Fusion Centers:
Turning Data into Actionable Intelligence

*White Paper*

_Sypherlink Inc._
6500 Emerald Parkway
Suite 175
Dublin, Ohio 43016
www.sypherlink.com

_Computer Aid Inc._
1390 Ridgeview Drive
Allentown, Pennsylvania 18104
www.compaid.com
Abstract

Although Fusion Centers have been identified as critical components in anti-terrorism efforts, many believe that existing Fusion Centers could be more useful and more effective. In addition, despite the available federal guidelines, many issues and questions remain regarding how to best implement a Fusion Center. One of the greatest challenges faced by Fusion Center officials is planning and implementing data integration and establishing an appropriate technology infrastructure. This paper discusses these challenges and provides best practices recommendations for overcoming them. Specifically, this paper describes best practices in achieving effective data integration, meeting federal standards for data integration, leveraging existing technology tools, and creating an infrastructure that supports your Fusion Center’s mission.
# Table of Contents

**Key Challenges Facing Fusion Centers**
- Lack of Compatibility ...................................................... 1
- Poor Compliance with Federal Data-Sharing Standards .......... 2

**Recommendations & Best Practices**
- Create a Data Management Strategy Leveraging Best Practices .................................................. 3
  - Define Your Mission and Objectives .................................. 3
  - Protect Investments in Existing Systems .............................. 3
  - Determine Critical Data and Implement in Phases .................. 4
  - Define the Data Integration Approach .............................. 6
  - Embrace Standards ......................................................... 7
  - Leverage Existing Technology ........................................ 7

- Tie Your Technology Infrastructure to Your Mission ........... 8

**Summary** ........................................................................... 10

**About the Authors** .......................................................... 11
- Sypherlink ......................................................................... 11
- Computer Aid, Inc. (CAI) .................................................. 11
Key Challenges Facing Fusion Centers

Since the events of September 11, 2001, there has been heightened emphasis throughout the federal, state, and local law enforcement, intelligence, and homeland security communities on the timely sharing of information across jurisdictional and geographic boundaries to produce actionable intelligence. At the federal, state, and local levels, the institution of Fusion Centers is envisioned as the most effective means of facilitating information sharing in a timely and cost-effective manner. Consequently, most states currently have an operational Center. While these Fusion Centers are deemed essential to thwart terrorism and abate criminal activity, Fusion Centers also facilitate counter-narcotics activities and play a key role in the policing of illegal immigrants. In fact, Fusion Centers are deemed by the Department of Homeland Security to be “all crimes” facilities.

Though many Fusion Centers are highly successful, there is still general concern in the field that these Centers are not as effective as they could be. Recognizing that Fusion Centers are vital to a nationwide exchange of intelligence used to prevent terrorism, the Government Accountability Office (GAO) of the federal government recently contacted Fusion Center officials to assess their current functions, challenges, and needs. In the resulting report to the subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, the GAO detailed several common challenges faced by Fusion Center directors and staff, including in the areas of planning the Center, acquiring security clearances, accessing data systems, utilizing vast amounts of data, hiring and retaining personnel, training personnel, and obtaining funding.

If you have been involved in planning, implementing, or operating a Fusion Center, you may recognize the challenges described in the GAO report from your own experience. Not only do you face staffing and funding issues, but you must control access to classified data, integrate data from disparate systems, ensure the system complies with ever-changing standards, and, in the end, produce information that is useful and valuable.

How should a Fusion Center turn data into actionable intelligence? The goal of this white paper is to address – and recommend best practices for overcoming – the key data management challenges facing Fusion Centers: lack of compatibility with existing law enforcement databases and poor compliance with federal data-sharing standards. Through these best practices, the directors and staff involved in planning, implementing, and operating your Fusion Center can be assured that your Center can more efficiently and effectively gather relevant intelligence.

Lack of Compatibility

While data exchange and sharing is the goal of Fusion Centers, a lack of compatibility among law enforcement databases makes this difficult. Fusion Center officials report that they have trouble accessing and managing multiple information systems. Further, the information they are able to access is often redundant and the high volume overwhelming. At the local level, relevant data is entered into multiple computer systems, which very often cannot share information. Adding state and federal databases to the mix further decreases compatibility. Although the Fusion Center Guidelines issued by the U.S. Department of Justice’s Global Justice Information Sharing Initiative (Guidelines) specify that a Fusion Center should leverage existing databases, systems, and networks to maximize information sharing, they do not specify how to accomplish this.

Information sharing is one thing; making sense of the information is another. Fusion Centers must do both, dealing with large amounts of data in disparate computer systems that cannot be analyzed until it is in comparable formats. In addition, the relevance of data must be considered. Fusion Centers must sort through large amounts of information to target information that is useful and important so that the right information is available for criminal analysis. Locating useful information and presenting it in a comparable format requires an initial review, followed by the collection of data into a unique system for analysis. Most states do not have a system in place to pool data from relevant databases and networks and face the burdensome task of evaluating and
preparing data for collection. The goal is clear: to collect relevant intelligence from the information already available. The means to do so, however, often proves complicated and cumbersome.

**Poor Compliance with Federal Data-Sharing Standards**

An additional challenge in the area of data sharing is poor compliance with federal data-sharing standards. Although standards exist, conformance to these standards has, until recently, been voluntary. Now that conformance is being written into grant requirements, maintaining standards at a Fusion Center is even more important. In fact, the *Guidelines* specify that the U.S. Department of Justice’s (DoJ) Global Justice Extensible Markup Language (XML) Data Model and the National Information Exchange Model (NIEM) standards should be used for database and network development. However, as federal data sharing standards evolve, adhering to them becomes costly. In addition, the *Guidelines* go on to say that the systems in place should allow for future connectivity, which further complicates developing a system. Establishing a Fusion Center that meets - and maintains - data sharing standards and anticipates future connectivity to other systems involves a great deal of time, money, and specialized resources.
Recommendations & Best Practices

The recommendations and best practices outlined here have been developed to address data management issues that Fusion Center officials face, and to specifically overcome the key challenges of incompatible data sources and lack of federal data sharing standards.

Create a Data Management Strategy Leveraging Best Practices

Collectively, Sypherlink and CAI have decades of experience in supporting local, regional, state, and federal information sharing and intelligence efforts. This first-hand knowledge of the development, implementation, and ongoing maintenance of these specialized efforts has allowed us to determine which data management approaches work well and which should be reconsidered. The following sections describe the best practices we recommend for implementing information sharing and intelligence efforts. These best practices will avoid and overcome many issues commonly encountered when planning data sharing strategies.

Define Your Mission and Objectives

The first step in creating your strategy is to clearly define the mission and objectives of your Fusion Center, even if the Center is operational. Agencies and entities that play a role in the Fusion Center should be included in these discussions, so that the mission and goals are defined collaboratively. A mission statement should include the Center’s name and function, and identify who the Center serves. For example, your Center may focus exclusively on counter-terrorism or it may be an “all crimes” facility that focuses on crime and terrorism. Maybe it is an “all hazards” facility that includes public safety elements such as weather, traffic, and fire. The expectations or needs of the key personnel involved in the Center, such as the director or lead agency, and the Center’s customers should also be defined.

In the process of defining goals, tasks, priorities, and objectives should be defined as well. The following are examples of common Fusion Center objectives:

- Assisting and supporting local and regional criminal investigations and intelligence functions by providing better and more timely information in the form of direct assistance (i.e. services offered through crime Center personnel) or through tools and services made available within the Center (i.e. a self-service model).
- Providing regular, ongoing interactions and sharing with other regional and national intelligence centers related to homeland security issues including terrorism threats, criminal activity, port security, illegal immigration, pandemics, weather threats, training, and more.
- Providing a strategic platform that delivers and encourages collaboration and increased sharing of information among agencies and within the hosting department.
- Providing both tactical and strategic information that will address current cases and provide better situational awareness, and that may also support determination of future initiatives and deployments, in response to emerging trends and threats.

Protect Investments in Existing Systems

A second best practice to consider is ensuring that existing investments are protected. It is a well-known fact that important law enforcement and criminal justice information exists in hundreds of different systems, applications, and formats. It is not feasible or cost-effective to standardize all of these systems. Therefore, a successful data management strategy avoids a “rip and replace” methodology and, instead, provides a plan for making information from disparate systems available to each other. The Florida Department of Law Enforcement (FDLE) Law Enforcement Exchange (FLEX) initiative is an example of such a strategy. The State of Florida sought a means to share data across its seven regions and across regional, county, and local levels of law
enforcement; however the available data was maintained in hundreds of different formats by more than 500 agencies. FDLE determined the best solution would be for each region to feed data to the state system without changing the agencies’ existing systems. In doing so, FDLE simplified the data exchange process and ensured that regional and local agencies maintained their investments in existing systems. Sypherlink’s technology was chosen to accelerate the data sharing process by identifying and mapping relationships across the disparate local and regional systems without interfering with existing data sources.

**Determine Critical Data and Implement in Phases**

Given the focus of Fusion Centers, it is critical to deliver information sharing capabilities as quickly as possible. Often, however, leaders of data sharing efforts fall into a misguided attempt at “Boiling the Ocean.” They believe, at first, that it is best to access and make available all of the data at once. Months or years of resources and effort are spent to ensure that all of the information is duplicated and loaded into the target application and made available to analysts. At that point, it becomes clear that, rather than all of the available information, analysts only need certain critical information. By prioritizing information, the Center could have focused on making critical information available to analysts first and added less relevant information at a later date.

Our experience is that data sharing and intelligence efforts can show more success quickly if they are implemented in phases using an iterative process, with a defined scope of data to be shared for each phase (Figure 1, below). In addition, the work done to date and the work of other prominent agencies with established integrated justice initiatives should be leveraged. When determining what data will be shared from which sources, it is best to start small. Beginning the data exchange process with a few sources will prevent the system - and users - from being overwhelmed. A smaller set of data allows you to create and test the data architecture on a manageable set of information to ensure its success. Once the data sharing architecture is in place, additional sources can be added. For example, you could establish data sharing among the local law enforcement systems first, adding state law enforcement systems or local public safety systems later. Adding sources at a later date may be more cost-effective than dealing with too many systems or too much data in the beginning.

![Figure 1: Phased buildout of a Fusion Center to avoid “Boiling the Ocean”](image)

This phased approach to implementation is best evident within the New York City Police Department’s Real Time Crime Center (RTCC). This Center is at the leading edge of Fusion Center technology and capability. CAI was responsible for the technical architecture of the application software and for the design, development, and implementation of this high tech...
Center that serves the largest police force in the world. In starting up this Center, CAI followed the Agile Development process approach, an evolutionary lifecycle model that focuses on early and continuous delivery of software. This evolutionary lifecycle approach is similar to the traditional spiral model in that the system is developed incrementally. It differs in that, as part of each “spiral” or phase, a deliverable product undergoes testing and verification and is then delivered to the user (a “design-build-test” cycle). It is essentially a series of little waterfalls, and like spiral development, each increment executes the portion of the lifecycle needed to address the next phase of the system.

Within this phased approach, rapid development practices establish a mechanism to achieve the necessary user buy-in and feedback. This substantially lowers costs associated with implementation through the ability to rapidly incorporate change. In addition, these practices minimize development risk in the presence of potential unknowns by involving the end user all through the process. For example, our approach minimizes risk related to:

- Immature or evolving technology
- The implementation process
- Unclear and incomplete requirements or process definitions

This approach is particularly valuable because the need driving RTCC requirements continues to change and evolve, particularly as new capabilities and law enforcement practices foster a new wave of “what/if” prototypes.

When determining the scope of data to be shared, a regional approach should be developed, with a multi-jurisdictional, multi-disciplinary team for sharing and evaluating data. The GAO report explains that utilizing a broad pool of data sources not only provides information about all threats but increases the Center’s sustainability by including multiple stakeholders. The agencies involved in data sharing should include traditional players in law enforcement, such as the local police, the sheriff’s office, jail systems, court systems, and state law enforcement agencies. To enhance the value of data, non-traditional sources should also be considered, such as data from fire dispatch and reporting, emergency management, business and consumer organizations, and universities and colleges.

The federal government has recommended that Fusion Centers leverage existing state, regional, and/or local systems, such as driver’s license information, motor vehicle registration data, and correctional data. If the lead agency in your Fusion Center currently has access to national, state, or regional systems, the systems should be incorporated into your plan. Fusion Centers should also become members of a regional law enforcement network, such as the FBI’s Law Enforcement Online (LEO) and Homeland Security Information Network (HSIN) systems. It is important, however, that participating agencies continue to utilize and maintain ownership of the individual systems already in place.

In addition, information sharing with the private sector should be considered. In the President’s recently-released National Strategy for Information Sharing report, “Information Sharing with the Private Sector” is listed as a foundational element. Because the private sector owns and operates over 85% of the nation’s critical infrastructure, it is a primary source of important vulnerability and other potentially relevant consequence information. While the government possesses vast amounts of data — across and down — through federal, state, and municipal government, and unifying this is a significant effort in and by itself, vast amounts of commercial information is also available. Plentiful commercial and business information from best-in-class entities such as Acxiom and Dun & Bradstreet should be utilized for both its uniqueness of data and to unite and enrich government data assets. Commercial data providers like these invest hundreds of millions of dollars each year with the goal of perfecting both data quality and unifying disparate data sources, such as vast amounts of public records, telephone records, address/postal records, and newsworthy records. By making global business information available, companies like Dun & Bradstreet add insight into data that is not possible using stand alone content collected by the government.
Sypherlink’s acclaimed National Information Exchange (NIE) Gateway solution incorporates the databases from both Dun and Bradstreet’s commercial database and Acxiom’s consumer risk reference database. Access to these robust information sources enables Fusion Centers to join disparate government data sources and provide one-stop-shopping of complete, accurate, timely, and associated information. Through increased and united quality information, a more complete picture is obtained, improving the investigative and detection tools for homeland security.

**Define the Data Integration Approach**

Once the data sources that will be utilized by the Fusion Center are identified, the data sharing architecture should be defined. This involves determining how the data will be collected from the individual systems, and how the data will be prepared for analysis.

Each data source should be evaluated to determine what information is relevant to the Fusion Center. A software application could be used to gather only relevant information from each system and ignore any remaining data. For example, demographic data may be relevant while an e-mail address may not. The application would be used to pool the demographic data while ignoring e-mail addresses. This evaluation of data should also include identifying redundant information, value of and levels of historic information such as the name and address of an individual in both the driver’s license and vehicle registration databases. Again, the software application could identify potentially duplicate information among databases, allowing users to determine which records are truly duplicates and which are unique as well as those that are the most complete, accurate, and timely. For example, the system would notify the user that Jane Smith of Columbus, Ohio in the driver’s license database and Jane Smith of Columbus, Ohio in the vehicle registration database may be the same person. The final determination would be up to the user but should consider completeness, accuracy, and timeliness, as well as ability to help unite associations between people, places, and things.

There are many challenges in integrating data and in making the integrated data valuable and useful. Manually reviewing, comparing, and mapping data from multiple disparate systems would not only be cost-prohibitive but would prohibit future growth. Collecting and comparing data from existing disparate systems provides a major obstacle due to the fact that data may be stored and labeled differently in each system. For example, one system may title a field “LName” while another system calls a field “LastName.” Figure 2 illustrates this issue, below.

![Figure 2: Data mapping remains the leading challenge in linking disparate data sources within and among agencies](image)

In order to effectively share this information, the data must be mapped to identify where relevant relationships exist between data sources. In other words, “LName” and “LastName” must be mapped to each other as the same type of information, an individual’s last name. When performed manually, such mapping is incredibly time-consuming and often cost-prohibitive. To reduce labor hours, this mapping process can be automated by the mapping application made
available within Sypherlink’s NIE Gateway solution. This mapping application highlights data similarities and provides probability statistics of a field pair. For example, the system would notify the user that “LName” and “LastName” are very likely the same type of information.

Once the data from multiple systems is mapped, it can be presented in a uniform format. By presenting only relevant data in a uniform way, analysis of the data for crime prevention and antiterrorist activities may begin.

**Embrace Standards**

In defining and developing the data sharing architecture, the data exchange model should be based on federal standards, including the DoJ’s National Information Exchange Model (NIEM) standard. This standard was developed to facilitate data sharing among law enforcement and government data systems and is a requirement for most federal funding. Applying this standard will not only facilitate adding data sources to your Fusion Center in the future but make your Fusion Center data accessible to other agencies and other data sharing efforts, such as the FBI’s National Data Exchange (N-DEx).

While your agency may fully intend to support the NIEM framework, the fact is, a considerable investment of resources, domain expertise, training, time, effort, and cost is required to do so. Sypherlink’s NIE Gateway is the first – and only – commercially-available, off-the-shelf solution for the timely, effective, and cost efficient conformance of NIEM standards. The NIE Gateway enables Centers to meet and maintain conformance, without having to build the physical and human infrastructure to support such an effort.

**Leverage Existing Technology**

Important advancements have been made in technology over the past few years across various aspects of data management and integration. At the analytic application level, there are now many high-functioning applications that provide automatic and intelligent link analysis across people, places, and things, saving analysts hours of time. There are also proven applications that can visually represent the relationships across thousands of pieces of seemingly unrelated data, providing analysts new ways to search for information.

New and proven technology also exists at the data architecture level. One such technology, available in Sypherlink’s NIE Gateway, can speed access to data and make better use of data at the analytics level. Designed to overcome the hurdles of data sharing among law enforcement agencies, the NIE Gateway provides automated, intelligent data linkage across disparate data sources. The NIE Gateway has already improved data exchange throughout the state of Florida, where the data analysis tool is available to 400 law enforcement agencies. Data from throughout the state can be accessed and analyzed as if it were housed in a single system rather than hundreds, improving crime prevention and detection through varied, relevant, and more complete data.

The NIE Gateway utilizes patented, heuristics matching technology to automate the data discovery and mapping process. The system can support a Fusion Center in which disparate data sources are brought together virtually or are centralized in a physical environment. Data integration is achieved by searching data sources, mapping relationships, and presenting information via a NIEM-conformant layer. In addition, the NIE Gateway:

- Meets federal data exchange standards.
- Provides data in a format that facilitates data exchange with other Fusion Centers and the federal government.
- Maintains data ownership in the disparate data systems.
- Ensures ongoing conformance with rapidly-changing standards by reusing existing mapping.
- Allows your Fusion Center to meet federal grant funding requirements.
Facilitates expanding the data exchange to other systems or previous versions of data exchange standards by repurposing data mappings.

Allows your Fusion Center to more effectively utilize your resources.

Provides relevant information as a result of a single system query.

Tie Your Technology Infrastructure to Your Mission

When acquiring the proper tools to equip a Fusion Center, you should use your Center’s mission and objectives as a guide for which hardware to obtain and which software tools to utilize. Before any application is built or any tool is purchased, it is important to develop a plan to define the role of your Fusion Center and to determine the technology needed to support the Center’s functions. An infusion of technology would allow a Center to carry out its mission on an automated, real-time basis. To reach this goal, the architecture and technology of your Center should support the Center’s current and future objectives.

In addition, there are several key factors to consider when looking at the hardware and software requirements of your facility, including:

- **Scalability** – Can your system work with the newer, open standards of today’s Fusion Centers? Building a Center that can handle not only today’s technological requirements but also tomorrow’s is key to efficiently managing hardware and software expenses.

- **Integration** – Solving one problem with a single point solution (vs. multi-point solution) may be short-sighted

- **Standards** – Conformance to NIEM is essential

- **Funding** – Most Centers are funded through grants. Looking at the long-term, ongoing expenses of the Center may help determine what software and hardware expenses make up your budget.

- **Training** – Fusion Center officials should take into account the ongoing expenses of the personnel operating the Center, including the training required for personnel utilizing the software. Obtaining software that is intuitive and requires minimal training may bring long-term operating costs down substantially.

Specific hardware and software technology recommendations cannot be made due to the unique mission of each Fusion Center. However, key software packages being utilized in Fusion Centers that you should consider are geo-spatial software for mapping, pattern matching, analytics, alerts based on query-over-time requests, language ontology, entity extraction, and detailed searches of federated and non-federated data.

The establishment of credibility and stability within your Center should revolve around several key “areas of focus” that will guide your Center, from an information technology perspective, into the future. These areas of focus could include:

- **Utilizing technology to supplant labor intensive processes.** This includes calls for service, crime pattern analysis, data mining and suspect identification, resource allocation, equipment readiness, emergency management, cross regional policing issues, homeland security, 311 systems, and CAD/CAM access among others.

- **Maximizing the existing investment in your Center so as not to waste time, effort, and technology already spent.** This means utilizing the existing software, where possible, as well as GIS mapping software and other investments to seamlessly marry them with the “best of breed” technologies needed for future growth, as determined by the formal plan for this growth.

- **Investing in technology and creating applications that work from the bottom up.** That is, make the output of a Center user-friendly and have it be the kind of data that the end-user needs and uses. This includes working closely with end-users in short software
development cycles that invite immediate feedback and provides your investigators and analysts with tools that they need and use.

- Automating the integration and searching of existing databases to provide real-time links between crimes, patterns, suspects, victims, and locations both internally and externally.

- Establishing systems to deliver information to field units with respect to crimes, suspects, victims, investigations, alerts, and locations, as appropriate. This may be in the form of a Blackberry message, cell phone notifications, e-mail, text message, or page.

- Establishing systems to examine the efficiency of deployment in respect to real-time crime patterns and trends.

- Grounding all this in a flexible process methodology so that the direction of your Center stays on-track and adheres to the vision and mission of the Fusion Center.
Summary

It is clear that a well-planned, well-funded Fusion Center is a vital tool in the fight against terrorism and crime. In this day and age, criminal analysis and anti-terrorism efforts greatly depend on turning data into actionable intelligence. Following the best practices outlined here will help your Fusion Center do just that. Regarding the information to be shared, consider starting with critical information from a few sources rather than complete information from an overwhelming number of systems. Further, you should leverage existing data sharing efforts and systems, such as the LEO and HSIN systems, and embrace data exchange standards. Finally, define the data integration approach to leverage existing technology and make sure that your technology infrastructure supports the Center’s mission.

The *Guidelines* published by DoJ's Global Justice Information Sharing Initiative recommend leveraging existing components to implement and operate your Fusion Center. We recommend that you also leverage existing knowledge, and take advantage of the expertise shared by Sypherlink and Computer Aid, Inc. Specifically, Sypherlink’s National Security Practice team can assist in developing and implementing your Fusion Center strategy and thereby help you obtain appropriate funding. Also, through the NIE Gateway, Sypherlink provides Fusion Centers with fielded, existing technology that supports data integration, incorporates data from the private sector, and complies with NIEM standards. Computer Aid’s knowledge in hardware and network systems ensures that your Fusion Center is properly equipped to support your current mission and to grow to fit the Center’s future needs for gathering intelligence. Our team’s expertise will not only make your Center a more effective crime-fighting tool, but a more efficient one as well.
About the Authors

Sypherlink

Sypherlink is an information-management-software company that intelligently links critical information across disparate data sources. Its two distinct patented technologies automate much of the data sharing and integration processes, providing both corporate and public sector organizations with faster, more cost-efficient ways to locate, manage and use information. Its core technology is a heuristics matching technology that automates the discovery and mapping of data. Its virtualization technology for rapid prototyping provides the capability to access multiple physical, disparate data sources from a single, virtual query. In May 2007 the company introduced its National Information Exchange Gateway solution for accelerating and enriching government data-sharing and intelligence efforts, which includes pre-built interfaces to such rich information sources as Dun & Bradstreet and Acxiom Risk Mitigation, and conformance to the national information exchange model. Other Sypherlink sales partners include ASG, Battelle, COPLINK, IBM, Keane, Northrop Grumman, Raytheon and Unisys. Customers include government agencies, such as U.S. Department of Education, U.S. Transportation Security Agency, U.S. Army, and Florida Department of Law Enforcement (FDLE), as well as multiple Fortune 1000 financial services, insurance and healthcare organizations. For more information about Sypherlink, visit: www.sypherlink.com.

Computer Aid, Inc. (CAI)

CAI has focused, for the past twenty-five years, on providing world-class, value-add IT solutions. CAI’s service offerings include IT process transformation, business consulting, application support, application development, desktop services, and staff augmentation. Our unique methodologies enable us to provide clients with practical solutions, strategies, and techniques. Our clients attest that their partnership with CAI has enabled them to become increasingly more competitive, productive, and profitable. CAI is able to meet and satisfy clients’ individual needs because of our field proven management techniques and methodologies, our comprehensive quality control program, our superb pool of technical talent, and our laser focus on leveraging core competencies to drive ROI.

Headquartered in Pennsylvania with offices throughout the United States, Canada, Europe, and the Philippines, CAI offers several delivery options including on-site and off-site solutions from five delivery centers in the U.S. and one offshore. These Solution Delivery Centers are successfully leveraged to enable technical and management professionals, knowledgeable in CAI’s strategic methodologies, to quickly respond to client requirements. CAI is proud of their ability to provide results on-time, within budget and at a fixed price. CAI strives to assist clients to compete and succeed in today's rapidly changing business environment. For more information about CAI, visit: www.compaid.com.