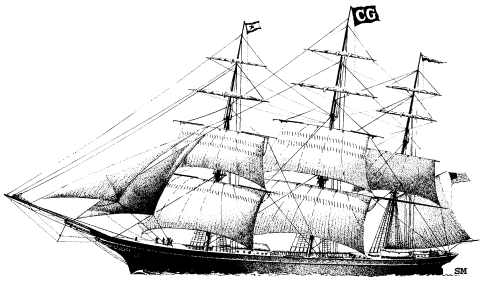
THE CLIPPER GROUP
Navigator™



Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2007094LI October 31, 2007

PCI DSS Compliance and System z — A Combination That Makes Sense

Analyst: Anne MacFarland

Management Summary

There have always been two common modes of business*: bilk-and-run* and *build-to-last*. It is in society's interest to discourage the bilk-and-run operations, and to foster businesses that will endure. With the coming of business over the Internet, any business that does not secure itself and its customer data can become a grazing ground for bilk-and-run illegal operations. It is not enough to be honest – you must also protect your assets and your customers from those who are not.

Use of external networks for business and, most particularly, for payments is here to stay. **This means that enterprise IT systems are no longer primarily IT systems. They are primarily *business systems* – and, in business, security cannot be a haphazard afterthought.** When IT systems amass customer data, they assume the task of caring for its security. Many companies have ignored the ramifications of this assumption and are paying a stiff price.

Many imperatives to secure financial and personal information have been imposed by various governing bodies. The latest payment card industry security standard (PCI DSS) addresses the part of e-business operations most valuable to malfeasants. Its approach is broadly prescriptive in a number of areas, for insecurity is a problem whose solution is only as strong as its weakest link. The requirements cannot be met with a single product, like a magic diet pill, or single strategy.

The PCI DSS requirements cover the handling of sensitive information, of course – but also the physical infrastructure in which it resides, and over which it travels. They also address the operational and governance practices that rule that infrastructure. The requirements are all things that a prudent organization should be doing anyway. But the PCI-DSS initiative also demands that they all be considered as a linked capability - and one whose completeness is auditable. **The auditability – which, again, any prudent organization would want to have in place for its own benefit – adds a gotcha for all strategies that rely on piecemeal security initiatives and piecemeal documentation thereof.**

Is your infrastructure built for discipline? You may think that if you have standardized on an industry-standard hardware you have an easier time of it – but PCI DSS is not just a matter of hardware management. It is a matter of comprehensive and pervasive focus on the protection of sensitive information. Organizations that do not comply with PCI DSS can be financially responsible for losses that their failure to protect private transactional information can incur. For companies that have hoped to cut costs by slighting security and governance, it should be a wake-up call to do better now.

However, if you have a *System z* Mainframe, you have a valuable asset to leverage in the attainment of PCI DSS compliance. Because it is built for multi-tenancy, it secures its resources as an inherent part of operations. This pervasive control baked into the hardware and software prevents many of the intrusions that plague other platforms. It has the scalability, availability, and security to safely coordinate cross-application security and audit. For more on how PCI DSS compliance goes better with System z, please read on.

IN THIS ISSUE

Exhibit 1

- **Build and Maintain a Secure Network**
  - *Requirement 1:* Install and maintain a firewall configuration to protect cardholder data
  - *Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters
- **Protect Cardholder Data**
  - *Requirement 3:* Protect stored cardholder data
  - *Requirement 4:* Encrypt transmission of cardholder data across open, public networks
- **Maintain a Vulnerability Management Program**
  - *Requirement 5:* Use and regularly update anti-virus software
  - *Requirement 6:* Develop and maintain secure systems and applications
- **Implement Strong Access Control Measures**
  - *Requirement 7:* Restrict access to cardholder data by business need-to-know
  - *Requirement 8:* Assign a unique ID to each person with computer access
  - *Requirement 9:* Restrict physical access to cardholder data
- **Regularly Monitor and Test Networks**
  - *Requirement 10:* Track and monitor all access to network resources and cardholder data
  - *Requirement 11:* Regularly test security systems and processes
- **Maintain an Information Security Policy**
  - *Requirement 12:* Maintain a policy that addresses information security

Source: PCI Security Standards Council

Designing PCI DSS-Style Security

Designing for security is an ongoing process. For the short term, a common strategy is to address the most glaring vulnerabilities with some form of remediation. The mid-term strategy is to divide and conquer into securable silos – either geographic or by asset type. However, to complete the picture and achieve a long-term, evolvable solution, you need to secure everything – silos, connections between them, gateways and incidental assets, in a coordinated, consistent way, all from a point of security.

IBM's System z integrity statement focuses on the Mainframe capabilities to prevent unauthorized applications, systems, or users from gaining access to, overwhelming, disabling, altering, or gaining control of key z/OS system processing resources. Malfeasants cannot bypass the lock on system resources. This is a large and significant step beyond reactive solutions.

PCI DSS mandates a quick move to the long-term, comprehensive approach. It consists of six control objectives, covering a dozen specific requirements. (See Exhibit 1, above.)

Objective 1: Build and Maintain a Secure Network

The first requirement in this section mandates stringent firewall, server configurations, DMZs[1], IP masking, and network disciplines to protect data. The other requires that vendor-supplied default settings be changed for system passwords and other security parameters, institution of standards to harden the infrastructure, and encrypting all non-console administrative access. Both come with mandatory documentation, testing, and review that must become part of operational discipline. All these requirements are easier to meet with a System z in your environment.

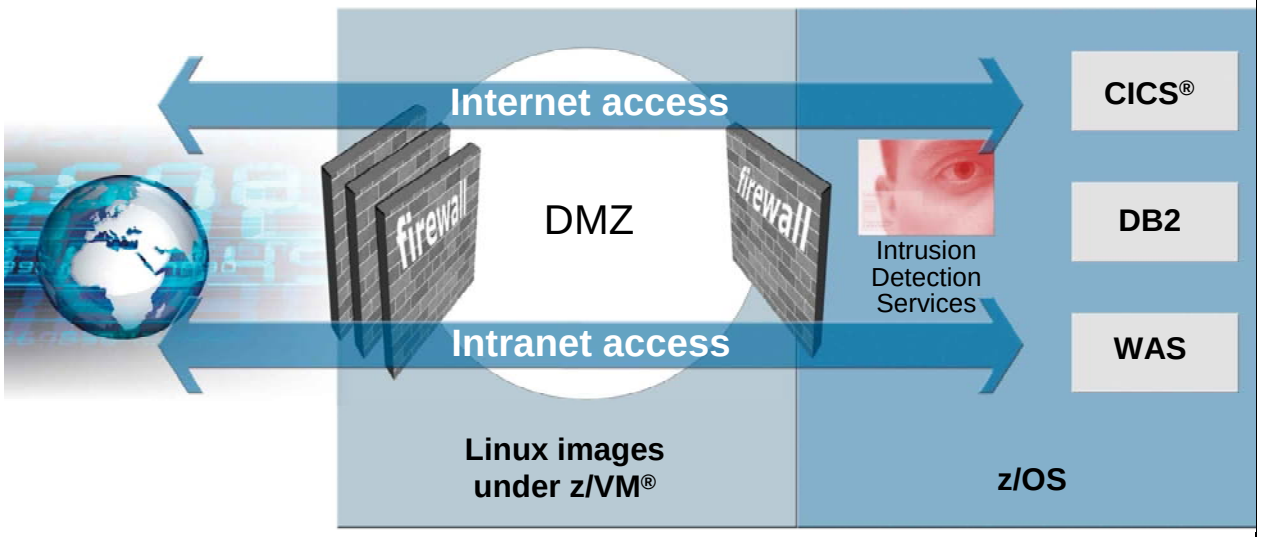
In System z, the hardware equivalents of firewalls are the basis of its support for many workloads. Controls are built into its hardware microcode to support data integrity by both memory access disciplines and resource isolation. All processes running on z are limited in their authority by the firmware and by z's *Resource Access Control Facility* (RACF)[2], and are, by default, not exposed to the system z administrator[3]. *IBM Tivoli zSecure* gives administrators a way to assure that all vendor-supplied defaults are changed. The *z/OS Network Policy Agent* and *z/OS System Health Checker* check system

[1] Demilitarized Zones (think: Korea). These are a buffer zone where traffic can be inspected, evaluated for threats, and blocked where appropriate.

[2] This means that denial of service attacks do not have the resources to be effective, even if they should penetrate the system.

[3] RACF tracks all resource usage on System z and supports full auditability of transactions performed in its jurisdiction.

Exhibit 2 — Demilitarized Zones on the Mainframe



Source: IBM (Used with permission.)

configurations. With *Tivoli zLock*, even a privileged System z administrator has his or her actions logged and questioned, if they are significant. This covers the basics – but there is more.

For passwords, configuration, and security settings for other, non-Mainframe assets in the environment, System z offers a *Secure Vault* that is a highly secure place to keep documentation that can be the golden record against which security monitoring can compare. For encryption of web-based administrative traffic, System z offers many modes of encryption, detailed in Objective 2, below.

System z, its *LPARs*[4], *z/OS*[5] and *z/VM*[6] containers are highly secure. Because of this, the Mainframe is an excellent place for a Web-facing demilitarized zone – often deployed in Linux[7] in System z *IFLs*[8]. (See Exhibit 2, above.) These features are a matter of competence – but in meeting PCI DSS compliance, these competencies take a lot of sources of risk off the table.

That the Mainframe inherently can support multi-tenancy in a way that satisfies PCI DSS lets enterprises consolidate workloads and place them where it makes sense to business process. But there is more.

Objective 2: Protecting Cardholder Data

The third PCI-DSS requirement mandates protection of cardholder data[9], if it is stored, processed, or transmitted. The details state that sensitive data is not to be stored unnecessarily, that where such data is stored, the PANs should be truncated where possible, and that use of PANs in e-mail must be avoided. Use of a System z can reduce the risk by leveraging z's in-the-box completeness. It offers multiple options for encryption. And, since encryption is only as good as the protection of its keys, System z offers significant capabilities in that area, as well.

Within-the-Box Completeness

System z offers, within the box, the entire array of elements necessary to store and process customer data, and the security to protect it. The multi-tenancy that System z supports, and the security within the box that isolates and secures each application running, sharply reduces the number of points of vulnerability at which cardholder data must be secured. The applications[10] hosted on System z can communicate across the

[4] System z LPARS have an EAL certification of 5. The LPAR capability can support up to 60 isolated system images and can provide system resources to them according to policy.

[5] z/OS has EAL 4+ certification.

[6] z/VM has EAL 5 certification.

[7] On System z, *SUSE LES9* is certified EAL 3 with CAPP (Controlled Access Protection Profile), and *Red Hat RHEL 4* is certified EAL 4 with CAPP and LSPP (Labeled Security Protection Profile).

[8] *Integrated Facility for Linux*.

[9] This refers primarily to the *Primary Account Number (PAN)*, but also covers all information such as name, service code, expiration date, etc., that is stored with the PAN.

[10] On System z, application encryption is accomplished by PCKS#11 and JEEC.

integrated TCP/IP in-memory stack, *HiperSockets*, which in this way supports a datacenter-in-a-box with no open[11] or public network. And, with z/OS' *Integrated Intrusion Detection*, the TCP/IP link to other system assets is constantly monitored for attack patterns. Therefore, if the processing and storing to database done on System z, the points of vulnerability are reduced to the first and last hop traffic when the transaction is initiated and concluded.[12]

Encryption

The fourth requirement addresses encryption. It states that sensitive data must be protected with encryption while in storage and when transmitted across open public networks. System z encryption can be done in various ways, depending on how the System z is equipped and what the business requirements demand.

Protecting cardholder data with encryption is best done on a highly-secure platform. It is also best done comprehensively, rather than by multiple systems, whose coordination becomes a point of vulnerability. All told, System z has the capabilities needed to support and manage pervasive encryption in heterogeneous, distributed environments.

Data at Rest

Stored data, in System z, is protected by Storage Protection Keys, Cross-Memory Services, enforced workload isolation, and *z/OS Communications Server* (see more details below). *DB2* offers a Regulatory Compliance Suite with tools to encrypt, test, audit, and safely archive data for long-term retention.

Data transferred by or archived to tape is also protected. The *IBM TS1120*, a tape drive that encrypts, locally, at close to line speed.[13] You can secure the access to these tapes by managing and distributing public keys and securely hosting private keys using the Mainframe's key management technologies (discussed below). In the future, IBM will also encrypt the disks within the array.

Another often-overlooked case of data at rest is the test environment. Transaction environments must work well at speed. The constant improvements to them that are made must be well tested under load with what looks like valid data. Of course, using actual valid data opens a gaping vulnerability. *IBM Optim* can offer data masking – a mapping from the actual sensitive data to something in the same format but not correct – so that customer data is never exposed, internally or externally.

Over the Network

System z offers several ways to do encryption – by the hardware or within z/OS.

- DB2 v.7 features the implementation of SSL encryption for sending and receiving data.
- *SSL* and its successor-standard *TLS (Transport Layer Security)*, along with *IPSec*, are frequently used with a Virtual Private Network (VPN) in Internet-based commerce. z/OS supports SSL, TLS, IPSec, OpenSSH, and OpenPGP, plus multiple symmetric and asymmetric encryption methods.
- *z/OS Communications Server* provides z/OS Intrusion Detection Services to compliment network-based IDS. It can detect known and unknown attacks, and can detect problems in real time, providing another layer of network defense.
- All network connections are controlled by RACF to manage access and disallow untrusted networks and hosts.
- Offloading[14] IPSec to a specialty *zIIP*[15] processor, supported in z/OS 1.8, accelerates processing in the same way System z offloads *Java* execution to one of its *zAAP* specialty processors. This improves the price/performance of end-to-end encryption
- FTP, which is cited as a "risky protocol" in PCI-DSS Requirement 1.1.7, can be protected, on System z, with IPSec or SSL.
- For distributed enterprises, meeting PCI DSS requirements well dictates that encryption should cover endpoint-to-endpoint, not merely endpoint to a network switch**.** System z supports true end-to-end encryption, even to a

[11] Due to insider threats, your LAN must be considered, for security purposes, a public network.

[12] Mainframe storage is connected by FICON, which uses Fibre Channel optic cables but its own Layer 4 protocol.

[13] For more information about the TS 1120, see **The Clipper Group Navigator** entitled *IBM Gives Enterprise Options for Encryption*, dated August 28, 2006, and available at http://www.clipper.com/research/TCG2006077.pdf.

[14] Note that the LPARs and z/VMs that contain System z applications can include access to System z specialty engines.

[15] For more information, see **The Clipper Group Navigator** entitled *System z9 adds zIIP to Ally with DB2 on z/OS to Better Serve the Onslaught of Business Data*, dated January 24, 2006, and available at http://www.clipper.com/research/TCG2006006.pdf.

laptop[16] or a printer,[17] with IPSec. This removes the connection to the switch as a point of compromise. Because z/OS implements IPSec within the secure environment of System z, another risk exposure is removed.

During Processing

System z's memory disciplines protect data in memory from other applications running on the same environment, in z/VMs running in System z, all traces of memory can be erased when the memory is swapped out so that another application can use the processor. This is not necessarily the case with the use of other virtual machines.

System z Encryption Options

Integrated Cryptographic Service Facility

The *Integrated Cryptographic Service Facility* or *ICSF* is a component of z/OS. You can create a key today and store it securely (by encrypting it under your master key), and that same key value can be available 10 or 20 years from now. Even though the external representation of that key might change over time (i.e., with master key changes or key rotation policies), the underlying key is preserved. These keys can be further protected with the *Crytpo Express2* feature ICSF is not instantiated (not implemented) in the hardware. ICSF provides the interface to the hardware, both CPACF and Crypto Express2.

CPACF

CPACF[18], a feature on z9, adds cryptographic acceleration to every processor, making routine use of cryptography more transparent. But System z can also do more.

Cryptographic Coprocessor

System z's optional Crypto Express2[19] hardware encryption co-processor *accelerates the handshakes of SSL/TLS* to support a very-high rate of transactions. It supports ATM and POS environments with Remote Key Loading.

As it is tamper-resistant, the Crypto Express2 card can also be a secure vault for encryption keys. This vault can contain both *secure key* – keys that are only visible in the Crypto Express2 hardware card – and clear key applications, based on configuration options. Crypto Express2 also offers support for PIN processing associated with financial transactions including PIN generation and verification based on industry standards and formats. This centralized key management can play a part in securing larger environments with ICSF, RACF and *Parallel Sysplex*, used to extend security across distances and geographies.

System z as Digital Certificate Repository

The actual exchange of encryption public keys usually is accomplished using digital certificates. The *PKI Services*[20] component of z/OS provides an attractive alternative to third-party digital certificate hosting. It allows enterprises using z/OS to become their own Certificate Authority. This cuts out a trip on a public network (always an occasion of risk) – and also reduces costs**.** This eliminates the cost of expensive certificates from an independent Certificate Authority. This is particularly valuable to establishments with hundreds or thousands of remote servers and devices. System z can be the sole Certificate Authority for all of your enterprise's technology platforms.

Objective 3: Maintain a Vulnerability Assessment Program

Satisfying the fifth requirement to maintain anti-virus protection is somewhat less arduous on System z than on other platforms[21] because System z does it as part of its operations. Vulnerability assessments, such as those by z/OS Communications Server mentioned above, are part of System z-wide operations, is an IFL a process? Does z/OS protect an IFL? You might argue that it can protect unauthorized work from getting to a zIIP or zAAP, but not sure it prevents work from getting to an independent IFL) that are running on the box. This is due to the System Integrity features, the RACF access controls, and z/OS's *in-context* ability to detect known and unknown threats, be they scams, external attacks – either in single or multiple packets[22]. Linux on z, working as a DMZ, can provide integrated anti-virus firewall protection for the z/OS systems.

Requirement 6, to secure systems and applications, is covered by SMP/E, z/OS's software

[16] With the no-charge Java decryption client.

[17] With the IBM *InfoPrinters*.

[18] CP Assist for Cryptographic Function

[19] Crypto Express has been certified FIPS 140-2 Level 4, the highest hardware security rating.

[20] System z's PKI Services have IdenTrust certification. It supports split knowledge and control of keys, which is part of Requirement 3.

[21] The PCI-DSS requirements note that the Mainframe, by its nature, is not vulnerable to viruses to the extent that Intel platforms are.

[22] These are merely some highlights of some features in z/OS Intrusion Detection Services.

maintenance and installation tool, LPARs (EAL 5), Storage Protection Keys, and System z's isolation of sensitive executables as part of its processing routine.

On a Mainframe, security operations are a separate dashboard from systems administration. This separation of concerns is as much a part of business prudence as having the person who signs the checks not also write them. It addresses the *who watches the watcher* conundrum – they watch each other.

Objective 4: Implement Strong Access Control Measures

In System z, each unit of work has an identity and access to resources is based on that identity. An application cannot bypass the security controls, and each user of the application must be granted the appropriate access. There is not only no way in, but there is no way for an interloper process to get control of resources with which to do something.

Removable media, in the System z world, are protected by the access controls that are part of the labels, even if they are not encrypted. There is a bypass process that can be used to read a foreign tape, but this must be specifically invoked by an authenticated and authorized identity.

RACF and Tivoli zSecure provide the protection as well as the means to monitor and audit access to valuable resources by both typical and privileged users. This meets Requirement 7, which mandates restriction of access to those with a business need.

Requirement 8 addresses the assignment of a unique ID to each person with computer access. RACF *Digital Certificate Mapper*, working with the digital certificate capabilities discussed earlier, traces the trails back from the Mainframe through feeder applications to end users. RACF's *SAF*[23] Password management includes rules for password values (enhancing data security) and expiration of passwords. In addition, DB2, and *WebSphere Application Server* (host to many J2EE application) can be configured to share a trusted context, making that environment more secure.

Objective 5: Regularly monitor and test environment

Monitoring and testing is best done from a point of security – or the whole process is less than secure. IBM offers a plethora of monitoring tools like RACF can generate audit records for successful as well as failed access attempts. *System HealthChecker* (built into z/OS), SMF[24] auditing, Tivoli zSecure, and DB2 Audit can interface with enterprise-wide auditing via the Tivoli platform to monitor and test the environment wherever it extends. Of course, the more that activity involving customer information is done on System z, the less complex the compliance with PCI-DSS.

Some IBM Services

IBM offers many services that can help an enterprise design a PCI-DSS Strategy for their particular business situation. IBM's *Information Security Assessment, Threat Risk Assessment* and *Security Process Assessment* address information security specifically and can identify vulnerabilities and security gaps in the existing environment. IBM Rational's *AppScan* can test Web applications for weaknesses and generate a to-do list of tasks needed to address them.

IBM also offers a number of implementation services. *Security and Privacy Implementation, Encryption Architecture, Design and Implementation*, and *Data Security Solutions* are relevant to PCI DSS compliance. In addition, there are many IBM product-specific solutions.

For monitoring and controlling Data Security, IBM offers many services including the following:

- *IBM Tivoli Compliance Insight Suite*
- *IBM Audit Management Expert*
- *IBM Optim Data Growth Solution*
- *IBM Tivoli Security Operations Manager*
- *IBM ISS Proventia Site Protector*
- *IBM ISS Penetration Testing*
- *IBM ISS Anomaly Detection*

Any seasoned business will experience a change in both its risk profile and its appetite for risk. Services by a broadly experienced third party can bring a fresh eye to chronic risks and organize the remedial actions that are needed.

Objective 6: Maintain an Information Security Policy

The Mainframe gives many ways to instantiate and enforce a security policy for maintaining Information Security. z/OS RACF forms the basis. It is extended and enhanced by *Tivoli*

[23] *System Authorization Facility* in z/OS.

[24] *System Management Function*, hardware-based change monitoring instituted back in the s/360.

Insight Suite and z/OS' *Network Policy Agents*. Of course, keeping the policy intact means being prudent about where you deploy new applications, particularly those that touch or work with customer information. Deploying new applications on the Mainframe will reduce the security ramifications of an infrastructure change.

Your PCI DSS Strategy

In most environments, there are information security policies for different kinds of information, and for different kinds of service platforms. Enterprises are not going to limit the kinds of data they use – in fact, they want to use new sources of data and leverage what they have in different ways. Unless there is a unified policy, this can add security complexity. Most enterprises are not going to run all workloads on one platform – there are too many differing considerations of performance and budget. Some presumption of heterogeneity and a relentless focus on extensibility is part of a forward-looking infrastructure strategy.

System z can be the cornerstone of that strategy in its role as a security hub. As you can see from the above, compliance with the PCI-DSS standards is a discipline that touches deployment, IT operations, IT networks, data protection, and IT governance.

Using System z as a site for identity management, element monitoring, and alerting, can simplify the correlation of all the security elements, and support a quicker audit. Running them in Linux on z cuts down the software costs and still benefits from many z security features.

For many businesses, moving sensitive workloads to System z will be an attractive option, especially once all costs are taken into consideration. The extensibility, resource sharing, low energy costs, and low administrative headcount may more than make up for possibly higher acquisition costs of hardware and software.

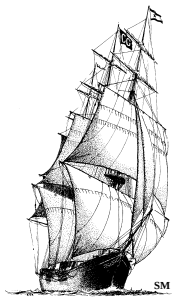
Conclusion

We are in an era of *trick or treat* – all enterprises must deal with parties they do not truly trust. To get the treats, you must avoid the tricks via comprehensive security not just of the elements of your system, or of the processes that run across them, but also of the customer data that is used and reused by more and more processes with every new BI and CRM capability.

Think about the high price of insecurity. If you were a bilk-and-run player, you might be able to afford it, as long as you can switch to a new line of business early and often, and find insecure systems to prey on. Build-to-last organizations want no part of that lifestyle, as either predators or prey.

PCI DSS gives you a clear mandate to secure customer-facing operations. For some organizations, the dozen requirements may be overwhelmingly complex. Leveraging System z's inherent design can reduce that complexity, and can let you concentrate on the cultural imperatives that underlie growing and changing things safely.

Use of the System z Mainframe can sequester much of your customer data processing from many threats. As a security hub, it can coordinate a preventative response to others. Use it well, and you can sleep easier and innovate in your customer-facing operations with confidence.



About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

Anne MacFarland **is Director of Data Strategies and Information Solutions for The Clipper Group.** Ms. MacFarland specializes in strategic business solutions offered by enterprise systems, software, and storage vendors, in trends in enterprise systems and networks, and in explaining these trends and the underlying technologies in simple business terms. She joined The Clipper Group after a long career in library systems, business archives, consulting, research, and freelance writing. Ms. MacFarland earned a Bachelor of Arts degree from Cornell University, where she was a College Scholar, and a Masters of Library Science from Southern Connecticut State University.

- ***Reach Anne MacFarland via e-mail at Anne.MacFarland@clipper.com or at 781-235-0085 Ext. 128. (Please dial "128" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group** *Captain's Log*, **The Clipper Group Voyager**, **Clipper Notes**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, *"Navigating Information Technology Horizons"*, and *"teraproductivity"* are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.