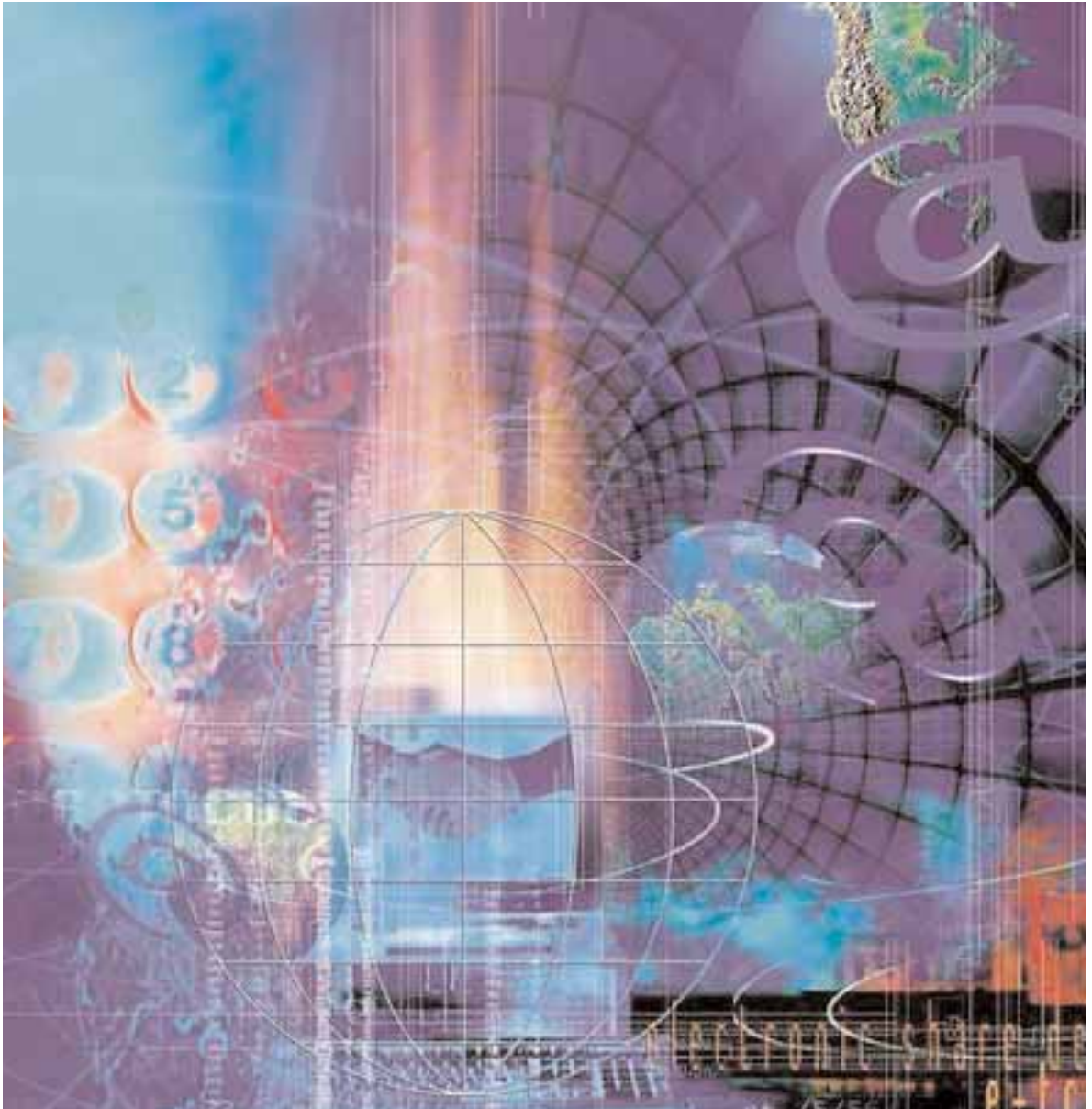




# Information Sharing & Analysis

Full strategic report at:

[www.FCW.com/InformationSharing](http://www.FCW.com/InformationSharing)



## Inside:

Social Networking, Government Experiments Drive Information Sharing into Limelight, s2  
Tips and Tricks to Improve Information Sharing, s4  
Tracking Security in Federal Information Sharing Initiatives, s5  
NHIN Showcases Information Sharing At Work, s6  
Federal Efforts to Ease Sharing of Information, s8

# Social Networking, Government Experiments Drive Information Sharing into Limelight

Information sharing has moved up and down the food chain of important federal initiatives since becoming a critical imperative in the aftermath of the attacks of Sept. 11, 2001.

Today, while many observers may cast doubt on the success of this initiative so far, others claim information sharing is gaining traction among a range of federal audiences via the advent of technologies such as social media/social networking, cloud computing and software as a service.

When the July 2004 9/11 Commission's report concluded that a failure to share information is what led to U.S. government's inability to stop the hijacking and bombing of the World Trade Center, Pentagon and United Flight 93, the initiative gained steam among federal organizations. By 2005, however, the Government Accounting Office placed information sharing on its 'high risk' list of programs facing significant management programs. Unfortunately, that's where information sharing remains in 2009, because as GAO officials reported in January, while agencies are developing an information sharing environment, the scope, projects and milestones for the future haven't been fully defined. And along with OMB, GAO also reported this initiative also lacks the metrics, or a system of accountability, which is required to ensure progress.

## Enter Social Media

The advent of social networking has breathed new life into the information sharing initiative, observers maintain. According to industry estimates there are more than 270 million Facebook users today, with 15 million who update their status daily. There are also six million Twitter users. In the government sector, "several high profile projects, such as the intelligence community's Intellipedia and the State Department's use of a wiki have peeled away the old 'need to know' mentality, and have built instead 'a need to share' culture," said Ross Mayfield, co-founder and CEO of Socialtext Inc.

Meanwhile, market research giant Nielsen estimates that one of every 11 minutes of online activity on a global basis is attributable to social networks, blogging sites and other

types of member communities. Moreover, these social computing sites are visited by more than 67 percent of the global online population, which is a trend that shows no signs of slowing, according to John Burbank, CEO of Nielsen Online. "Social networking has become a fundamental part of the global online experience," and will continue "to alter not just the global online landscape, but the consumer experience at large," he added.

Among the most notable examples of federal information sharing today comes from the intelligence community, which



is responsible for the Intellipedia wiki. Wikis are online documents that allow users to edit, add or delete information, and leave comments as necessary, to share the latest information on a given topic. Intellipedia is widely considered a resounding success because it has allowed users, including federal agents, to share information, intelligence, evidence, tips and background information across agency boundaries.

Other examples of information sharing include the Web 2.0 techniques and collaborative tools used by the Homeland Security Information Network, within the Department of Homeland Security. HSIN is a comprehensive, nationally secure and trusted web-based platform able to facilitate Sensitive But Unclassified (SBU) information sharing and collaboration among federal, state, local, tribal, private

sector and international partners.

Also, the National Information Exchange Model (NIEM) is a program originally created at the Department of Justice to standardize reporting and communication of data regarding law enforcement. Now run by the DHS, NIEM serves as a standards framework for message exchange across the entire Homeland Security community. At the same time, the Federal Emergency Management Administration has added blogging and stakeholder feedback to boost information sharing. And the Federal Health Architecture's Nationwide Health Information Network (NHIN) is working to connect federal health information systems (See related story in this special report.)

Despite the strides made so far, serious concerns remain about the privacy and security work that still must be done to improve information sharing. In March, the Markle Foundation Task Force on National Security in the Information Age reported that immediate action is needed, and President Barack Obama and Congress must reaffirm their commitment to information sharing as a top priority.

In a report for Congress and the president, the group said the sense of urgency about information sharing has lessened since the terrorist attacks of September 2001. Formed in 2002, the task force's previous recommendations served as a basis for laws and policies designed to improve information sharing. Since April 2002, the Markle Foundation Task Force, a diverse, bipartisan group of former policymakers from the Carter, Reagan, Bush, Clinton and Bush administrations, along with senior executives from the information technology industry and privacy advocates, have made numerous recommendations re: how to improve national security decision making by transforming processes and the way information is shared. Early in 2009, the Markle Task Force interviewed multiple officials on the state of information sharing to identify priorities for the new administration.

Among the top recommendations made in March:

- Make government information discoverable and accessible by increasing the use of commercially available technology.
- Enhance security and privacy protections.
- Employ metrics and incentives to measure information sharing.
- Help users drive information sharing by forming communities of interest.

According to the March report, Obama should transfer the Program Manager for the Information Sharing Environment, now under the Office of the Director of National Intelligence, to the Executive Office of the President to ensure the post has the necessary authorities. The PM-ISE was established in 2005 and coordinates the federal government's Information

Sharing Environment. The task force also recommended Obama order an initial 60-day review of the ISE's policy, privacy guidelines and processes, and conduct similar annual reviews. The reviews should focus on the overlap between law enforcement and domestic intelligence and apply best practices more broadly to areas such as cybersecurity and energy security. The task force also recommended Obama require national security agencies to use IT to make data more discoverable by tagging it when it's collected and contributing key categories of information to data indices. The group suggested having an authorized use standard so different details of the same information would be made available to different people, depending on their authorization. The group also recommended the administration link funding of programs to how well national security agencies makes information discoverable. The task force suggested conducting real-time audits of how users share information. Furthermore, according to the report, the administration should create government-wide policies on privacy and civil liberties to provide consistency, and the president and Congress should move quickly to nominate and confirm members of the Privacy and Civil Liberties Oversight Board.

To follow through on the Markle Group's recommendations, the Obama administration will likely seek help from its new CTO. According to a recent White House statement, the new CTO "is responsible for overseeing all federal IT spending and for establishing a secure IT architecture that will facilitate information sharing and interoperability among systems."

Industry observers anticipate information sharing social media platforms will continue to grow, and online information sharing and user-defined data aggregation (also known as mashups) will also continue unabated. As federal organizations seek more cost-effective alternatives to traditional, on-premise software solutions, the concepts of software as a service, cloud computing and other managed services will increase as agencies work to deploy applications more quickly. The growing trend toward 'pay-as-you-go' services, can help agencies offload various IT responsibilities to external providers so they can redirect limited internal staff resources toward more pertinent mission goals.

Meanwhile, industry observers warn that as social media grows, privacy becomes an endangered species. Users must assume no expectation of online data privacy and should participate in online information sharing communities with a full understanding that they bear responsibility for protecting sensitive or classified information. Some observers claim the "experiments" in social networking cropping up within federal organizations today require a more full examination of privacy policies and security controls. □

# Tips and Tricks to Improve Information Sharing

As federal agencies and departments strive to improve information sharing, industry experts such as Ross Mayfield, co-founder and CEO of Socialtext Inc., maintain there are several tips, tricks and best practice techniques that can be used to boost the chances for success in implementing any kind of collaborative, information sharing solution. These suggestions include:

**Tip: Start small.** Select a small project, program or process that can be made more efficient by incorporating better information sharing. Collaborative tools such as social networks, wikis, blogs and other online solutions must be used to help make information more transparent and discoverable, which can help an agency move more quickly and productively, and speed decision-making.

**Tip: Adoption is all important.** Focus not solely on the collaborative technology to be implemented, but on the adoption of that technology. Adoption is critical because the promise of enterprise collaboration solutions to dramatically improve decision cycle times and organizational effectiveness relies upon people actually using it.

**Tip: Recruit champions.** It's important to find leaders within the organization who will encourage the adoption of information sharing and connect the benefits of sharing information to a critical operational goal. Well-networked people with enthusiasm and a willingness to take a stand are more important than high-ranking officials in the organization.

**Tip: Measure adoption rates.** It's important to set metrics to help determine the benefits to be derived from, for example, sharing more information from the field. While certain implementation strategies encourage fastest adoption, adoption is not something that can be mandated. Adoption occurs when users decide that the solution provides them with a net benefit. It happens when users want to use the product, and when they take action as a result. Users very quickly weigh 'what's in it for me?' against any perceived pain, such as giving up the comfort of an old way of doing something, Mayfield explained.

For example, he continued, are users saving time in their search for personnel, expertise and information? This task

alone can take a week or more in large organizations. Creating a collaborative environment that enables employees to locate internal experts quickly, based on profiles, blogs or other work-related information posted online can be an invaluable tool for users in large organizations, Mayfield said.



**Tip: Make info sharing a byproduct of getting the job done.** The implementation of an information sharing environment can't be solely about sharing, just to share information. Instead, federal organizations should instead view the effort as an investment in a shared repository that can help employees discover information they need. Socialtext, for example, can automatically populate an information sharing environment using LDAP organizational directory information, and making that available to everyone on the social network. "A big bang approach to implementation would be to take an entire agency or department and build an online social network using LDAP and inviting employees to personalize their profiles. Where users once sent out a big email, disrupting others to locate expertise within the organization, using a Twitter-like interface instead, users can instead ask question and watch what experts say, or follow the blogs to seek out the knowledgeable experts in an organization, Mayfield explained.

**Tip: Provide incentives.** Employees should be trained in secure methods of data exchange, rewarded when they participate in information sharing initiatives and penalized when they don't. Mayfield foresees incorporating information sharing into performance appraisal systems, rating managers on how well they encourage collaboration, and workers on whether they follow through. Agencies have been asked to report their progress on participation and training. □

# Tracking Security in Federal Information Sharing Initiatives

Nowadays, risks associated with not sharing information can lead to missing clues of an attack, cost lives and endanger the nation's security. This realization has spurred the federal government's intelligence community, for example, to move from a 'need to know' mentality to a 'responsibility to provide' culture, to ensure all intelligence community members can retrieve information and effectively support intelligence requirements.

The biggest challenge federal agencies face in ongoing information sharing initiatives is in managing risks associated with the unauthorized disclosure of sensitive information. This is what led officials at the Office of the Director of National Intelligence (ODNI) to set the goal for establishing a common trust environment. ODNI's common trust environment will enable the free flow of intelligence information among intelligence community participants, based on their identity attributes mission focus and affiliations. ODNI set forth its information sharing security goals in 2008, including:

- Define a uniform identity structure and uniform attributes to enable identity management, develop uniform standards and guidance for identity management, and support decentralized, agency-specific implementation.
- Establish identity management standards for authentication, authorization, auditing, and cross-domain services.
- Develop information security policies to support logical and physical data protection efforts.
- Create a common classification guide for the intelligence community.
- Establish a risk management approach that supports the common trust and information environment while still protecting sources and methods as well as sensitive information from disclosure.

## DHS Security Efforts

Meanwhile, in the past two years, the Department of Homeland Security (DHS) has launched a number of initiatives and pilot tests to increase operational information sharing, including the DHS Secure Border Initiative; the Coast Guard-led Inter-agency Operational Centers; and the ICE Agreements of Cooperation in Communities to Enhance Safety and Security (ACCESS) program. According to a Feb.

2009 DoD Directive (number 8000.1), the primary challenge both within DHS and with external information sharing partners is creating a widely accepted process for sharing mission-relevant information, while adequately protecting the information.

According to the directive, lack of trust stems from fears that shared information will not be protected adequately or used appropriately, and that sharing will not always occur in both directions. For example, law enforcement and the intelligence community are concerned that competing information uses will compromise ongoing investigations, sources and methods. State, local, territorial, tribal and private sector partners want assurances that information held at the federal level will be shared adequately with them.

Undoubtedly, federal agencies are forced to comply with multiple security regulations while striving to implement information sharing initiatives. At the federal level, statutory and other policy mandates such as the Privacy Act of 1974, the E-Government Act of 2002, the Homeland Security Act of 2002, the Federal Information Security Management Act of 2002 (FISMA), and Executive Order 12333 require careful safeguarding of information that personally identifies U.S. citizens. Meanwhile, Executive Order 12958, as amended, defines the safeguarding requirements for classified national security information. Other federal regulations and department and agency policies set requirements for the various categories of sensitive but unclassified information. And state and local governments also have enacted privacy and data security laws.

According to the DHS's latest information sharing directive, key security components will include:

- Develop robust information protection and data security protocols that comply with applicable laws, regulations and agreements;
- Devote sufficient resources to train DHS personnel and the department's information sharing partners in appropriate security requirements, protocols, practices, and privacy and civil liberties standards; and
- Adopt technology solutions that support the appropriate level of information and data security and commit sufficient resources to the electronic and physical protection of information media. □

# NHIN Showcases Information Sharing At Work

Perhaps one of the best examples of federal information sharing today involves the work currently under way to connect federal health information systems to the Nationwide Health Information Network (NHIN).

As an eGov initiative, the Federal Health Architecture (FHA) coordinates federal efforts to work with more than 20 federal agencies, along with private hospitals and doctors' offices to build and use the NHIN to share information and support patient care, including benefits claims, public health information and numerous other health-related goals. "FHA's efforts are driven by an overwhelming need to improve information sharing," said Vish Sankaran, program director for the FHA.

Of the \$2.1 trillion spent annually on healthcare in the U.S., Sankaran reports, the federal government accounts for 40% of that total. "We needed to come together to build a common solution that will help the government reduce overall costs," he explained.

Once in operation, government organizations at all levels, along with private sector healthcare providers will connect to the NHIN to exchange information on the network. Through FHA's efforts, 20 federal agencies have already combined forces to create the open source gateway, now called CONNECT, which provides each agency with a way to tie into the NHIN. Version 1.0 of CONNECT was released last year, and six agencies have already demonstrated its viability. In late March, Version 2.0 was rolled out to federal agencies and the public to encourage software development, according to Sankaran.

CONNECT enables secure and interoperable electronic health information exchanges with other NHIN participating organizations, including federal agencies, state, tribal and local-level health organizations, and healthcare participants in the private sector. The NHIN will eventually be a vast network of public and private-sector organizations sharing information under clearly defined specifications, agreements and policies.

When CONNECT is ready for full release later this year, agencies will receive a deployable package that includes the CONNECT Gateway, along with enterprise service components and an adapter software development kit (SDK). In the meantime, a growing number of federal agencies will participate in trial implementations that

deploy an initial set of services for the secure exchange of interoperable health information.

Government agencies such as the Department of Defense, the Department of Veterans Affairs, the Social Security Administration participated in development and have demonstrated how CONNECT works. For the Social Security Administration (SSA) which processes disability claims for over 2.6 million people every year, the NHIN will provide a way to more quickly evaluate healthcare records and provide benefits to those citizens with disabilities, said Debbie Somers, senior advisor to the deputy commissioner for systems at SSA. If the provider is on the NHIN network, the medical evidence process that once took 90 days or more can be completed in minutes, which dramatically improves speed of treatment, helping the patient concentrate on getting better, rather than gaining social security benefits, she said.

"The NHIN provides us with much needed bi-directional communication," said Barry Rhodes, PhD., acting director for the division of emergency preparedness and response within the Centers for Disease Control.

The flow of information will help practitioners as it won't be just about hospitals reporting conditions. Instead, the CDC will be able to report back to hospitals and providers about outbreaks or other important information, Rhodes explained in an interview with the 1105 Government Information Group.

Each agency has unique reasons for connecting to the NHIN, and will use CONNECT to tap into this nationwide network. Among the benefits of linking to NHIN include:

- Enabling warfighters to receive coordinated care across the public and private sector. Providers will have access to medical records throughout the continuum of care, including when a soldier transitions from active duty to veteran status;
- Ensuring U.S. citizens receive health-related federal benefits to which they are entitled, in a timely manner;
- Enhancing federal, state and local agency response to public health emergencies, including disasters and pandemic diseases;
- Speeding the dissemination of clinical and scientific research results to government, industry and the scientific community;
- Improving regulation of pharmaceutical products and



medical devices through faster, more comprehensive and more accurate detection of adverse drug events.

SSA is looking forward to partnering with more health and insurance industry partners on the NHIN in 2009. Providers with electronic health records and health information exchanges can be brought on quickly, said Somers, which “will help further demonstrate the benefits, especially the speed of processing eligibility requests for

patients and providers,” she said.

Rhodes said the CDC is looking forward to sharing information at least at a summary level with hospitals and practitioners across the nation. For example, he explained, “it would be helpful to be able to provide information on how many cases of the flu are showing up in specific geographic regions at any given time.” □

### Agencies Advised to Get Started Now

As a very early adopter of the Nationwide Health Information Network (NHIN) the Social Security Administration sees a strong requirement for other federal organizations to get involved now, rather than waiting for the maturation of NHIN to learn how to share information among federal and private sector healthcare providers. “I would strongly recommend to any federal agencies involved in healthcare provision or other related services that it’s wise to participate now,” said Debbie Somers, senior advisor to the deputy commissioner for systems at SSA, rather than waiting for everything to be completed and fully matured in five years.

Involvement in this project requires participants to understand that not everything will work perfectly, and there are undoubtedly calculated risks involved. This is why she also recommends that agencies take it slowly, testing the network thoroughly and learning how the processes work. “Obviously, federal agencies can’t risk jeopardizing the security of medical records, and much additional work in both functionality and governance is still to be finalized,” she explained.

Barry Rhodes, PhD., acting director for the division of emergency preparedness and response within the Centers for Disease Control,

recommends that federal agencies or departments must realize that involvement in this evolving NHIN project requires a strong commitment, and backing from the highest levels of an organization. “Agency personnel must gain buy-in from leadership, and be will to participate in conference calls and technical meetings,” he explained.

But the sooner federal agencies participate, the more they will learn, and the more they will be able to influence the evolution of this nationwide healthcare information sharing network, Somers added. And Vish Sankaran, program director for the Federal Health Architecture maintains “the stars have aligned” to make NHIN possible as a viable network for healthcare information sharing. “We luckily have a president who wants this to happen. Congress also wants this. And citizens, too, are demanding at the point of care, to have access to their electronic health records.”

Working with 20 federal agencies has been no simple task, but Sankaran said because the agencies involved have a real need, not just a federal regulatory mandate, they have been able to come together to resolve challenges and successfully build out such an ambitious network.



# Federal Efforts to Ease Sharing of Information

As the government's efforts in improving information sharing have demonstrated, challenges remain in getting everyone in government to accept and move forward with actual information sharing initiatives.

This is why, for example, the president called for the declassification of government information on the day after his swearing in. On January 21, 2009, the President signed the Presidential Memorandum on Transparency and Open Government, and the Presidential Memorandum on the Freedom of Information Act, instructing all members of his administration to operate under principles of openness, transparency and of engaging citizens with their government.

And this is also why the recently reintroduced HR553 bill has been referred to the Committee on Homeland Security and Governmental Affairs, after being previously approved by the House of Representatives. Sponsored by Congresswoman Jane Harmon, D-Ca., the HR553 bill was reintroduced because so many law enforcement officials still find it difficult to get accurate, actionable and timely information about threats and tactics to police officers in the field. "Though hard to believe, sheriffs and police chiefs can't readily access the information they need to prevent or disrupt a potential terrorist attack because those at the federal level resist sharing information. Over-classification and pseudo-classification – stamping with any number of sensitive but unclassified markings – remain rampant," Harmon explained.

While protecting sources is often required, classifying information for the wrong reasons - to protect turf or to avoid embarrassment - is wrong, Harmon asserted in her explanation of the bill, which requires that all classified intelligence products created at the DHS be simultaneously created in a standard unclassified format. Furthermore, the bill requires portion marking – the identification of paragraphs in a document that are classified – permitting the remainder of the document to remain unclassified.

The measure is designed to promote accountability by requiring the DHS Inspector General to sample randomly classified intelligence products and identify problems that exist in those samples. It also directs the Secretary to develop a plan to track electronically how and where information classified by DHS is disseminated so that misuse can be prevented. Finally, the legislation requires



the Secretary to establish extensive annual training on the proper use of the classification regime, and penalties for staff who repeatedly fail to comply with applicable classification policies. □

[Advanced Search](#)   [Intranet](#)   [Directory](#)   [Database](#)

how to tap into our wealth of knowledge without spending a fortune



## The search is over.

Quickly find key information across your organization no matter who created it or where it resides. Use Google's powerful search engine technology to make the most of your business knowledge assets. A proven Google Enterprise Partner, Onix Networking can provide a quick and efficient deployment of the Google Search Appliance for your organization.

CALL 800-ONIX.NET OR 800-664-9638 TO FIND OUT ABOUT YOUR FREE SEARCH ASSESSMENT.



*World Class IT Solutions and Services*



Contract Holder

[www.onixnet.com](http://www.onixnet.com)