

Statement of John Kern  
Director of Network Continuity  
AT&T  
Written Testimony Given Before  
The House Committee on Government Reform  
April 22, 2004

Good morning, Mr. Chairman. My name is John Kern, Director of Network Continuity for AT&T. Thank you for the opportunity to testify today about how AT&T implements its own Continuity of Operations Plan and how we provide COOP services to our customers. As you know, AT&T provides premier telecommunications including network services, information systems and professional services to the government and to the private sector. I will share with you our recommendations regarding how Federal agencies can cost-effectively obtain COOP-supporting services from the commercial sector.

AT&T provides resilient connectivity, hosting and application services to meet or exceed our customers' business needs and continuity requirements. As the nation's largest Internet backbone provider, interexchange carrier, non-Regional Bell Operating Company Local Exchange Provider, and provider of network services to businesses, we are routinely challenged to engineer and operate a network of unparalleled scale. Like our colleagues in the industry, the National Communications System has tasked us since the peak of the Cold War to provide a variety of National Security/Emergency Preparedness (NS/EP) services built to meet very unique requirements. Some of these requirements have resulted in COOP initiatives to help ensure that the AT&T network is resilient and survives, thus ensuring COOP functionality for the government. We regularly exercise these capabilities and our proprietary disaster recovery strategies that are unique and unparalleled in the industry. We exercise under a simulated, and unfortunately, sometimes a real incident environment, as evidenced by our response to the terrorist attacks of 9/11. Our response and recovery capabilities enabled us to be responsive to the needs of maintaining critical telecommunications services for the Nation as well as our most demanding customers. We continually work closely with customers to accommodate their increasing business continuity needs – such as those recently defined by legislation.

Providing resilient COOP services for our large portfolio of customers begins with having integrated continuity capabilities and built in security best practices. We have built these

Statement of John Kern  
Director of Network Continuity  
AT&T  
Written Testimony Given Before  
The House Committee on Government Reform  
April 22, 2004

capabilities into an organizational framework that facilitates their execution, both during quiet times and times of great stress. We established and utilize a rigid methodology of governance, risk assessment, protection, attack detection, and response. From the Chairman on down, every manager and organization is appropriately tasked for successful program execution.

AT&T established a system level Certification and Assurance governance process whereby we measure our estimated likelihood of recovery in the event of an incident. We then drill down to the component level and assess the consequences of a potential failure and the impact to our business. We work to mitigate the risk of failure by either eliminating the threat and the vulnerability, or mitigation of the exposure. This process constitutes our rigorous business case analysis and brings clarity to investment decisions. We have broken down COOP activities into manageable components, such as physical and logical. We assess these components both for ourselves and on behalf of our customers.

Physical level COOP has many facets. It begins by having diversity of communications links and equipment. When links and associated systems fail, there must be instantaneous and seamless rollover to backup facilities. This capability must be periodically tested, and given the frequency of cable dig-ups throughout the country, this testing occurs frequently. Service restoration must begin immediately after a disaster occurs. Our unique Network Disaster Recovery capability, the product of a \$300M+ investment over the last ten years, enables us to replicate all of the components housed in our switching centers so that we can recover full functionality within 72 hours of destruction. To my knowledge, AT&T is the only telecommunications provider with this capability. Over 150 trailers stored in multiple locations around the country are staged to be deployed at a moment's notice. We exercise this capability at least four times per year by deploying the equipment and trained personnel to the designated recovery site. If you will let me know of your interest, I would welcome the opportunity to host

Statement of John Kern  
Director of Network Continuity  
AT&T  
Written Testimony Given Before  
The House Committee on Government Reform  
April 22, 2004

your visit to one of our exercises. We will be in Miami next month, as well as San Francisco and Minneapolis later this year.

The next level of resiliency, the logical level, is where we sustain and protect our computer network facilities and interconnecting systems. We use a combination of firewalls and intrusion detection sensors and systems to ward off potential attackers. As you know, the sophistication and frequency of worms, viruses and Trojan horses is steadily rising. We are combating this phenomenon by anticipating attacks and executing strategies to defend our self and our customers. Then, rather than take it for granted that we've stopped all malevolent traffic at the perimeter, we perform similar functions within our network borders. We proactively analyze the traffic as it crosses our network to detect anomalies that would signal abnormal behavior. We essentially send a copy of all the traffic to a central computing facility that analyzes all the traffic flows for possible virus and worm signatures. When we find something that does not fit our normal signature patterns through our alarm systems, we perform forensics and may determine the traffic is a potential cyber threat. In such cases, a filter is created and deployed for network protection. Viruses and worms do not instantaneously appear but are developed over time and tested slowly and carefully so as not to attract notice. We have created the ability to evaluate the signature of customer data packets across our Internet backbone, detect attacks, and create filters for our network and information system assets and for those of our customers. As the level of sophistication steadily increases, we must provide updated tools and knowledge for continued increased vigilance to the detection of new viruses, worms, and Trojans.

Customers that host their applications with AT&T, or choose AT&T-provided applications, are routinely provided these protections and more. The same technology that we use for scanning our systems for security breaches is applied to our customers' host systems. We've also expanded our disaster recovery offering capability to include the back-up of customer data centers.

Statement of John Kern  
Director of Network Continuity  
AT&T  
Written Testimony Given Before  
The House Committee on Government Reform  
April 22, 2004

In the Federal government markets we've been working closely with the GSA to provide agencies a portfolio of security services. Government missions are too important to not have COOP. Fortunately, industry now has the ability to be responsive to these needs. After extensively surveying agency security needs, with industry they developed a Multi Tiered Security Profile that provides agencies 4 suites of security services to accommodate 4 generally accepted levels of needed security. FTS-2001 contracts, including AT&T's, were modified last year to provide this capability; and there is now traction in the uptake. For example, the recent award of the Justice Unified Telecommunications Network, or JUTNET, to AT&T included the GSA-sponsored profile.

Now, as GSA is working the next generation FTS, called FTS Networkx, we know from their industry surveys that GSA will be asking industry to provide varying levels of resilient services, defined by Service Level Agreement, to accommodate an agency's specific requirements. Through this open dialog we're confident that GSA has the understanding of the options, both commercial and non-commercial, so that FTS Networkx will provide agencies a responsive suite of security products and services to accommodate COOP needs. As appropriate, AT&T will continue to work with the agencies, GSA and the Interagency Management Council, to assure the availability of our tested and scalable security solutions.

In summary, I would like to leave you with these three key points:

- 1) Industry faces many of the same COOP challenges that agencies face
- 2) Industry has developed solutions to these challenges for both internal use and for use by customers
- 3) The scale of industry network, IT security investment, and capability should be leveraged by the government so that COOP can be affordably and timely acquired. AT&T's multibillion-dollar investment in security and business continuity in multiple levels of the business, and those of our colleague carriers, should be exploited by the government to the maximum degree possible to minimize overall government expenditures.

I thank you for your time and I am available to answer any questions that you may have.

# AT&T COOP Overview

---

Presented by John E. Kern, Network Continuity Director

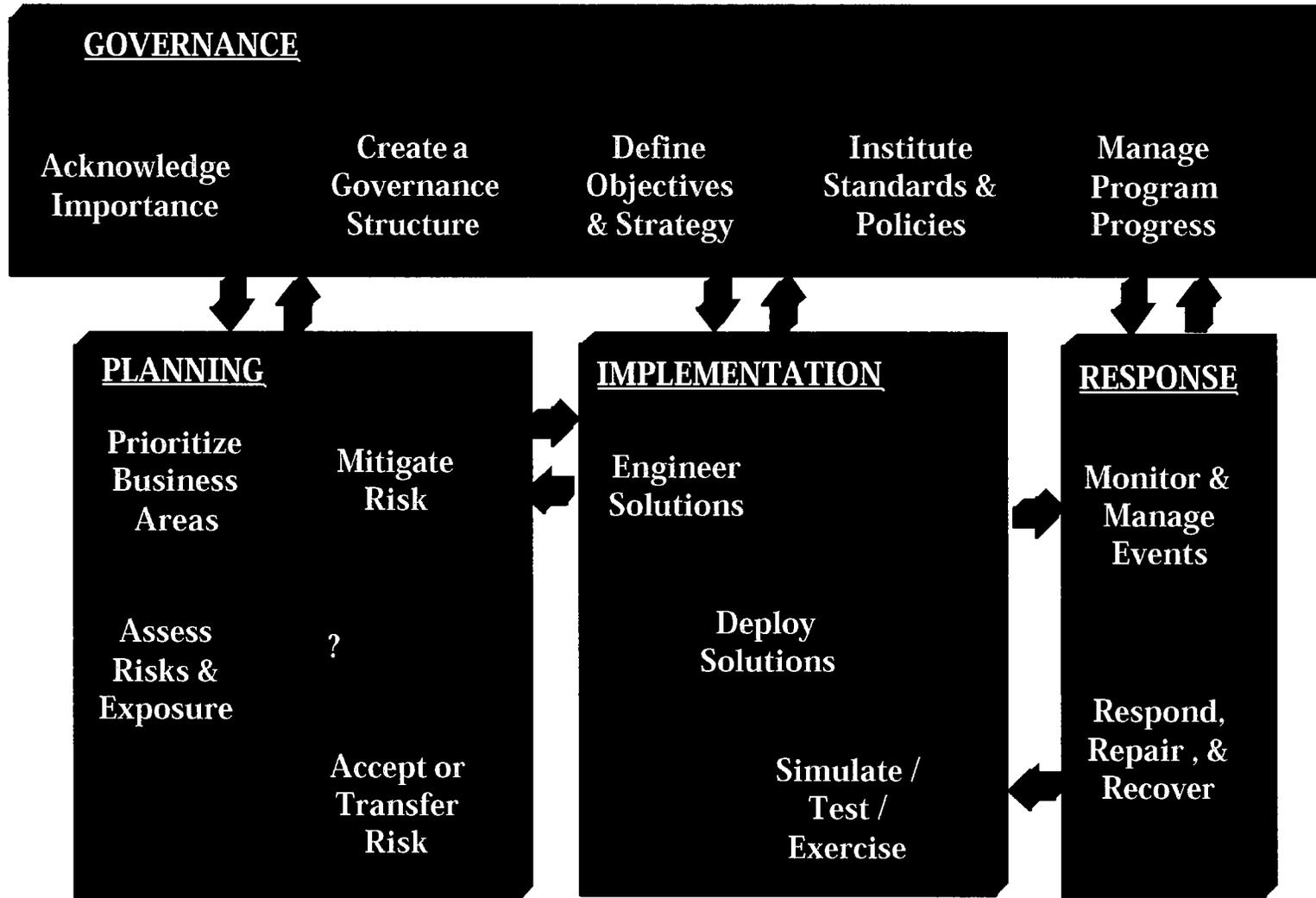


The world's networking company <sup>SM</sup>



# AT&T BC/DR Best Practices Process Overview

AT&T Global Networking Technology Services – Network Operations





# AT&T BC/DR Best Practices – Implementation

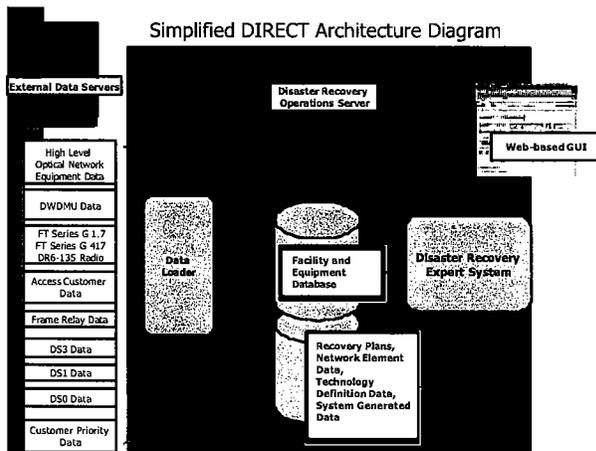
## AT&T NDR - Balanced Equation

AT&T Global Networking Technology Services – Network Operations

### NDR Operations Team



### NDR DECT



### NDR Technology Trailers





# AT&T BC/DR Best Practices – Implementation/Response Test, Manage, and Recover

AT&T Global Networking Technology Services – Network Operations

