Chairman Tom Davis. Everybody take their seats. We are going to move to our second panel. It is a very distinguished panel.

We have Mr. Scott Kriens, who is the chairman and CEO of Juniper Networks. We have Paul Kurtz, the executive director of the Cyber Security Industry Alliance, and I think we have Alonzo Plough, who will be out in just a minute.

Let me just say it is our policy that all witnesses be sworn before you testify, and he will be here—oh, here he comes. Just raise your hand and say “I do.” Will you please rise and raise your right hands?

[Witnesses sworn.]

Chairman Tom Davis. Thank you, and be seated.

Mr. Kriens, we will start with you.

STATEMENTS OF SCOTT KRIENS, CHAIRMAN AND CEO, JUNIPER NETWORKS; PAUL B. KURTZ, EXECUTIVE DIRECTOR, CYBER SECURITY INDUSTRY ALLIANCE; AND ALONZO PLOUGH, BOARD OF DIRECTORS, TRUST FOR AMERICA’S HEALTH

STATEMENT OF SCOTT KRIENS

Mr. Kriens. Thank you, Mr. Chairman and members of the committee.

I’d just like to make a couple of comments today in light of what we heard earlier. And I will skip over the alarming statistics, because I’ve certainly personally heard plenty of those, and get to the question of what can we do here? And how can we make this better?

Because the real risk of the pandemic is not in the although tragic consequences of the pandemic itself; the real risk of loss is going to be in how well we do or do not handle it. And we have a great tool here. The Internet itself was, as many of you know—and I know you know, Mr. Chairman—was born from research work done by the Government in the 1960’s.

But sometimes what’s not known about that is it was actually founded on the concern in the cold war days that centers of communication and through threats from other enemies we would be disrupted as a Nation. And the Internet and the structure of its design was meant to recover communications in the event that major centers were disrupted and were out of service. And here we are, 40 or 45 years later, with an opportunity to see that vision help us through other crises.

And yet, while we can do that, we also have evidence presented earlier from Mr. Walker that isn’t what is happening. While we have 9 of 23 agencies expected to be able to respond to telework and to be able to continue operations in the COOP planning that’s been spoken about, only 1 of those has notified, zero have really demonstrated the readiness, and only 3 of 23 have tested to be prepared for teleworking.

So while we have plenty of evidence—certainly not only in our company at Juniper, but throughout Silicon Valley and in other examples across the country and private industry—there are literally millions of people capable of teleworking and prepared and using technologies to do so, we somehow find ourselves mysteriously
underprepared to see the same kind of continuous operations in command and control exhibited either in the face of a pandemic or other concerns. So it isn’t what is happening, even though it can be.

And yet, in Afghanistan, Jim Vanderhoff, the CIO of the State Department, has deployed telework capabilities for our staff, both military and civilian, in Afghanistan, who are using telework and remote capabilities to protect themselves from the dangers in a country that remote with difficulties of that magnitude in order to save life and limb, in order to continue operations there.

So while we see ourselves less prepared than we should be in our own country, we also have examples in locations as remote as Afghanistan where teleworking and the benefits of it and the ability to operate through difficulty continues.

So in light of that, I’d like to make just a couple of recommendations. And in doing so, perhaps we can use the alarm of this pandemic to make something good come out of something that may be, in fact, very bad. And the first of those recommendations is, in fact, to start at the top.

This is a capability that can be deployed today, and we need to set an example. And our first recommendation I would make and offer to the committee for consideration is that the executives and the leadership in Government are those who should adopt teleworking as a primary priority and as an example to set for others. And that with those proven examples, we have the ability to then start a wave of acceptance. Not so much by staff reports and by guidance and by hope and prayer, as was said earlier, but by actual examples set by senior leadership.

Using telework today to conduct operations before the pandemic and before the crises so that when it does happen, it’s a capability that is proven and tested and that we’re all comfortable with. So that would be probably first and primary recommendation would be let’s start this at the top and let’s make it work.

The second is to rely on the proven examples. There is proven capability, and my colleague Mr. Kurtz will speak to some of this in a moment about the ability of technology to authorize, to authenticate, and to demonstrate the legitimacy and the safety and security of this use.

It’s protecting our troops in battle. It can certainly protect our leaders in Government in our own country as a reliable tool. So we should rely on the safety, security, and proven capabilities of the technology.

And finally, to call for open standards in the implementation. These are systems which have been proven, which must and do interoperate today. And to any extent possible the committee can provide that kind of open requirement and guidance in the specifics that it drives to us in industry to deliver these technologies, it will be enormously valuable.

As a final thought and perhaps a reference, again, to where this capability has been used, one of the primary directives in engaging with the enemy is to be able to move, shoot, and communicate. And we have a very dangerous enemy facing us in this pandemic threat, and we must be able to move. We must be able to pick the targets that we are going to attack, and primarily to enable that, we must
be able to communicate as a Nation and for the Government to communicate across its leadership in order to make these capabilities a tool and a weapon in the battle that we face.

So, with that, I would like to thank you, Mr. Chairman and the committee, for the time to come and speak with you today. And certainly I look forward to answering any questions you might have.

[The prepared statement of Mr. Kriens follows:]
Statement by Mr. Scott Kriens
Chairman and CEO
Juniper Networks, Inc.
Before the Committee on Government Reform

May 11, 2006

Mr. Chairman, Congressman Waxman, members of the Committee. It is a great pleasure to testify here today about continuity of operations in the event of a serious pandemic.

A mutation of the much publicized bird or avian flu virus, one that precipitates and accelerates human-to-human transmission, is almost unimaginable to most of us here. Over crowded hospitals, quarantined communities, millions of lives at risk, our national economy crippled, stand in sharp contrast to the comforts of this room, our homes and our workplaces today.

Of course, one year ago who among us could have imagined New Orleans under water just a few months later? Five years ago, no one imagined human beings would actually hijack commercial aircraft and deliberately crash them into the World Trade Center or the Pentagon. The tsunami in Indonesia, bombings in the United Kingdom and Spain, a world at war, and the United States as the world’s only superpower, stands at center stage both for its own domestic crises and for world crises as well.

In light of these catastrophes, Americans recognize the importance of emergency preparedness by the U.S. government, the private sector, and individuals, in times of national crisis. Being prepared translates into the ability of essential employees to communicate and execute their responsibilities 24/7 anywhere, anytime. This capability is known as continuity of operations or COOP. When working with our enterprise customers to prepare for such a “perfect storm” scenario, we at Juniper Networks believe in insuring they have a secure and resilient infrastructure. The cornerstone of this round-the-clock COOP capability is a technically robust and cost-effective telework system that can deliver instant, highly secure access to every remote user – where and when they need it.

Telework, or remote work, is a concept that has gained much attention as a means for improving the productivity of the workforce while addressing pressing environmental and transportation challenges for American society. In the commercial world, private sector companies have been taking advantage of telework for years. Business managers realize that telework is a way to get optimal performance from their workers, allowing employees to get work done from home or the road, providing the operational flexibility that our modern economy demands. I find it ironic that many government managers reportedly equate telework with reduced employee work hours and lower productivity,
believing in the outdated management philosophy that “if I can’t see you, I can’t
manage you.” Business sees it the other way around, as a means of maximizing
worker productivity, with the added benefits of lower commuting costs and
improved quality of life as motivators and morale-builders.

Beyond these issues of day-to-day telework applications, it is our task in the
context of today’s hearing to concentrate on the critical linkage between telework
and national security, and to provide the most effective telework capability for
COOP given limited resources. It is worth noting that the internet was first
conceived and created by the Defense Advanced Research Projects Agency
(DARPA) as a means for sending information over a skeleton communications
system in the case of a nuclear war. So from its genesis, the internet was
envisioned as a communications system to support COOP in a national
emergency. Today the internet is a pillar of our national economy and
government operations at all levels. Executive branch agencies need only take
technologies and management practices that are readily available and bring
them to bear on this task to ensure that essential personnel can perform their
vital duties in the case of a pandemic or other national crisis.

The Executive Branch agencies are not alone in needing to enhance their remote
work plans for COOP. My bet is that Congress could benefit from an improved
remote work plan, as could state and local government and American industry.
There is no question that all of us can and must do a better job of COOP
planning generally, but remote work planning especially.

At Juniper Networks, telework is not only a critical component of how we work as
a company, but also how we think about our customers and develop our
products. I offer this Committee four recommendations that I hope will prove
helpful as you consider how the government needs to prepare for a potential
pandemic.

1. TECHNOLOGY IS AVAILABLE TODAY - FOR EFFECTIVE CONTINUITY OF
OPERATIONS THROUGH TELEWORK

We are all personally familiar with the connectivity to the workplace the Internet
affords us. It has changed our lives. With email and web access, we are able to
log on and accomplish work from out of the office that we would never have
dreamed of until a few years ago. Achieving the connectivity and control that is
necessary to maintain government operations in a crisis, however, offers a much
more technically demanding set of requirements than simply surfing the web.
Cutting edge technology enables us to meet these requirements. With the
hardware and software currently on the market, we can create a network of
remote users who, using phone, internet, and an array of collaborative tools
could continue to execute essential government operations from remote
locations.
Juniper Networks Testimony

What are the requirements we must meet to establish an effective remote work system for COOP? At the most basic level, there are two.

First, there needs to be an integrated and intelligent infrastructure that provides for the ready transmission of data, through close “integration” of all the components of the system and the right “intelligence” to help make this happen. The teleworking infrastructure is most likely the same one we use on a daily basis to communicate from our homes, consisting of the wires, fiber, and transmission towers that we all rely upon. For more challenging scenarios, however, emergency communications systems that rely on satellite communications may be required. Data flow is the essential requirement, and whether it moves through wires, fiber, or the air, it will have to be robust enough to function through a crisis.

The second requirement is network security—guaranteeing end-to-end security across the teleworking infrastructure as that remote user is gaining access to critical resources.

For example, a telework system for COOP will require virtually 100 percent confidence that the system can remotely authenticate who is accessing and using what information, and ensure that they access and use only information for which they have authorization.

Users must be able to access files securely and share information from a headquarters location anywhere, anytime, on multiple products operating on multiple platforms. The system must provide high confidence that computing technologies it uses also are authenticated as to their “trustworthiness” vis-à-vis viruses or other security breaches.

The products needed to establish and maintain just such a secure system are available now, waiting on the shelf for deployment. So the question is not whether we can establish a trusted and secure teleworking environment to support COOP, but rather how and when the system is put in place.

2. FOCUS ON CRITICAL EMPLOYEES

In our view, the best place to launch an effective telework implementation for COOP is to start with our Nation’s leaders, senior and critical executives. These are the individuals who must be able to plan, organize, and execute their agencies responses in disaster or emergency situations. Their ability to work is essential. They will set the example for how their agencies will be able to expand remote work to all of their employees to maintain operations in emergencies. Moreover, a successful COOP system will demonstrate the viability of remote work for telework during day-to-day operations as well.
Juniper Networks Testimony

The equipment and installation costs for establishing the COOP system will not bust agency budgets. The functionality the system would provide is well worth the investment in terms of the capability for COOP the system will provide. Perhaps the most challenging aspect of making the remote work system effective is putting policies and procedures in place that support orderly operations and that complement the ability of today’s technologies to allow secure, auditable information sharing. While this is a challenge, it is crucial for the system’s success, and therefore worth the effort.

I think it is important not to focus this effort solely on Executive Agencies, but on Congress as well. You as Members, and Congress as an institution, should write a plan and establish a remote work system. Putting a system in place and conducting, say, quarterly exercises yourselves and with your key staff would make the plan operational and allow you to identify and implement improvements to the business rules and technical environments that make it work. If you had possessed such a system back in 2001 during the anthrax attacks, when the House office buildings were shut for over a week, and the Senate Hart Building was closed for over three months, it would have made an enormous difference to your ability to continue your vital work.

Imagine if this were done among essential employees across the Federal government as well. I believe the result would be improved preparedness certainly, but more importantly, I believe local and state jurisdictions and American industry would better appreciate the problem and would follow the Federal lead.

3. MAINTAIN THE INTEGRITY OF THE NETWORK—BY AUTHENTICATING AND AUTHORIZING END USERS

Effective remote work plans have two significant components: business rules to determine who has access to what information and under what conditions, and the technical environment that supports the business rules. It is the technical environment that constitutes Juniper’s expertise and it is my intention to show you that information can be securely and effectively managed and tracked from multiple remote locations by any number of authorized users. The key is to have qualified guards at the gates of your critical information, guards that authenticate those seeking access and the equipment they are using to gain that access. These “guards” are technologies that easily reside on your network and navigate user and equipment access according to rules set by the governing organization. We call this comprehensive “network policing” of end user/equipment Unified Access Control.

Just a few years ago, the security of information could only be secured by equipping computers with software and component hardware that required expensive and routine maintenance and upgrade. Today, your network can function as the guard at the gate, performing that same function, more effectively,
at lower cost and with greater ease for the user. Access and information management protocols are set within the network in accordance with the business rules that are established. The network will determine whether your home PC, hotel business center or other access tool meets network standards to access information resources. And remember, unified access control ensures that the individual seeking access also is authorized.

The bottom line is that today, through your network, you can authenticate the user seeking access to ensure appropriate authorization and the equipment being used to protect against viruses, intrusions and other breaches.

4. OPEN STANDARDS ALLOW USE OF BEST-OF-BREED TECHNOLOGIES AND LOWER COSTS

In an emergency, communications necessarily will come from many sources. Technologies that govern information access and authentication must be able to recognize and interoperate with a spectrum of these technologies. The governing technologies themselves should be as interoperable as practicable with technologies from any number of manufacturers. This not only allows implementation of the best-of-breed solutions and increases operational efficiency, but also leads to lower operating cost.

CONCLUSION

To summarize, “top down” remote or telework planning and execution is critical for dealing with the grave impacts of a national crisis like an avian flu outbreak. We must get our Nation where we need to be in terms of a 24/7 essential employee, work anywhere, capability. We, as a country can be prepared for this impending perfect storm, by working together to ensure a secure and resilient infrastructure is in place and ready throughout our government; and we can start right here. The ability to effectively manage information and authorize and authenticate remote users and their equipment is both possible and practical today.

The President’s Implementation Plan for the National Strategy for Pandemic Influenza speaks to the need to improve telework capability to maintain COOP during a pandemic. It specifically requires the Office of Personnel Management to update its key telework management documents to include guidance for how best to use telework in support of COOP. I recommend that to the extent possible, this guidance focus on applying telework practices and procedures used by agencies on a daily basis to support the special circumstances of a pandemic outbreak or other emergency. A specialized telework system that is used only during an emergency will run a higher risk of problems and failures than a system that is familiar to the workforce through use on a daily or weekly basis.
Finally and just as importantly, an added benefit of “top down” remote work planning is that expansion of telework, and hence the broader benefits referenced earlier, are more likely and achievable when senior management experiences firsthand the processes involved. The United States then gains not only critical COOP advantages, but also the potential for the most advanced 21st century workforce anywhere.

I look forward to assisting the Committee in every possible way as you move forward. I would be pleased to answer any questions you might have.

On behalf of Juniper Networks, thank you for the opportunity to speak before you today. I look forward to answering your questions.

Contact:
MacKenzie Ruggiero
Juniper Networks
mruggiero@juniper.net
571-203-1987
Chairman TOM DAVIS. Thank you very much.

Mr. Kurtz.

STATEMENT OF PAUL B. KURTZ

Mr. KURTZ. Mr. Chairman, it’s a pleasure to be here today. And

beginning, I wanted to recall the little quote on the front of your

report on Katrina, which talked about the five frogs sitting on a

log. And four of the frogs decided to jump off, and how many are

left? And the answer was five.

And I think that’s the theme of what I heard earlier today. There’s a lot of, if you will, people deciding, but not doing. A lot of

guidance, but no action. And I think the flu pandemic planning

that we all must go through is an opportunity to fundamentally

change the way we do business in the Federal Government.

Obviously, my comments will focus on one of the White House’s

key goals of sustaining the infrastructure and mitigating the im-

pact of a flu pandemic. I note in 1918, there was an ad in a Cana-

dian newspaper, Canadian Bell, which talked about only using tele-

phones for emergency use. Obviously, IT has a much wider use
today. It’s integral to our society. So it’s much more than just emer-
gency use.

We know from what’s happened over the past several years that

we need to take an all-hazards approach to emergency prepared-

ness. We need to have a more resilient society. So with that in

mind, I want to cover four areas today.

First, investing in the capability to distribute—to have a distrib-

uted Federal work force. Second, using the flu pandemic to break
down Federal barriers. Third, addressing the burden that a flu

pandemic could have on the overall information infrastructure. And

fourth, offer a few recommendations.

The scenarios that play out that we see on various network TV

shows, I don’t think we need to recall necessarily what could hap-

pen during a flu pandemic. But the reality is that today’s Federal

work force, most of the contingency plans are designed for a maxi-
mum downtime of 2 or 3 days. And if you actually look at the circu-
lars that are put together, they go out to, if you will, 30 days.

Ensuring the continuity of Government operations for an ex-
tended period is a central responsibility of this Government’s lead-
ership. Moreover, when you look at the continuity plans as they
exist today, often they have people moving from one facility to-
gether to another facility. And as we know from the White House
plans, that’s not going to play out right in a flu pandemic.

The private sector has been pursuing telework for a long period
of time. In fact, with the events of September 11, a lot of the finan-
cial industry, if you will, moved their physical facilities outside
lower Manhattan. Now they’re going one step further, and they’re
actually dispersing their personnel, enabling them to work from a
variety of locations. They call this a distributed work force capabil-
ity.

AT&T, prior to the merger, of course, had a very aggressive
telework program where a variety of employees involving man-
gers, if you will, essential and nonessential employees were able
to telework on a frequent basis. The benefits are, if you will, well
known and widely accepted in the private sector. But we have
roughly one tenth of the Federal work force that is able to telework today, where you have at least 20 percent in the private sector.

When we look at the barriers to a distributed work force, I think there are a number of issues that would come to mind. In large part, they’re systemic. I think it’s interesting to note there was a lot of conversation earlier today about guidance. But just this March, GSA issued guidance which had a few very key points in it. First, agencies now are able to pay for broadband installation and monthly access. Second, they can provide new or excess equipment for people to use. Third, they can provide help desk support so we can keep on having task forces, if you will, that talk about issuing new guidance, or we can actually implement the guidance.

I note that Emergency Preparedness Circular No. 65, which was recently redone, also includes a reference to telework. So the guidance exists today for Federal agencies to do more in telework.

I do want to note, before I move on to my recommendations, that we do need to think about the burden on the overall information infrastructure during a crisis. We saw this after September 11th. We saw it in Katrina. I know your committee has looked at this. But we need to think more widely about what would happen. We need to get the appropriate private sector folks involved from whether it’s the NSTAC or NIAC, which are both Presidential advisory committees.

If I can look at recommendations, I would say, first of all, we need a top-down approach from the White House involving the Office of Management and Budget and the Homeland Security to push down into Federal agencies the need to telework and to set strict metrics.

Second, as I mentioned, I think NSTAC and NIAC, these Presidential advisory committees need to look closely at the issue of the burden on the information infrastructure. And third, I would encourage Congress to pursue a three-pronged strategy. A look at what statutory barriers there might be to the expansion of telework. For example, I understand from my conversations that agencies, if you will, don’t have the incentive to pursue telework because any gains they may make or—excuse me, savings they may make have to be returned to the Treasury.

Also there was a recent study that was done that talked about FISMA being perceived as a potential barrier to telework. I think it’s worthwhile exploring that issue as well.

And then, finally, I think we ought to think about, if you will, a carrot and stick approach. Incentivize agencies so they can win at telework.

Finally, to close, Mr. Chairman, I know last year at this time, you talked about the need to decentralize Federal agency—Federal agency operations. And I really don’t think, you know, since last year, even since September 11th, we’ve really had that change in mindset, to change from brick and mortar mentality to a decentralized Federal Government operation.

Thank you.

[The prepared statement of Mr. Kurtz follows:]
Prepared testimony of
Paul B. Kurtz
Executive Director
The Cyber Security Industry Alliance

Before the
House Committee on Government Reform
May 11, 2006
Chairman Davis, Ranking Member Wexler and members of the committee, thank you for the opportunity to testify here today.

The Cyber Security Industry Alliance is the only advocacy group dedicated to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. The organization is led by CEOs from the world’s top security providers who offer the technical expertise, depth and focus needed to encourage a better understanding of security issues. It is our belief that a comprehensive approach to ensuring the security and resilience of information systems is fundamental to global protection, national security, and economic stability.

Before joining CSIA, I served at the White House on the National Security Council and Homeland Security Council. On the NSC, I served as Director of Counterterrorism and Senior Director of the Office of Cyberspace Security. On the HSC, I was Special Assistant to the President and Senior Director for Critical Infrastructure Protection.

As I begin my remarks, I want to commend Representative Frank Wolf for his leadership in the area of telework. Congressman Wolf has been a leader in federal telework because of his passion to improve productivity and quality of life, to achieve cost savings and reduce traffic congestion and other important goals. He also recognizes that telework can enable continuity of operations regardless of disruptions like the attacks of September 11, the anthrax scare, Hurricanes Katrina and Rita, and whatever the future may hold.

I also want to commend the White House for assembling the Implementation Plan for the National Strategy to battle and contain a pandemic influenza. My comments today will focus on one of the plan’s key goals: sustaining the infrastructure and mitigating the impact of a pandemic on the economy and functioning of society.

In the early twentieth century, more than 20 million people around the world perished in the out-break of Spanish influenza. During this epidemic, technology played a key role in continuity of operations. An ad placed by Bell Canada in the fall of 1918 urged quarantined citizens to use the phone - which was relatively new at the time for the general public - for emergencies only. “You will thus be helping to keep the service intact to meet the urgent needs of the community in the present emergency.”

In the face of a flu pandemic today, information technology should not be for emergency use only, because it is integral to our daily lives and business operations. It sustains and fuels our economy, and in a crisis situation would not only help keep the public informed, but also enable us to continue working, remaining productive.

We’ve already seen, in just the past several years, the wide range of bad things that can and will happen to the United States: terrorists will strike; hurricanes and earthquakes will flood and flatten

---

1 Letter from Representative Frank Wolf to the President, September 13, 2005.
cities, major accidents will happen, and health epidemics will continue to appear. Resilience in the face of these challenges – an “all hazards” approach – encompasses protection, preparedness, and recovery. In our society, information technology holds the key to all three.

There are four areas I will cover today:

- First, the need to invest in the capability to distribute the federal workforce, by which I mean enabling Federal agency employees to function under normal and adverse conditions — not only at home, under the traditional definition of telework, but from anywhere at any time. The private sector has made great strides in this arena, for a number of reasons I’ll go over in a minute, but the federal government is unfortunately well behind.

- Second, to use the process of planning for a possible flu pandemic as an opportunity to break down some of the institutional barriers that have prevented the federal government from keeping pace with the private sector in distributing its workforce. We have an opportunity here for a paradigm shift in the federal government, from a brick and mortar mentality to a more agile, efficient workforce. The technology exists today to do so securely. Doing so would pay significant, recurring long-term dividends to the government and taxpayers well beyond just crisis management.

- Third, to address the burden that a flu pandemic would have on the overall information infrastructure, including some of the challenges of the “last mile.”

- And fourth, to offer recommendations for actions that the Federal government can take, in the near and long term, to make distributed workforce capability a reality.

**Pandemic Flu – A Biological Winter**

Leaving aside recent sensational network TV specials, I would like to emphasize the gravity of this situation by briefly describing some of the very real potential results of a flu pandemic or similar crisis.

According to the White House plan, a flu pandemic could take as long as 18 months to run its course. During this time:

- Many workers will be unable to report to their offices, either because those offices will be closed, or because they must stay at home to care for children (because schools will also be closed) or the elderly. The White House’s plan recommends that government and the private sector start with the assumption that up to 40 percent of staff may be absent for two weeks at the height of a pandemic wave, with lower levels for a few weeks on either side of a wave.

- Travel restrictions will likely include multiple forms of mass transit, ranging from subways to air travel. The safest course for many people will be to simply not leave their homes, where eventually they may have to depend on the government to provide “last mile” delivery of food and other supplies.
• Many industries—particularly those in the service sector—will significantly reduce operations. Supply chains will be disrupted, production placed on hold. However, some industries must continue to function in order to avert social breakdown: basic utilities, of course, as well as banks, hospitals, grocery stores and so forth. Even as it comes under heavy strain at the onset of the pandemic, operation of the nation’s telecommunications network will be essential for front responders to do their jobs, and for law enforcement agencies to preserve order. This is a first order concern.

• The public will need timely, reliable information about ongoing developments, because a sudden sense of both catastrophe and isolation can quickly lead to mass panic. That, in turn would quite possibly spawn a vicious cycle of looting and destruction that increases suffering and makes ultimate recovery all the more difficult.

• Most importantly, the medical community simply must have access to secure, reliable communications systems if they are to save as many lives as possible. Frontline health care providers will need to coordinate treatment services, vaccine distribution and quarantines. Academic researchers will need to exchange test results and discuss new treatment modalities. The Centers for Disease Control will need to be able to track virus vectors and mutating strains and coordinate with their counterparts overseas. Much of this type of communications traffic rides on today’s public Internet.

The Value of a Distributed Workforce

Against this backdrop, the unforgiving reality of today’s federal workforce is that most contingency plans for emergency operations are designed for a maximum downtime of two or three days. As the White House has said, pandemics play out over weeks and months. Ensuring the continuity of key government operations under that kind of an extended period is a central responsibility of the nation’s leadership.

The private sector has already begun to move aggressively in this direction. In the financial community, for example, many firms moved quickly after the attacks of September 11th to dispense critical facilities outside of lower Manhattan. Now they have gone one step further, so that their workers can work any time, anywhere. Another example is AT&T. Thirty percent of management works outside traditional offices, another 41 percent are regular teleworkers, and 91 percent of salaried employees are teleworkers. Productivity by teleworkers increased by 12.5 percent, or one hour per day. AT&T calculates $900 million in annual benefits through productivity, lower overhead, enhanced retention and recruitment.3 Note that AT&T’s efforts are not limited to “essential personnel” only.

A distributed workforce helps in all hazards – a terrorist attack, a natural disaster, or an accident. As the White House implementation plan states, during a flu pandemic, “systems that facilitate communication in the absence of person-to-person contact can be used to minimize workplace risk for essential employees and can potentially be used to minimize workplace entry of people with influ-

3 Telework at AT&T, Annual Surveys in 2004 and 2003.
enza symptoms. "During a crisis, ordinary Americans' primary and immediate concern will surely be for the safety and health of their loved ones. As the initial shock wears off, however, the ability to continue meeting their primary professional responsibilities will offer many people solace, comfort and hope.

Fortunately, as Scott Kreps explained in detail, the technology exists to make this all possible. Much of the private sector has already adopted collaborative, secure, mobile technologies – there are various options – that allow employees to work wherever they need to, be it at home, at an Internet cafe or on the road. There are also technologies available that do not require a wholesale change in infrastructure, for example through secure remote access. In many cases companies have had no choice; the world is an increasingly difficult and dangerous place to do business, and they have had to adopt new technologies to ensure that they can weather any storm that comes along. But there are also widely recognized second-order benefits to workforce distribution: productivity increases, reduced traffic congestion and gas consumption, a cleaner environment, greater personal flexibility and a higher quality of life. These benefits are well documented by such organizations as the Telework Consortium.

A serious effort to develop a distributed workforce capability in the Federal government will have a lasting impact well beyond a possible flu pandemic. In other words, building out telework is not a one-time sunk cost. Happy employees are more efficient ones, something the Office of Personnel Management has noted as it contemplates retention and recruitment challenges after the retirement of the baby boom generation. Workforce distribution holds the potential to simply make life better in countless ways. As frightening as a flu pandemic might be, it also provides us with the opportunity, and the impetus, to break down structural barriers to reform.

**Barriers to a Distributed Workforce**

So what are those barriers? The White House Plan raises the issue of telework and acknowledges its importance, and calls for updating guidance and establishing performance metrics. In fact, much of the necessary guidance exists already.

GSA issued a publication in March entitled "Guidelines for Alternative Workplace Arrangements." It covers telecommuting, hoteling, virtual offices, telework centers, and so forth, and affirms that for approved teleworkers, agencies can:

- Pay for broadband installation and monthly access fees;
- Provide new or excess equipment, including computers; and
- Provide helpdesk and technical support.

There is also Federal Preparedness Circular (FPC) 65, from FEMA, which focuses on emergency scenarios and the potential value of telework in continuity of operations planning. But despite this guidance, the various federal telework programs remain fragmentary and uncoordinated. Just over 100,000 employees, or less than ten percent of the civilian federal workforce, teleworked according to
a GAO analysis in July 2004. By contrast, more than 20 million people, or almost 20 percent of the adult American workforce overall, works remotely one or more days per month.¹

The reasons for this disparity involve the budget, statutory limitations and management.

The structure of the Federal budget may be the biggest obstacle to the expansion of telework. We understand that there is little incentive for agency leadership to adopt telework, as any savings resulting from reduced overhead are returned to the Federal treasury and cannot be applied elsewhere in an agency’s operations. Enabling agencies to realize such savings appears to at least require the intervention by the White House’s Office of Management and Budget (OMB), and possibly a change in current law. In addition, a recent CDW survey indicated that only 5 percent of IT managers believed the Federal Information Security Management Act hampered the expansion of telework.²

Finally, telework would require changes in the ways that managers interact and evaluate employees. Many supervisors insist on having “eyes on” employees, and as we all know, change is hard. There are technologies available today that help with the management of telecommuters. Technologies help managers understand who signed on when and accessed what applications, and for how long. The private sector has already demonstrated that they work, and work well.

That is why, as frightening as a pandemic influenza might be, it also provides a real opportunity to fundamentally change the way the Federal government does business – the kind of opportunity that doesn’t come along very often. As a kind of action-forcing event, it makes the kind of structural reforms possible that might otherwise be strangled by bureaucracy.

But only Congress, in partnership with the White House, can set this kind of process in motion, with a combination of statutory requirements, incentives, deadlines and evaluation criteria.

One thing worth reinforcing before I move on is that, of all the barriers to a distributed workforce, security is not among them. Again, as Scott explained, private industry has led the way. Two types of security are crucial for securing telework. They include network security for interagency communications and connections used by teleworkers, and physical security for data on mobile devices.

Devices for telework that require protection include notebook personal computers, desktop personal computers used at home, handheld personal digital assistants, telephones (regular, cell, and voice over IP [VoIP]) and desktop video conferencing. Technologies to secure these devices exist today, including, encryption, virtual private networks, authentication and access control technologies.

Burden on the Information Infrastructure

That said, there is another factor that must be taken into consideration. Little empirical evaluation has been done of the ability of the Internet infrastructure to support the traffic created when large

---

¹ 2006 American Interactive Consumer Survey conducted by the Dresner Research Group and data from the International Telework Association and Council (ITAC).
numbers of employees—from both public and private sector—suddenly attempt to log on. There will surely be a spike in telecommunications traffic overall at the first onset of a crisis.

The continued operation of the information infrastructure deserves critical attention as it underlies so many aspects of the White House’s Plan. The Plan states that the Federal Government has primary responsibility in a number of areas, including containment efforts overseas, guidance related to protective measures, modifications to law, regulation and monetary policy in order to mitigate the impact of a pandemic. The Plan pointedly does not identify the backbone of the information infrastructure as an area of primary responsibility for the Federal Government. This is proper given the private sector owns and operates the vast majority of the critical information infrastructure. However, the government must play a leading role in coordinating its continued operation during a flu pandemic, as the same pressures that would affect the nation would also affect the people who operate the Internet.

We simply do not know what the impact would be if, for example, even half the 60,000-plus employees of the Department of Health and Human Services—who help coordinate the entire national health care system—were to attempt to work offshore. We do know that any limitations on their ability to do their jobs would have a cascading effect throughout the medical system, and at the worst possible time, when large numbers of Americans are in need of emergency care.

Thus we must act to ensure that the basic information infrastructure itself is robust enough to handle the surge of, potentially, millions of teleworkers. If we do not, we run the risk of creating a virtual bottleneck that is stuck in traffic jams for twelve hours a day.

Recommendations

These are a number of strategic options that could help move the federal government toward workforce distribution capability, and strengthen America’s Internet infrastructure so it is there when we need it.

- President Bush has made clear that he is in charge of overall crisis response. Given the burdens and afflictions currently facing DHS, the role of other federal agencies should be closely examined, particularly by the Office of Management and Budget (OMB), in coordination with the Homeland Security Council, should convene a task force to aggressively expand telework. The Federal government’s efforts should not be limited to enabling “essential personnel.” They should be far more aggressive in seeking to encompass as many Federal employees as possible. As I mentioned earlier, telework within the Federal government is less than ten percent, compared with more than twenty percent in the private sector. This makes no sense. In fact, it is exactly backwards considering the critical nature of many federal programs to many Americans’ day-to-day lives. The Federal government should at the very least seek to match the private sector’s capabilities, even if it takes a crash program to do it.

- The President’s National Security and Telecommunications Advisory Committee and National Infrastructure Advisory Council should undertake an immediate review of the burden that a flu
A year ago, I, at a hearing just like this one, Mr. Chairman, you stated that “The decentralization of federal agency functions inherent in a healthy telework strategy can greatly increase the survivability of those agencies in the event of a terrorist attack or other disruptive crisis. Federal governmental agencies need to be prepared with a plan to continue doing the most important tasks to serve the American people under any circumstances.”

I wish I could sit here and testify that this goal had been met. It is true that many agencies have made strides within their own internal operations and continuity of operations planning. But they have a long way to go before they are ready to work together in a crisis like an outbreak of avian flu.

Preparing for a pandemic influenza that could last up to 18 months means the Federal government must ensure employees can provide essential services for an extended period of time in a distributed and resilient manner. And doing so requires an information technology infrastructure robust enough to handle the job. We do not have the workforce distribution capability that we need today. Mr. Chairman, and ultimately only Congress can ask the hard questions, and use both the carrots and the sticks necessary, to make telework happen.

With that, I would be happy to answer any of your questions.
Chairman Tom Davis. Thank you very much.

Dr. Plough.

STATEMENT OF ALONZO PLOUGH

Mr. PLOUGH. Thank you, Mr. Chairman and members of the committee.

On behalf of Trust for America’s Health, I really appreciate this opportunity to testify on this critically important issue of pandemic influenza preparedness.

I am here representing Trust for America’s Health, where I serve on the board of directors. I’m currently vice president for the California Endowment, a private philanthropy in the State of California also focused on these issues. But my comments are really with my hat on as a board member.

My comments are really gleaned from my 20 years of experience, though, as a local public health official—the last 10, as of last July, as director of the Seattle and King County Department of Public Health. And that on-the-ground perspective of what it means to be an effective responder in communities in disasters are the contexts that I’m drawing on today.

Recently, the public is catching up with the concern we have had in the public health community around pandemic influenza. It’s something that we have warned about for years, but I think recent events and certainly the visibility of these hearings and the visibility of the recently released report, not to mention heightened media coverage and made-for-TV movies, has raised these concerns to new levels.

The question is, how do we make sure that we have operationalized these responses on the ground that can serve the public well in the event of a pandemic?

Trust for America’s Health and other health organizations actually hear, and I heard a lot when I was a local health official, of frustration from individuals and businesses that actually believe that little or nothing can be done. And certainly a sense of fatalism does not lead to the kind of collaboration needed to develop a good response to pandemic influenza.

We have gone over in the previous panel the frightening data on the infection rates and the absenteeism of 40 percent. When I was a public health official, I was always asked, “What keeps you up at night?” Pandemic influenza planning was the single factor that kept me up at night in the complexity of what I looked at in public health, mainly because a true response is a collaboration between Government at all levels, business, schools, faith-based organization, the medical community. We’re behind the curve. We need to prepare now.

I’m very, very proud that Seattle and King County are recognized as among the most prepared communities in America for pandemic influenza, and I think it serves as an example of how a community can prepare, how the Federal Government can best encourage what local preparedness looks like. And I’m going to tell you briefly some of the things we did over those last 10 years to get to that position.

We started by defining clear lines of authority and accountability during health emergencies. The public health department is in charge in that jurisdiction, maintaining central coordinating role,
incident command role around all other governmental structures. This operational clarity is one of the—or lack of operational clarity is one of the weakest points of many other local plans, as well as the Federal plan.

Seattle and King County also benefit from having a unified public health department that includes emergency medical services. It serves both all the 40 cities in the county as well as the county as a whole. It means that public health, health care providers, first responders, trauma units, and hospitals are all connected on the ground in a way that is not common practice in most cities and counties across the country.

Additionally, Seattle and King County have an all-hazards approach to Federal preparedness. Despite of how the targeting of the funds might go, this health department thinks about what do we have to do to be ready for all kinds of threats? So clear authority, collaboration throughout the community, judicious use of Federal funds are the ingredients that led to our success and could be modeled across the Nation.

On May 3rd, the White House unveiled the detailed implementation plan for pandemic influenza. Three hundred activities already cited today—tied to specific accountability, measured in timelines—are part of that plan. And while we commend that plan in many ways, the real measure of effectiveness of a plan is its implementation and how it works on the ground.

And Trust for America’s Health plans to actively monitor the progress of how this plan is actually carried out with the nuances of community responsibility, and through that lens, we’ve identified a few specific concerns.

Well, first, it’s unclear what individual and which agency will lead the Federal response during a pandemic. The plan currently gives responsibilities to both the Department of Health and Human Services and the Department of Homeland Security without making clear which of these departments is ultimately accountable. We know that at a local level, you do need single accountability.

And Trust for America’s Health strongly believes that HHS should be designated as the lead agency, with the Secretary charged with coordinating other Federal efforts. This is a health crisis, and health expertise should guide all of the decisions. It would mirror the structure that’s worked so well in Seattle and King County.

Second, the plan does not adequately address the financial blow that the country would take during a pandemic outbreak. For example, once an effective vaccine is available, there are no measures in place to figure out how much it will cost, who will purchase the 600 million doses. We really cannot leave such important implementation decisions to the middle of a national crisis.

Beyond improving the plan, there are other steps that must be taken to ensure the Nation is prepared. Trust for America’s Health has identified some specific recommendations that are detailed in my written testimony. Let me just highlight a couple of those.

Where you live in this country, shouldn’t—rural, urban—where in the country shouldn’t determine what your level of preparedness is. We need to be much more even on that. Right now, planning largely rests on State and local shoulders. It’s unacceptable to leave
communities virtually on their own with respect to preparing for pandemic flu, particularly leaving communities with large non-
English speaking populations, like in California, with fewer re-
sources at higher risk.

Health and Human Service, in consultation with public health and medical professionals, should develop much more detailed guidance for State and local officials so this on-the-ground response matches the diversity of what preparedness means across our country. There should be priorities for—clear prioritization for the populations that are going to get limited vaccines, incentivizing mechanisms for health care workers, and equitable distribution of federally held stockpile.

Second point is that there will be ongoing life and activity after a pandemic, and we really need to ensure that the consequence management system is sound. The Government needs to take steps right now to ensure sustainability of the health industry.

This kind of response that hospitals and health providers will have to a pandemic could shut down our emergency care facilities just at the point when we need them most. People could not seek diagnostic care because they don’t—can’t pay for this. This is not a time to have individuals, because they are uninsured, also become high probability carriers of a flu in a flu outbreak.

So it’s very important that we not let affordability of the health care be a barrier to people seeking treatment and not spreading this influenza. So Trust has proposed the creation of a standby Medicaid authority that would grant emergency temporary Medicaid eligibility to individuals who are uninsured. This really helps to preserve our hospital infrastructure and make sure that individuals get treated and don’t spread the disease.

In conclusion, considerable progress has been made, really even since the 10 months that I have not been a health officer. Given where we were a year ago, I’m actually really shocked where we are today. This plan is a great improvement over the past, and a lot of progress has been made.

Lots of flaws to fix. A lot of specificity is needed. And Congress needs to really act now.

Thank you for letting me talk to you.

[The prepared statement of Mr. Plough follows:]
Written Testimony of

Alonzo Plough, MA, MPH, PhD
Member, Board of Directors
Trust for America’s Health

Submitted to

U.S. House of Representatives
Committee on Government Reform

May 11, 2006

Working Through an Outbreak:
Pandemic Flu Planning and Continuity of Operations

For further information:
Richard S. Hamburg
Director of Government Relations
Trust for America’s Health
202-223-9876 (ph)
rhamburg@tfah.org
Mr. Chairman, Ranking Member Waxman, and Members of the Committee, on behalf of Trust for America’s Health, thank you for this opportunity to testify on pandemic influenza preparedness.

My name is Dr. Alonzo Plough. I am here representing Trust for America’s Health, where I serve as a member of the Board of Directors. I also am currently Vice President of Program, Planning and Evaluation for the California Endowment but this testimony does not represent the view or policies of that organization. Additionally, my perspective is greatly influenced by my serving the last ten years as Director of the Seattle and King County Department of Public Health.

Increasingly, the American public is being made aware of the possibility of a flu pandemic. Media reports have detailed that spread of avian or bird flu across Asia, Africa and Europe. Recent television programs have documented past influenza pandemics and dramatized possible future pandemic scenarios. Sometimes this information is alarming and fear-provoking and leaves the impression that there is nothing anyone can do to prepare for or respond to a pandemic flu outbreak. That is simply not the case.

First of all, governments at every level -- federal, state and local -- have an obligation to prepare for a flu pandemic and anticipate the response to an outbreak. Last week, the Administration issued its implementation plan for pandemic influenza which builds on the National Strategy for Pandemic Influenza and the Department of Health and Human Services’ (HHS) Pandemic Influenza Plan issued last November. State and local governments are refining their pandemic flu plans and beginning to exercise them. Governments worldwide are asking all sectors of society -- businesses, schools, faith-based organizations, and the medical community -- to prepare now for a health emergency that might result in infection rates of 30 percent in the general population and absenteeism rates of up to 40 percent over a period of months. In other words, the good news is that lot of attention is being paid to pandemic preparedness. However, the bad news is that if an influenza pandemic were to strike soon, no community in the nation would be adequately prepared. As a nation we need to ratchet pandemic preparedness and response to a new level and provide the financial and human resources to deal with a health emergency of this magnitude.

Seattle and King County: A Model of Preparedness

Seattle and King County are among the most prepared communities in America for a flu pandemic. But that does not mean they are fully prepared. Even so, Seattle and King County can serve as an example of how a community can prepare, and how the federal government can best encourage and support local preparedness activities.

A series of public health threats and potential vulnerabilities provided Seattle and King County a preview of what public health threats might be coming down the line and what might be needed to do to prepare. In December of 1999, Seattle hosted the World Trade Organization (WTO)
meetings. At that time, the possible threat of a bioterrorist attack at those meetings led the Centers for Disease Control and Prevention (CDC) to make Seattle the first recipient of new syndromic disease surveillance systems, which allowed real-time monitoring of diseases in the region’s hospitals. In 2003, Seattle experienced the second largest number of suspected SARS cases in the United States. In 2004, Seattle and King County experienced a smallpox scare that was reported on a flight from Taiwan to the Seattle/Tacoma airport. These events tested the local public health system and helped government officials understand that in an infectious disease emergency, the public health department is in charge, and has a central coordinating role with other governmental agencies. In the case of a health crisis, in Seattle and King County there are clear lines of authority and accountability. This sort of operational clarity does not necessarily exist in other localities or at the federal level.

Seattle and King County also benefit from the collaborative structure of a unified public health department. The department serves both the city and county, and the Health Officer serves on both cabinets. This gives the department access to all the relevant government agencies and personnel. The Department is also responsible for the Emergency Medical Systems serving Seattle and King County, connecting it with health care providers in a way not common for other public health departments. Because of this arrangement, the public health department has a long history of interaction with first responders, trauma units and hospitals. The collaboration that comes from these relationships is essential to successful preparations and response. Other communities should build on this model as pandemic preparations are made.

Ultimately Seattle and King County preparations come from the smart use of federal funding. When CDC and the Health Resources and Services Administration (HRSA) provided funds to prepare for bioterrorism, local public health officials recognized that an all-hazards approach to preparedness would be the most effective use of those funds. Instead of focusing on hypothetical threats, the public health department used its resources to prepare for pandemic flu, knowing that based on historical trends, it was statistically more likely to occur than certain bioterrorism scenarios and that these preparations also would improve the response to smallpox, anthrax, or other public health emergencies. Seattle and King County leveraged its relatively small share of federal bioterrorism dollars and local resources to maximize preparedness across a spectrum of potential hazards.

Clear authority for the public health department, a history of collaboration within the community, experience responding to public health threats, and the judicious use of federal funding are the ingredients for Seattle and King County’s success. These components of public health preparedness can be replicated by other communities and the federal government in their planning and response to a pandemic.

The National Strategy for Pandemic Influenza Implementation Plan

On May 3rd, the White House unveiled its implementation plan for pandemic influenza. This government-wide plan represents serious progress for our national readiness to respond to a pandemic flu outbreak. It recognizes that a pandemic would impact every sector of society, and a comprehensive response involves engaging every federal agency and constituency. Significant
thought clearly went into the plan’s development, and its depth and breadth, including over 300 activities that are tied to specific accountability measures and timelines, should be commended.

We all know, however, the real test of a plan is how it is implemented. TFAH plans to actively monitor the progress of how the plan is carried out.

TFAH has also identified a number of specific concerns about the plan. First, the document is unclear about what federal official and which federal agency would take the lead in responding to a pandemic. As we saw during and after Katrina, any lack of clarity in this area can slow response time, hamper response efforts, and allow important activities to fall through the cracks. The plan currently gives responsibilities to both HHS and the Department of Homeland Security (DHS) without making clear which of these departments is ultimately accountable for pandemic response. This is too important a matter to not be resolved prior to onset of the pandemic. We, at Trust for America’s Health strongly believe that HHS should be designated as the lead agency, with the Secretary charged with coordinating the work of other federal departments and agencies. This would mirror the structure that has worked so well in Seattle and King County.

Second, the plan does not adequately address the financial impact of the pandemic once an outbreak happens. The resources it will take to implement a comprehensive response effort will be enormous. For example, once an effective vaccine is available, will the federal government purchase the 600 million doses needed to protect Americans against the pandemic strain? If so, at what cost? If not, who will be responsible for the vaccine purchase? We must think through these kinds of problems now, when we have time. We can’t leave such important decisions to be made in the midst of a health crisis.

Also, we need to take concrete steps to assure the sustainability of our nation’s health care services in a pandemic. A pandemic won’t discriminate between people who are insured or uninsured. We need policies that will encourage those who are uninsured to seek care to help contain the spread of the disease, and ensure that health care providers won’t be bankrupted by providing this care. There will be life after a pandemic, and we need to take measures so our health care system will still be standing.

**Government Progress in Preparing for Pandemic Flu**

Beyond improving the plan, there are other important steps that must be taken to ensure we are prepared. TFAH has several specific recommendations designed to ensure that the U.S. is better prepared, regardless of when the pandemic occurs.

- **Funding**

  In FY 2006, Congress provided an important down payment of $3.8 billion towards adequately preparing the nation for a pandemic outbreak, and for that we are grateful. This funding has already helped jump start pandemic readiness efforts at a number of federal agencies, including the departments of Health and Human Services, Veterans Affairs, Defense, Agriculture, Interior, Homeland Security and State
However, these funds fall well short of the President’s proposed $7.1 billion, leaving a minimum of an additional $3.3 billion to fulfill his request. The proposed FY 2007 budget proposal contains an additional $2.63 billion for HHS, $82 million for the Department of Agriculture, $10.6 million for the Department of the Interior, and $55 million for the United States Agency for International Development (USAID). The recent emergency supplemental appropriations measure approved by the Senate would accelerate the expenditure of the $2.3 billion allowance provided in the President’s FY 2007 budget. TFAH urges House and Senate conferees to include these funds in the final conference report. Congress must do all in its power to provide full funding for pandemic influenza initiatives now so that investments in vaccine technology and manufacturing, state and local preparedness and adding medicines and equipment to the Strategic National Stockpile can be made.

- **Assistance for States and Localities**

Where you live shouldn’t determine your level of protection against a pandemic in America. It is unacceptable to leave communities virtually on their own with respect to preparing for pandemic flu. A pandemic will not just strike individual states like Virginia or California or Washington. It will strike the entire United States of America, and our response must be as one. The federal government must take responsibility for many aspects of pandemic readiness, including setting a basic standard for preparedness across America. HHS, in consultation with public health and medical professionals, should develop more detailed guidance for state and local officials so that the pandemic response will be consistent and appropriate across jurisdictions. This should include guidance on prioritizing the population in the event of limited vaccine/antiviral medications; incentivizing health care workers to go to work during a pandemic; setting policies regarding isolation and travel that are uniform across the country; providing for equitable distribution of federally held stockpiles; and setting minimum standards of prevention, containment and care.

HHS, and more specifically CDC, needs to be quicker to release funds to state and local health departments. This is especially true when there are deadlines. Grantees must meet with respect to obligating funds. HHS should disburse 50 percent of the funds appropriated for state and local health department preparedness in no less than 60 days after this appropriation becomes available. However, this by no means should preclude the setting of conditions and performance measures for all funds provided to state and local health departments.

We also believe that a small amount of state and local preparedness funds should be withheld by HHS for the provision of technical assistance to state and local health departments regarding pandemic preparedness. An amount up to three percent of the funds appropriated should be sufficient.

- **State Pandemic Preparedness Plans**

Both the federal government and the states should be regularly testing their planning assumptions through exercises. HHS needs to conduct rigorous evaluations of state and local pandemic preparedness plan exercises and after-action reports. HHS should then provide
technical assistance and guidance to state and local health departments to address
deficiencies in their plans.

The ability to rapidly distribute influenza vaccine is a critical element of pandemic response. To assure that rapid, mass distribution plans are appropriately exercised, states and localities should be able to use funding provided for pandemic preparedness to purchase and distribute seasonal influenza vaccine, provided the vaccine is used in the context of a pandemic preparedness distribution exercise.

- **Communications**

The public needs to be educated about the nature of a pandemic and how they can protect themselves, both before an incident and during an outbreak. Much more needs to be done in this area. Inaccurate or incomplete information will undermine any effort to control the spread of a pandemic. The response to Hurricane Katrina and the anthrax incidents here in Congress demonstrated just how far the government has to go with respect to communicating effectively before and during a crisis in the modern 24 hour news cycle.

Officials must do a better job of taking into account the likely real-world reactions from the public, media, and decision-makers. Planning must also take into account the shortcomings in the response systems and what will happen to these systems when they are overwhelmed in mass emergency events.

Currently, most public health risk communications plans focus on how to get accurate information about health threats to the public. They rarely take into account the way the media operate in the United States, which is freely and openly. The government will not be able to tightly control every message that the public will hear during a pandemic flu outbreak. The public will witness and hear accounts of what are often worst-case scenarios and unconfirmed rumors. They will also be exposed to criticism of the government’s strategies and actions. These realities need to be factored into government plans to communicate about pandemic flu. The risk communications strategies must go beyond hourly press conferences and advisories on Web sites. The media can be an effective partner in transmitting proper information, but only if consistent and clear messages are pre-established and public distribution channels are pre-arranged.

To help fill the void, TFAH has produced a series of pamphlets entitled, *It’s Not Flu as Usual*, aimed at educating various sectors of society on steps to be taken to better prepare for a pandemic. We have already produced pieces targeted at businesses, faith-based organizations and health care providers. I respectfully request that you accept copies of these publications into the hearing record.

- **Stockpiles**

In a pandemic, development of an effective vaccine will take months. Production and distribution on the scale that will be needed may take even longer. In the meantime, we will
be dependent on traditional infection control measures and on stockpiles of medications and equipment. It is critical that these stockpiles be sufficient.

States should not be expected to cover 75 percent of the purchase price for 31 million courses of antiviral medications, as the Administration’s current plan assumes. A pandemic will be a national emergency that demands a national stockpile of medications that might mitigate the spread of the disease. Public health officials must have the flexibility to provide the medication where outbreaks are most severe, not based on a state’s ability to purchase the medication. The current Administration proposal may lead to geographic inequities which could have disastrous public health outcomes.

Most health providers order and stock supplies on a “just-in-time” basis. They often have only a few days of reserve supplies, equipment like portable respirators, and commonly prescribed medications. Therefore, CDC should also stockpile medical supplies necessary to combat a pandemic beyond vaccines and antiviral medications. This should include many basic protective items, such as protective N95 masks, gloves, gowns, and clean hospital linens, many of which are produced abroad and may not be available during a global health emergency.

- **Sustaining Our Nation’s Health Care Services**

The U.S. government must take concrete steps now to assure the sustainability of our nation’s health care services in a pandemic. A pandemic won’t discriminate between people who are insured or uninsured. We need policies that will encourage those who are uninsured to seek care to help contain the spread of the disease, and ensure that health care providers won’t be bankrupted by providing this care. There will be life after a pandemic, and we need to take measures so our health care system will still be standing.

The extraordinary health care costs of an influenza pandemic could jeopardize efforts to control it. The potential for health care providers to be overwhelmed with providing emergency care, while forgoing revenue generating activities (such as elective surgery), could force hospitals and other health care providers to close down during or immediately after a pandemic. The uninsured and underinsured could delay seeking diagnosis and treatment because of out of pocket costs they might not be able to afford. Delayed diagnosis may eliminate the value of isolation or quarantine measures and render useless potential treatments. Providers should be guaranteed some level of compensation for the services they provide during a pandemic and individuals need to recognize that cost should not delay their coming forward for diagnosis or treatment.

TFAH proposes the creation of a stand-by Medicaid authority that would permit the HHS Secretary to declare a public health emergency and grant immediate, temporary Medicaid eligibility to individuals who are uninsured or underinsured during a pandemic. The federal government would guarantee payment for 100 percent of the costs – as these additional costs are probably beyond the capacity of most states to absorb in an emergency, at a time when tax revenues are likely to be reduced. The benefit would last as long as the state of emergency is in effect.
HHS should also require operational contingency planning for a pandemic outbreak and other health emergencies from all grantees and sub-grantees that provide direct services to individuals or families as a condition of funding. It is imperative that social, health and welfare services continue during a pandemic.

Conclusion

The government has made considerable progress in preparing for a pandemic, far more than some might have expected. But there is still much to do and there are flaws in the government’s efforts that need to be corrected quickly.

The clock is ticking as the threat is growing. The Administration’s strategy, plan, and budget request help move the country toward better preparedness. But, Congress must now act expeditiously to fill the remaining weaknesses and ensure that America is as prepared as possible to face this serious health threat.

Every level of government -- federal, state and local -- must prepare for pandemic flu. Every American must hold government accountable for ensuring that every community nationwide is prepared for a worst case flu outbreak. Americans must demand that elected officials provide the leadership, funding and public policies that will mitigate the spread of pandemic flu and provide medical treatment to all those who need it.

I thank you again for this opportunity to express TFAH’s views on evaluating the U.S. readiness for the next flu pandemic.
Chairman Tom Davis. Thank you.

Mr. Kriens, you have to leave in a couple of minutes is my understanding. Is that——

Mr. Kriens. We've extended a bit of time. So please.

Chairman Tom Davis. All right. Thank you.

Well, let me start. Why do you think that Federal employees have been slow to roll out or the Federal Government has been slow to roll out teleworking employees? Now that you are sitting there, both to ask you and Mr. Kurtz. And how can we get buy-in from senior management? How do you do it in the private sector?

I will start with you, Mr. Kriens.

Mr. Kriens. It's, as you know, multi-faceted, Mr. Chairman. But if I were to put it in a commonly used phrase, I think we're trying to boil the ocean. And what we really need to do is to have use of teleworking spread in the same way the Internet itself developed, which was to sprout up in pockets and then have those pockets communicate with one another.

Ironically, as we sit here talking about pandemics, it's something we call "viral progress" in the deployment of communications and new technology. Because as people see the benefit of it through use by others and talk amongst themselves, it makes more progress in deploying these technologies than anything we can legislate or that we can dictate or that we can plan a report on.

So it's one of the reasons for our recommendation that, really, if this starts with the leadership, such as yourselves and others who are familiar with this and do use it, taking it to heart and spreading it from the top down, that will do more to motivate progress and acceleration than anything that we can do from the bottom up.

Chairman Tom Davis. We try here at the legislative branch. But ultimately, this is an executive branch function. We have continued—Mr. Davis has legislation moving, trying to get the Government to move on it. And it has just been very, very slow.

Mr. Kurtz, any comment on that?

Mr. Kurtz. Yes, I would—there are three factors that I intend to contribute. I think one is Cabinet-level agencies don't necessarily have the incentive to aggressively pursue telework. I know that in the GSA survey that was released last year, it talks about, you know, who has more telework versus less.

And it's very interesting to look at several of the senior agencies, including Labor, Treasury, and HUD. The actual number of people who are eligible for telework has gone down. So I think, you know, there is a budgetary issue that needs to be addressed.

Second, I think there is a perception among IT managers that perhaps FISMA is a barrier. I think that's probably misplaced. But FISMA could be used as, if you will, a reason as to why one cannot pursue telework.

I understand at DHS, at least, that they don't allow the use of wireless. Well, it's kind of hard to telework if you don't have any sort of wireless technology capabilities. There are technologies today to handle all of the security, the authentication issues associated with telework.

The third issue I think is basically managers wanting to have eyes on their employees. And once again, we have technology that
is available today that helps managers understand what their employees may be doing from afar. In other words, when I might come onto the computer, what applications I may access. Those type—you know, how long I'm on the system.

Those kind of issues, I think, combined, those three, create an environment where senior-level managers and agencies are not pursuing telework. You'll note that I have not said security is an issue. The technologies are out there today in order to have secure, reliable telework, and the private sector is case in point.

One final point that I think is fascinating, and you look at AT&T, the old AT&T, if you will, before the merger. Forty percent of their management was able to telework. When you ask that question of Federal executive managers, 30 percent are not allowed. That was the response, 30 percent are not allowed to telework.

And so, you know, set the standard at the top. Have managers themselves begun to telework. The guidance is in place. We don't need more guidance. It's just starting to do it.

Chairman Tom Davis. In fact, until I think a couple of years ago, when we passed legislation out of this committee, Federal contractors weren't allowed to charge telework back to the Government. And sometimes that is the most productive work.

Mr. Kriens, let me ask you the last-mile solution, such as residential broadband, will be relied on if the Federal civilian employees are to telework. How are these networks designed to ensure resilience?

Mr. Kriens. The primary source of the resilience is actually in the dispersity and the breadth of the physical infrastructure itself. By the time one gets to the last mile, whether that's a copper wire or a coaxial cable or, in some cases, as Paul mentioned, a wireless access, the pure dispersion of that is the very diversity that we need.

Any one of those points or perhaps even a neighborhood can be affected, but the protection is in the dispersion of the work force across many tens or hundreds of square miles. And there are also for key executives or for key needs an ability to, by the very nature of the competing entities here as service providers, the cable operator and the wireless operator and the traditional wire line telephone company have built three separate infrastructures.

So in the case of critical executives, it's quite possible for literally $50 a month to duplicate redundant capabilities and facilities all the way into the offices in the home of critical executives. So it's a cost issue, but it's a very modest one in the case of protecting senior leadership from any physical diversity requirement——

Chairman Tom Davis. It has to be done now. I mean, you don't want to sit and wait until this thing is on top of us.

Mr. Kriens. We cannot wait to put this in place when the work force has been immobilized. Not just the work force that we speak of, but those who must enable and go out and deploy and make those connections.

We have the ability to do that now. I think it's clearly within reach and within technical means without question. And so, now is certainly the time, and it's easily doable.
Chairman Tom Davis. And you don’t feel that basically from that, that our agency employees that deal with sensitive and classified information, those are very resolvable if we stay ahead of the game?

Mr. Kriens. Again, the best example of that is we’re using the very same technology to protect our troops in battle with the ultimate reliability requirement. They are relying today in work we do with the defense agency, you know, we are relying on battlefield information as an alternative to deploying contingent troops and materiel in battle because we need that information to know the specificity and location and magnitude of enemy force.

And we are relying on it to that degree that we are keeping our men and women out of harm’s way as a result of the use of this technology every day in conditions much more demanding than those that would be required to reach a given neighborhood in this country.

Chairman Tom Davis. Thank you.

Mr. Issa.

Mr. Issa [presiding]. Thank you, Mr. Chairman.

I will be fairly brief. I realize that you are, even with an extension, on a short leash time wise. And Mr.—I apologize—Klines?

Mr. Kriens. Kriens.

Mr. Issa. Kriens. I apologize. I am a little concerned, though, about the statement you made on $50 a month. I telecommute relatively effectively, but—and by necessity. But you can’t do it for $50 a month.

Are you saying that you think that the average Federal employee or health care provider, first responder will provide all of the software and hardware, and all we have to do is pay for the connection? Where do you get the $50 figure?

Mr. Kriens. And let me clarify, Congressman Issa, the—I was really specifically answering the question of redundancy. So there is an initial cost, as you accurately described, for setting up the computing capability, the software and security. And that will vary depending on the amount of performance and processing power.

The $50 a month is actually probably more than it would cost to deliver the physical redundancy. So that if there were a capability via your traditional telephone supplier on a DSL line over copper and one were to seek a cable line for backup or wireless access for backup, the incremental cost of that access in various counties and States around this country is in the sometimes $29 to $30 a month range.

But I was really referring purely to the cost of the chairman’s question on providing physical diversity. That’s a cost, it would probably be more in the $100 range, which would be the establishment of the capability, maybe $150 if you wanted to amortize the equipment as well, in setting up the telecommuting/telework capability.

And then the additional moneys would be for providing the physical redundancy for critical need.

Mr. Issa. And how many health care professionals do you think would be required? In other words, give me the gross number of people so we can do the multiple.
Mr. Kriens. The gross number of people that would need to telework in an emergency?

Mr. Issa. Yes.

Mr. Kriens. I’m not sure one would be capable or I’m not capable certainly of predicting that here without having a guess as to the magnitude——

Mr. Issa. More than 100,000?

Mr. Kriens. More than 100,000 people?

Mr. Issa. Well, if we look at every location in the Nation——

Mr. Kriens. Uh-huh.

Mr. Issa. And we look at every person that you would like to have this redundancy capability—and I am not trying to be unfair to your proposal. I actually want to embrace it. I am looking at when we try to turn, you know, it is like, you know, Dr. Plough?

Mr. Plough. Plough.

Mr. Issa. Plough. Thank you. Had—I am not doing good on names today.

Mr. Plough. That’s OK.

Mr. Issa. But, you know, I appreciate that we need 600 million doses of X worldwide. But then there is X, Y, Z, A, B, C. In a recent trip to Geneva, one of the questions, you know, that you have to ask is, do we invest in the ability to quickly find or quickly refine and distribute in the future Z when it comes along, or do we stockpile A, B, C, D, E, F, G of various known? And what are the cost tradeoffs?

So I really believe, and you have Virginia’s former secretary of technology right behind you. So he will smile when I say this. I really believe America needs to be connected from a redundancy standpoint in every home and that this has to be a basic capability.

Then the question is whether you are a health care professional, an AT&T executive, or a Congressman, or a school teacher, how do we analyze how much is going to be borne by our middle class citizens, and how much is going to be borne by potentially Government agencies?

Mr. Kriens. It’s an excellent point, and I have an affinity for practicality. So let me respond in kind. The actual physical redundancy requirement, I would believe, is actually quite limited because it’s only the senior executive and senior leadership for whom that degree of accessibility on an uninterrupted basis would be required.

As the reports and various study of this has delineated, there are executive leadership, there is essential and potentially non-essential, or I would prefer to think of them as perhaps less essential, for whom the redundancy is not a requirement because there are others who could substitute. And the real availability, which is a different term, is borne by the fact that the dispersed work force is scattered over hundreds or, in the case of the country, millions of square miles.

So there is no effect that would likely take out more than a pocket of them, and there are others who could substitute and fill in and come from other areas. And as a result, there isn’t a need for this kind of redundancy or additional expense other than for the senior.
And I would just start at the ultimate irreplaceable leadership. The President of the United States literally has a mobile cell that follows him across his ranch in Crawford, TX, and goes down into the gullies when he decides to go chop wood so that he is accessible, obviously, on a moment’s notice.

From there, one could step down——

Mr. Issa. And his is fully secure at the highest possible security level, too?

Mr. Kriens. We spend a lot of time at Juniper making sure of that, as a matter of fact. But we can quickly move to a case where much of the leadership really can be substituted for or for which contingency planning could avoid the hard cost, and it certainly would echo your point that we have to be practical about this and reserve those kinds of duplicate costs for only the premium and really irreplaceable leadership requirements.

Mr. Issa. And would that number be relatively similar if, instead of talking about a pandemic, we were looking at the next Hurricane Katrina?

Mr. Kriens. It’s an interesting thing. Yesterday, I’m in town also as a member of the National Security Telecommunications Advisory Committee that reports to the President, and we had our meeting yesterday. And one of the comments that was made was that Katrina itself actually replicates in many cases a nuclear threat example and certainly a pandemic example because the water didn’t come in and go out.

Most hurricanes and floods and tornadoes and other events happen over the course of 24 or 48 hours, and then we are able to rebuild the infrastructure and recover. And Katrina is actually a fantastically frightening example of what can happen if the threat is sustained and carries over weeks and months. And there’s an inability to reach infrastructure, to reestablish power, to reestablish communications, command, and control.

So it’s quite an opportunity for us to learn about how we would conduct continuous operations, and the pandemic is going to be another example of that, if and when and to what magnitude it hits. Because we will have extended loss of access to facilities and resources, and we have the wherewithal to continue operations during that extended and very difficult condition.

Mr. Issa. OK. I am going to not belabor this point, but is one that I am sure this committee was going to deal with in the future.

One last sort of the exit question that often we ask. When looking at the President’s recent proposals, 300 and some items, if you were to break them down, how many of them are dual or multi-use and have relatively small cost other than the, if you will, the preparation, the thinking, the one-time cost of preparing versus what are the major, when you get to the other extreme, what are the major items that we have to look at—not in this committee, but in the Committee on Appropriations—that are significant, very significant dollars and not one time? If you would just touch on the key ones.

Mr. Kurtz. Maybe I’ll try to come to your—let me try to come to your question a different way. I’m not going to position myself as being able to analyze the full plan that the President has put together. But in your previous question——
Mr. Issa. Pick five or six. That would probably do it.
Mr. Kurtz. We're talking about cost.
Mr. Issa. Yes.
Mr. Kurtz. And I think there are a couple of things that strike me when we talk about the area that I know best, and that is on a communications side. And first of all, just 2 or 3 years ago, we couldn't talk about having, if you will, Web-based applications. They're far more prevalent than there are today.

You made a statement that, you know, who's going to buy all the software? Well, the fact is, I can be at home now, and I can tap in through technologies that are available today that don't require me to have software on my computer. I can use a Web-based application to go in, to tap into the home bank or the enterprise, and see what I need to do and do my business.

The other thing—the other issue I'd highlight with regard to cost. A lot of the cost associated with the pandemic or planning a pandemic, if you will, may be one-time cost or a sum cost. That's not the case when you think about telework.

Telework helps us with routine activity every day, everyday business activity in the Federal Government. It also helps us with all hazards. It's not just a one-time sum cost to help us with a pandemic. It helps us with a hurricane. It helps us with a terrorist attack. It helps us with a blizzard. And so, if we can change our mindset to think more broadly about this, then I think it would be helpful.

And the final comment, if I can, is to think about scope. There's a lot of conversation about only essential employees. I disagree. I think we ought to dig deeper into the agency and think more broadly about who is included and just as an estimate, you know, the top third or so of the agency.

So that when we look at contingency plans as the guidance that the Federal Government has today, it's 72 hours or so that you can exist on essential employees. Then you're dispersing to a location for like 30 days. It's only the top employees.

Well, when you look at the plan that the White House has put together, we're well beyond 30 days. So the essential employees are not—not—going to be able to keep the operation going for an extended period of time. So we have to dig down more deeply into agencies as we think about the flu pandemic.

Mr. Plough. If I could just respond from the public health side?
Mr. Issa. Yes, please.

Mr. Plough. The President's plan builds multi-use capacity that is applicable to many kinds of infectious diseases, earthquake, floods, because it heightens the connectivity of first responders with community in a way that, if funded appropriately, is sustainable and builds a missing piece of our protective structure for public health.

So those—there are sustainable and multi-use components of this. Pandemic is one of the worst cases. If you are properly prepared for pandemic influenza, you are prepared for SARS, you are prepared for West Nile, you are prepared for an earthquake. You are prepared for a variety of public health disasters.

Mr. Issa. Excellent. Well, I don't have any other questions.
The record will remain open for 5 legislative days for any additional questions from people that are not able to be at the dais and so you may revise and extend as your rather cogent capabilities allow you to think of things.

In addition, I would like to thank you very much for the generosity of your time, being here today, and the thoroughness, including the fact that no one is rubber-stamping somebody else and that we do have a very active debate because of this hearing between what happens on day 1 and what happens after day 30.

And with that, we stand adjourned.

[Whereupon, at 12:17 p.m., the committee was adjourned.]

[The prepared statements of Hon. Dan Burton and Hon. Darrell E. Issa follow:]
Mr. Chairman, thank you for holding this important and timely hearing on our public health system’s pandemic flu response capabilities at the federal, state, and local levels. As the Committee has rightly observed, the past few annual influenza seasons, as well as recent avian flu activity in Asia, raise disturbing questions about whether the U.S. is truly prepared to deal with the threat of a flu pandemic and whether our country is capable of working through a pandemic should one strike.

Health professionals around the world remain deeply concerned about the continued spread of the deadly avian H5N1 virus which has swept across eastern Asia and has started to be seen in the Middle East and Europe. The virus is highly virulent – more than half of the people infected with the H5N1 virus have died – and is rapidly being spread across the globe by migratory birds; can be transmitted from birds to mammals and in some limited circumstances to humans, and, most importantly, like other influenza viruses, it continues to evolve. Many scientists and health professionals believe it is only a matter of time before H5N1 mutates into a virus capable of human-to-human transmission, sparking a global pandemic. The Spanish Flu pandemic of 1918-1919 killed 40 to 50 million worldwide and some scientists predict that an avian flu pandemic could be as severe. I think it is safe to say that all of us here today fervently hope that a pandemic never happens but it is also fair to say that we would be remiss in our responsibilities if we did not do everything in our power to prepare our nation for that eventuality.

Last fall President Bush unveiled his National Strategy for Pandemic Influenza – a $7.1 Billion plan built around the three pillars of preparedness and communication, surveillance and detection, and finally, response and containment. I applaud the President for his leadership on this issue and I believe the Administration’s three-pronged approach is basically sound. However, the devil is always in the details, and I look forward to hearing from our witness today about how the Administration proposes to turn strategy into action.

Back in November of 2005, I expressed deep concern that the Administration’s Strategy did not go far enough to address one critically important question; namely what do we do if a pandemic flu vaccine causes dangerous side effects and ends up injuring millions of Americans? The reality of vaccines is that rare and dangerous events may not come to light before licensure. Even when there is sufficient time to study a vaccine for potential side effects – and the vaccine manufacturer has done everything legally required to ensure a vaccine’s safety – sometimes safety issues can only be detected following vaccination of a much larger and more diverse population. Unfortunately, in a pandemic
flu situation or bioterrorist attack the risks increase because we will not have the luxury of time to uncover all the potential side affects of an experimental vaccine before we are forced to start inoculating people.

I firmly believe that our avian flu preparedness plan will fail miserably if the American people do not trust that the vaccines and drugs they may receive to protect them may in fact harm them instead. For example, recent studies have indicated that more than half of pediatricians are already encountering at least one family a year that refused all vaccines, while 85 percent say they’d had a parent turn down at least one shot. Whether it’s because of fear that mercury used as a preservative in vaccines causes autism, or that the dangers of immunizations far outweigh their benefits, or that there is a conspiracy by drug companies, doctors and vaccine makers to conceal the harm, the facts are clear, more and more American families are fighting immunization.

We also saw this pattern unfold when we attempted a smallpox vaccination program for first responders in 2003. First responders and other health care workers balked at being vaccinated because the compensation programs we put in place was neither clear enough nor adequately funded enough to overcome their concerns about the financial well-being of themselves and their families if they were injured by the vaccine. Under those circumstances our first responders were faced with a very difficult choice; either refuse to take the vaccine or take it and be prepared to sue the vaccine manufacturer if something went wrong. In the end, the vast majority choose not to take the vaccine.

We as a nation are about to repeat the smallpox vaccination mistake again, but this time in spades. Because this time around people won’t even have the choice of suing the vaccine manufacturers thanks to a provision contained in the Fiscal Year 2006 Department of Defense Appropriations bill. This provision granted vaccine companies sweeping legal protections for pandemic countermeasures; almost blanket immunity except in the case of clear and convincing evidence of willful misconduct. Granted the appropriators did include another provision creating a pandemic vaccine compensation fund but the fund was a paper tiger, it contained no money.

Let’s be very clear, without a fully-funded compensation component in place, we are asking the American public to trust the pharmaceutical industry to keep them safe. And if that trust is broken – recent cases like celebrex and vioxx come to mind – we have left Americans with no place to turn for a remedy – no access to the court system and no access to appropriate compensation when they or their loved ones are injured or killed by a covered countermeasure.

I hope you will agree Mr. Chairman that this is an unacceptable situation and I hope this Committee can work with the appropriate authorizing and appropriations committees to install rigorous safeguards on the manufacture of pandemic vaccines or medical devices and fully-fund the compensation program created by the Department of Defense bill. I also look forward to hearing from our witnesses about what steps the Administration can take or is already taking to close this glaring loophole in our pandemic preparedness plan. Thank you.
Opening remarks by Congressman Darrell Issa to the House Committee on Government Reform for May 11, 2006.

Thank you Mr. Chairman and Ranking Member Waxman for holding this important hearing on “Working Through an Outbreak: Pandemic Flu Planning and Continuity of Operations.” I also want to thank the witnesses for taking time out of their busy schedules to testify before the full Committee.

In the event of an outbreak of pandemic flu, a coordinated response between our federal, state and local authorities - from the Departments of Homeland Security and Health and Human Services to public health offices and emergency response teams in the smallest of American towns - will be the key to ensuring the health and safety of the American public.

The administration should be commended for their foresight in planning for a pandemic and their development of both the National Strategy for Pandemic Influenza and the Implementation Plan. Not only will these plans be essential for mitigating loss of life, but also easing the potentially devastating effects that an outbreak of pandemic flu could have on our nation’s economy. It is crucial that we do as much as possible to ensure that the American people will be able to continue working and maintain, as much as possible, their way of life.

Integrating health information technology into the response plan can help to ensure the health of the American people. President Bush has been pushing to stimulate health IT for the past 5 years. Transitioning to an electronic form of records will allow HHS to determine in real time what response is required to a pandemic outbreak. Obviously, we should address this issue now, rather than after a pandemic flu hits the United States and demonstrates our weaknesses and devastates us through our failures.