CYBER SECURITY®
INDUSTRY ALLIANCE

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 Waxman 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.[1]

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 outbreak 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." [2]

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 15, 2005.

2 "Lessons of 1918-19 Spanish flu epidemic guiding preparedness" Bill Eekhof, October 5, 2005, http://www.mykawartha.com/ka/news/peterborough/

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 first-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. Front-line 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 commnications 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 disperse 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 $150 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 Kriens 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 café 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 work force 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 noticed 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.[4]

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 atleast 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 55 percent of IT managers believed the Federal Information Security Management Act hampered the expansion of telework.[5] 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

---

4 2004 American Interactive Consumer Survey conducted by the Dieringer Research Group and data from the International Telework Association and Council (ITAC)

5 "CDW Survey Reveals Increase in Telework," Rob Thorneyer and Roseanne Gerin, Washington Technology, March 6, 2006

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 about what the impact would be if, for example, even *half* of 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 offsite. 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 beltway that is stuck in traffic jams for twelve hours a day.

Recommendations

There 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

pandemic would have on the information infrastructure. Recommendations and plans for "surge" capability in the opening phase of a pandemic should be assembled and ready to activate.

- We should all learn from what works. In preparation for the 2004 Republican and Democratic National Conventions, the Office of Personnel Management conducted emergency preparedness surveys in Boston and New York, and used them to develop program training, in partnership with other agencies, to reduce the number of employees who had to report to work in the secured areas. The project was an unqualified success. This illustrates why the Federal Government should test existing distributed work force plans now, by designating both essential and non-essential employees to work from home for a day or two. Through such exercises, managers will be able to make better informed policy and procurement decisions. Inviting participation from the private sector would also help analyze the potential impact on contract support.
- Congress should seek to remove any real or perceived barriers for Federal agencies to pursue telework by pursuing a three-prong strategy. First, it should consider legislation that enables agencies to win by participating and deploying teleworking programs. In particular, agency budgets for FY '07 should allow the flexibility for agencies to retain savings from teleworking and deploy them elsewhere, so they are not punished for their success. Second, Congress should also wield a "stick," creating the means to cut budgets for failing to take the "carrot." Finally, Congress should also seek to address any perceived barriers FISMA has on the expansion of telework.

A year ago, 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.