

W A S A T C H  
DIGITAL

Connecting Business and Technology in Utah

iQ

October 2002  
Volume 2  
Issue 10  
u.s. \$3.95  
1,333 SPAM

# Homeland Security's High-Tech Honcho

Governor Mike Leavitt

Stop the In-Spam-ity

Taking Heat for High Tech

Get Smart, eBuild





# Bringing Homeland Security Home

By Bill Kerig

Homeland security. The phrase conjures images of coastal forts, high-stacked citadels — of guns and aircraft, the Alamo, the Maine. Yet when we try to bring a more modern definition to the phrase it just sort of spins into vaporware. Exactly what are these guys talking about? Is this more politico double-speak? Some glib salve for a festering wound? Another oxymoron like government efficiency? Utah Gov. Mike Leavitt says no. Not only that, he has a vision, a plan, and the position to put it into policy.

On October 5, 2001 President George Bush established the Office of Homeland Security and appointed Pennsylvania Gov. Tom Ridge as its director. The establishment of the new agency also called for a task force of nonfederal employees to study the situation and make recommendations. Leavitt was one of the first people Ridge called.

At the time, the Utah governor was staring down an immense security problem right in his own back yard: The 2002 Winter Olympic Games. The challenges that Gov. Leavitt would face in pulling off a post-September-11th Games in a peaceful and secure manner were seen as a microcosm of the nation's challenge to create real homeland security. When the Games went off without a hitch (or as you'll read about in the interview below, at least without a publicized hitch) Utah's third-term governor became one of the most sought-after experts in not only homeland security, but also the appropriate use of technology in the battle.

Today more than \$35 billion in federal money has been earmarked for homeland security and Leavitt is one of only two elected officials on the group that advises Bush on how to spend it. Not only does Gov. Leavitt serve on the President's Homeland Security Council, he also serves on the Task Force on National Security in the Information Age, which is spearheaded by the Markle Foundation in alliance with the Center for Strategic and International Studies and the Brookings Institution. The co-chairs are Markle Foundation president Zoë Baird and James Barksdale, the former chairman of Netscape Communications. Other participants include EdVenture Holdings chairman Esther Dyson, Sun Microsystems chief researcher John Gage, and former National Security Agency deputy director Bill Crowell.

In addition, Gov. Leavitt also chairs a committee on State and Local Homeland Security that was commissioned by the President's Council, co-chairs the National Governors Association Homeland Security Task Force, and is in charge of Utah's Homeland Security Task Force (which was created by Executive Order on October 4, 2001).

Accordingly, he is a man well-versed in the role information technology plays in homeland security, the rights of the states to maintain their own intelligence, and the challenge of preserving civil liberties. Digital iQ caught up with him in his office at the Capitol.

**Digital iQ:** Governor, when we think about homeland security we think about forts and Star Wars missile systems and maybe the Pentagon, but you seem to have some different ideas about it.

**Governor Mike Leavitt:** National defense is, by its very nature, a federal government responsibility. It's a top-down, mainframe organization. You do tend to think of missiles and generals and foreign lands, but homeland security is fundamentally different. Homeland security is really hometown security. The assets that have to be deployed to protect the hometowns across America are local police, fire departments, sheriffs, state and health departments, transportation systems, etc. They cannot be organized in a mainframe structure.

We're fighting a networked enemy and you can't defeat a networked enemy with a mainframe defense. You have to have a networked defense.

**DiQ:** I like the analogy, but how does that work?

**Leavitt:** We have to focus on the problems of interoperability and integration as opposed to the creation of a new system. If we try to create a new top-down system it won't work because all the information, all the data bases, all the capability lies within the 7,500 state and local entities throughout the country.

**DiQ:** So the problem with the system today is it all feeds up to the federal government and then it —

**Leavitt:** No. Nothing feeds up. Short of picking up the telephone and calling the FBI, there is no formal mechanism for transporting intelligence from a local entity to the federal agencies at this moment. Then, if the intelligence does get to the federal agencies, it's landlocked again; the FBI doesn't talk to the CIA and the CIA doesn't talk to the FBI.

That's precisely the challenge. We have to integrate horizontally — agencies within the federal government need to be able to integrate within themselves; state governments need to integrate, but at the same time there needs to be real vertical integration. That doesn't exist today.

**DiQ:** So we need a massive new infrastructure to share this information in order to make homeland security work?

**Leavitt:** No. If we tried to re-do the entire system it would be beyond our capability financially and also beyond our reach sociologically. People like to be in control of their own priorities. We need a massive project to integrate the infrastructure that exists and make sure systems are interoperable.

**DiQ:** This shifts the power to state and local governments.

**Leavitt:** In a way, yes. Homeland security will be primarily conducted by people who have another full-time job. Their role in homeland security only comes into play in rare and remote circumstances. The county sheriff in Millard County does not get up in the morning thinking, "I've got to fill my role as a soldier in the army for homeland defense."

**DiQ:** So the new system is going to change the local cop's mindset?

**Leavitt:** Part of our job is to make the county sheriff's job easier; if we can do that, he is much more likely to look after his obligations in homeland defense. By making his job more efficient we'll be able to put into play the need to transfer information to the federal government. The goal is not just to connect everybody, it's to connect with a much better system of delivering services at the local level.

**DiQ:** Making things more efficient and connecting data. That sounds like the historical province of technology.

**Leavitt:** There's no question that technology is the key to effective homeland defense. It's the only thing that makes it possible. There's virtually no other way I can see to protect every target; you can't do it on a command and control centralized basis. We would not want that kind of a system in America. We would not want control of our local communities turned over to some federale someplace. We would be suspicious of that and rightly so.

**DiQ:** So we're talking about a peer-to-peer network of homeland security?

**Leavitt:** Yes, that's basically it. A network is strong because you can knock out one piece and it continues to work. That isn't true of a centralized system. Another reason is it's less expensive. The third reason to do it is because it provides people with a series of assets that improve their lives otherwise. We have to organize vertically integrated communities of practice.

**DiQ:** Hold on, what's a community of practice?

**Leavitt:** A community of practice would be the law enforcement community or the justice (courts) community. Within each of those communities of practice there are federal agencies, state agencies, local, and private agencies. All have some responsibility for our homeland security. Let's have all the law enforcement, for example, find ways to become interoperable.

**DiQ:** Which is vertical integration, right up to the top.

**Leavitt:** Yes, that's where you start. Then you create ways to share information horizontally, between communities of practice.

**DiQ:** Do we have specific technologies in place that will facilitate these bridges?

**Leavitt:** Yes. All the existing technologies play a role. Much of this will be Web based, so as XML becomes more pervasive and systems begin to migrate to that it will provide a basis on which those things can be integrated. There also may be the creation of some new servers that state, local, and federal agencies will use to ship data to so that as things happen these servers can be notified by PDA, or cell phone, or by whatever devices are handy.

# There's no question that technology is the key to effective homeland defense. It's the only thing that makes it possible.

**DIQ:** Let's talk about your role for a second. You're on four high-level committees, including the President's Task Force on Homeland Security. With all due respect, why did the feds come to the Utah governor for help with this?

**Leavitt:** The Olympics is the primary reason. They view the Olympics as a laboratory of what needs to be accomplished in broader terms throughout the country. The fact that I've had a long-standing relationship with Governor Ridge and the President was also a factor.

**DIQ:** So what did you do at the Olympics that led them to believe that Utah and you knew something about homeland security that other people didn't?

**Leavitt:** The most important thing was the level of cooperation [we achieved] between federal, state, and local law enforcement agencies. We shared intelligence and that had not happened before.

**DIQ:** And that's remarkable? Someone outside the government just figures that the government knows what the government is doing.

**Leavitt:** Well, (a long exhale) the government is broken into many pieces. Regrettably, the government, like a lot of other large organizations, operates on a silo basis. There are a lot of contributors to that. One is our budget. We haven't had any budgets in the federal government for the development of integrated systems between agencies. Consequently when people can get a system funded in their own agency they do it. Another agency gets funded, they do it. There's no way for them to talk back and forth.

**DIQ:** And they're in competition for the same funds, so they don't really want to share.

**Leavitt:** Often. So, the number one thing we did in Utah for the Games was create a command and control mechanism that we called Utah Olympic Public Safety Command, and the legislation very clearly put the commissioner of public safety in control of that. Then we negotiated agreements among the local, state, and federal entities that when it came to law enforcement during the Games UOPSC would be the police force. As a result of that relationship we were able to have real intelligence sharing. We were able to do joint exercises, joint planning. It truly was a model of cooperation.

**DIQ:** Maybe you can provide a concrete example of that cooperation.

**Leavitt:** All our police agencies were able to talk to each other on radio. As simple as that sounds, that does not happen anywhere. The fire department typically can't talk to the police department in another town. Look at Salt Lake County: we've got 45 cities and counties. How do you coordinate all of that? How do you coordinate the highway patrol's need to communicate with the ambulance in Sandy, or the Fish and Game Department's need to have contact with the County Sheriff in Summit? We were able to create a system that did that. It took us six years to build it. It wasn't technologically that tough, it was sociologically that tough.

**DIQ:** I bet. And how long did it run?

**Leavitt:** It's still running. It's our system. Every police agency uses it every day. It not only does voice, it does data, too.

**DIQ:** So Utah may be one of the safest states out there.

**Leavitt:** We're one of the better organized, but before we jump to the conclusion that we're smarter we need to acknowledge that it's really because we started on it earlier, we had help from the Olympics for financing it, and we had a deadline. That helps a lot. We are a ways ahead of most communities because of the [Olympic] experience.

**DIQ:** So you had this unprecedented system for communication, did it work? Were there times when you needed to use it?

**Leavitt:** Yes. On the third night of the Olympics, I got a call from Bob Flowers (Utah Commissioner of Public Safety). He said, "We've got a problem. One of our monitors at the airport has detected anthrax." They had tested and retested, and all four times it tested positive.

**DIQ:** So you were the first call on this?

**Leavitt:** Yes. I was the head of the chain of command in that situation. We set up a command center at the health center at the University of Utah. [The situation] was extraordinarily complicated. I knew that tens of thousands of people would be moving through the Delta terminal, either coming to the Games or making a plane transfer. I knew that if I closed the airport, the nature of the Olympic Games would be changed permanently. The focus would shift away from athletes, the communities, and the positive things that were happening.

There were substantial moral, financial, and humanitarian needs to consider. [At first] there were those surreal “this can’t be happening to us” thoughts, then I began trying to think through what could’ve happened.

I began to conjure a circumstance where a terrorist cell had placed someone at the airport. They had gained access to the ventilation system, waited until the right moment, and then released it. Those white powdery spores had gone to every corner of the airport and people were getting off their airplanes, breathing it, and marching to other airplanes. Within a period of three hours we would have affected 100 cities and 50,000 people and no one would know it.

So I thought, how do we combat this? Who do we call? I guess I could’ve called the president, but what good would that do since we already called the EPA. The people I needed to call were the governors of the states because they would be the people who would deploy the local assets, the health departments, and the local law enforcement. And right then it became evident to me that only way this works is to create a network to deal with this kind of a situation.

**DiQ:** But it wasn’t a real threat.

**Leavitt:** Every indication told us it was a real threat and for three hours it felt very, very real. We all sat around a table and I made the decision that we were going to wait until we had a more delineating test. That would take another hour. In the meantime I brought in all the hazardous materials crews and told them to stay out of sight. I put them on the borders and perimeters of the airport.

**DiQ:** That could’ve been a real PR nightmare.

**Leavitt:** Yes, one TV news tape ... Anyway, we got them into place and we waited. I was thinking to myself that this could be a world-altering event. We had, by that time, pulled the command together to decide what we should do. Then the call came and it was a false read. What a good call to get.

**DiQ:** So the system worked?

**Leavitt:** Yes and those three hours really taught us that the only way you combat or deal with a circumstance like this is through a combination of technology and a network of local and state governments that are interoperable.

**DiQ:** So you didn’t run to the feds for anything. You didn’t call FEMA (the Federal Emergency Management Agency) first?

**Leavitt:** Do you know what FEMA is? FEMA is a federal person in a federal office who coordinates state people. They dispatch the teams, but the teams are state people. That’s the only way it can work. Who responded to 9-11? It wasn’t federal troops; it was city fire fighters and police.

**DiQ:** So in your networked scenario, homeland security shifts the balance between federal and state power toward the states. It decentralizes governmental power in much the same way the Internet has decentralized information.

**Leavitt:** This is the question and this is a real important time [for answering it]. We need to get the federal government to do its job and not try and run the states. As we organize and re-think it, most people are going to want to follow the mainframe model. And that’s not going to work. [Trying to do that] could do some real damage to the system.

**DiQ:** So you’re making recommendations to the President and to many other entities. Are you making recommendations for any technologies that Utah companies are developing?

**Leavitt:** Not directly, but I am aware of a couple companies that are making quite a profound impact on security. For example, there’s Attensity, a company that the CIA has invested in. [Attensity] provides the ability to take information from lots of different sources and find the common links. Given the state that I described to you in respect to our intelligence gathering, that technology is almost invaluable. There’s an overload of intelligence and someone needs to be able to sort through and make some sense of it.

**DiQ:** But does having you on all these task forces and committees help out Utah technology companies a little?

**Leavitt:** To the extent that I’m aware of technologies from any source, I work to connect them to the right people. Obviously I’d be more likely to see Utah companies than any other state’s because I spend more time here than in any other state. Attensity, for example, had been noticed by the CIA already, but I was able to connect them with a number of other people as well.

**DiQ:** So, there’s this huge pot of money and opportunities created by homeland security that Utah companies could get a piece of, but what should they do?

**Leavitt:** You know that old phrase, “Find a need and sell it?” Well, nowhere does that apply better than here.

**DiQ:** What needs do you have today that haven’t been filled?

**Leavitt:** I think anything to do with interoperability and integration. The capacity for computers to talk to computers, systems to talk to systems. That can happen at a lot of places in the layering of a network. There’s a heavy demand in the area of wireless. And there will obviously be a huge need for people who know how to integrate systems well.

**DiQ:** Utah has historically been a world leader in networking computers.

**Leavitt:** That’s right, so we ought to be able to contribute. I am not involved in the actual system design. What I do is help bring the levels of government together to work collaboratively to reach the objectives of interoperability and integration. If we accomplish that it will have required a lot of technical expertise, but it will also have required a lot of good politics. It’s divided in so many different ways.

# We're fighting a networked enemy. You can't defeat a networked enemy with a mainframe defense.

**DiQ:** This focus on shared information starts to sound Orwellian; Big Brother is watching from all corners of the country and he's sharing information about you. Is privacy and freedom going to be a casualty of homeland security?

**Leavitt:** It's a worry. I'd like to draw from an Olympic experience to answer this. The first day of the Olympics we were very concerned about how long it would take to get people into the opening ceremonies. For the dress rehearsal they set the magnetometer (the metal detector at the gates of the stadium) quite high and it took people an hour and a half to get through.

Then there was a big discussion about how high to set the magnetometer [for the real ceremonies]. Put it at zero and people could walk through quickly, but there would be no security. Set it at ten and there would be two hour delays, but a lot of security. Ultimately we decided we were looking for people with bombs. They weren't going to do a lot of damage with a pair of scissors. So we were able to turn the magnetometer down a bit and accomplish our goals.

In society today we're balancing that same liberty versus security quotient. It will be answered in many different ways by many different communities. It's going to be the aggregate of hundreds of different policy issues and thousands of judgments that will roll up into a state of balance.

**DiQ:** So if today our magnetometer is at five, where's it going to be in a year, five years?

**Leavitt:** I suspect that it's going to go up a notch. If it doesn't now, it will the next time there's a terrorist event. And there will be another terrorist event. At that point we'll all become concerned again. Our objective has to be to create a network of security in time to prevent it or minimize it when it occurs.

**DiQ:** Is that the mindset? Are we now going to have to tolerate a world where these terrorist attacks occur and we can't stop them? That it's all about minimizing the damage each time?

**Leavitt:** There are three priorities: To prevent, to minimize, and to respond. Is the mindset that the event will occur again? Yes.

**DiQ:** What's the basis of that?

**Leavitt:** Accurate and clear information that we're up against an enemy that has for some time been putting into our neighborhoods cells of people who are waiting for the right moment. It's just one of the risks

we deal with as a civilization. It's the reason George Bush is in the position of having to decide what to do about Iraq. If you have very serious suspicion that there is a danger it's hard to justify not acting. And yet, it's impossible in this world to know things with absolute certainty.

**DiQ:** Since Utah was already building a large security system for the Games, I'm wondering what facilities existed and what you did on September 11th.

**Leavitt:** We have a command center where we bring people from all the agencies. We got together in there and stood ready to respond. It was just watch and wait. Our first round was to inventory every crop duster in the state. I wanted to know where they were, and if they weren't where they were supposed to be, I wanted to know about it.

**DiQ:** And the federal government had a list of the crop dusters in Utah?

**Leavitt:** Yes, through the FAA. Now, you go back to the question of who does this? Well, the federal government had the list but it was powerless to do anything about it. The network asked, "Where are the crop dusters?" And the PCs came up with a plan on how to answer the question on their own. We sent the local sheriffs out to the airports to find the crop dusters. That is a good example of how the system will have to work, only we're going to have to get a lot more efficient at it.

**DiQ:** How about one other specific example of how we can get more efficient with homeland security through technology?

**Leavitt:** Okay, let's go back to the anthrax scare at the airport. We had monitors at the airport because of the Games, but what if an anthrax [attack] happened in a place where we didn't have monitors? There's no system right now for the identification of the patterns that would tell us in a timely manner that there was a huge increase in anthrax symptoms.

If we knew that all these people in a certain area were developing symptoms early, we could do something about it. But right now we have to wait weeks for people [who've been infected] to go to their doctors and then the doctors to notice an increase and report it up to a federal agency and then the federal agency to sift through the data and then call the states to deploy a solution. It just takes too long. It's completely ineffective and there's no solution for that right now. We need all this information to be networked efficiently. That's the real challenge. 