations on day two of the blackout. Additionally, to reassure the financial markets and its customers in the United States and abroad, DTCC put out a public statement that settlement of securities transactions would be completed as usual.

DTCC is also convinced that a key part of the industry's overall response to the business continuity issue is the pressing need to streamline and accelerate business procedures. The less convoluted and more direct industry processes are, the easier they are to maintain under difficult circumstances and the more quickly they can be restarted if stopped. This is a key reason—in addition to the greater efficiency we achieve—that we work to apply straight-through processing (STP) wherever we can.

For example, the implementation of real-time trade reporting from the major equity marketplaces and the Real-Time Trade Matching (RTTM) service for fixed-income securities allow us to capture and record data on trades as they take place, rather than minutes or even hours later. The capture and movement of the data to our systems on a straight-through basis minimizes the likelihood of a data loss.

Had RTTM been in place on 9/11, for example, it would have been much easier for firms evacuated from their offices to recover trading records and avoid the snowballing confusion about inventory positions and the status of trades that followed this catastrophic event. Meeting the challenge of business continuity includes placing a high priority on industry STP initiatives.

Over the last few years, DTCC has developed and implemented action plans to deal with the challenges

noted above. We completed and implemented some of the planning initiatives well ahead of industry and government timetables. Others, while operational, are undergoing additional development. In our role as a leader in business continuity planning, we continue to look for and try to cull best practices from throughout our own industry and, where applicable, other industries.

Implementing, advocating and redefining business continuity best practices on multiple fronts

1. PROTECTING PEOPLE AND SUSTAINING BUSINESS OPERATIONS

DTCC shares the view of many industry leaders that concern for the safety and security of the people who work in the financial services industry must be the number-one priority. The continued ability of the industry to meet the financial needs of investors in the United States and around the globe is critically dependent on its people, and DTCC's ability to help the industry meet those needs is critically dependent on DTCC's employees. Consequently, DTCC regards the safety and security of its employees as the highest-priority objective of its infrastructure protection efforts. Without our staff, we cannot deliver the resiliency and assured continuity of business operations that the industry and investors everywhere expect. We have reinforced emergency procedures at each of DTCC's locations and practice them on an ongoing basis. They are described in the sections that follow. In addition, to gain knowledge of best practices, we continue to examine the practices and operating procedures of other companies in the industry.

STAFF DECENTRALIZATION — As a way to avoid concentrating the critical expertise or “knowledge capital” of our staff at one location, we have decentralized DTCC's staff more than ever before. We now provide daily operations support on a regular basis from multiple locations. Similarly, we have redistributed technology staff and other key operating personnel. In addition, we have relocated a portion of DTCC's relationship management staff away from headquarters to ensure an ongoing ability to interact with customers in the event of an emergency. To further decentralize staff, we expect to begin the implementation of an out-of-region center for business operations by year-end 2004 and to have it fully staffed and operational by year-end 2005. This involves relocating a number of our employees and mirrors the thinking in the federal government's inter-agency white paper, which requires stronger measures to ensure recovery from a widespread regional disaster. The interagency paper says that “core clearing and settlement organizations...whose back-up sites depend primarily on the same labor pool as the primary site should address the risk that a wide-scale disruption could impact *either or both of the sites and their labor pools* [emphasis added]. Such organizations should establish even more distant back-up arrangements...” The staff decentralization efforts we now have under way already address this concern, and the further dispersal of our staff over the next 18 months to the new out-of-region business operations center should make this a moot point for DTCC.

MANAGEMENT DISPERSAL AND ROTATION — DTCC has established an officer rotation program which mandates that key executives from the major operational and support areas do not all work at the same site on any given day. For example, the members of DTCC's senior executive team are never all to be at the same work location at the same time. Avoiding having our entire executive team in one place simultaneously ensures that a cadre of officers capable of continuing all key operational functions is always available to run the company, even in the event of a catastrophic event at any particular site. We maintain an “officer rotation” database to keep track of which officers are at which sites on which days, so that key management staff has access to this information as needed.

COMMUNICATIONS are critical in an emergency — particularly staff communications. We deploy various means of staying in touch with staff during emergencies. These include public address systems at all locations which permit DTCC senior executives to speak directly to the staff in emergency situations, an employee telephone hot line with up-to-the-minute information, a telephone service that allows us to deliver messages to specific groups of employees, the capability to broadcast e-mail to employees and message centers on DTCC's Internet sites. Employee contact information and responsibilities for calling employees in particular operating units are also embedded in "calling trees." Every DTCC unit must maintain and periodically update its calling trees.

PRIORITY PHONE SERVICE AND EMERGENCY ACCESS — Twice a year senior managers receive wallet cards with updated contact numbers (home phone, cell phone and pager numbers) for the top levels of management and other critical contacts. Critical employees are also equipped with cell phones, pagers, Blackberry communicators and other devices. In addition, DTCC has arranged to have senior managers covered under the U.S. government's Government Emergency Telecommunications Service (the "GETS" program), giving them access to the U.S. government's emergency telephone priority service. The City of New York also has recently implemented a pilot of its Corporate Emergency Access System (the "CEAS" program), which permits certain personnel access to areas that have been restricted in the event of an emergency; DTCC senior executives and critical staff also participate in the CEAS program.

EMPLOYEE SAFETY is DTCC's primary focus in an emergency, and a sweeping program has been put in place to address training and procedures for employees. The company's emergency response plan also includes evacuation procedures and points of assembly for each operating facility.

- DTCC's staff now undergo more extensive formal safety training, with refresher sessions scheduled several times a year; attendance at these sessions is mandatory, with financial penalties for staff who fail to attend a session at least annually. Online safety training modules are being made available over DTCC's intranet.
- Employees also practice evacuation procedures several times during the year. Since some of DTCC's locations are in multi-tenant buildings, DTCC's own evacuation drills provide only a partial test of what an actual evacuation would be like (because in an actual situation other building tenants would also be evacuating). To identify any issues that could come up in such a situation, DTCC is currently in discussion with other tenants in certain of its locations on conducting tests involving a total building evacuation.
- Maps have been posted on all floors in all DTCC locations, and included in employee emergency guides, identifying the "points of assembly" to be used in the event of a building evacuation. The map on a particular floor identifies the assembly point for the staff on that floor.
- DTCC staff members have been given "safety kits," with safety equipment and devices (such as an anti-dust breathing mask) to be used in an emergency situation. DTCC had outfitted its staff with similar safety kits prior to September 11th, and many employees found them very helpful on the day of the attacks.

PHYSICAL SECURITY remains a top priority. As a matter of practice, DTCC has always maintained strong

physical security measures for its premises. Over the last two years, we have further enhanced our security program to include coordinating efforts with the building management at each of DTCC's various locations to strengthen protections in these buildings. At our headquarters building, for example, heavy concrete planters and bollards have been installed to provide protection against a physical attack on the building perimeter. Tenant identification is rigorously checked at building entrances, and an X-ray machine and a magnetometer are utilized to screen visitors for weapons or explosives. A security canine team periodically checks building perimeters and, in our message centers, all packages are screened via X-ray. We also coordinate our security activities closely with local law enforcement as well as with federal authorities.

2. ENSURING CERTAINTY OF DATA AND SYSTEMS

Create multiple, geographically dispersed facilities to ensure system redundancy and data safekeeping

In addition to its headquarters facilities, DTCC now has operations and staff in multiple locations elsewhere in North America. All of DTCC's data processing locations are now fully operational, all support data replication and disaster recovery capabilities, and DTCC can conduct all critical systems functions from any location.

GEOGRAPHICALLY DISPERSED BACK-UP FACILITIES — Not only does DTCC now have operations and staff in multiple locations, including sites outside the New York City area, but those locations, including remote data centers, are fully operational. If a major disaster were to destroy or cut off DTCC's New York region data processing locations, DTCC would still be able to resume critical data processing operations including all key depository functions and, at the moment, several key clearing functions. Additional clearing functions will be backed up over the next two years. (See "Expanded back-up resources for clearing services," pg. 16.) We can use any center if our primary work sites are not accessible or operable. Likewise, we can conduct all critical systems functions supporting DTCC's delivery of its clearance, settlement, income processing and corporate actions services from these various locations. All sites have the computer capacity for total data replication and are linked to DTCC's SMART network. (For a more detailed description of SMART, see "The SMART backbone," pg. 14.) The sites are also equipped with infrastructure facilities and required equipment, such as personal computers and system consoles. These out-of-region capabilities were certified as operational in mid-2003.

REDUNDANT FUNCTIONALITY — The alternate sites are also equipped to sustain business functionality for periods of time. We have emergency power systems to ensure continuity in case of power outages. In addition, our most critical operating departments use at least two separate sites to process data, so that if one goes down, loses connectivity or becomes inaccessible, we can continue processing at the other. Moreover, to guard against the loss of data and ensure a flexible structure for quick recovery in an emergency, we now route communications from our customers among our widely distributed data processing centers on a daily basis.

TWO-HOUR RECOVERY — Tests conducted last year assure us that, in the event of a major disaster, DTCC can activate its out-of-region capabilities and resume data processing operations within the two-hour window stipulated in the interagency paper on business continuity issued by financial regulatory authorities in 2003.

In the unlikely event that DTCC would lose its New York data centers simultaneously, some transactional data might be lost when service is restored at a remote site. We are working on a number of improvements that should allow customers to determine easily whether or not any transactional data might have been lost during a recovery and, if so, what it was. DTCC also anticipates that technology improvements in the near future will further reduce considerably the quantity of data that potentially could be lost. Given the distances involved, however, it will not be possible to have synchronous data replication to the remote sites for the foreseeable future.

MOVING HIGHER VOLUMES OF DATA OVER LONGER DISTANCES — Prior to the outfitting and testing of DTCC's remote data centers, accurate, large-volume, "real-time" data replication was seldom achievable much beyond distances of 30 miles. In conjunction with its technology partners, DTCC has implemented an innovative solution that substantially improves data replication. The result is that we can now achieve high-speed asynchronous data replication over distances of a thousand miles and more. This functionality runs in the background, is fully transparent to users, requires no manual intervention and has no performance impact on the processing environment. The replication capacity, among other things, is what allows DTCC to function over a multi-level, widely dispersed disaster recovery infrastructure, and we will be further strengthening this capability in the coming months. We believe our experience and the technology solution we have implemented may provide a useful model for other organizations in financial services to consider, and DTCC's technology staff is prepared to share this knowledge with interested participants.

ASSEMBLING HIGH-END, HIGHLY RESPONSIVE DATA STORAGE SYSTEMS — Concomitant with DTCC's ability to move huge volumes of data rapidly was the need for storage systems that could accept and process the data quickly. DTCC was able, within a year, to assemble high-end data storage systems and to acquire the storage management software needed to run them. In the course of this, DTCC automated many of the key functions including the ability to restart the highly complex replication process automatically after an interruption. DTCC now puts these systems through exhaustive testing and routinely upgrades them to ensure non-disruptive operations.

Sustain a resilient communications network and telecom system

DTCC has increased the resiliency of its communications network and enhanced connectivity with all major depository customers to ensure that all its data processing locations can be linked not only to customers' primary business locations but also to their back-up locations. DTCC is also mandating connectivity testing for these same customers and may look to expand this mandate in 2004.

THE SMART BACKBONE — The backbone of DTCC's ability to communicate with customers is its network infrastructure, called the "SMART" (Securely Managed and Reliable Technology) network. The redundant telecommunications security engineered into the SMART network in the 1990s proved invaluable in the aftermath of September 11th, preserving DTCC's ability to interact with the major depository participants and continue depository operations throughout that week. Since 9/11, DTCC has moved aggressively to complete the

task of building SMART into a seamless, end-to-end, managed communications system encompassing a geographically dispersed complex of processing centers, communications networks and control facilities. Each element of SMART is highly secure, engineered with multiple independent levels of redundancy, and capable of handling DTCC's entire clearance and settlement workload. SMART is resilient and, in effect, "self-healing," providing, for example, a web of multiple networks and back-up levels to deliver mission-critical data. These capabilities are now being made available for DTCC's clearing services.

THE SMART ROLE IN BUSINESS CONTINUITY — All of DTCC's data processing operations, as well as the entire SMART complex, are fully redundant and can be controlled from any of DTCC's multiple command centers. SMART is a key element of DTCC's business continuity strategy. All components of SMART across the multiple centers are managed and used daily, providing multiple levels of redundancy. Rather than maintain business continuity capabilities in standby, we treat all sites, networks and management centers as a unified complex that is always accessible. Customer connectivity to our processing complex is supported by several layers of fallback capabilities, with each processing site able to communicate synchronously with peer sites over multiple connections. All these sites, in turn, are linked to all our customer firms through their SMART connections. As long as we can get an instruction to any of our multiple processing sites, SMART will route it to the site or sites responsible for processing it. This provides DTCC the flexibility to use any of its various redundant back-up components at any of the multiple facilities at any time.

PROTECTING TELECOMMUNICATIONS — DTCC provisions and manages all elements of its SMART complex—from DTCC's processing sites all the way through to its customers' premises, including communications hardware, software and the relationships with multiple telecommunication providers. Since we provision all elements of the network, we are able to register all communications circuits with the Department of Homeland Security's Telecommunications Service Priority (TSP) program for priority restoration in the event of an outage. The TSP program provides national security and emergency preparedness users priority restoration of telecommunications services that are vital to coordinating and responding to crises.

EXPANDING THE NETWORK — DTCC and the Securities Industry Automation Corporation (SIAC) have completed the linkages between the Secure Financial Transaction Infrastructure (SFTI) network managed by SIAC and DTCC's SMART complex. The internetworking of these facilities provides interconnectivity between the SFTI access centers and the SMART complex, adding yet another level of resiliency to the industry's infrastructure. Details about the interconnectivity between SMART and SFTI are available on DTCC's Web site.⁴

REMOTE COMMAND AND CONTROL — With the creation of out-of-region capabilities, DTCC has also established a command center network that interconnects all DTCC's data processing capabilities while providing remote command and control of these capabilities from any of DTCC's other data centers. Customers' transactions and calls are now routinely routed among these different communications centers on a daily basis. This distributed "command and control" configuration provides an added level of recovery capabilities in the event a data center has to be evacuated even though its systems remain fully functional (and, in fact, these capabilities

were exercised during the August blackout in the northeastern United States). The command and control function is now actively rotated among the data centers on a regular basis, assuring that all data center staff have the necessary experience to run the production environment.

EXPANDED BACK-UP RESOURCES FOR CLEARING SERVICES — DTCC is in the process of extending its out-of-region capabilities to cover all DTCC subsidiaries. We have been working with SIAC, which has provided a range of technology support services to DTCC's clearing subsidiaries, to integrate those support services into DTCC. The objective is to reduce operational costs and provide consistent business continuity planning capabilities across all DTCC services, including those provided by National Securities Clearing Corporation (NSCC), Fixed Income Clearing Corporation (FICC) and Emerging Markets Clearing Corporation (EMCC). DTCC has already completed this "insourcing" effort for several key NSCC applications, which are now backed up remotely. DTCC has also successfully configured and operates on a regular basis the operating system and logical mainframe partitions necessary to support other NSCC services as they are insourced, both at headquarters and remotely. As the remaining NSCC applications are moved into DTCC, they will utilize the infrastructure supporting our out-of-region business recovery capabilities. The scheduled date to complete insourcing and out-of-region back-up for all NSCC and EMCC applications is year-end 2004. Different time schedules apply to FICC applications. We will communicate more details about DTCC's insourcing efforts throughout 2004 via Important Notices and our Web site.

Managing cyber-risk vulnerabilities

In addition to configuring systems architecture to maintain security and building extensive "firewalls" and other defenses, such as automated scanning software, to prevent unauthorized entry into its servers and systems, DTCC also maintains a Computer Security Incident Response Team (CSIRT) which monitors systems and communications security. Among other activities, the team continually scans for vulnerabilities in DTCC's networks and systems, reviewing suspect incidents, analyzing them and determining if they suggest a coordinated probing of DTCC defenses, hacker attack or a denial-of-service attack. The goal is to identify potential system weaknesses before they become risks or actual cyber-security incidents. Further, by continually monitoring all activity on DTCC's diverse networks, Web servers and databases, the team is able to efficiently coordinate the communication of and responses to suspect security events across departments and business lines at DTCC. Team membership, currently comprising executives from DTCC's technology infrastructure unit, will be broadened in 2004 to include the heads of our business units. This will enhance the team's ability to monitor and understand the business impact of our various response strategies. The team reports on security-related incidents to our regulators and notes how we respond to or deal with them. In addition, following the focused procedure model for electronic crime scenes from the U.S. Department of Homeland Security, DTCC can call on government agencies if required for assistance with external cyber investigations. We also continue to partner with other major financial services organizations in support of the efforts of the Financial Services/Information Sharing and Analysis Center (FS/ISAC) to strengthen the industry's cyber-security through improved dissemination of information about vulnerabilities, alerts about attacks in progress, and education about best practices in this area. (See the discussion of the FS/ISAC on pg. 21.)

3. MANAGING THROUGH A CRISIS

Strengthen DTCC's continuity and control process

Since the experience of the business disruptions following the September 11th terrorist attacks, DTCC has extensively reconfigured its preparations for managing in a crisis, including the revision of its crisis management planning. DTCC had long-standing requirements that all business operations and support departments develop business contingency plans in which, among other things, the departments identify critical tasks to be performed during emergencies, list the recovery time objectives for each, and designate first-response staff. As part of more rigorous planning criteria, DTCC revised its crisis management control structure, which now consists of (1) an executive command team, (2) several subordinate command teams focusing on particular business areas, and (3) a crisis command center.

EXECUTIVE COMMAND TEAM — In the event of a crisis, the company would activate an executive command team to manage the company's response. This team is composed of senior executives from each of the company's principal line and staff departments, including legal, human resources, executive management, information technology, operations, relationship management, security, and facilities. Each team member has specific responsibilities in a crisis, such as employee communication, external communication, technology continuity, business relationships, government liaison and so forth. In addition, each team member has several people identified as back-ups to ensure that a particular area of expertise is covered. All DTCC subsidiaries are represented on the executive command team. Our executive rotation program, combined with multiple back-ups for each of the team members, minimizes the probability that all members of the command team and their back-ups will ever be in the same location together.

FIRST-RESPONSE ACTION TEAMS — At each of DTCC's operating locations the company now has designated "first-response" action teams to deal with immediate crisis situations. The location teams have taken on greater importance in coping with crises as DTCC has dispersed its facilities more widely across North America. The responsibility of the location teams is to respond to a crisis as it affects their specific location, facilities and staff, reporting their activities to a designated member of the executive command team. This creates a clearly understood chain of command and reporting structure with appropriately designated responsibilities for dealing with crisis situations from the bottom to the top of the organization.

CORE BUSINESS CONTINUITY COMMAND GROUPS — DTCC also now maintains three core business continuity groups. The technology infrastructure group focuses on crisis response and business continuity for all aspects of the corporate data processing infrastructure, including computer operations, facilities, telecommunications, systems support, distributed systems and so forth. The operations continuity group has responsibility for ensuring operational and processing continuity. Individual managers of DTCC's business lines form the third group and are charged with making sure specific DTCC business lines, including individual products and services, are functional and can be accessed. If there are issues affecting a particular business line, this group manages those issues to mitigate their impact on customers. Membership on the continuity command groups includes senior managers from each of those areas, as well as their back-ups.

These groups also report up to designated members of the executive command team.

CRISIS COMMAND CENTER — DTCC has designated specific areas both in its headquarters location and at other locations as Crisis Command Centers for use by the executive command team. These centers are equipped with all the necessary data processing and telecommunications capabilities — including voice communications independent of DTCC’s normal telecommunications system — to permit the team to quickly assemble, assess the situation, give appropriate direction to the operating units of the company in a crisis, and communicate with others outside DTCC even if DTCC’s own voice communications systems are down. All DTCC operating areas also have public address system capabilities permitting senior managers to communicate directly to employees in the event of an emergency.

4. KEEPING CUSTOMERS AND REGULATORS INFORMED

Instill confidence during a crisis by providing customers, markets and regulatory authorities the information necessary to assess the situation and make decisions

DTCC continues to work closely with government and industry groups to assess and mitigate potential risks to DTCC’s own operations or operational recovery capabilities, as well as to the industry processes they support. We are in a pilot program with New York City officials to coordinate access to our various facilities during an emergency. We work with a range of industry organizations. And we continue to work with the various government agencies and units charged with overseeing the functioning and infrastructure of the financial services industry.

CRISIS COMMUNICATION — One of our principal concerns is the capability to communicate broad, often non-technical information to our customers, the marketplaces and regulatory agencies during an emergency. Communicating during a crisis is paramount. One objective of the meetings we will conduct with customer groups during 2004 is to examine management and staff communication during an emergency. In the meantime, the initiatives we now have under way are discussed below.

COMMUNICATING WITH CUSTOMERS — The industry generally has shifted to the use of the Internet as a quick way of communicating information, and would look to DTCC’s Web sites as a way of getting up-to-the-minute information during crises. In response to this, DTCC has enhanced the Internet-based DTCC Customer Desktop messaging facility to include cumulative message reporting and archival capability for all users. In effect, this creates a “bulletin board” where notices can be posted and questions raised. We have assigned a category within this facility specifically to target business continuity coordinators with emergency message viewing and archiving services. We have, in turn, completed the automated registration of client business continuity coordinators for this emergency service. We will provide more information on the messaging capability during 2004. At the same time, we encourage all our customers to provide their DTCC relationship manager with updated business continuity coordinator contact information to ensure that the appropriate people are included in this messaging group.

5. AN OPERATIONAL RISK MANAGEMENT PROGRAM SUPPORTS BUSINESS CONTINUITY PLANNING OBJECTIVES

Over the past two years, DTCC has expanded its company-wide enterprise risk program, to focus more resources, training and monitoring on quantitative, credit, market and operational risk factors. The aim is twofold. One is to have a “snapshot” of individual and collective customer risk positions, collateral and market risk at any given time, so that DTCC will have an accurate picture for planning purposes in the event of an emergency. The other is to bring new methodologies and controls to bear on DTCC’s own operational risk management.

DTCC has substantially speeded up and expanded its capacity to oversee its customers’ daily position risk and evaluate customers’ credit and collateral status.

MANAGING OPERATIONAL RISK ON A DAILY BASIS — Meanwhile, DTCC has launched an ambitious and far-reaching program to evaluate, monitor and manage its operational risk on a daily basis. To initiate the program, DTCC established an operational risk management unit charged with instituting risk measurement and monitoring procedures — and instilling operational risk management techniques throughout DTCC and its subsidiaries. Created in 2002, the unit designed a multi-year plan for implementing its program, and began conducting pilot tests of its new risk assessment and evaluation procedures in 2003. In addition to a company-wide effort to identify and weigh operating risks within each department, DTCC is building a reporting system and database to capture and analyze possible “risk incidents.” Another methodology to establish and monitor key risk indicators will also be introduced in 2004 as employees go through revised operational risk evaluation and management training. In addition, internal and external auditing of risk assessment and management techniques is also now a key element of the company’s operational risk management program.

6. TESTING BUSINESS CONTINUITY PLANS

Conduct rigorous, regular testing of DTCC’s continuity plans and contingencies

DTCC TESTING — For more than a decade, DTCC has routinely conducted semi-annual emergency response tests and then evaluated the results. Since 9/11, however, DTCC has stepped up the scale and urgency of its formal contingency exercises and has begun conducting “tabletop” exercises more frequently throughout the year to test crisis management team knowledge and resourcefulness in the face of catastrophic events. As an example, in 2003 DTCC conducted a “tabletop” exercise of how its command teams would respond in the event of a catastrophic loss of the company’s headquarters location. The staff conducting the exercise identified the officers who were scheduled to rotate off-site on the day used in the simulation, who then participated in a half-day workshop to work through how they would respond to such an event. In 2004, DTCC plans to time some of these exercises to be concurrent with the semi-annual emergency response testing of its business recovery procedures.

As with real events, these various exercises involve debriefing sessions and checklists that are used to identify weaknesses or opportunities for improvement. In addition, we require that staff from every functional area of

the company visit one or more of our alternate sites several times a year to familiarize themselves with the facilities, test connectivity and check supplies and equipment.

Work with customers to strengthen their business continuity plans and infrastructures

Throughout 2003, DTCC continued to work with its customers and other industry infrastructure organizations to discuss the industry's business continuity preparations and DTCC's expectations regarding customers' own business continuity capabilities. We are also prepared to provide business continuity planning services to our customers and others. The *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* draws industry attention to a number of the aspects presented by customer continuity planning, and some of the key steps we have taken to strengthen the industry in this regard are discussed below.

ENSURING CONNECTIVITY — We have enhanced DTCC's telecommunications network with major participants to ensure continued connectivity from all our data processing locations not only to our customers' primary locations but also to their back-up locations.

CONNECTIVITY TESTING — In 2002 and early 2003, the depository (DTC), as well as NSCC and FICC, released Important Notices that established additional telecommunications connectivity requirements for major participants and customers. We now require our larger-volume customers to test their connectivity with us at least once a year. This includes testing of connectivity from customers' primary and back-up locations to all of the DTCC data processing locations. While DTCC's larger customers must undergo connectivity tests now, the company contemplates expanding that requirement to a broader group of customers in 2004. Customer connectivity testing for clearing corporation participants is currently handled and tracked by SIAC, which reports the results back to DTCC. As DTCC migrates technology support services for the clearing corporations from SIAC to DTCC, DTCC will perform these connectivity tests in the future. DTCC maintains a record of those who have tested successfully and will be reporting the results to regulatory agencies as requested. Completing connectivity testing in 2003 were 32.5% of NSCC major participants, 72% of DTC major participants, and 57% of FICC major participants.

Customer firms that have failed to complete tests so far, or wish to schedule testing for 2004, should contact DTCC or SIAC immediately. To schedule a test of connectivity to the DTCC data centers, depository customers should contact the Participant Interface Planning group at 212 855-1482. Clearing corporation customers should contact SIAC at 212 383-HELP.

CUSTOMER RECOVERY PLANNING — DTCC representatives participate in several industry committees focusing on business continuity issues at the industry level. Discussions with participants, however, suggest that it would be useful to supplement these industry-wide discussions with more focused consideration of business continuity in participants' interactions with DTCC. During 2004, DTCC will be organizing meetings with groups of customers to discuss these more specific business continuity issues. The meetings will be used to exchange information on our mutual recovery capabilities, to discuss the various scenarios we may face, and to review whatever mutual efforts may be needed to successfully recover industry processing in a timely fashion.

Depending on the success of these meetings and demonstrated participant interest, DTCC may elect to continue them on a more formal basis in the future. More information on the meetings will be made available in mid-2004.

7. BUSINESS CONTINUITY — “RELEASE 3.0”

As this paper has described, the experience of the disruptions following the terrorist attacks of September 11th led to a dramatic transformation in the thinking of DTCC and the industry about business continuity as an issue. Driven by that transformation, DTCC over the past two years has achieved a quantum leap in the level of resiliency in its systems and operations and in its preparedness to deal with crisis situations. Many industry members have implemented similarly sweeping changes in their business continuity practices.

In parallel with all of these efforts, our perspective has evolved to recognize the need for an even more sophisticated understanding and approach to aspects of the business continuity issue. The industry’s overwhelming dependence on its information technology and telecommunications — the “fourth dimension” of cyberspace — creates new vulnerabilities that are thus far only partially understood. The complex web of interdependencies within the industry — both in its processes and its interactions — creates risks and “points of failure” that weaken our resiliency. The transformed nature of the threats we face requires a heightened level of coordination between the public and private sectors. And the increasingly international nature of the financial services markets demands greater coordination of business continuity practices across borders. The “next generation” of business continuity practices must be shaped by these new perceptions — we truly need a “release 3.0” of how the industry thinks about and deals with business continuity.

Addressing our dependence on cyberspace

In DTCC’s view the industry has prepared itself well to respond to incidents affecting its physical infrastructure. In contrast, the industry is still learning about its vulnerabilities in cyberspace, and preparations to address incidents in cyberspace are in their earlier stages. Further, the networked nature of the cyber infrastructure means that everyone connected to the network has to be concerned with the “cyber resiliency” of both the network itself and of the other participants in the network. As the recent “MyDoom” incident graphically illustrates, poor cyber security practices at some network participants can create a perfect platform for attacks on other network participants.

The industry needs a more concentrated focus on improving its “cyber resiliency,” and one that permits a sharing of information about improved practices to ensure that all parties connecting to the industry’s cyber infrastructure can do their part in addressing information security issues and ensuring the safety of the infrastructure. DTCC believes a particularly important initiative in this area is the current effort to expand the services and capabilities of the Financial Services/Information Sharing and Analysis Center (FS/ISAC). The FS/ISAC was founded by industry members in the late 1990s as a way to allow financial services companies to share sensitive security information safely and to create a dialogue between the financial services industry and government agencies on information security issues. In 2003 the FS/ISAC Board approved a plan for a broad

expansion of the FS/ISAC's services to provide much wider access to information security alerts and best practice standards throughout the financial services industry generally. This broader availability of the FS/ISAC's information will help address the "network effects" that permit vulnerabilities at some network participants to be leveraged as a means of attacking the broad network community itself. DTCC views this as a substantial step forward in safeguarding the industry's cyber infrastructure and is pleased to participate in the "next generation" FS/ISAC as a charter member. We have communicated with our customers individually about the FS/ISAC urging your participation as well. More information is available from the organization's Web site: www.fsisac.com.

Addressing our interdependencies

As noted, the industry's cyber infrastructure creates a strong interdependency within the industry as to information security practices, which the FS/ISAC and other initiatives will address. There is a more fundamental interdependency, however, within the industry's business processes, which today are designed in a way that often requires constant and continuing intervention by individual industry members to ensure that transactions process and are completed correctly. This more fundamental interdependency can only be addressed through continued industry focus on straight-through processing.

Straight-through processing

Ironically, the industry's focus on business continuity planning after September 11th has diverted management attention and investment from one of the key constructs of responsive business continuity — and that is the adoption of straight-through processing or STP. Companies generally undertake STP projects because they expect a strong payback in higher efficiency. In our experience, however, STP is also valuable in strengthening business continuity. The more the processing of transactions can be handled straight through, the less vulnerable that processing is to disruption from events that might impact or dislocate the industry's infrastructure. The G30's recent recommendations recognize this, and consequently we have continued to review our own operations and the broader industry processes we support to see where they might be improved by STP techniques. We also continue to urge our colleagues and customers throughout the industry to do the same. The more broadly STP can be implemented, the better the industry infrastructure will be able to withstand severe dislocations and to be restarted quickly after disruptions.

DTCC has initiated and implemented nearly two dozen STP projects over the last 30 months. It is not the purpose of this report to list or discuss them in detail. Instead, we cite several here to show the impact they can have on business continuity and resiliency. We now have real-time capture of equity trade data from many of the major markets and exchanges, ensuring that trades conducted minutes prior to a financial system dislocation will not be lost or have to be painstakingly pieced back together. We have also expanded real-time trade matching (RTTM) broadly throughout the fixed income industry. We have instituted an RTTM Web-based interface that gives our fixed income customers the ability to identify exceptions to routine clearance and to make the trade process work more smoothly. RTTM lets us capture, process and report trade data much more quickly. As a result of these innovations, a breakdown in the reporting of data on the scale of what occurred on 9/11 is now unlikely to take place.

Within our depository we have undertaken a range of initiatives to speed up the settlement of securities trades “straight through.” In June 2003, for example, we implemented a “look-ahead” facility that links transactions for settlement. This has, on average, reduced the number of transactions normally recycled in the system by more than 20 percent, or approximately USD 10-15 billion during the 1 p.m. peak processing period. The result, in turn, is lower customer intra-day funding needs and higher certainty of settlement. In 2004 we will be completing the development of features of the depository’s Inventory Management System that permit participants to use central facilities to manage the flow of their delivery processing, eliminating the need for constant interactions throughout each day to manage this process.

Internationally, we have launched a number of STP initiatives to speed up processing and strengthen infrastructure resilience. One example is DTCC’s new matching service for the swiftly growing market in credit default swaps. The service speeds up the current matching practice dramatically, and thus makes the multi-billion-dollar swaps market far less vulnerable to the impact of a single catastrophic event.

Each of these initiatives helps reduce the need for time-critical interventions in the handling of transactions, thereby making the industry’s processing infrastructure more resilient and less exposed to disruptions that might make those interventions more difficult. The industry’s continued investment in STP will pay dividends not only in processing efficiency but in processing resiliency as well.

Coordinating between public and private sectors

The experience of September 11th also made clear that protecting the industry’s critical infrastructure will involve significant levels of coordination between public sector and private sector organizations. The U.S. Department of Homeland Security is charged with this overall responsibility in the United States, but the DHS explicitly recognizes that the overwhelming portion of the nation’s critical infrastructure is privately owned and, therefore, that infrastructure protection must involve the private sector to a major degree.

The U.S. Department of the Treasury has been named the lead agency with responsibility for infrastructure protection efforts for the financial services sector in the United States. The Treasury Department is assisted in this effort by the Financial and Banking Information Infrastructure Committee (FBIIC), a working group of representatives of the federal financial regulatory bodies.

Along with other financial industry organizations, DTCC is an active participant in the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC), a private sector group that interfaces with Treasury and the FBIIC on infrastructure protection issues. A DTCC executive currently serves as vice chairman of this council. The FSSCC works to coordinate the financial services industry’s initiatives to protect critical financial services infrastructure. The goal is to ensure that these efforts focus on complementary objectives and contribute to achieving the highest possible level of overall industry resiliency. More information about the council may be obtained from its Web site: www.fsscc.org.

Coordinating across borders

The financial services industry is a global industry, with securities trading around the clock, transactions routinely crossing borders, and international payment flows booked daily in money transfer systems around the world. The industry's interdependencies also are increasingly global ones, with events in one market potentially impacting many others and disruptions in one region potentially spreading well beyond. The excellent work the industry has done in improving business continuity procedures within individual markets, too, must be "globalized" to ensure that the same levels of resiliency and coordination can be achieved at the global level.

For example, efforts to improve coordination and information flow during a crisis will need to have a global dimension, since the interconnected nature of the markets means that industry members outside the affected region will also need to know what decisions have been made and how they will be implemented. DTCC will be participating in a dialogue with key global financial firms over 2004 to develop processes to support that type of coordination.

DTCC also will seek to interact with its industry counterparts to discuss best practices in ensuring the resiliency of market infrastructures and the possibility of collaborative responses to some of the new business continuity demands. In line with the recommendations of the G30, these discussions may seek to explore alternative back-up approaches in the event a market infrastructure is disabled in an incident. As an example, DTCC has already raised the idea of developing plans to share processing capabilities for clearing and settling securities trades in emergencies. DTCC will be pursuing these discussions further in 2004.

¹ *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*, issued by the Board of Governors of the Federal Reserve System; Office of the Comptroller of the Currency; and Securities and Exchange Commission. April 7, 2003.

² *Global Clearing and Settlement: a Plan of Action*, issued by the Group of Thirty. January 23, 2003.

³ The results of our analysis are, of course, reflected in the many changes described throughout this paper. Principal issues identified included:

- The need for greater staff decentralization given potential obstacles in moving personnel to back-up locations.
- The need to establish alternative arrangements for package and parcel deliveries in case existing methods and delivery points are disrupted.
- The need to deal with certain network issues that emerged. DTCC's SMART network generally withstood the attacks very well and, in some instances, data connections were reestablished with customers at unanticipated sites, which permitted processing to continue with little intervention. SMART also provided emergency relays to move critical data between our customers and other industry processing entities that didn't have the resiliency DTCC enjoyed.
- The need for crisis communications to keep customers and government decision-makers informed of the status of our business. Among government agencies, DTCC's long-standing low profile proved a hindrance, for example, in obtaining ready access to emergency communications.
- The need to reinforce crisis command decision-making.

⁴ See DTCC Important Notice #Z0008, dated October 30, 2003.