



Statement of

Kevin Fitzgerald  
Senior Vice President  
Oracle Government, Education and Health Care

Before the

Subcommittee on Technology, Information Policy,  
Intergovernmental Relations and the Census  
Committee on Government Reform

US House of Representatives

15 July 2003

Chairman Putnam, Ranking Member Clay and members of the Subcommittee, I am Kevin Fitzgerald, Senior Vice President of Oracle Government, Education and Health Care. I appreciate the opportunity to appear before you today to share Oracle's perspective on federal information systems integration and consolidation. This is an extraordinary topic that represents an even more extraordinary opportunity for government to provide better services to their customers, innovative processes for their workers, and cost effective operations for taxpayers.

Fundamentally, what we're here to discuss is how technology can enable the federal government to better manage the vast amounts of information it has in order to achieve vital policy and administrative objectives in a world where information is needed quickly and securely. It was a similar challenge within our intelligence community that gave birth to Oracle Corporation twenty-six years ago. Today, Oracle is the world's largest enterprise software company, providing information management software and expertise to 98 out of the Fortune 100, and to hundreds of departments and agencies in federal, state and local governments. We at Oracle are extremely proud to call the federal government a valued and strategic partner.

Central to that partnership is working with Mark Forman and his team at the Office of Management and Budget toward a successful implementation of the federal enterprise architecture. I don't believe anyone here can overstate the significance of this vast, complicated program. We at Oracle know all too well the challenges, opportunities, and yes, even resistance, that comes from pushing an enterprise-based information infrastructure. The reason why is simple: The enterprise approach is more than about hardware and software. It truly represents a paradigm shift in how large organizations view themselves, their functions, their capabilities, and their interdependencies.

When fully implemented, an enterprise architecture will be an enabler for the federal government, and work to the benefit of its customers, workers, and its shareholders, otherwise known as taxpayers. For the past three years, more and more of the world's most profitable enterprises have adopted an enterprise approach to information management, as have many government entities. Oracle was the first software company to provide the private and public sectors with an integrated e-business suite of applications for business processes throughout an enterprise.

However, it wasn't enough for us to simply tell our potential customers we built an entire enterprise suite. In the tradition of Orville and Wilbur Wright, we took our own creation out for a test flight to show our customers that it can work. Since an enterprise suite of software is designed to automate business processes across an entire organization, we used it to automate and transform our business processes across our entire organization. Virtually every member of the Oracle team, from developers to accountants, was essential to the success of this transformation.

When we began this experiment three years ago, we did not plan on it coinciding with the dramatic downturn in the high tech industry. Despite a significant decline in sales revenue, Oracle maintained unprecedented profitability. Our operating margins have

remained well over 30% annually over the last three years, and we stayed profitable without significant layoffs, and maintaining a global workforce of 41,000 over the last two years. By automating our own functions and processes, Oracle generated savings in excess of a billion dollars.

To understand the themes central to the success of an enterprise approach to information management, it's important to take a step back to see how businesses and government have traditionally bought and utilized information management software across the enterprise, and how an enterprise architecture dramatically changes that approach.

[[ SEE SLIDE #2 ]] Traditionally, businesses and government agencies have bought software to solve a specific operational challenge, and many of today's major software companies began by offering a very specific software solution, such as software to manage your supply chain, your sales information, or to handle your financial statements, or to market your products. In the case of very large government enterprises, like the Defense Department, there are hundreds of organizations that have this basic approach to systems and information management. So, organizations within the Air Force, for example, have their own financial management, human resource, and asset tracking systems.

[[ SEE SLIDE #3 ]] This automation age created disparate systems within an organization, each system with its own access to information. This 'best of breed' approach makes it next to impossible for the top levels of a massive agency to know what they're doing, and whether or not their achieving missions effectively and efficiently. Bottom line: the individual organization is not fulfilling its mission, and the larger enterprise is not getting the return on its IT investments.

It wasn't all that long ago when large commercial enterprises operated this way. Many still do. [[ SEE SLIDE #4 ]] Some enterprises believe the solution to this fragmentation is integration, or to stitch these individual, best of breed systems together.

[[ SEE SLIDE #5 ]] Of course, the obvious problem with stitching disparate systems together in this fashion is that it is very expensive. Imagine the enormous challenge of trying to integrate a massive government agency, like the Defense Department, by stitching, patching, maintaining, upgrading and customizing these different components within each of the services, and then stitching the systems between services in order for the entire enterprise to access and analyze information. Frankly, achieving integration in the federal government under this approach would be impossible, and a massive investment in failure. [[ SEE SLIDE #6 ]] An organization will certainly encounter information inconsistencies because stitching systems doesn't usually get to the issue of data standards. [[ SEE SLIDE #7]] Fundamentally, from a business sense, you haven't really solved the problem for your customers, you haven't been able to gain real time information access, and you certainly haven't gotten a return on your investment. [[ SEE SLIDE #8 ]] It's no surprise that, according to the IDC, in 2002, more than 75% of an IT budget is spent on maintenance-related costs. No business or government agency can

fully maximize its IT investments if it doesn't have an information infrastructure designed with the entire enterprise in mind.

What is central to the success of an enterprise architecture, whether in the commercial or public sector is a unified data model – a virtual database -- that will empower companies to solve specific challenges, like financial management, but also to take it one step further by mapping actual business processes, or business flows, across the entire enterprise. Business flows are based on real world customer experiences, and allow for businesses to have processes across multiple organizations within one enterprise.

To achieve these business flows, a business must start by focusing on the functions and processes required to achieve a business objective. This is consistent with the federal enterprise architecture – it calls for agencies to look at its functions, establishing its lines of business, so that agencies with similar missions, such as law enforcement and public health in the area of bioterror, are able to pool both resources and information so that the overall government enterprise can work against criminal activities, or to deploy medical and community resources quickly in response to a disease outbreak.

In order to achieve an integrated system across government as an enterprise, it has to start within the agencies themselves. This means that the architecture can be put together under a modular approach with each module of software pre-designed to integrate and collaborate with the other software modules, making for one family or suite of applications. Different businesses or different government agencies that utilize this enterprise suite approach also are able to share data under a common data standard, which I will discuss in greater detail in a moment. As much as we would like to think we can download some software and instantly become integrated, the current federal IT infrastructure, with disparate systems of varying levels of effectiveness, and information literally scattered everywhere, requires a modular approach to achieving effective integration and consolidation.

So, the immediate task at hand for the federal government is to achieve business flows that cut across the agency, such as the Financial Management Modernization Program within the Defense Department. At the same time, OMB is targeting key functions that will establish business flows that cut across several agencies, which is at the heart of OMB's E-Gov initiatives. A modular approach in those instances not only makes it possible for agencies to build an enterprise-based system, but also makes it possible to achieve the enterprise architecture objectives incrementally. We're currently applying this modular approach in several key government agencies, including the Department of Transportation and the Department of Homeland Security's Transportation Security Administration.

Our partnerships with Transportation and TSA represent two extremes in building an agency enterprise. In both cases, we are working to incrementally build an enterprise system on a module-by-module basis. However, with TSA, a brand-new agency, building an enterprise suite enables them to achieve the benefits of a single suite of applications right out of the box because each of the modules has been developed to work

together, saving the TSA and the taxpayer the costs associated with stitching together different systems.

An enterprise approach enables enterprises to use the information and systems initially designed to solve functional challenges, like human resource management, to broader, mission challenges, like homeland security, intelligence gathering, and benefits distribution. Marty Gruhn of Summit Strategies had one of the better characterizations of what this approach is all about: “it means that executives can focus on where their business wagon train is going, rather than on the colors of the wagon wheels.”

We agree with Mr. Forman that the federal enterprise effort first requires agencies to focus on their lines of business, but agencies should also focus on the information that is central to the success of those lines of business. Our CEO, Larry Ellison, often marvels that corporate leaders spend a dollar every day to get all the information they can out of the Wall Street Journal, but often are unable to get information on how their own businesses are doing out of systems they spent hundreds millions of dollars to install. Even though businesses are automating their processes, as I highlighted earlier, information is still all over the place -- easily fragmented, but not so easily brought together. The challenge is even greater in government, and the consequences of fragmentation can be far more costly to our own society. There was plenty of information about the 9/11 plotters scattered throughout our law enforcement and intelligence systems, but no way to bring that information together real-time. The challenges can be seen in three layers: first, information is fragmented and not easy to access; second, information is not easily shared across agencies; and third, information can be easily compromised.

When we started our e-business enterprise, we found customer information stored in different databases across the country. Our marketing, telesales, web sales, and marketing teams each had their own database of customer information. Our field sales forces also had their own customer data. And I’m just talking about the US. Imagine replicating that fragmented customer information system in the other 140 countries where we do business. That’s a lot of information scattered all over the world, and we’re just one company. The same fundamental problem exists in the federal government. All we can see are the trees – the federal agencies – and not the entire forest that is the federal government.

We can’t get information out of these fragmented systems, and we the taxpayers are paying so much more not to know and not to get the most out of this information. In looking out the external lines of business outlined in the Business Reference Model 2.0, one line of business – Defense and National Security – is going to need access to information critical to another line of business -- Intelligence Operations. The same is true for the separate lines of business for homeland security and law enforcement.

So, yes, when thinking about our federal enterprise architecture, we should be taking a functional approach, but we also have to have a simplified data model to ensure different lines of business can access mutually important information. Because, after all, bioterror

information is important to the Department of Homeland Security, but it is also important to the Centers for Disease Control, and the Department of Health and Human Services. While mutual functions will help eliminate redundancies and reduce costs, a unified data model can also be an enormous cost saver. In the end, a unified data model containing information on suspected terrorists is better than 100 scattered all over the globe, enabling all the agencies charged with fighting terrorism to be mutually cost effective and most important, mission effective.

If different agencies are going to have access to the same data, we need to solve the next layer, which is interorganizational integration. Central to this integration effort is a standardized, common data model – so that data means the same thing to all that are using it. Again, automation may have inadvertently created a problem while solving a problem. We have invested in automating individual tasks, and that’s important, but this automation has created barriers to information sharing. An enterprise architecture is an effort to complete the move from the automation age to the information age. This is obviously important in many of the functional areas identified by OMB for potential consolidation in the next round of its e-government initiative. Let me pick one of these – public health monitoring – as an example of why data element standards are so important.

It’s no secret to anyone that our current health care infrastructure is fragmented in terms of both process and the information itself. Chances are, your medical records are in a folder in a file cabinet manned by a teenage intern. In an age where bioterror threats and disease outbreaks are very real concerns, we can’t entrust medical data to a paper-based system.

Fortunately, last year, the Center for Disease Control launched the Public Health Care Information Network – a long-term commitment to modernizing, streamlining and integrating the various components of our public health reporting infrastructure. We at Oracle have put our best innovators together in developing a health care transactions base, or HTB, which utilizes our highly secure, core database technology to gather, store and relay critical health care information to those that need it, whether it is for disease surveillance, patient safety, or medical research.

For health data to flow seamlessly from a radiologist in a hospital to a general practitioner, and from there to an insurance company, requires standards to ensure data is understood by all users, protects a person’s privacy, and cannot be compromised.

The good news is that healthcare industry standards, including industry-accepted clinical, administrative, and financial terminologies are in existence to enable data to flow seamlessly. Privacy requirements mandated by Congress under the Health Insurance Portability and Accountability Act (HIPAA) also have to be met. Oracle’s healthcare transactions base is designed to operate consistent with current industry standards, adapt to changes in those standards, and protect individual privacy, while utilizing the most stable and secure database in the world.

Just as we have the technological foundation for law enforcement to collaborate to prevent another 9/11, we have similar capabilities ready to go to improve the quality of our health care infrastructure. Mark Forman often has said that the major obstacle to achieving an enterprise approach is cultural, not technological. I agree. There has to be a commitment throughout the enterprise to succeed. We at Oracle could not have achieved the financial and administrative benefits of our enterprise system without the support and participation of the entire Oracle team.

Lastly, if there is to be an enterprise approach to building an information infrastructure in government, an enterprise approach to information security is essential. Right now, not every agency factors information assurance when they buy commercial software. Given the enormous costs associated with software viruses, and the human and material resources required to apply an endless array of security patches, federal agencies, especially those that have highly sensitive information in their systems, can no longer afford to buy software that is inherently insecure.

The most significant barrier to information sharing will most likely be driven by concerns raised by organizations – private and public -- about exposing their data to potentially insecure systems. There are well-established standards for securing data and auditing its use. These standards have matured around the world and are now accepted globally. In the United States, their use is managed by NIAP, the National Information Assurance Partnership – an effective collaboration between the National Security Agency and the National Institute of Standards and Technology. The NSA and NIST jointly manage the standards and independent evaluations processes required to ensure that technology providers like Oracle are implementing secure products.

Oracle is one of a number of software companies that build security into its software development process, rather than bolting it on through a constant barrage of patches. A build-in, as opposed to a bolt-on approach to security produces better products. We even go the extra step and invest in having our software tested against internationally recognized information assurance standards, such as the Common Criteria.

An enterprise approach to security by the federal government — collectively the single largest buyer of commercial off-the-shelf software products — can change the software marketplace for the better overnight. In January of 2000, a committee within the NSA proposed that federal agencies with information systems involved in national security can only purchase commercial information assurance software that has been independently evaluated to be secure. This policy went into affect last July, and the Defense Department has developed regulations consistent with this policy, which Congress endorsed last year.

Mr. Chairman, I understand you recently expressed an interested in looking at the Defense Department regulations, and exploring the potential effectiveness of applying this approach throughout the federal government. We believe that kind of review is needed, and was also called for in the President's cybersecurity strategy.

The approach to security being pursued by DOD and the intelligence agencies should be the cornerstone of a federal enterprise security strategy. If we are going to have greater coordination and integration of information throughout and beyond the federal enterprise, strong information assurance strategies, including those involving the purchase of information assurance systems in the commercial market, are needed.

Everyone, from software CEOs to congressional committee chairmen, should get behind Mark Forman and his OMB team to ensure the federal enterprise architecture is achieved with maximum mission and financial benefits. In the end, as complicated as technology appears to be, what we're here to talk about is so, so fundamental: how can government better manage and use information in these challenging times. Oracle began its partnership with the federal government by helping the intelligence community meet this fundamental challenge, and we look forward to continuing that partnership with successes that will be felt throughout the government enterprise.

Thank you again, Mr. Chairman, and members of the Subcommittee, for the opportunity to participate in this important discussion.