



## **Implications of a Large-Scale Telework Response to a Major Pandemic Event**

**Prepared by ACT-IAC Shared Interest Groups:**

**Acquisition Management  
Emerging Technology  
Human Capital  
Networks &  
Telecommunications**

**Enterprise Architecture  
Homeland Protection  
Information Security & Privacy  
Small Business**

Date Released: December 2008

### **Synopsis:**

**This white paper uses the preparation for a national disaster to encourage the United States federal government management to implement a telework strategy. It represents the output of ACT-IAC Shared Interest Groups (SIGs) addressing a common problem from the specific perspective of each group. The problem statement stems from a report delivered by the ACT Future Forum in November 2006. To summarize: Insufficient work is being done by government and industry to implement and support a large-scale telework program, and in the case of a large-scale disaster such as a pandemic, the government's innate capabilities could be seriously curtailed.**

## **American Council for Technology/Industry Advisory Council**

The American Council for Technology (ACT) is a non-profit educational organization established in 1979 to assist government in acquiring and using information technology resources effectively. In 1989, ACT established the Industry Advisory Council (IAC) to bring together industry and government executives to collaborate on IT issues of interest to the government. In 1997, ACT established the Intergovernmental Advisory Board (IAB) to foster communication and collaboration between IT executives at all levels of federal service—federal, state, local, and tribal governments.

The American Council for Technology, in cooperation with the Industry Advisory Council and Intergovernmental Advisory Board, is a unique, public-private partnership dedicated to helping government use technology to serve the public. The purposes of the organization are to communicate, educate, inform and collaborate. ACT also works to promote the profession of public IT management. ACT and IAC offer a wide range of programs to accomplish these purposes.

ACT and IAC welcome the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of information technology. For membership and other information, visit the ACT/IAC website at [www.actgov.org](http://www.actgov.org).

### **Collaboration of Shared Interest Groups**

This document was created in conjunction with eight of the IAC Shared Interest Groups.

#### **Disclaimer**

This document has been prepared to provide information regarding a specific issue. This document does not and is not intended to take a position on any specific course of action or proposal. This document does not and is not intended to endorse or recommend any specific technology, product or vendor. The views expressed in this document do not necessarily represent the official views of the individuals and organizations who participated in its development. Every effort has been made to present accurate and reliable information in this report. However, ACT/IAC assumes no responsibility for consequences resulting from the use of the information herein.

#### **Copyright**

**©American Council for Technology, 2008. This document may be quoted, reproduced and/or distributed without permission if credit is given to the American Council for Technology and Industry Advisory Council.**

#### **Further Information**

For further information, contact the American Council for Technology and Industry Advisory Council at (703) 208-4800 or [www.actgov.org](http://www.actgov.org).



## TABLE OF CONTENTS

I. Introduction and Terms of Reference .....	8
II. The Scenario.....	9
III. The Human Component of Human Capital in a Crisis.....	10
IV. What Enterprise Architecture must communicate .....	17
V. Security and Privacy in a large-scale Telework environment .....	25
VI. DOES our IT infrastructure support large-scale telework? .....	30
VII. Emerging Technologies that Enable Telework And Workforce Mobility .....	34
VIII. Telework for the Homeland Protection Mission .....	43
IX. Investing in a Secure Telework Infrastructure – A Small Business Perspective .....	49
X. Executing the Acquisition Mission in a Telework Environment.....	52
List of Authors & Contributors .....	57

## Executive Summary

What would happen if there were an influenza pandemic and as many as 40 percent of federal workers could not report to the office? The situation could be dire. There could be universal susceptibility to the influenza virus, no natural immunity, insufficient medications, and an assumption by public health officials that the 20 percent of all working adults will become ill during the outbreak. Workers either would be sick, afraid of being infected or have to stay home to care for loved ones. It may sound like a B-rated science fiction movie, but it could be reality.

Would all or even part of the government keep running in such an emergency that could last for weeks, and perhaps many months? Would there be sufficient infrastructure to allow federal workers and contractors to work from home or off-site for an extended period? Would the federal government be prepared to deal with the coordination needs, the technical issues and support, the issues of data security and privacy? Would they have access to IT resources and be able to deal with the emotional toll of operating in a disrupted, uncertain environment?

A report delivered by the ACT Future Forum in November 2006 reached one basic conclusion that has not changed. There is insufficient work by government and industry to implement and support large-scale telework programs. In the case of a large-scale disaster such as a pandemic, the government's innate capabilities could be seriously curtailed.

A number of ACT-IAC Shared Interest Groups (SIGs) looked closely from their own specific perspectives at the preparations needed to deal with a major disaster and the problems that the government would face.

This white paper is a compilation of these reports, focusing on issues that should be addressed to deal with a catastrophic event in hopes of encouraging U.S. government managers to implement a comprehensive and effective telework strategy before a disaster strikes.

There are two critical and fundamental themes. One focuses on how to prepare the federal government to continue operations at as close to maximum efficiency as possible in the face of a national crisis. The second looks at the opportunity to implement a telework strategy by leveraging today's technology in a way that reduces costs and meets national needs.

Several agencies have prototyped the concept with limited success on a small-scale basis. However, insufficient focus has been paid to the telework strategy as a lasting and more permanent paradigm.

The bottom line is that it is possible to implement an effective plan, and it is time to act now. Teleworking in the federal government must move from rhetoric to execution.

The need to be prepared for emergency incidents is evident from the 9/11 terrorist attacks and problems stemming from Hurricanes Katrina and Rita. The government must heed the lessons from these experiences, including knowing that the citizens of the United States demand both speed and availability of services and assurance that government tax dollars are not wasted.

There is no doubt that an event like an influenza pandemic has the potential to seriously disrupt normal government business operations and challenge an agency's ability to remain fully staffed and functioning. How a staff responds to this kind of disaster depends on how well trained federal employees are and how well prepared they are for any event.

The IT infrastructure, the networks, the systems, and the applications all have to be up and running in a robust, reliable mode. That means, well in advance of any such event, there must be a

concerted effort to draw up the plans, prepare the environment, and have staff in place to execute the plan. The IT environment, if set-up correctly, can continue to perform in an unattended mode and even self-correct and repair itself to continue operating. If the world were totally robotic, there would be, theoretically, no loss of service. However, skilled professionals are critical to executing the government's business during a crisis.

The concepts, plans, and IT components for a remote system should be evaluated and tested. Training and testing should be conducted for those carrying out these plans. This preparation will have a secondary and lasting effect. As the systems are tested, the concept of telework will move from a conceptual discussion phase to a real-life working model. The result will be a well-defined working model for teleworking. Through necessity of preparation for a national crisis, the government will, in effect, be prototyping a new employment paradigm. The benefit will be two-fold. The government will be prepared for a national crisis, and the personnel will be ready to take advantage of the technology to reduce costs and improve productivity.

An additional benefit is that the next generation of employees – those in their GenX and Millennium years - already use today's technology as part of their daily routine. By implementing a telework strategy, the government will be positioned to leverage the technical savvy of the next generation of employees.

The following chapters raise serious questions that can lay the groundwork for action, and provide the rationale to make teleworking a much higher priority.

### **The Human Component of Human Capital in a Crisis**

Although all agencies are required to have a telework policy (Public Law 106-346), there is little guidance to address the human element of telework, including the skills, knowledge, abilities and attitudes necessary for individuals to successfully perform their assigned tasks under contingency conditions. This chapter addresses that topic and raises concerns that if this element is not addressed, the likelihood of a successful telework-based response to a catastrophic event will be severely impacted. "One thing is certain- people will be scared. That is a fact that cannot be overlooked," the report notes. This means employees must be trained and credible people must communicate accurate information.

### **What Enterprise Architecture Must Communicate**

A standardized set of capabilities at each level of an agency's enterprise architecture can help support continued government operations using telework in the case of a pandemic or other natural disaster. Consideration for supporting and achieving remote, offline, and/or occasionally connected capabilities should be an integral part of the government's enterprise architecture to support telecommuting capabilities and to be in place as preparation for a pandemic scenario.

### **Security and Privacy in a Large-Scale Telework Environment.**

Those working from non-government sites, including their homes during a pandemic or other crisis situation, will need to access, create, store or transmit agency sensitive information as they seek to do their jobs and provide at least a minimum level of essential services to citizens, state and local governments and other federal agencies. There are tools and technologies to protect information privacy and security in all situations, but this goal should be balanced against the need to permit the telework required to provide essential services. This means that, as a practical matter, agencies may not be able to safeguard and protect information during an emergency telework situation at the

same level as would apply during ordinary times. Agencies must develop policies, protection and document protocols as part of their Continuity of Operations Planning. They must set priorities to maximize information security and privacy while still providing effective fulfillment of an agency's mission.

### **Does Our IT Infrastructure Support Large-Scale Telework?**

Employees will need to communicate with their peers, managers and citizens during a pandemic to carry out their work functions, but many government workers have only limited physical connectivity to the outside world that is suitable to conduct their agency business. It is recommended that government workers have broadband access to their homes via DSL, cable modem, or high speed satellite, and that Virtual Private Network (VPN) technology be deployed, tested and used to provide a secure tunnel around data traveling between government worker's PC's and the office network. It is incumbent upon the agencies to put in place a standardized set of technology solutions including laptops, the VPN system for secure remote access, a competent help desk, and Federated Authentication products to produce digitally signed, standard XML-based assertions that vouch for a user's identity. Federal agencies must have all these assets in place and tested with a trained workforce prior to a crisis.

### **Emerging Technologies That Enable Telework and Workforce Mobility**


There are emerging, best practice technologies for telework and workforce mobility that have been proven in private industry. These technologies can enable federal agencies to expand their initiatives with minimal budget and staff resources, while providing employees with simple yet secure access to the information they need to be productive while working remotely under normal conditions and in a crisis like a pandemic. The technologies include wireless cards or tethering capability to mobile devices, application virtualization software, new desktop virtualization technology, application streaming, data security tools, sophisticated security, password management techniques, Web-based collaboration solutions and much more. The government must purchase and deploy the right technologies to support users on various computers and portable devices to provide employees with simple yet secure access to information they need to be productive when working remotely.

### **Telework for the Homeland Protection Mission**

Three distinct case studies show that having an established telework infrastructure in place can significantly affect our nation's ability to respond more effectively in times of crisis. This will enable the workforce to leverage commonly owned devices to access information without risking data loss or leaks in critical situations where on-site physical access is not available. The first two cases demonstrate how telework enables business continuity in times of crisis, whether in a public or private organization, and whether a short or long-term recovery is required. The third case shows how telework can enable leadership to shift workforce roles and responsibilities in times of crisis, surging access to systems that are critical in response and recovery missions. Delaying an initial telework strategy while waiting for a "perfect solution" or "total consensus" only increases the risk of being unprepared on even a basic operational level in response to a crisis.

### **Investing in a Secure Telework Infrastructure - A Small Business Perspective**

Small business is especially sensitive to the cost of acquiring, implementing and supporting a security-compliant infrastructure to support a telework capability for its employees. On the other hand, small businesses play an increasingly important role in the execution of government missions. As the federal government addresses telework in the pandemic environment, it is realistic



to expect that current federal contracts and new federal acquisitions will increasingly incorporate requirements specific to meeting minimum telework capabilities to address continuity of operations. To assist small business contractors, the government has the option of incorporating telework requirements into contracts with cost reimbursements.

### **Executing the Acquisition Mission in a Telework Environment**

Agencies must obtain items or services they need at the right time and at the right prices. They must meet everyday concerns and at the same time prepare for emergencies. There must be a balance between the government's needs to acquire products and services and follow good acquisition practices including Federal Acquisition Regulations. Agencies should develop emergency contracting practices. As part of an agency's preparation, telework should be encouraged as a normal course of business so that, in case of a pandemic, the workforce will be prepared to execute the mission and the agency will be equipped to support the workforce. Failure to be prepared could leave an agency disabled when most needed to address the needs of citizens, business and government.

#### **Authors**

Walt Grabowski, SI International, Inc.  
Rick Schrader, Appian Corporation

## I. INTRODUCTION AND TERMS OF REFERENCE

The ACT Future Forum of 2006<sup>1</sup> met in Williamsburg, VA on October 30 and 31 of 2006. The Forum, co-chaired by Robert Shea of OMB and John Marshall of CGI, addressed three important subject areas: Telework, Disaster Response and Recovery, and Science, Technology, Engineering and Math Education. Future Forum participants formed three teams to consider those topic areas, identify gaps and shortfalls, and report on their recommendations. The Disaster Response and Recovery Team used a large-scale influenza pandemic as a disaster scenario. Such a pandemic could be national in scope and have a wide, sustained impact on all sectors of the U.S. economy. As such, it represents a particularly challenging scenario. Among the teams' conclusions were (1) that not nearly enough was being done by government and industry to implement and support large-scale telework, and that (2), in the case of a large-scale disaster such as a pandemic, the government's innate capabilities and those of its contractors could be seriously curtailed.

Early in 2007, the leadership of the ACT-IAC Shared Interest Groups (SIGs) met to consider possible contributions to the issues raised by the Future Forum. The SIG leadership concluded that an examination of issues associated with a large-scale implementation of telework would be valuable and that such an implementation, driven by a major, nationwide influenza pandemic, could form a limiting or extreme case of telework. In other words, telework should be a key element of disaster planning and response, and, conversely, a pandemic flu scenario would "stress" a telework response to the needs of government to maintain continuity of operations. The SIG leadership agreed to develop a white paper incorporating contributions from multiple SIGs, and provide guidance on what the government should do to ensure that telework is a viable response to a large-scale disaster.

To facilitate the development of this paper, the SIG leadership agreed that each of the SIGs would develop guidance, recommendations and suggestions from the perspective of their shared interests. This paper is a compendium of the SIGs' individual contributions.

### **Author**

Walt Grabowski, SI International, Inc.

---

<sup>1</sup> The presentation from the ACT Future Forum may be downloaded at:  
[http://www.actgov.org/actiac/documents/pdfs/FutureForum\\_FinalPresentation\\_103106.pdf](http://www.actgov.org/actiac/documents/pdfs/FutureForum_FinalPresentation_103106.pdf)

## II. THE SCENARIO

The scenario that the SIG Leadership used is based on the “Determined Accord” tabletop exercise developed by the Office of National Security Coordination, Federal Emergency Management Agency (FEMA).<sup>2</sup> In summary, the scenario provides that a pandemic flu has assaulted the U.S. Specifically, the scenario assumes that there is universal susceptibility to influenza virus, there is no natural immunity, there are no significant anti-viral medications, and that non-medical countermeasures will have limited effect. The scenario assumes that the disease attack rate will be 30% of the overall population, that each ‘infectee’ will transmit the virus to two other people, and that among working adults, 20% will become ill during a community outbreak. The scenario posits that worker absenteeism will reach 40% during peak periods. These absentees will include not only those who are ill with the influenza, but “worried well” who are concerned they may have the influenza or who want to reduce contact with ill individuals, well individuals who stay away from the workplace to care for ill family members, and not-infected individuals who may express symptoms and assume pandemic influenza.

The scenario includes multiple waves of illness, with each wave lasting two or three months. The waves of illness will move across geographical areas. The severity of waves, including symptoms and infectiousness, will vary.

A pandemic influenza would have widespread implications. A large number of government and contractor employees would avoid their normal workplaces. Personnel would attempt to work from home, or, more generally, off-site, for extended periods. The ramp up to large-scale telework would be brief and could involve many employees for whom telework is not a common practice. Personnel management, performance management, training and recruiting may be problematic. Motivation and capacity to continue work in a highly disrupted personal environment could be limited. Resource user identification and authorization to remote access information resources will be tested. Information privacy in a non-prepared environment may be challenging and could result in unfortunate post-pandemic-event privacy concerns. Access to IT resources via VPN or other means could be capacity limited. Costs associated with large-scale telework may not have been included in agency budgets, and cost-recovery mechanisms may not be available to government contractors.

A large-scale pandemic will have implications across the full spectrum of government services. The SIG reports that follow shed light on those implications from the perspective of the groups. They set the stage for future examination of critical issues in resource planning, training, infrastructure preparation and, perhaps most importantly, expectation management.

### Authors

Walt Grabowski, SI International, Inc.

Janis Keating, Constellation Inc.

---

<sup>2</sup> The facilitator slides outlining the pandemic scenario may be downloaded at: [http://www.actgov.org/actiac/documents/pdfs/DraftDETERMINEDACCORDFacilitatorSlides\\_Version\\_1.Aug29.pdf](http://www.actgov.org/actiac/documents/pdfs/DraftDETERMINEDACCORDFacilitatorSlides_Version_1.Aug29.pdf). It is important to note that FEMA is no longer using this particular set of slides, which are now considered out of date. An updated version is currently under development by FEMA. For the purpose of this paper, the slides are used solely to establish a common scenario that could lead to a large-scale, government-wide telework situation.

### III. THE HUMAN COMPONENT OF HUMAN CAPITAL IN A CRISIS

#### *Human Capital Shared Interest Group*

#### **Purpose**

§359 of Public Law 106-346, all agencies must have a telework policy.

Most federal agencies have developed extensive plans to meet the requirements of this statute. Various agencies also have conducted research and put considerable thought into the physical aspect of catastrophe survival through telework.

There is, however, little guidance to address the human component of human capital - the skills, knowledge, abilities and attitudes necessary for individuals to perform successfully their assigned tasks under contingency conditions. If the human component is not part of the equation, the potential success of a telework program under emergency conditions will be diminished.

An influenza pandemic has the potential to seriously disrupt normal business operations and challenge an agency's ability to remain fully staffed and functioning. How the staff will respond depends on how educated they are about how to survive and how prepared they are for the event. Professional opinions vary on the extent of the impact, and it is anyone's guess how people will react. One thing is certain—people will be scared. This fact cannot be over looked and should be addressed.

#### **Background**

The Office of Personnel Management has published Human Capital Management Preparedness guidelines and strategies to ensure continuity of government operations in the event of an emergency. OPM has identified how to handle temporary workers, provisions for leave and extended leave, layoffs and benefits.

Yet the emotional and psychological realities have not been considered for employees, contractors and health care workers facing a crisis.

There are unanswered questions about how employees will be notified if an emergency declaration comes at a time other than normal business hours. It needs to be determined whether preliminary warnings about an impending crisis will help reduce the trauma and what remedies will be available to deal with the emotional consequences of the sudden loss of communication.

These issues were evident in the controversy and confusion surrounding the lack of notification of students, faculty and staff during the Virginia Tech campus shootings in April 2007. One also need only look back to Sept. 11, 2001 when communications in the Northeast temporarily went down as the World Trade Center towers fell. Cell phone service lapsed and the Internet slowed to a crawl as hundreds of millions of users searched for information. In New York City, people were in a state of shock. First responders acting totally on adrenalin were unprepared to handle the massive responsibility of maintaining a calm environment. People walked around for days in a daze.

In addition to full time government employees, it is also crucial to consider the impact on contractors who are important to the day-to-day operations of many agencies. It should be determined whether contracts reflect a policy for contractor employees' attendance during a declared disaster; whether contractors should show up when the federal workers are not be permitted in their normally assigned workspace; and how the emotional condition of the contractors will affect their ability to work?

One thing is for sure: The goal of personal survival will trump an agency desire to maintain a consistent work environment. Employees will focus on their immediate personal and family needs, and on basic survival items such as food, water and emergency medical supplies. If the government physically shuts down, a panic could ensue. It may not be the loot and pillage version, but the appearance of doom will grip the area if it has not been prepared properly. Employees and contractors normally accustomed to working in an office environment will be dealing with a sense of isolation and disassociation.

The health care workforce also deserves special mention due to the demands that will fall on these workers during a pandemic. During the SARS outbreak in Toronto, about half of the city's 850 paramedics were quarantined.<sup>(5)</sup> A reduced workforce and an increased call volume during a pandemic could seriously disrupt a community's ability to respond to medical emergencies.

One study has documented that over 40% of the SARS patients in Toronto were hospital or healthcare workers.<sup>(6)</sup> In an unpublished study, Hanfling found that "Between a quarter and a third of (hospital worker) respondents said they would not report to work if contaminated patients were in the hospital."<sup>2</sup>

These two findings lead us to expect that a large portion of the healthcare workforce will be unavailable during a pandemic. Further, anecdotal evidence suggests that large portions of a potential healthcare workforce—non-hospital-based physicians, nurses and other health professionals—are not included in community preparedness or response plans.

Large numbers of patients will arrive at overwhelmed and understaffed hospitals. Nursing homes and other health care facilities may not have adequate staff, there may be an insufficient supply of health care workers and many ill citizens may decide to stay home rather than face the overcrowded hospitals and gymnasiums. Without a community system to care for them, many may perish not from the disease but from dehydration or starvation.

In contrast to the extensive studies on the effects of natural disasters like hurricanes and tornadoes on human performance, there is very little information available on the effects of a disease pandemic. However, studies of the SARS outbreak give a preliminary view of what to expect.

The data from the SARS outbreaks indicated that upwards of 40% of the community population experienced increased stress in family and work settings; 16% showed signs of traumatic stress levels; and high percentages of the population felt helpless, apprehensive, and horrified by the outbreak.<sup>(4)</sup>

In another community survey, 30% thought they would contract SARS, while only a quarter believed they would survive if they contracted the disease despite an actual survival rate of 80% or more. This indicated a high rate of perceived risk that might have preceded widespread panic had the outbreak been either more widespread or more lethal. Community residents were diligent about adopting appropriate person-to-person transmission precautions. However, precautions were adopted differentially based upon anxiety levels and perceived risk of contracting the disease, indicating the importance of stress and anxiety levels, as well as baseline mental health, on a public response to taking necessary precautions.<sup>(2)</sup>

## **Discussion**

The background information casts an ominous perspective of what could happen. How do we prepare the personnel to face the challenges and keep working?

Physical, fiscal and emotional preparation is critical to the success and survival of the federal work force. While all of the federal agency guidelines stress the mechanics of telework, it is imperative to remember the most basic aspect of the crisis is that people will be scared - a point documented by the American Psychological Association (APA).

Experts on public health and risk perception say that fear about catastrophic incidents often originates from a feeling of lack of control and a perceived inability to prevent the problem or threat. Some level of anxiety is constructive in that it motivates people to take appropriate action assuming such actions are available and recommended. Without any recommended course of action, however, anxiety around these threats has the potential to become debilitating.

Psychologists who study people's reactions to health, safety and environmental risks say fear is a normal response to an unpredictable threat. Anxiety is also a normal response to ambiguous situations over which one has little or no control. Anxiety about the future and fears of terrorism were quite normal after Sept. 11<sup>th</sup>, and some people continue to feel anxious about the future.<sup>1</sup>

A pandemic is a very different type of emergency. It is potentially much longer and more complex than other disasters that business continuity planners typically address and it represents a threat that leaves facilities and infrastructure intact and primarily targets an organization's people. As such, the physical and emotional factors become critical aspects of preparedness, response and recovery.

The cascading financial impact on markets, businesses and households also can further exacerbate the emotional impact of a pandemic. As mentioned, there are myriad factors related to pandemic influenza that may stimulate intense emotional and behavioral reactions that in turn may represent great challenges to the overall response and recovery from the event.

A comprehensive review of the literature yields no empirical studies addressing the behavioral or emotional consequences of a pandemic.

The concepts used today to discuss mental health and human behaviors were not in existence during the last great pandemic. The concept of a diagnosable traumatic stress disorder did not fully come into the literature until after the Vietnam War. The bottom line: There are no existing models showing the emotional and behavioral response that may grip the public during a long emergency such as a global disease outbreak. What is called for now is an entirely new paradigm for anticipating the human response to such a threat that may truly inform planners and responders in a way that facilitates the best-possible response to the worst-case scenario.<sup>(3)</sup>

## **Analysis of Options**

How resilient will the workforce be? In a recent edition of *Government Executive*, (Snapping Back 06/15/2007), the topic of resiliency was discussed in terms of agency realignments. The same resiliency is needed to overcome the possible human effects of the pandemic.

Once the agencies accept that the psychological implications of a disaster must be factored into the planning of a telework strategy, they can begin to construct a solution. One of the problems agencies will experience as they develop a plan is to find qualified expertise to guide them. Intra-agency cooperation will be necessary to secure the proper resources. IT professionals will have to work closely with the HC branches to develop user requirements. Human priority levels need to be established and coordinated with logistical issues. Our divergent and scattered federal workforce will compound the issues of implementation.

Some points are clear. Psychologists who specialize in managing stress and anxiety say that people who feel some sense of control while dealing with a fearful, unknown situation handle the unexpected better than those who are unprepared or fearful. The evidence also shows that panic only occurs when people lose connection with their entire social network.

Research on collective behavior by Kathleen Tierney of the Department of Sociology and Natural Hazards Research and Applications Information Center at the University of Colorado at Boulder shows that during conditions of severe threat, “panic only occurs when individuals feel completely isolated and when pre-existing social bonds break down to such a degree that those who are in danger feel totally on their own in seeking safety.”

Other research on social behavior shows that panic is more likely when those entrusted with managing disasters fail to provide accurate information about what to do and where to go during impending threats.<sup>(1)</sup>

## **Recommendations**

**+ During a pandemic, IT management will need to address psychological issues. This will require advance preparation.**

Group training sessions should prepare agency staff members for the psychological trauma that will ensue from a pandemic. However, management must also determine the best time sequence and cycle for administering training. There also may be a concern that ongoing training may actually desensitize employees to the importance of preparation by eliciting a “Chicken Little” effect?

**+ OPM should engage the American Psychological Association or other expert organizations to determine the best solution to the type of training for a crisis like a pandemic that will be most successful.**

**+ Training should not be limited to a pandemic scenario. Instead, the training should focus on community preparedness and response to any type of hazard. The focus should not be to train a group of pandemic technicians, but instead build communities that have a foundation solid enough to withstand, respond to and recover from many types of disasters.<sup>(7)</sup>**

**+ Federal Executive Boards (FEBs), under the direction of OPM, perform highly valuable functions and should be utilized in a pandemic crisis.**

FEB activities now include the conduct of emergency operations such as those in effect under hazardous weather conditions and natural and manmade disasters; responding to blood donation needs; communicating related leave policies. Pooling these resources to provide common services such as training courses and alternative dispute resolution consortiums could be helpful.

**+ Any information alerts or communications to deal with a pandemic should be coordinated with the CDC.**

The Centers for Disease Control and Prevention has initiated a program to provide timely and accurate health information to the public on the web specifically to mitigate the spread of misinformation. According to CDC, the complexity, duration, and scope of a pandemic influenza event, and subsequent adverse events, require the ability to provide timely, accurate, clear, and consistent health messages to both broad and specific audience bases. The development of scientifically sound messages and educational materials regarding pandemic influenza prevention behaviors are critical to assist people in all communities and targeted through multiple channels.

**+ Credible expert spokespersons should convey clear, concise and truthful information, and provide concrete advice on how what people can do to protect themselves.**

Experts on trauma reactions say that panic is a preventable response with credible communication of accurate information. According to experts who study crisis communication, it is important that the message be clear, concise, truthful and delivered repeatedly. It is critical that those involved in such communication process coordinate efforts prior to any health emergency. The agency responsible for communicating with the public and the agency's lead spokesperson should be identified in advance, and a clear chain of command should be established. Health communications research further points to the need for identifying evidence-based strategies for the communication message, and identifying an organizational entity that is responsible for mental health response and recovery. In addition, public health officials need to provide clear information on possible preparation and safety actions and provide concrete recommendations about what to do. Public health officials must avoid multiple authorities with differing political and policy agendas, and avoid inconsistent or conflicting messages. Finally, it is important to recognize that with repeated false alarms, many will acclimate to the threat and may fail to notice genuine danger.

Those communicating in an emergency need to understand that fear and other emotions may interfere with people's decision-making and judgment. In addition, because people in crisis management usually have not had to communicate about health threats of this magnitude before, it is important that they evaluate and test the messages before releasing them to the public. Lastly, social scientists should be part of emergency planning teams to assist in formulating messages and communications strategies that will achieve the desired outcomes.

Specific, concrete advice should be communicated so that people know what they can actually do to protect themselves. Information in the absence of concrete action is far less effective.

Experts on risk and decision-making can identify what is critical to convey to the different audiences. Young people have different information needs than do older people. Those with

children or those taking care of elderly parents, those with health problems, and those who are away from home at the time of the emergency, all have different information needs. Psychologists and other social scientists can identify these different groups' belief systems and aid in designing comprehensible messages and evaluating their success.

Furthermore, research shows that people listen to messages more often when they come from professional experts rather than when they come from politicians, particularly when the messages are emergency messages and the audiences are racial/ethnic minority groups.

Researchers who have studied communication find that certain ways of presenting information increase the perception of risk and thus fear. Specifically, people are more fearful when they see individuals or situations similar to themselves rather than statistics. The greater the lack of perceived control associated with the fear message, the greater the fear and discomfort. Thus, it is important to communicate a reason for concern, but it is also important to include tactics or strategies for controlling the feared situation. Also important is reminding people of the degree of risk presented by the situation. Psychologists who specialize on how the design of warnings affects human behavior have learned that people want easy-to-comprehend information and be able to find more information if they want it. The news media will play a critical role if a health emergency were to occur. Information flow to the public about very bad news should not be controlled in the name of trying to avoid an outbreak of mass panic. The public should be armed with information. <sup>(1)</sup>

Limited resources are better devoted to “those that need them most.” If a hospital were to adopt this plan for evacuation, for example, they might devote five workers to move one non-ambulatory patient. On the other hand, if they adopted a “greatest good” approach, one worker could evacuate five ambulatory patients. Obviously, both extremes have inherent problems. Hospitals and communities should consider such issues and agree on priorities before a disaster. <sup>(7)</sup>

## References

1.) Produced by the APA Office of Public Communications, May 2006. Based in Washington, DC, the American Psychological Association (APA) is a scientific and professional organization that represents psychology in the United States. With 148,000 members, APA is the largest association of psychologists worldwide. <http://www.apa.org/releases/healthpandemic.html>

The information from this advisory was compiled from the following subject matter experts:

Scott Geller, PhD, Director for Applied Behavior Systems, Department of Psychology, Professor of Psychology, Virginia Polytechnic Institute and State University

Margaret Gibbs, PhD, Professor of Psychology, School of Psychology, Fairleigh Dickinson University, Private Practitioner

Toni Vaughn Heineman, DMH, Clinical Associate Professor of Pediatrics and Psychiatry, University of California, San Francisco, Private Practice

Laura Kubzansky, PhD, Assistant Professor, Department of Society, Human Development, and Health; Harvard School of Public Health

Vicki Mays, PhD, MSPh, Professor of Psychology, University of California, Los Angeles

Roxane Cohen Silver, PhD, Professor of Psychology, Department of Psychology and Social Behavior and Department of Medicine, University of California, Irvine

Kathleen Tierny, PhD, Professor of Sociology, Department of Sociology and Natural Hazards Research and Applications Information Center – University of Colorado at Boulder

Michael Wogalter, PhD, Professor of Ergonomics and Experimental Psychology Program and Director, Cognitive Ergonomics Laboratory, North Carolina State University

2.) Mental Health and Behavioral Guidelines for Response to a Pandemic Flu Outbreak

Prepared by the Center for the Study of Traumatic Stress in collaboration with the

Mental Health Section of the American Public Health Association.

<http://www.usuhs.mil/psy/CSTSPandemicAvianInfluenza.pdf>.

3.) © Big Medicine 2001-2006. <http://www.bigmedicine.ca/stevencrimando.htm>

4.) McAlonan GM, Lee AM, Cheung V, Wong JW, Chua SE. Psychological morbidity related to the SARS outbreak in Hong Kong. *Psychological Medicine*. 2005 Mar;35(3):459-60.

5.) Silverman A, Loutfy MR, Simor A. Toronto emergency medical services and SARS [letter]. *Emerg Infect Dis*. CDC. 2004 Sep. Available from: <http://www.cdc.gov/ncidod/EID/vol10no9/04-0170.htm>. Accessed July 27, 2007.

6.) Varia M, Wilson S, Sarwal S, McGeer A, Gournis E, Galanis E, Henry B; Hospital Outbreak Investigation Team. Investigation of a nosocomial outbreak of severe acute respiratory syndrome (SARS) in Toronto, Canada. *CMAJ*. 2003;169(4):285-92.

7.) Levine S. Leaders Share Flu Pandemic Concerns: Federal Plan Prompts a Deeper Look Into Worst-Case Health, Business Scenarios. *Washington Post*. November 7, 2005; B01

## **Appendices**

Disaster Response Education and Training Project, Center for the Study of Traumatic Stress  
[http://www.osha.gov/Publications/influenza\\_pandemic.html](http://www.osha.gov/Publications/influenza_pandemic.html)

Pandemic Influenza Preparedness: Preparing for Corporate Crisis Communications  
Freda Colbourne, Senior VP, Edelman, Corporate & Public Affairs  
Thaddeus Pennas, Senior Account Supervisor, Edelman, Corporate & Public Affairs

## **Author**

Rick Schrader, Appian Corporation

## IV. WHAT ENTERPRISE ARCHITECTURE MUST COMMUNICATE

### *Enterprise Architecture Shared Interest Group*

#### **Purpose**

Enterprise Architecture across the government can support legitimate analysis, planning, business cases for and resourcing of teleworking capabilities. This chapter outlines a model for a standardized set of capabilities at each level of agency enterprise architecture to support continued government operations using telework if there is a pandemic. Enterprise Architecture is the means to logically describe what has to be done, for whom, when and how in each agency and cross-agency initiative during a pandemic to properly enable a telework system to properly function.

#### **Background**

Each agency has an Enterprise Architecture and an architected continuity of operations plan (COOP) supporting critical functions within its lines of businesses and common support services. It must be mapped to the Business Reference Model sub functions, and must follow OMB circulars and guidelines in the identification of business cases for needed investments. In some cases, services must tap one or more Infrastructure Line of Business (LoB) service providers. This is one area where policy clarification is necessary.

There are a number of other issues to be resolved. For example, infrastructure that already exists should have a common government-wide access vehicle provided to identify capability that others can tap into as a service. If not, something like the DoD's GIG could be put in place. This could facilitate the standardization of the solutions in the other Enterprise Architecture layers.

Another consideration is to the extent it is necessary under a pandemic scenario to fully support employees while off site. How far and to what extent should a telework capability be established for any active service capability in an emergency pandemic situation?

This chapter identifies other touch points and areas in the layers of the EA that must include considerations for supporting the mission, even when the infrastructure of the agencies home site or offices are not accessible or are closed.

#### **Discussion**

There are numerous considerations necessary to make sure planning and design solutions for Enterprise Architecture are in alignment. They include:

- + The various levels of security employees will have built into their remote accessibility; how this relates to available E-authentication services; and the use of collaboration tools as part of any remote computing set of support capabilities.
- + The deployment of mobile transportable workstations and other wireless and transportable devices so executives, managers and employees can have access to the same applications from home as from their offices. It must be determined who should have them and when and whether contractors should be part of the equation.
- + Use of government standards or standardizations giving applications standard Web interfaces and service components.

+ Determining whether work from an Internet-enabled workstation is of value, and whether the Internet will be reliable during a pandemic.

+ How and when to use of virtualization.

+ Deciding if increased prevalence of Composite Applications and Composite Application Builders will enable adoption of SOA's and enhances capabilities to leverage current services, data and systems across agencies towards a more robust, occasionally connected, remote or disconnected capability.

+ If an architected set of remote applications is developed and maximized for business process management (BPM) efficiency, would these considerations apply:

- Intuitive user interfaces that provide access to BPM driven applications that logically guide telecommuters through critical processes to include features, including specific written instructions, embedded in the services at each step of the processes (as well as policy or operating rules look-ups).
- Access controls securely linked to authorization knowledge bases so duties can be performed by personnel who otherwise do not perform these tasks or others reassigned as needed to ensure continuity of critical services and capabilities under legitimate purposes.

+ Whether content and records management should stay in still in effect during a pandemic or whether these requirements can be suspended based on a determination of an emergency.

Options could include:

- Creation of paperless offices, where key work products are available on special backup or reserve workstations and servers.
- Making documents and files remotely accessible from mirrored or backup capability.
- Types of devices and capabilities that should or could be provided like tablet paces, electronic white boards, scanning devices and other hand held devices for interconnection, which affect systems designs for services.

+ Ways to access content and perform duties without Internet enabled workstations where inaccessibility of online access must be addressed. This would include situations where disconnected personnel must have access to not just static content and forms, but appropriate workflows, processes and content associated with tasks, responsibilities and duties. The EA may assess when and whether entire applications could or should be packaged to enable them to run in an offline state, and if there should be application development platforms that are already architected for offline capabilities?

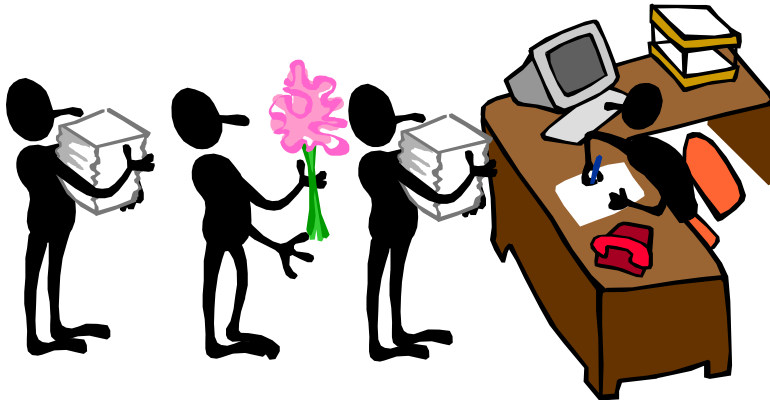
+ Whether accessibility requirements apply for all teleworking initiatives under the pandemic scenario or could the requirement be waived in some circumstances given the potential added complexity and cost for the capabilities.

These are just some issues that would affect the articulation of telework within Enterprise Architectures.

To further frame the issue, we offer three generic architectural operations in graphic form. The first represents the past scenarios where no real electronic infrastructure existed, barring the analog phones and radios. The second constitutes today with additional options and capabilities and the third represents a post-Enterprise Architecture period when additional capabilities can rapidly be deployed or accessed that would replace, restore or create channels for continuity of work through ubiquitous telecommuting capabilities in place for a pandemic or other emergency scenarios.

## PICTURE 1

### The Past

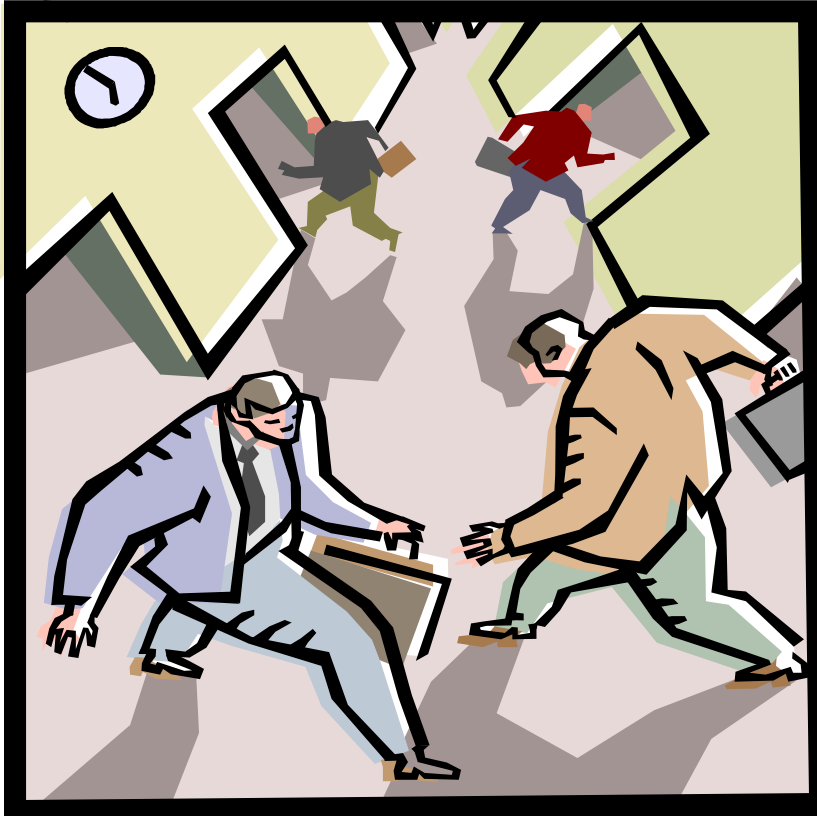


All data, rules, decisions and actions revolve around a physical office.

Pro	Con
Comfortable and effective for its time	Centralized data that needed to be physically accessible—no redundancies for disaster management
Communications channels were limited so interoperability not really an issue.	Limited communication capabilities
Critical decision makers had backup locations and often duplicated files and information	Centralized decision making where data, decision makers, rules, procedures needed to be in one location or accessible via phone

**PICTURE 2**

**The Present**

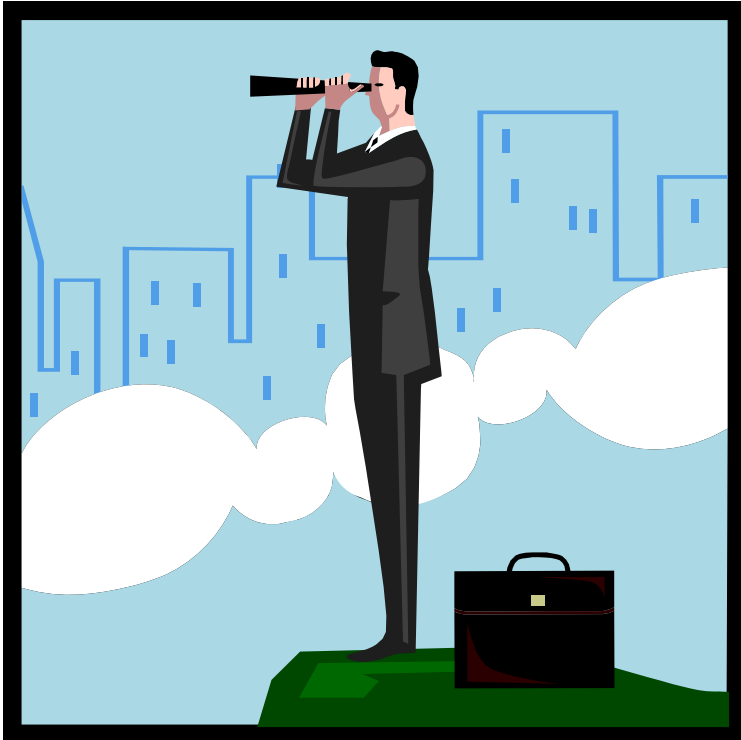


Executives and decision makers are still dependent on their office. However, it is often now remotely accessible or at a minimum, cell phones and PDA's allow continuous connectivity while on the go. Most data, rules, decisions and actions are remotely accessible but are still dependent on centralized data, processes and rules.

<b>Pro</b>	<b>Con</b>
Vastly increased accessibility to people, processes and decisions	Still centralized data, rules, processes, systems and key human dependent
Constant communication capabilities with access to volumes of real time information	Redundancies and fault tolerant capabilities are not prevalent or widespread
	Information cannot be accessed and acted upon, by all key personnel, from all locations, to support LOB missions and functions

**PICTURE 3**

**Future**



Future Office – The virtual office is wherever the decision maker is located. Redundancies where necessary are built-in and fault tolerant, centralized repositories are unnecessary, and the LoB mission continues without a dedicated physical infrastructure or locations. Data, systems, rules and processes are safely and securely replicated across multiple servers and devices in a grid fashion. In some sense, this mimics the Internet except that it is a federal capability like the DoD’s GIG. Enough redundancies are built into the system so that it can withstand and support any mission assigned under any circumstances short of total annihilation.

<b>Pro</b>	<b>Con</b>
Office is virtual and decentralized. It is redundant, as necessary and fault tolerant.	Proper Security, Privacy and Accessibility must be robust and built in
Data, systems, rules, processes are not physically centralized. They can be accessed and acted upon from multiple locations, while connected or disconnected, by multiple humans, even if they are not the primary LoB Personnel.	Governance, especially collaboration based, becomes more difficult, while it remains critical to good decision making.
Not dependent on a physical office	

Using the above general views, the following analysis describes the touch points for a pandemic driven telecommuting solution approach in each of the FEA Reference Models.

### **Business Reference Models (BRMs)**

In every case where the command and control of the various functions and sub-functions defined within the BRM are determined to be critical to the continuity of government and for which certain national priority determinations are made, the vision established for a common government-wide architectural view of virtual distributed decision-making should be covered. To make a determination, the COOP rules and provisions should be identified by sub-functions and used by all agencies in their architectures for those areas and processes. In other words, in all mission areas where functions and processes must go on, there must be architectural provisioning and transition plans to put capabilities in place. This also affects the other reference models as well.

### **Performance Reference Models (PRMs)**

The line of sight is a primary determination to show the viability of a telecommuting capability as a robust and flexible solution set for any disaster or event like a pandemic. The inputs would be telecommuting capabilities provided to the appropriate decision makers that would enable their functions to continue wherever they are. This means that a telecommuting approach could be deployed and governmental functions running to allow for mission continuity. When sub-functions are identified, there should be a performance plan created to measure the impact of the capability when and as needed. It should utilize the Line of Sight to define and describe the major benefits relative to the capabilities inputs and requirement resources.

### **Services Components Reference Models (SRMs)**

There are capabilities identified within the SRM that are critical to enabling telecommuting and provisioning of all the types of services that would be necessary. It is hard to estimate the total of core decision-maker support capabilities that translate into the services currently identified in the highest level of the SRM. These would need to be described and attributes added within them clarifying the special significance and prioritization for continuity during times of national emergencies like a pandemic. As these services are architected within agencies and in response to a need for continuity, they need to funnel into the solution decisions as appropriate. This also has implications for the technologies that are supplied or supported, and to the data that is handled during the virtual office or telecommuting capabilities supplied in response to situational requirements like those a pandemic produces.

### **Technical Reference Models (TRMs)**

The TRM has significant implications that critically underpin any architected solutions for telecommuting under a variety of scenarios including pandemics. These affect the standards profiles and the definitions of a variety of capabilities. The strategy chosen and the policy guidance issued will alter the impact on department and agency TRMs.

### **Data Reference Models (DRMs)**

It is important to codify all data that would be required for COOP. This is a massive task but it can be handled by adherence to DRM. 2.0 and simply adding a commonly agreed to set of data identifiers or attributes in their definitions. This should be determined quickly as much of the DRM work across government remains to be codified. This could be an integral part of the analysis at the agency levels. Within every sub-function where COOP is an attribute, the core data for those sub-functions business mission areas must be assessed and a critical subset of data attributes determinations made. These must be documented and govern the use of the data within any telecommuting capabilities regardless of scenarios. This is another area where the policy is

mandatory because of the COOP driver. This will affect the security, accuracy, privacy and efficacy of the data within all situations including a pandemic where a telecommuting strategy is providing the COOP.

## **Analysis of Options**

In order to enable the decentralized or virtualized office through a transitional telecommuting solution, there are specific features and capabilities that must support the continuity of mission. These features and capabilities include provisioning of disconnected operations for sophisticated multi-tier applications supporting processes that will require many architected services like replicated business rules and a variety of data use and management capabilities. It is unrealistic to think that each capability or service to support this set of horizontal COOP can be enhanced for telecommuting or for a virtualized workspace. Therefore, we must rely on either the infrastructure (functional services and capabilities supported by hardware and software) to enable this new decentralized office. Currently, there is no way to enable all of the applications to have this capability at the hardware infrastructure layer because it does not currently exist. Therefore, one must look to the software application layer. This has a number of architectural ramifications. For example, most custom applications do not use a common software infrastructure or runtime. They are custom applications that interface with other custom applications. By using an approach of representing applications as data (such as xml), one can create a common software infrastructure. This common software infrastructure can then provide innate functionality for the features that are required to have a truly decentralized office. This has implications for a government-wide adoption of standards relevant to COOP. There may be enough of a business case that this could be resourced as or within the appropriate LoBs or even a new LoB to do provisioning with a DoD-like federal GIG architecture to which all other architectures in the federal government connect. Data are encoded with COOP designations in order to be automatically provisioned in a COOP sense during normal operations. Other similar features that affect a national solution for any COOP scenario including a pandemic.

## **Recommendations**

Within the current set of architecture guidance, special considerations and definitions should be incorporated to capture and make explicit the aspects of COOP. This includes those that occur in major disasters or emergencies like a pandemic. This would change the architectures to ensure the legitimization of line-of-sight linkages to the mission outcomes that are critical to operations of government. The appropriate policies including A-130, A-11 and all existing guidance should be amended accordingly.

In particular, emphasis should be given to:

- + The security and privacy of data and the definition of the full DRM 2.0 for all COOP aligned data.**
- + The assignment of COOP attributes to functions, sub-function and further lower taxonomic divisions of the BRM at the agency levels to establish a clear view of the COOP footprint across missions.**
- + An analysis of the business case for a consistent and robust GIG like capability (with a core set of services designed into it commonly) architected with or as a LoB.**



**+ All layers of agency architectures should be assessed to ensure that COOP considerations and telecommuting, and remote office decision-making by appropriate roles and processes are provisioned.**

**+ Insuring the FEA and agency Enterprise Architectures are the primary driving mechanisms within which solutions to a pandemic or any other emergency should be designed and implemented.**

### **Authors**

Joe Brophy, ObjectBuilders, Inc.

Mike Tiemann, EA Werks / FEAC Institute

## V. SECURITY AND PRIVACY IN A LARGE-SCALE TELEWORK ENVIRONMENT

### *Information Security & Privacy Shared Interest Group*

#### **Purpose**

The challenges of a nationwide pandemic or other major event that causes disruption of the government and private sectors on a national scale are so severe that existing federal telecommuting policies, procedures, processes (collectively, “PnPs”), directives and guidance memorandums are not adequate to assure the information security and privacy of sensitive or classified agency information.<sup>3</sup>

Regardless of an event's duration or scope, federal agencies must continue to operate to provide at least a minimum level of essential services to citizens, to state and local governments and other federal agencies. A pandemic would result in significant increase in workforce demand. It also would require individuals to perform duties at locations other than an established government facility, using non-government issued or configured equipment across non-government controlled or monitored networks. Those working from non-government sites (including but not limited to their homes) will need to access, create, store or transmit agency sensitive information. Information security, privacy and data protection issues for paper and electronic formats will exist for workforce members telecommuting in a pandemic environment.

The purpose of this chapter is two-fold: The first is to address pandemic telework issues from an information security and privacy perspective when, as government scenarios project, a high percentage of employees and contractors will be unable or unwilling to work in their assigned offices using their normal systems. Secondly, we look to provide key recommendations on how information security and privacy can be maximized while still providing effective fulfillment of an agency's mission.

#### **Background**

Expected worker absenteeism from government worksites may reach 40% during peak periods of a pandemic. Because this level of absenteeism may last across two to three month waves of illness, business as usual will be anything but usual. Yet the need for information will be critical. The experiences of September 11, 2001, Hurricane Katrina, and Hurricane Rita point to a need for more information across government entities in times of emergencies. Preparation from a policy, implementation, and technology perspectives are the key to success.

#### **Discussion**

Rapidly expanding the size of an agency's workforce that will be accessing, creating, storing and transmitting sensitive information from non-governmental facilities while a pandemic runs its course will require agencies to depart from established standards. This raises issues of administrative, physical and technical information security and privacy safeguards. During the period in which the workforce faces both real and imagined effects of a pandemic, federal agencies must employ a different approach to risk analysis, information security, privacy and data protection than they developed with their normal operations telecommunicating and remote workforce PnPs.

---

<sup>3</sup> Agency sensitive and/or classified information is, for purposes of this Chapter, collectively referred to as “sensitive information.”

The approaches dictated by a pandemic will require agencies to adjust and most likely, lower sensitive information confidentiality, integrity and availability safeguards. Without such action, an agency may not be able to achieve a reasonable and appropriate level of the services. For example, a telework and remote access policy that requires use of government furnished and configured hardware may not be practical in a pandemic. Agencies may not be able to stockpile configured hardware to meet the demand and delivery times—not to mention funding—for new hardware in a pandemic environment. Information security, privacy and data protection risk analysis—and real time fine tuning management of that risk—will be a constant and on-going challenge.

In addition to policies, procedures and processes, there are tools and technologies to protect information privacy and security during a pandemic. For example, protecting sensitive information from being lodged on home computers may be accomplished by implementing a thin-client application at the agency's server. Through a thin-client application, an employee or contractor may use an agency's system to perform essential services and never remove or store any data to his or her home computer. If this type of tool is not implemented before a pandemic, the likelihood of it happening during a pandemic is relatively low.

Regardless of how an agency balances sensitive information security and privacy risks against the need to permit telework required to provide essential services, any rapidly expanded telework scenario has multiple, potentially invalid assumptions. These assumptions for a "thin client" solution—and their possible invalidity—highlight the importance of a strong policy plan before jumping into possible solutions. These questionable assumptions include employees having a computer if government equipment is not available. The user will need, and may not have access to a secured VPN connection to the agency systems and data, a thin-client application, appropriate training, and a persistent network or dial-up connection. Additionally, if any employee incurs out of pocket expenses for this setup, the assumption exists that the employee will be repaid for the costs. For this thin client scenario to be effective all these assumptions must be valid, which is unlikely the case.

Discussions and decisions on information security and privacy should take place before a crisis and focus on the expected course of action to be initiated, specific pandemic policies, education, training, and the tools and systems that will be needed. During a pandemic, the discussions and decisions are mostly about demands, policy implementation, and changes that need to take place to meet the mission within a rapidly changing situation. Each agency may be required to determine what level of risk to protected information confidentiality, integrity and availability it will accept.

### **Analysis of Options**

If September 11, 2001, Hurricane Katrina, and Hurricane Rita are a frame or reference for a pandemic or major event, information access will be more critical than ever. Simultaneously, access to administrative, physical, technical, and information resources will be limited. It is likely that a crisis will cause decisions to loosen the security and privacy requirements to meet an agency's mission goal. The key is to make security and privacy decisions as a risk decision and implement a robust set of policies, plans, and tools in place prior to an event ever taking place to be ready for remote operations of an agency's mission.

## Recommendations

### + Include pandemic scenario within COOP.

Information security, privacy and data protection safeguards implemented by a federal agency in response expanded emergency telework situations for workforce members resulting from a pandemic event should be a subset of the agency's Continuity of Operations Planning (COOP). COOP for a pandemic influenza event must take into account core aspects of emergency telework environments. Workforce members performing their jobs through emergency telework will in many instances use personal rather than government provided tools and equipment, will have limited or no information technology skills, and may not be able to fully secure their non-government provided work areas or equipment in a manner consistent with normal information security and privacy best practices. Furthermore, they may not be able to bar other family members from using personal or home computers and equipment.

### + Implement a non-emergency telework plan.

For an agency to obtain basic assurances that it has implemented reasonable and appropriate information security and privacy safeguards, it must first assure itself that has developed and implemented general policies, procedures and documentation (PnPs) applicable to non-emergency telework situations. The agency's information security and privacy PnPs for basic telework, work extension and mobile work situations provide a baseline for emergency telework. From this baseline, an agency may conduct risk analysis on those PnPs that may be impractical to apply and effectively enforce in an emergency pandemic telework environment. The result of such risk analysis will support decisions on how to manage the identified risks in the context of performing its core government functions during the course of a pandemic or other emergency operations event.

Pre-pandemic planning focuses on "[e]nsuring the continuity of essential Government functions in the event of national or local emergencies."<sup>4</sup> Toward this end, the OPM Guidance provides that all agencies must have policies on information systems and technology security. Managers must ensure their equipment choices and telework agreements comply with this policy, and information security must include protection of sensitive "hard copy" files and documents. Security training, administered at the agency level, is mandatory. Federal employees and their managers are responsible for security of federal government property and information, regardless of their work location. Agency security policies also do not change and should be enforced at the same rigorous level when employees telework as when they are in the office.

### + Have a process to determine and document when non-emergency telework plans are no longer applicable.

To conduct reasonable and appropriate analysis of the information security and privacy risks associated with rapidly expanded telework demands, an agency must have an understanding of the basic federal telework guidelines and advice. If an agency determines that a guideline cannot be fully implemented, there should be a process that includes documentation. That documentation should include analysis of the risks to the confidentiality, integrity and availability of the agency's protected and sensitive information and whether assumption of those risks is reasonable and appropriate in the context of the agency's ability to fulfill its core missions in a pandemic environment.

With respect to emergency telework situations, the OPM Guidance recommends that that managers must ensure teleworkers complete this training and understand their responsibilities in safeguarding work-related information. There must be security measures for teleworkers to cover information

---

<sup>4</sup> OPM Guidance

systems and technology. This includes information systems used by the teleworking employee, including paper files, other media, storage devices and telecommunications equipment (e.g., laptops, PDAs, and cell phones). In addition, teleworkers must comply with the agency security and telework policies. Home-based telework employees need to keep government property and information safe, secure, and separate from their personal property and information.

These OPM recommendations may not be a practical response to teleworking in a pandemic environment. For example, if an individual engaging in telework for the first time in reaction to a pandemic uses his or her cell phone to transact government business, will the agency be able to “secure” that cell phone? If the individual must use a personal computer located in the family room because the agency cannot furnish government equipment, how can the individual or agency comply with OPM’s guidance on keeping government information separate?

Whether from OPM or OMB, agencies may need guidance on the pandemic/emergency scenarios and environments in which they may deviate from basic telework information security, privacy and data protection mandates. Agencies managers may also need guidance on when they can waive or modify these mandates in order to meet citizen needs or the needs of other federal, state or local service demands.

**+ Prioritize the mission based on roles, personnel, and systems. Allocate appropriate systems, tools, communication, and equipment to minimize the amount of secure and private information that leaves government computers.**

Whether as part of its general COOP activities or as part of its pandemic/emergency operations planning, an agency must clearly determine and document the priorities. It must be determined which job functions are essential to perform the agency’s mission, and what service functions should be handled remotely. These determinations will become a basis for follow-up analysis to create recommendations on the need to modify laptops and system access. This analysis will assist an agency in knowing the information and activities requiring use of and access to exceptionally sensitive or private information that can only be protected if access, storage, and transmission are limited to secure government furnished and configured equipment.

**+ Manage data security and privacy across all agency systems.**

The loss of 26.5 million citizen identities by the VA in mid 2006 highlighted the fact that sensitive information resides on laptops and desktops as well in systems and networks. Therefore, a need exists to manage the security of government data, not just networks and systems.

Active management and logging of sensitive information as per OMB guidance across all areas of M-06-16 and M-07-16 is recommended to know where sensitive data resides, where it is going and how it is being managed throughout an event. There needs to be necessary scrubbing of various systems, or changing of data rights during and after the pandemic to stop the loss of sensitive data. This can only occur if one is in compliance of these OMB policies.

**+ Train and rehearse.**

Training is critical to effective preparation, especially for emergencies. A pandemic will affect every aspect of how government operates. Training is a key component of effective preparation.



## References

<sup>3</sup>Agency sensitive and/or classified information is, for purposes of this Chapter, collectively referred to as “sensitive information.”

<sup>4</sup>OPM Guidance

## Authors

Thomas C. Evans, KMK Systems Technology

Peter McDonald, CIPP Symantec

David Edwards, Sprint

Information Security & Privacy SIG's Privacy and Data Protection Committee Members

## VI. DOES OUR IT INFRASTRUCTURE SUPPORT LARGE-SCALE TELEWORK?

### *Networks & Telecommunications Shared Interest Group*

#### **Purpose**

The implementation of the federal telework requirements tend to focus on the infrastructure at agency locations and the wireless devices of the agency management team. There are broader communications infrastructure issues including a single point of failure in the agencies planning scenarios—the fact that agency employees in their homes will have only limited physical connectivity to conduct their agency work. As a rule, cellular service is not suited for the conduct of agency business with the public given its inability to retrieve and store the data needed to interact with the citizens. We begin with an overview of the typical systems that an agency needs to accommodate a heavily dispersed workforce and the public backbone infrastructure where redundancies are commonplace unlike workers remote work locations.

#### **Background**

Workforce resiliency during a pandemic or other major crisis that interrupts the normal work patterns will be dependent upon a number of factors. Foremost among those factors will be the infrastructure that allows the government employees to communicate in a manner that resembles normalcy. Employees will need to communicate with peers, managers and citizens to carry out their work functions in a manner that mirrors their daily routine and conveys a sense of calm to all parties.

This chapter discusses the major attributes of the current telecommunications infrastructure that typically exists in the larger metropolitan areas where the federal government work force tends to be concentrated. The telecommunications infrastructure is defined as the end-to-end connectivity consisting of the hardware and software systems, the terrestrial and wireless facilities, the applications and processes that will allow teleworkers to mimic their office productivity environment.

Enabling safe, effective telework has a series of technological and management challenges. Fortunately, many private companies for years have successfully enabled their employees to telework from their homes or from remote locations. Because of this, solutions exist to address the primary concerns that government agencies have with telework: management, support, security and the same access to people and tools they have while in the office.

One must assume that in a pandemic, many government employees will find themselves working from home for the first time. These employees will require a high level of support for the first week or two while they figure out how to log into their office networks remotely, how to configure their PCs to printers, and how to use new applications. This includes VPN clients, secure chat and desktop video applications. Even questions such as how to access office voicemail remotely will arise. No matter how ubiquitously instructions are deployed ahead of time and how much training is provided, there will still be an extremely high number of instances during the first two weeks where people will need the real-time assistance of an expert to help them get comfortable with these new procedures and to address unanticipated technological challenges. We strongly recommend that contracting firms that provide helpdesk services as a key preparatory step to addressing any pandemic scenario. These firms should have extensive experience providing 24x7 help desk support for the entire array of applications used by the government workers. They also should have the demonstrated ability to ramp up their services on short notice to address the inevitable spike in demand during the first two weeks of a pandemic event (up to 20 times the normal helpdesk volume).

In terms of providing secure access to applications while working remotely and preventing hacking by a third party, we recommend ensuring that government workers have broadband access to their homes via DSL, cable modem or high-speed satellite ahead of time. They also should have Virtual Private Network (VPN) technology deployed, tested and used to provide a secure "tunnel" around the data traveling back and forth between their PC at home and the network at the office. To leverage this investment, the agencies should implement policies promoting teleworking at least one day a week to test the viability of the policies, applications and assets associated working from remote locations. Learning how to work from remote locations and how to manage workers that are dispersed during times of non-crisis will provide the agencies with huge advantages during periods of crisis or turbulence such as a pandemic.

In terms of providing secure access to applications that ensures the privacy of citizens and protection against malicious use of records and applications, there are commercial applications that can be used to create a thin-client environment for the remote worker. Essentially, the remote worker can access all of the applications they normally would at the office via a browser-like environment where they are able to view, enter data into, and have complete control over what is on their screens. Unlike a normal office environment, all of the applications and records should reside on a remote server and are at no time shall stored on the user's PC. The remote user would have no ability to save or print this information if this level of security were so desired.

There are also "remote agent" applications that have been used in private industry for a number of years to allow employees to log in, have their presence and availability known and reported, and have all of the their inbound and outbound voice, e-mail, chat, collaborative browsing and video conversations directed to their remote location. These "agent desktop" applications can be either thick client (an application loaded on the PC) or thin client (a website they log into that provides the same look, feel and functionality.)

This technology can be leveraged by outsourcers who are contracted to perform government functions. The technology exists to federate their environment with the government application and communication environment in a secure and seamless manner. Because outsourcers play such a large role in government today, it is strongly advised that agencies require all of their outsourcers to have pre-defined telework technology deployed prior to contract award and integrated with the government technology and communications environment in question immediately after contract award.

The major cause of telecommunications failures during disasters is network congestion or overload. Crises generate intense human need for communication—to coordinate response activities, to convey news and information about affected groups and individuals, and as a panic reaction to crisis. Historically, major disasters are the most intense generators of telecommunications traffic, and the resulting surge of demand can clog even well managed networks. Under this strain, calls are blocked and messages are lost. As urban disasters over the last decade have shown, catastrophic events routinely overwhelm communications grids. In fact, the sheer variety and complexity of network infrastructure and the far-greater needs and expectations of victims and responders increases the likelihood that any single system may fail.

However, modern telecommunications infrastructure has also provided powerful and flexible tools to enable cities to cope with crisis, and quickly relocate and restore displaced or disrupted social and economic activities. The Internet, mobile telephony, and satellite communications provide unprecedented communications capabilities to a wide range of institutions and communities in disaster areas. Current domestic preparedness efforts are almost exclusively focused on improving the reliability, capability, and interoperability of official communications systems. The telephone

network, for example, utilizes a branching structure in which destruction of a single network segment can disconnect entire neighborhoods instantaneously. Wireless links, whose links are constructed out of intangible electromagnetic radiation, reduce some of the vulnerability of wired networks.

## **Discussion**

In recent disasters, especially in developed nations that have high rates of personal ownership of computers and mobile phones, telecommunications has been a powerful tool in helping rapidly resume normal social and economic activities. While “teleworking” or “telecommuting” received considerable attention from pundits and futurists in the 1980s as a means of reducing congestion and commute times, the two California earthquakes (1989, 1994) first provided the impetus for large-scale implementation. Because of extensive damage to regional freeway networks, many firms quickly established telecommuting centers that helped workers return to work while many more worked from home using personal computers. While widely believed to be a temporary measure, approximately eight months after the Northridge earthquake, reports indicated that 9 out of 10 post-disaster telecommuters Los Angeles area were continuing to do so. Telecommuting of the workers displaced by the 9/11 attacks from Lower Manhattan, such as the 334 employees of the Securities and Exchange Commission, were largely temporary. However, many private firms began to rely on telecommuting after Sept. 11 and this practice continued long after the event.

Disasters also focus attention on the need to manage network congestion during emergencies, and to provide priority access to public officials and key civilian responders. The recognition of the importance of the public cellular telephone network in coordinating complex multi-agency responses to large disasters has spurred the deployment of priority access to that service through the Wireless Priority System. In place during the 2003 blackout in parts of the Northeast and Midwest, this system performed as expected. Priority users experienced a 95% success rate making calls using the prioritized system. Voice over Internet Protocol (VoIP) is also being touted as a way to “engineer... survivability during disaster scenarios that involve the failure of network components and/or extremely high call volumes that often occur during times of regional or national crisis.”<sup>5</sup>

## **Analysis of Options**

Despite their best precautions to secure diverse telecommunications connections to their facilities, many networks were routed back to same local switching facilities. The proverbial Achilles heel of the telecommunications infrastructure remains the “last mile.” The alternative access methodologies, wireless and cable, have not yet demonstrated sufficient capacity and flexibility to transport the volume. Recent advances in wireless technologies, such as WiMax, and upgrades to cable systems’ local service telephone offerings are addressing the issue.

Another area of concern is the mobility of the worker since many may have to travel to locations other than their home for extended periods to care for family or to escape their home area. Mobility is becoming the trend for many organizations. Virtually all of these organizations have standardized a set of technology solutions which include laptop computers, a Virtual Private Network (VPN) for secure remote access, and extended help desk support which is often on a 24/7 basis and frequently outsourced

---

<sup>5</sup> “Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communications,” Anthony M. Townsend and Mitchell L. Moss.

Concurrent with implementing telework assets and policies must be a complete understanding of authentication, which is the process of verifying that a client is who or what it claims to be. Agencies must implement “Federated Authentication” that enables security products to integrate with all existing and future authentication mechanisms. This produces digitally signed, standard XML-based assertions that vouch for the user’s identity. Federated authentication technology works with smart cards, digital certificates, tokens, Personal Identification Numbers, user names, passwords and many other identity schemes. Origin authentication ensures that a message actually came from the indicated sender and not from an impostor. This is accomplished by attaching a digital signature to the message to prove the sender’s identity. A digital signature is a value appended or associated with digital data that can easily be confirmed as belonging to only one key of a key pair (the signing key), and incorporates a hash of the document to provide integrity protection.

### **Recommendations**

Infrastructure, defined as the end-to-end system assets, is the great enabler of communications. Workforce resiliency in a time of crisis is dependent on these systems working reliably and consistently. It is incumbent on the agencies to have these assets in place and tested with a trained workforce prior to the crisis to help maintain work routines and provide services to the citizens. The appearance of the government working in a normal manner will provide the public assurance that the crisis is manageable and that the government is there to help. Agencies should implement policies requiring personnel to work from home on specified occasions to test the capabilities of employees to carry on their responsibilities while effectively “quarantined” as they would be during an extensive outbreak. Once deficiencies are identified, each agency can implement policies that encourage employees to install services dialup modems, cable based ISP or the fiber optic services such as FiOS. Failure to consider the employees access to the larger infrastructure, plus the training and support required prior to a major event, leaves the agencies vulnerable during a pandemic.

### **References**

<sup>5</sup>“Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communications,” Anthony M. Townsend and Mitchell L. Moss.

### **Author**

Frank Ellmore, Verizon Business

## VII. EMERGING TECHNOLOGIES THAT ENABLE TELEWORK AND WORKFORCE MOBILITY

### *Emerging Technology Shared Interest Group*

#### **Purpose**

A critically important enabler of telework and mobility is information technology (IT). There are many different requirements placed on an IT solution for telework/mobile work. It must provide a high level of application and data security. It should be easy and cost-effective to implement, use and support. It needs to deliver excellent reliability and consistent performance across different usage scenarios. It also must be flexible to accommodate a variety of remote computers, PDAs, web-enabled cell phones, network connections, and existing agency software and infrastructure.

This white paper will describe emerging, best-practice technologies for telework and workforce mobility proven in private industry. These technologies can enable federal agencies to expand their initiatives with the least amount of budget and staff resources while providing employees with simple yet secure access to the information they need to be productive while working remotely.

#### **Background**

If a pandemic strikes in the United States, the ability of the federal government to support a mobile workforce will be a critical component of any agency's Continuity of Operations (COOP) plan. Moreover, as much as 40% of the workforce will not be able to commute to their designated work locations because they have contracted the flu, are scared that they might catch the flu when exposed to a public environment like the workplace, or are providing care giving services to family members.

Encouraging a mobile workforce extends well beyond the confines of pandemic preparedness. Federal agencies are also being encouraged to promote telework and workforce mobility as a way to comply with Public Law 106-346 and achieve goals including recruitment and retention of staff; increased productivity, reduction of traffic, fuel consumption and emissions; and improved work/life balance. Specifically, Section 359 of Public Law 106-346 (the FY 2001 Department of Transportation and Related Agencies Appropriations Act), defines telecommuting as "any arrangement in which an employee regularly performs officially assigned duties at home or other work sites geographically convenient to the residence of the employee." While this law required 100% of eligible federal employees to telework by 2004, as of June 2007, agencies have only achieved 14% compliance.<sup>6</sup>

Some federal agencies including the Patent and Trademark Office and Treasury Inspector General for Tax Administration have institutionalized a telework plan, but they still face major challenges. Among these challenges are concerns about information security, privacy protection, the ability to meet the needs of each individual teleworker (e.g., avoiding a "one-size-fits-all" package), the ability to provide proper service and support to the teleworker, and the ability to facilitate collaboration between colleagues.

---

<sup>6</sup> Testimony of David Isaacs, Director of Federal Government Affairs for Hewlett Packard, before the Senate Committee on Homeland Security and Government Affairs - Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia. June 12, 2007.

## Discussion

### Access to Important Resources

The best way to make sure that employees can access their applications and data remotely is by adopting policy that promotes broadband use at home, in the field, or at alternate locations. Wireless cards or tethering capability to mobile devices may be a cost-effective alternative even if only used in the home. Offices like the Treasury Inspector General for Tax Administration promotes telework by paying for approximately 50% of their employees' home high-speed Internet costs.<sup>7</sup> The Patent and Trademark Office also provides employees with the same equipment and computers that are “basically identical to what they would have in the office so that they are logging on at home to the same environment.”<sup>8</sup> Once employees have a means for remote access, the access to specific applications and files must be addressed.

### Application Virtualization: Access from Any Computer, Connection or Location

The traditional approach to application access for alternative workplace or traveling users is to install software programs or client software on each device, and then attempt to manage, upgrade, patch and support them on site. This model quickly leads to major costs as IT personnel are often dispatched into the field. It can also potentially limit access from multiple devices or require maintenance for each device the employee uses to access applications or data. When employees are traveling, it may be impossible to do any maintenance until the individual returns to the office with the laptop. If a device is damaged, lost or stolen and there are not alternate devices, the workers may not be able to be productive for days or weeks.

To solve these challenges, industry has developed a model known as application virtualization. Software applications are installed on servers in the datacenter where they can be easily managed by a small staff. Then the applications are “virtualized”—the server enables many users to access private “sessions” of each individual application over the network. They can also support multiple devices, operating systems or other variant access using ‘everywhere’ types of capabilities available commercially. Users view and work with the application interface, sending keystrokes and mouse clicks to the server, which returns an updated screen view. In other words, the applications appear to be running on a remote desktop or laptop but they are hosted on the server.

Application virtualization technology also allows users to work with local printers and other peripherals.

The advantages of application virtualization for telework and workforce mobility are enormous. Users enjoy the convenience of accessing applications from any device with a network connection: because the applications are not running on the user’s computer. Agency IT personnel no longer have to travel to remote locations to maintain applications. Everything is done quickly and efficiently in the data center. Thus, application virtualization promotes flexible working while significantly reducing the costs of computing.

Developing or procuring applications that can work offline when there is limited or no connectivity and then synchronize up when connected is also highly useful. Given pandemic or other threats, there may be intermittent, limited or no connectivity for some time. To provide additional support this, downloading key applications or data may be useful to enable some capability even without connectivity for some period.

---

<sup>7</sup> Telework Exchange best practices presentation. TIGTA: A Telecommuting Success Story. June 27, 2006. Telework Exchange is available on the Web at <http://www.teleworkexchange.com/resource-center-resources.asp>.

<sup>8</sup> Government Executive magazine. April 15, 2003.

## **Desktop Virtualization: Fast, Simple Access to a Complete Desktop of Applications**

For agencies that wish to provide desktop applications to their teleworking and mobile employees, new desktop virtualization technology can make this process simple and easy. Similar to application virtualization, desktop virtualization enables centralized delivery and management of the entire desktop or suite of supported devices. In this scenario, the user's desktop is located in the data center on a server, and the user accesses the desktop or capability over the network. There are many benefits to this approach including instant provisioning, centralized management of desktops and easy de-provisioning. If appropriately provisioned, this can enable users to take advantage of a variety of communication devices besides traditional desktops as appropriate to user, agency or situational needs.

## **Remote Desktop Access: Direct Access to Employee Office Desktops**

While virtualization provides many benefits, it does not provide a complete solution.. The cost can be significant when licensing, configuring, and deploying a server farm capable of supporting an entire organization simultaneously accessing virtualized desktops and applications. In addition, it does not provide access to unique data or applications that may be resident on employees' office desktop PCs.

In order to leverage agencies' existing investments in PC hardware, software, and data storage, and to complement a virtualization strategy, secure remote desktop access can play a significant role in a complete operational continuity solution. No productivity is lost, as workers are literally logging into the same desktop they use at work, with all their standard data and applications at their fingertips. Only limited additional cost is incurred for the access technology because this type of technology leverages the systems already in place.

Recent COTS products in this space have emerged to provide centralized control and built-in security, addressing some of the traditional concerns about utilizing remote desktop technology in the government.

## **Application Streaming: As Simple as Record, Download and Play**

Another approach when mobile employees are disconnected from a network-based application virtualization or desktop virtualization solution is application streaming. For example, anyone who is taking a long flight or working in an extremely remote area may need to work on an application that resides locally rather than one delivered from the datacenter. Application streaming technology addresses this situation. Just like streaming and downloading music, this technology delivers applications to the employee's computer for use whenever and wherever desired—even when not connected to a network. To avoid the problems of installing the application on the computer—such as incompatibilities, configuration and security concerns—applications are cached locally in an “isolation environment.”

For the employee, it is as easy as clicking on an icon on the desktop. Once the worker is finished with the application, it disappears from the machine for enhanced security. Application streaming benefits IT by eliminating application conflicts and the need for extensive regression testing.

## **Data Security: End-to-End Protection**

### **Ease of Use with IT Control**

Delivering applications over the network—particularly the Internet—demands a security solution that can safeguard data from hackers and other cyberspace threats. For telecommuting security, the National Institute of Standards and Technology (NIST) recommended installation of anti-virus and spyware-removal software on each computer. However, it is very difficult to ensure that remote

devices, especially public terminals, have full and up-to-date protection. Therefore, it is critical to have a method for remotely controlling the degree of user access to applications based on the security of each device.

There are also ways to restrict thumb drives, disk drives or removable media as well as limit copying available. While in locations outside the traditional office, applications can also employ splash screens or other employee verification methods that filter images of specific data that should not be visible to others prior to display. For example, if a mobile user were connecting from a public Internet kiosk, it would be undesirable to allow data to be downloaded, perhaps shown in a public setting, and possibly left on the machine. If a teleworker's antivirus protection were not current, it would be unwise to allow data to be saved on the computer until the antivirus has been updated. For practical reasons, IT staff must be able to enforce these controls from the data center.

Traditional solutions for application security, such as virtual private networks (VPNs), are focused on access to networks. Next-generation VPNs based on the Secure Sockets Layer (SSL) protocol can provide secure access to specific application resources. They use a downloadable Web software client that does not require on-site installation or updating by IT staff. In addition to stringent encryption of application data over the network—also called for by NIST—and support for two-factor authentication devices such as tokens, these new SSL VPNs offer centralized, dynamic controls over user actions.

With this technology, remote employees enjoy a single, secure point of access to applications and data. IT staff gain sophisticated security controls while avoiding the cost and complexity of maintaining traditional VPN solutions. A risk assessment and mitigation plan may be useful in balancing the cost, complexity and other aspects to meet mission objectives.

### **Protection Against Theft and Loss**

There have been a number of recent cases involving exposure of highly confidential data such as Social Security numbers when government computers have been lost or stolen. To avoid this possibility, application virtualization keeps sensitive application data behind the agency firewall instead of stored locally on laptops, PCs or other devices. If a computer is lost or stolen, this data is not at risk because it remains securely in the datacenter.

Another way to protect against theft and data loss is by using two or three-factor authentication. Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token such as a card, and the other is typically something memorized such as a security code. In this context, the two factors involved are sometimes spoken of as something you have and something you know. A common example of two-factor authentication is a bankcard: the card itself is the physical item and the personal identification number (PIN) is the data that goes with it. The Department of Defense (DoD) has been a leader in this area by issuing a Common Access Card (CAC) smartcard as standard identification for active duty military personnel, reserve personnel, civilian employees, and eligible contractor personnel. The CAC is used as a general identification card as well as for authentication to enable access to DoD computers, networks, and certain DoD facilities. The CAC enables encrypting and cryptographically signing email, facilitating the use of PKI authentication tools, and establishes an authoritative process for the use of identity credentials.

Some security procedures now require three-factor authentication which involves possession of a physical token and a password used in conjunction with biometric data such as finger scanning, facial recognition or a voiceprint.

Additionally, some PC and other device providers or add-on suppliers provide ways to remotely allow the system to be located and the system or data to be disabled or erased through GPS or other capabilities.

Many PC and operating system providers can now offer safety measures against a theft calamity as part of a “package.” Such services include next-day disk retention services and accidental damage protection, data encryption, tracking of a stolen or missing computer, and remote deletion of data in the event a device is missing.

These capabilities should be supplemented by strong IT and other security capabilities that allow access to be revoked or observed after a device is reported missing or an employee or contractor is separated. There are also capabilities that observe behavioral changes in access. This can detect devices being misused by others prior to the authorized user realizing that a device is missing. This also supports detection of authorized user misuse of access.

### **Single Sign-on Access and Password Management**

The use and management of application passwords can be a big security issue for federal agencies and a giant headache for users and IT staff alike. Many applications are password-protected, forcing users to remember multiple logins and take care of password changes on a regular basis. With so many different passwords to manage, employees may write them down or use weak passwords, increasing security risks—especially when working from an un-trusted device. They also may overload the help desk with requests for password assistance and resets.

Implementing an enterprise single sign-on (ESSO) solution reduces the burden of application passwords for users and IT staff while strengthening security. With an ESSO solution, the log-on procedure for individual applications is automated. The users log on just once to the agency’s system and the solution authenticates them to each application. This means a single password to remember instead of many, and consequently, fewer help desk calls.

An ESSO solution typically provides powerful, centralized management tools for IT staff, allowing them to specify strong passwords, automate application password changes and quickly terminate a user’s access. These solutions also support the use of two-factor authentication tokens, biometrics and other technologies.

### **Identity and Access Management**

Currently, many agencies rely on antiquated processes to provide access to systems such as filling out paper forms or simply calling another employee to obtain access. Identity and access management systems can simplify your system access request process and make it paperless. A robust identity and access management tool not only provides features like ESSO, but will also allow Federal agencies to use advanced features such as end-user self-registration for system access and automatic provisioning to systems upon approval. If a pandemic struck the United States, these features could be critical to a seamless COOP plan. It will facilitate critical employees getting access to the systems and information they need with little delay; irrespective of where the employees are located

### **Service and Support:**

#### **Application Performance Optimization: High Productivity and Satisfaction**

Another challenge posed by telework and mobile work is slow performance of applications over wide-area networks. As employees work at greater distances from the datacenter, WAN latency—particularly when data-intensive or graphics-heavy applications are involved—can significantly affect response time and force workers to wait for software to launch or actions to be implemented. Slow application performance can cause productivity loss and dissatisfaction.

Fortunately, there is technology available to optimize application delivery over IP-based WANs including private leased lines, public Internet VPNs, and satellite and wireless WANs. This technology, installed in the datacenter, automatically and dynamically applies to each data flow the best combination of performance-boosting techniques depending on the application, the data and the network conditions. Teleworkers and mobile employees will experience LAN-line application performance over the WAN, which means less time waiting for slow applications and more time using the application.

### **End-user Performance Monitoring: A Positive Work Experience**

Nothing can discourage employees from teleworking faster than a poor experience with application access. Whether caused by network problems, computer issues, server issues or even the application itself, the result can be frustration, lost productivity and repeated calls to the help desk. Instead of guessing at the source of the difficulty, federal agencies need tools that can monitor system performance, alert staff when problems occur, and pinpoint the source for fast resolution.

Advanced technology is available to monitor the end user's experience and report to the IT team about potential and existing problems. This technology is based on a server in the datacenter, and it relies on a small "agent," or software component, on each worker's computer to report to the server on a regular basis. A wide range of metrics can be tracked, allowing for a detailed look at the entire system or individual issues. You can also set allowable end-to-end performance bands and have the system alert you via a variety of mechanisms when it fails to achieve these service levels. It can also be refined to determine the failing components and ensure those teams are alerted as well based on a call-out or other scheduling tool.

The benefits of end-user performance monitoring include better support for remote users, proactive identification and management of system performance, and reduction of the IT team's workload.

### **Collaboration**

Teambuilding and interpersonal relationships can suffer when individuals lack regular contact with colleagues and managers. To make telework and workforce mobility more effective, agencies need a tool that enables employees to collaborate on projects and documents, and hold meetings without requiring travel. Web-based communications can bridge the gap between "islands of data" and get decision-makers onto the same page—in a virtual workplace.

### **Online Collaboration: Effective Teams Regardless of Employee Location**

With employees scattered to unpredictable remote locations, restoring communication and collaboration is a top priority in a pandemic response scenario. Most employees typically work collaboratively with colleagues throughout the day, from structured meetings to ad-hoc one-on-one visits to look over someone's shoulder, provide an opinion, or answer a question. A collaboration solution can play a critical role in re-establishing these connections in a distributed environment. Users should be able to view the online availability status of their colleagues (also known as "presence management"), and contact those individuals, typically by way of text messaging or text chat. Screen sharing and file sharing are also useful functionality to restore the capabilities usually exercised by walking down the hall. This type of functionality should be made available for regular telework use as well as in on-demand fashion for continuity scenarios, most likely by hosting redundant servers or relying at least in part on systems hosted by a third party—known as "software as a service"

Web-based collaboration solutions, either centrally managed or deployed in a "software as a service" model, can provide the benefits of restoring structured meeting capabilities simply and without adding a new function to the IT office's list of responsibilities. With a hosted service, users simply access a website to set up a meeting or conference and issue invitations. Meeting attendees

do not need pre-loaded software or administrative privileges to participate—they can attend by simply clicking a Web link sent from the meeting host. Once all invited attendees are in the meeting, the presenter can instantly share any file or application on the desktop, change presenters, or give keyboard and mouse control to an attendee.

Not only does online collaboration boost productivity while reducing travel costs, but it also helps to build and maintain work relationships when individuals are away from the office for extended periods or permanently while allowing workers to continue to leverage existing relationships to continue their job functions. As long as the technology provides for centralized control, logging of content and strong encryption and authentication, IT can rest assured that there is no security risk to the enterprise.

### **File Sharing**

In recent years, many federal agencies have begun to use web-based file sharing solutions. These solutions are an important part of an overall collaboration vision and integrate with other collaborative products to offer a comprehensive infrastructure for working with others. Web-based file sharing tools allow employees to author, review, publish, and share documents. These tools also allow users to share best practices in expert communities, broadcast information with blogs and Really Simple Syndication (RSS), capture community knowledge with wikis, and encourage dialogue with surveys and discussions.

### **Peer-to-Peer Networking at Telework Centers**

In the remote likelihood that the Wide Area Network (WAN) is not be available at all and services are “down,” collaboration may become even more difficult. If this is the case, and employees are able to get to a designated “telework center,” peer-to-peer networking may prove helpful. Shared workspace applications allow for the creation of ad-hoc work groups and then allow the work group owners to populate the shared workspace with the tools and content that will allow the group to solve a problem. This could include message boards, productivity tools, and files. The sharing of files can be enhanced through peer-to-peer networking to make file content available in an easy and friendly way. Allowing easy access to the incredible wealth of content at the edge of the Internet or in ad-hoc computing environments increases the value of network computing.

### **Training**

If a pandemic flu strikes the United States, essential personnel may not be available to perform their jobs. Thus, non-essential personnel may have to perform some essential tasks that they are not trained to do. This is why it is important to provide COOP preparedness training and “after-the-fact” training for those who have to respond to the pandemic. This training may need to be provided quickly, remotely, and to multiple locations across the country.

Because of this need, some agencies are focusing on Web-based training that does more than just augment classroom training. According to Michael Miller, the National Defense University’s chief information officer, they are moving all resident courses “into having online course sites, not just to support the classroom teaching but in the case of a continuity-of-operations situation. When, for whatever reasons, students might not be able to come to the university, we would use the online system to continue to support learning.”<sup>9</sup>

Even though online learning has been available for years, the emerging versions of the technology integrate better with a wider array of file formats, such as streaming video, interactive 3-D modeling and gaming technology. The success of consumer systems like Nintendo’s Wii<sup>®</sup> should encourage government agencies like FEMA to customize the product for temporary workers during an

---

<sup>9</sup> Washington Technology. April 23, 2007.

emergency—such as the creation of specialized “game” to facilitate rapid training on wearing a mask. Given the specialization of some approaches, this may be more appropriate for a telework center or a specialized deployment location in an emergency.

### **Wireless Warning and Alert Systems**

As part of enabling a mobile workforce during a pandemic, agencies must be able to give the right information to the right people instantaneously. For private companies, the results of this capability would be measured in dollars and cents. For the government, the results could be tallied in human lives. If a pandemic flu strikes the United States, it is important for agencies to set up an alert/warning system that allows them to communicate with key personnel like first responders from FEMA or critical health services providers from the CDC. Critical employees will have to know where and when the next wave of pandemic is occurring as well learn instructions related to their mission, and alert systems can serve this purpose.

Wireless alert messages can be sent to hand held mobile devices or by email. One example of a wireless message cooperative effort is the national Wireless AMBER Alerts Initiative. This is a voluntary partnership among the wireless industry, the United States Department of Justice, and the National Center for Missing & Exploited Children (NCMEC) to distribute AMBER Alerts to wireless subscribers. While the AMBER alert example is geared towards subscribers, these types of messages could also be “blasted” to all key personnel or to entire populations.

### **Recommendations**

There are a number of different issues that must be resolved before a federal telework initiative can succeed. One major factor is the IT system: if people have a fast, simple, secure and effective way to access applications, data and teammates, they can focus on getting work done instead of struggling to resolve technical problems outside the office. Similarly, the right technology can ease the IT department’s challenges of supporting users on various computers or portable devices. It also can allay agency concerns about security breaches and high costs for infrastructure and support. Additionally, if policy-driven security and privacy approaches can be adapted in near real-time to update access and ensure policy changes, this will support the flexibility needed in a real threat environment.

Thousands of companies have successfully implemented technologies that provide the latest in application delivery, application security, application optimization, end-user performance monitoring and collaboration. These best-practice solutions are making it practical and cost-effective for people to work productively from anywhere, and are delivering benefits of improved retention and satisfaction, reduced travel and greater flexibility.

### **References**

<sup>6</sup>Testimony of David Isaacs, Director of Federal Government Affairs for Hewlett Packard, before the Senate Committee on Homeland Security and Government Affairs- Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia. June 12, 2007.

<sup>7</sup>Telework Exchange best practices presentation. TIGTA: A Telecommuting Success Story. June 27, 2006. Telework Exchange is available on the Web at <http://www.teleworkexchange.com/resource-center-resources.asp>

<sup>8</sup>Government Executive magazine. April 15, 2003.

<sup>9</sup>Washington Technology. April 23, 2007.

## **Appendices**

National Institute of Standards and Technology report, "Security for Telecommuting and Broadband Communications," available on the Web at <http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf>

General Services Administration FMR Bulletin 2007-B1, "Information Technology and Telecommunications Guidelines for Federal Telework and Other Alternative

Workplace Arrangement Programs," available on the Web at <http://www.teleworkexchange.com/FMR2007-B1.pdf>

## **Authors**

Bud Kinzer, NetApp

Janis Keating, Constellation Inc.

Joi Greg, IBM

Steve Charles, immixGroup

## VIII. TELEWORK FOR THE HOMELAND PROTECTION MISSION

### *Homeland Protection Shared Interest Group*

#### **Purpose**

This chapter will demonstrate, via three distinct case studies, how having an established telework infrastructure in place can significantly affect our nation's ability to respond more effectively in times of crisis. This means enabling the workforce to leverage commonly owned devices to access information without risking data loss or leaks in critical situations where on-site physical access may be impossible or undesirable. The first two cases demonstrate how telework enables business continuity in times of crisis. The third case shows how telework can enable leadership to shift workforce roles and responsibilities in times of crisis, surging access to systems that are critical in response and recovery missions.

#### **Background**

A telework strategy has become an important provision in IT planning because of the need to support an ever-changing workforce. However, today's Homeland Protection requirements could take telework to the next level.

Today's federal field workforce has a priority to remain flexible, connected, and mobile. As the work environment or threat level changes, a field agent's mission may also drastically change. A change of priority, new objectives, or a different set of tools needed to respond before, during and after a disaster can be overwhelming for an IT department to support. By planning with proven telework strategies, the surge support requirements would be far less cumbersome to execute in an emergency. The advantage to implementing telework sooner rather than later stretches far beyond the resource savings from lessening traffic and environmental impacts. It creates an established framework for maximizing continuity of operations in pandemic or other disaster scenarios. Further, reducing the associated chaos by having a flexible IT infrastructure empowers leadership and workforce to stay focused on their respective agency or organizational missions.

A major lesson learned from past disasters is that without a secure and scalable telework infrastructure, there will be shortfalls in supporting the workforce. In the case of Hurricane Katrina, there was no choice but to deploy open wireless networks to provide access to the onsite surge in support. However, because of the lack of an established telework solution or the resources to manage the different types of users needing access, there was no choice but to remove all security from this network.

#### **Discussion**

##### **CASE 1: U.S. General Services Administration – Involuntary COOP/Telework Event**

As an example of how an operational telework infrastructure can ensure functional agility to a federal organization, the General Services Administration had to overcome a sudden and unplanned office closure that threatened to bring office productivity to its knees:

During the spring of 2004, our regional office was notified by GSA headquarters that the Democratic National Convention would be coming to the Boston Garden. The arena is next door to our federal building. We were advised that the U.S. Secret Service would be classifying the DNC as a National Special Security Event. This designation has specific significance. The plan was to completely secure and lock down our building, post sharpshooters on the roof and generally make it off limits to anyone without special credentials.

From an IT perspective, we were told to expect that the building would be shutdown and that 100% of the GSA employees that we support would be required to telework for that entire week with no access to the federal building at all. The good news for us is that 4+ years prior to this, our senior management had championed the concept of telework for our regional employees. IT already had implemented an in house 'Application Service Provider' concept using secure, remote access COTS software, issued a single laptop computer for every employee, and had remote asset management / recovery using COTS software and an IT support strategy that allowed for easy support of remote users using COTS software.

As the week of the convention approached, our office attempted to confirm the work locations of each employee to ensure that we could provide adequate support for each person. We made detailed lists of who would be working where and when. By the end of the week before the event, it was becoming clear that almost everyone would be working a day here and a day there, and generally would be in a different location every day. We had moved our helpdesk to a field location and rerouted the helpdesk number so that users would not have to learn a new helpdesk number during the event. We positioned IT staff at several of the major locations and the IT manager drove from location to location ensuring that all was running well.

The week finished and we reviewed with employees and managers how things went and whether anyone had any significant problems or downtime. The comments from literally everyone were that the technology worked flawlessly. Many employees who had teleworked for several years were familiar with remote access and how to access applications and data. The universal print driver allowed seamless connection to any printer in any location they chose to work in, and the availability of using either their GSA laptop or their home computer provided complete flexibility in their workplace. The help desk had no problems providing remote support for any employee regardless of their work location. I am comfortable in saying that our plan was architected well, executed well and had the right technology partners along side us.

– Jim LeVerso, U.S. General Services Administration

The 2004 DNC event was a good real-world exercise that tested the GSA telework infrastructure that could also provide business continuity in the event of a pandemic or local disaster. This event proved the ability of GSA to respond quickly by leveraging a flexible architecture, and maintain a functional workforce.

## **CASE 2: Financial Services Sector**

The financial services industry, as part of planning for telework alternatives for employees in preparing for pandemic situations, has identified the ability of telecommunications networks to handle the increased use of remote business systems as a critical challenge.

The Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) recently formed the Infectious Disease Forum to discuss pandemic planning issues among banks and securities firms. Along with regulatory relief, human resources issues, and other cross-sector dependencies, FSSCC determined that telework issues during a pandemic are a major planning concern.

According to DHS National Communications System's (NCS) current modeling, there is sufficient bandwidth to accommodate increased traffic during a pandemic on a national level, but there could be problems in the "first mile/last mile" connections to the national system.

FSSCC members will assist NCS in refining the models used in determining the system needs in the event of a pandemic. The study is expected to result in recommendations to solve any problems it identifies. "Ensuring the resiliency of the nation's financial sector cannot be accomplished in isolation," said George S. Hender, Chairman of FSSCC. "Whether planning for a pandemic or any other type of business disruption, coordination between the financial services industry and those sectors upon which we depend for power, communications, and basic operations is crucial."

Members of the financial services sector have recently been focusing on the issues associated with the possibility of a serious outbreak of influenza. The potential for such an outbreak—and the likelihood that it would extend worldwide—raises significant issues in terms of business continuity and sector resilience practices, including an organization's telework capabilities.

Guidance from public health officials indicates that it is desirable for all financial firms to consider the implications for their operations of a pandemic that might develop in several "waves" over several months. Historic patterns suggest that staff absences due to illness might be in a range of 20% to 30%. If staff absences due to the need to care for ill family members and from fear of contagion are considered, the absenteeism rate might increase significantly—with some estimates approaching the 40% level.

### **Issues for Consideration Regarding Preparations for "Avian Flu"**

Financial institutions have recently become concerned that their current "all hazards" approach to business continuity planning may not be sufficient to address circumstances in which the organization must try to function during an outbreak of "avian flu" or another serious infectious disease.

A number of financial institutions with worldwide operations have already had to deal with the difficulties of maintaining staff and facilities in locations touched by the 2003 outbreak of Severe Acute Respiratory Syndrome ("SARS"). For many of these organizations, the 2003 experience showed that planning and preparation efforts could prove invaluable in providing their organizations with the ability to function effectively in an "avian flu" outbreak. Just as importantly, however, the SARS experience has convinced planners that, if a much more contagious outbreak does occur, it could present their organizations with difficult challenges that are unlike any in recent history:

- + A serious "avian flu" outbreak could erupt in waves over weeks or even months. Even after a particular wave appears to subside, follow-up waves could develop after safeguards are relaxed. As a result, business continuity plans that address discrete events that might affect organizations for limited periods may prove inadequate for the longer-term impact of an "avian flu" outbreak.

- + During an "avian flu" outbreak, organizations may have to deal with unprecedented absenteeism for weeks at a time, from illness, family demands or fear of contagion. Personnel absences may become so widespread that existing succession plans may prove inadequate to have sufficient personnel available to maintain even critical operations.

- + An "avian flu" outbreak is likely to affect multiple regions of the country and the globe. As a result, backup facilities have been established by many financial organizations. Even remote sites hundreds of miles distant from primary facilities may be just as affected by the outbreak.

- + Disruptions could spread to other key infrastructure such as power, transportation, telecommunications or water systems. Even police, fire, and emergency medical services could be affected.

+Basic retail services may be disrupted. These types of problems might make it very difficult for employees to function effectively at work. Further, since corporate business continuity strategies often rely heavily on the availability of public sector emergency service providers, disruptions in these services from high absenteeism could present significant challenges to corporate plans.

Financial institutions have been seeking to address some of key issues in their business continuity plans to respond to this potential threat: They include:

- +Identification of critical operations for the extended 'down time' caused by a pandemic
- +Identification of suspended operations considered non-essential.
- +Splitting and segregating staff and office quarantines
- +Expanded teleconferencing and videoconferencing
- +Long-distance travel limitations
- +Information-gathering issues
- +Phased implementation plans
- +Testing or exercises
- +Expanded telecommuting or telework

Expanded telework raises a number of issues in its own right:

- +Upgrades to firms' IT infrastructures to accommodate vastly expanded use of telework may require substantial budget resources and weeks or months of advance planning.
- +Expanded telework from diverse locations using a wide range of devices and communication links may raise significant cyber security issues that must be addressed to minimize the chances that sensitive information might be compromised.
- +In a severe "avian flu" outbreak, expanded use of online services by the public may result in slow Internet service that may interfere with telework capabilities.
- +Telework may not be permitted for some functions such as trading that entail significant compliance issues or require substantial IT support. Even if these issues can be resolved, supervisory and record-keeping regulations may preclude telework for these functions, and would have to be addressed.

The Financial Services Sector Coordinating Council's ability to assist the public sector in preparing our nations infrastructure to respond in during a pandemic has been embraced by the DHS National Communications System. The synergy between commercial and government in defining a telework infrastructure that can prepare our nation will certainly continue to grow, thanks in part to the contributions of the FSSCC.

### **CASE 3: Federal Emergency Management Agency (FEMA) – Mission Enablement**

Public and private sector organizations have many reasons to support telework initiatives in their respective organizations. This ranges from offering quality of life benefits to their employees to ensuring continuity of business operations after an incident. However, when you consider the mission of an organization like FEMA, the advantages of telework reach a new level. While FEMA supports telework for their employees in non-disaster situations, the true value of the FEMA telework infrastructure are realized post incident as the workforce surges from 2,400 to over 10,000, with both existing and new workers requiring access to critical response and recovery systems from the field.

Whether supporting the day-to-day flex worker or the post-disaster field responder, remote network access is accomplished using pre-installed, pre-configured software from iPass Inc. (Redwood Shores, CA). The iPass software is only installed on government issued laptops. Preventing workers from using personal or contractor computers to gain FEMA network access maintains a certain level of network integrity.<sup>10</sup>

FEMA maintains over 30,000 laptops, available as surge capacity, in their Disaster Information Systems Clearinghouse (DISC) facility. The laptop configurations are standardized for ease of maintenance and support. The units are re-evaluated annually based on rigorous testing that ensures field workers will remain 'up and running' when they are needed most. The units are also pre-installed with a standard FEMA image including the critical FEMA response and recovery applications. The DISC stores and recycles these assets, ensuring both centralized control and speed of response. For example, during the deadly series of storms in 2005, FEMA added 12,000 notebook computers, printers and their connections to its NEMIS (National Emergency Management Information System) platform. The DISC also has procedures in place to patch and update systems prior to field deployment.

In addition to FEMA's proven technology and distribution procedures, the agency continues to enhance their telework environment. One major area of focus is security. Some examples of security enhancements include updating their standard image with increased security measures. Another example is leveraging technology to help insure end users are benefiting from periodic patch, anti-virus, and security updates while deployed in the field.

It should not be surprising that FEMA is one of the federal leaders in telework. FEMA's federal COOP guidance states that all agencies should consider the use of telework in their continuity planning.<sup>11</sup> And with the potential for massive surges in the need for access to the wide range of FEMA's response and recovery systems, FEMA continues to focus on their telework processes and infrastructure as a core mission enabler.

## **Recommendations**

The benefits to supporting the growing demand for telework have proven value in workforce retention, flexibility, and cost savings in commuting time. However, the real value in a telework infrastructure as it applies to our first responders and homeland protection force, is that it will provide the foundation to support a dynamic and unplanned change in operations.

The three cases were provided to promote establishment of an operational framework for telework in the near term that could be enhanced and refined as new situations evolve. Delaying an initial telework strategy while waiting for the "perfect solution" or "total consensus" will only increase the risk of being unprepared on even a basic operational level in response to a crisis. .

---

<sup>10</sup> [http://www.gcn.com/online/vol1\\_no1/37657-1.html](http://www.gcn.com/online/vol1_no1/37657-1.html)

<sup>11</sup> <http://www.gao.gov/htext/d06740t.html>

## References

<sup>10</sup> [http://www.gcn.com/online/vol1\\_no1/37657-1.html](http://www.gcn.com/online/vol1_no1/37657-1.html)

<sup>11</sup> <http://www.gao.gov/htext/d06740t.html>

## Authors

Julie Baker, Citrix Systems

Mark Forsthoffer, Citrix Systems

## IX. INVESTING IN A SECURE TELEWORK INFRASTRUCTURE – A SMALL BUSINESS PERSPECTIVE

### *Small Business Shared Interest Group*

#### **Purpose**

The small business federal contractor community anticipates that formulation of policy addressing telework for pandemic events will begin very soon. The small business community recognizes that investment in an infrastructure capable of supporting telework will place an investment burden on them. Small business is somewhat more vulnerable than mid-sized and large business due to the cost of acquiring, implementing and supporting a security compliant infrastructure to support a telework capability for its employees. The Small Business SIG's contribution to this white paper seeks to call attention to the issues of concern associated with this small business investment. The small business community is willing to participate in and contribute to discussions leading to developing guidelines for establishing a policy and security compliant telework infrastructure capable of meeting telework requirements during a pandemic event.

#### **Background**

H. R. 3924, the Freedom to Telecommute Act of March 20, 2002 authorizes telecommuting for federal contractors and the FAR was amended to permit the use of telecommuting by employees of Federal contractors in the performance of contracts in support of executive agencies. H. R. 3924 makes no differentiation with respect to company size of federal contractors. There appears to be little to no data on the number of small businesses providing federal contracting support that have instituted telework programs for their employees.

Until recently, the focus of telework and telework policy has been on work/life balance for federal employees and on environmental factors. However, as the prospect of pandemic flu has become a factor of greater concern with respect to its impact on continuity of service/operations, the federal government is now looking to telework as one method of addressing these pandemic event concerns. According to Michael T. Osterhold, Director of the Center for Infectious Disease Research and Policy at the University of Minnesota in Minneapolis "the probability of a pandemic outbreak is 100%, it is just a matter of when." *ComputerWorld* Vol. 13 Issue 16, June 22, 2007.

As the federal government begins assessing pandemic event issues specifically, and formulating additional policies and guidelines to accommodate concerns, the expectation for meeting continuity of service/operations in a pandemic event will be applied to the federal contractors regardless of size. The requirements will be the same for small business federal contractors as it is for large business federal contractors. The small business community supporting the federal government has a major stake in the way in which policies and guidelines are formulated and they should contribute that process.

#### **Discussion**

Two primary concerns of telework include the technical and personnel components. Federal contractors, regardless of size, will be required to implement technical infrastructure that meets telework guidelines and policy including telecommunications and security requirements. This will include corporate infrastructure, agency specific infrastructure and software, access methodology and security (NIST Special Publication 800-53, Recommended Security Controls for Federal

Information Systems) and reliable and consistent performance. There will have to be flexible design for remote computers and network connections, and these connections will need classified/unclassified support, continuity of operations (COOP) and disaster recovery (DR) plans. Secondly, federal contractors regardless of size will be required to develop and implement telework administrative policies and processes that address employee requirements. These include written contractor employee pre-authorizations, training for pre-authorized employees, and periodic employee refresh on telework policies and guidelines

### **Analysis of Options**

Businesses must have infrastructure operationally ready and available when required by the government during a pandemic event. Small businesses can begin to implement this capability on their own and according to the body of information addressing the status of preparation, and should be actively undertaking this planning and implementation. However, there is very little evidence to indicate that this is happening.

Requiring telework capability in order for companies to bid and perform government contracts creates a financial burden on small businesses. This burden could be significant for many small businesses, and may affect the competitive field. While it is reasonable to take the position that a pandemic event is highly probable and businesses of all sizes should be establishing corporate planning appropriately and making the necessary investments, it may be beyond the financial and personnel resource capacity of many small businesses to prepare adequately in advance

To assist its small business contractors, the government has the option of incorporating telework requirements into contracts with cost reimbursement. Establishing the telework support requirement without cost reimbursement would likely reduce the competitive base of small business contractors in the federal contracting space.

### **Recommendations**

As the federal government addresses telework in a pandemic environment, it is realistic to expect that current federal contracts and new federal acquisitions will increasingly incorporate requirements specific to meeting minimum telework capabilities to address continuity of operations. The question is “How can the government assist their small business contractors in planning and implementing the infrastructure needed to meet a pandemic event without impacting the ability of the small business community to participate in federal procurements due to the added financial burden of telework requirements?”

Small business should build the capacity and establish the capability in advance that will meet government telework requirements designed for potential pandemic events in order to continue bidding in the federal space.

The impact to the government is the cost of revising the acquisition and procurement process to incorporate the telework requirements and the telework infrastructure costs associated with those procurements for both current and new contracts.

It is recommended the government consider ways to amend contracts to accommodate telework costs on ongoing contracts and prospective new contracts. It is reasonable for Statements of Work to define security compliant telework technical and administrative requirements and costs for meeting these requirements as part of bids. The role of Acquisition Management becomes very significant.

## **References**

Cyber Security Industry Alliance, Making Telework a Federal Priority: Security Is Not The Issue, July 2005.

U. S. Office of Personnel Management Fact Sheet, Telework and Emergency Preparedness, OPM-11-B-1, August 3, 2006.

A Guide to Telework in the Federal Government, OPM-11-A-1, August 3, 2006.

The Status of Telework In The Federal Government 2005, Office of Personnel Management/General Services Administration.

Trends and Directions in Disaster Recovery Management for Midsize Businesses, Midsize Enterprise Summit 2007, May 14-17, 2007, Donna Scott, Gartner.

Lessons Learned: Katrina, 9/11, SARS, s003 U. S. Blackout, London Bombings and the Avian Flu, Gartner Compliance and Risk Management Summit, May 9-11, 2007 Richard Hunter.

## **Author**

Carolyn Manetti, Advanced Technology Systems Corporation (ATSC)

## X. EXECUTING THE ACQUISITION MISSION IN A TELEWORK ENVIRONMENT

### *Acquisition Management Shared Interest Group*

#### **Purpose**

Acquisition of goods and services is an integral function of any federal agency's mission. Success depends largely on obtaining the items or services they need to the right people at the right time, and at the right price. Constant review and adjustments are made to balance the need for delivery speed with quality of goods and services and competitive pricing.

In emergencies, speed often appears to take precedence over quality and price of the goods and services. Obtaining balance between satisfying urgent mission needs and the other requirements levied by statute and regulation is sometimes difficult to achieve. The federal government, however, is still responsible to the taxpayers to be vigilant in its practices to ensure that fair value is achieved while the critical function of delivering needed services to the citizen is met.

#### **Background**

Experiences and lessons learned from previous emergency incidents such as 9/11, Hurricanes Katrina and Rita tells us that the citizens of the United States demand both speed of services and assurance from its government that their tax dollars are not being wasted. This is evidenced by numerous congressional hearings, GAO reports and articles in the press that cover this topic.

Public health disasters bear both similarities and differences to natural disasters. It is similar to the natural disasters in that it can significantly disrupt the normal mission operation even though there is no physical or infrastructure damage. However, the impact is expected to be widespread across the country rather than being localized.

In either case, one of the keys in mitigating impacts of the disaster is to have a published plan that addresses critical functions and mitigation strategies to ensure continuity of operation. Because no disruption of the infrastructure is expected, telework is one of the capabilities that can be leveraged to facilitate continued acquisition function during the pandemic outbreak.

#### **Discussion**

Fortunately, a great deal of analysis and guidance is already available to federal acquisition professionals who may be asked to operate in a pandemic telework environment thanks to the lessons learned from Hurricane Katrina, Iraqi reconstruction and other emergency situations. Although a pandemic is a different type of emergency than a hurricane or a war, certain similarities exist for executing the federal acquisition mission.

Because of the need to provide guidance for emergency preparedness for federal organizations and employees, the Office of Federal Procurement Policy and the Chief Acquisition Officer's Council jointly published "*Emergency Acquisitions*" in May 2007. This guidance in conjunction with FAR Part 18 "Emergency Acquisitions" and individual agency publications forms an excellent baseline for the development or refinement of governance models and processes that ensure that the overall federal acquisition process continues to be as competitive, fair and transparent as practicable in emergencies. Additional guidance can also be located in publications such as

FEMA's "Disaster Contracting Desk Guide" and "Emergency Acquisition Field Guide" along with a host of other policies and references, which can be found on the Defense Acquisition University's Emergency Response and Recovery Contracting Community of Practice Web Site, which is located at <https://acc.dau.mil/emergencyresponse>.

Agency managers and planners should also look for changes to the "HHS Pandemic Influenza Implementation Plan." There are updated versions of "Telework: A Management Priority, A Guide for Managers, Supervisors, and Telework Coordinators"; "Telework 101 for Managers: Making Telework Work for You"; and "Telework 101 for Employees: Making Telework Work for You" that can be used to determine what additional impacts might affect the successful execution of their agency's acquisition mission. More information on the HHS Plan and guidance to institutions can be found at [http://www.hhs.gov/pandemicflu/implementation\\_plan/](http://www.hhs.gov/pandemicflu/implementation_plan/).

The challenge will be for agencies to sift through the myriad of available materials and develop or adjust processes prior to an emergency so acquisitions can be made quickly in the event of an emergency while still subject to the stewardship of public funds that the American taxpayer demands. Below are five major process areas that should be considered:

### **Competition**

Balancing the preference for competition against the need of rapidly acquiring goods and services in an emergency will be a challenge that most contracting professionals will face. The FAR and other published emergency acquisition guidance provide plenty of discussion on procedures concerning the posting of contract actions, exceptions to competition, use of simplified acquisition procedures and price reasonableness determinations. Contracting professionals will have to address the needs individually. To achieve practicable competition under very trying circumstances, officials should make effective use of available interagency contracts; employ blanket purchase agreements; rely on indefinite-delivery indefinite-quantity contracts; use GSA's multiple award schedules; undertake multiple agency contracts, and use commercial item procedures for certain performance-based acquisitions.

### **Documentation and Reporting**

Emergency acquisitions should not preclude adequate file documentation or reporting to FPDS-NG or Fedspending.gov. Although documentation and reporting does take additional effort, many agencies use electronic contract management systems that have existing FPDS-NG interfaces which enable their contracting professionals to report their awards in near-real time. OFPP in "Emergency Acquisitions" indicates "...Decisions should be appropriately documented to adequately explain the basis for selection. The length of the explanation is less important than the cogency of the rationale for the action taken..." Documentation of the decision process will be very important for lessons-learned and sourcing analyses. A certain amount of forensic analysis likely will be conducted after the emergency by the agency itself, or by other organizations such as GAO.

### **Review, Surveillance and Oversight**

Management review and the surveillance/oversight of contractor performance may become increasingly difficult during emergencies such as a pandemic. OFPP suggests in "Emergency Acquisitions" that "agencies should examine current contract review procedures such as justifications and approvals to determine how these procedures may be modified to accommodate emergency situations." Other suggestions include establishing agency Mitigation Boards to facilitate communications, policy direction and resource utilization, and well as the development of Stewardship Plans to conduct sampling of acquisition actions. Agencies can also consider entering into agreements with other federal entities in order to ensure some level of contractor oversight and surveillance activities are conducted.

## **Pre-positioned Contracts and Agreements**

Agencies should analyze the types of goods and services that they buy to determine if any pre-positioned contracts need to be established so that these commodities can be acquired quickly and efficiently when an emergency strikes. Additionally, depending on the agency's needs, Interagency Agreements with other federal agencies or assisting entities might be formed to ensure that sufficient contractual vehicles and/or acquisition staff are available to meet the needs of an emergency.

## **Pre-positioned Acquisition Workforce**

Just as pre-positioning contracts is necessary, pre-positioning of acquisition workforce is vital for mission success during the epidemic outbreak. Negotiations with unions should be conducted ahead of time regarding work hours, work environment and time reporting requirements. Acquisition professionals need to understand the performance expectations, their individual rights and liability exposures, which may be different during the pandemic outbreak than normal telework conditions.

## **Analysis of Options**

Few realistic alternatives exist other than for federal agencies to plan, prepare and be ready for acquiring necessary goods and services during emergencies. "Contracting" is referenced repeatedly and cuts across many of the Emergency Support Function (ESF) areas of the *"National Response Plan."* The importance of acquisition as the underpinning support process or function to our nation has been made clear in the large number of reports, studies and analyses arising out of Hurricane Katrina, Iraqi reconstruction and other emergencies.

Agencies have no options but to have emergency acquisition management plans in place that address both public health and natural disasters. Without the plan, agencies will suffer loss of a range of services from minor disruptions to a possibility of a critical mission failure.

As a minimum, the impact for lack of preparedness or inadequate planning could include increased scrutiny from Congress, GAO or agency organizations. One of the many examples of this type of investigatory analysis is GAO's study GAO-06-714T *"Hurricane Katrina – Improving Federal Contracting Practices in Disaster Recovery Operations."* This short, but insightful, document cites three primary deficiencies which agencies should strive to avoid. They are inadequate planning and preparation; a lack of clearly communicated responsibilities; and insufficient numbers and inadequate deployment of personnel.

Although this specific study focused on GSA, FEMA and the US Army Corps of Engineers, federal managers could look at the broad conclusions and introspectively look at their own organizations. At the maximum, lack of preparedness could result in the mission failure of the agency to provide required goods and services to support the public need.

## **Recommendations**

There must be a review of current agency processes and procedures to ensure that the strategies for responses to an emergency are adequate. OFPP in the "Emergency Acquisitions" also suggests "...agencies should develop emergency contracting exercises to test processes and familiarize personnel with all phases of an emergency or contingency." As part of an agency's preparation to execute emergency or contingency plans, telework should be encouraged as a normal course of business so that, in case of a pandemic outbreak, the workforce will be prepared to execute the mission and agency will be equipped to support the workforce.

The plans that each agency develops to address a pandemic event should be widely communicated and readily accessible to all employees. The plan should include self-analysis of goods and services required during steady state of operation, as well as projected changes in goods or services consumption during the pandemic outbreak based on their agency mission. For example, the Army National Guard may have additional health and food-related buy-in support of rescue related mission than during normal operation.

The plan should address the following areas:

- + Determine the amount of goods and services needed and whether alternative sources of goods or services will be available if regular vendor community is not available.**
- + Have a primary and backup plan for telecommunications and IT infrastructure available to support acquisition activities as well as plans or exceptions for items that require physical access when that may not be possible due to quarantines.**
- + Insure maximum competition while meeting the possible shortened cycle time due to the need for speed of delivery, and consider alternatives to competition that might include automatic follow-on options of critical maintenance type contracts for a limited duration of time during the outbreak.**
- + Make sure there is the required minimal documentation and reporting during the outbreak with possible extension of reporting period for non-critical items.**
- + Consider alternatives for reviews and sign-off on procurements during the outbreak, which could include increasing CO signature authority level or allowing for concurrent approvals at the various levels within the agency. It could include automatically allowing for delegation of signature authority to multiple people in different parts of the country to mitigate risks of a region being out.**
- + Make sure the publicized list of pre-positioned contracts can be accessed and correctly utilized.**
- + Consider union issues relating to work conditions as well as training, cross training and advanced procurement of expected equipment such as upgraded computers, personal printers/fax/copiers, webcams and broadband access that would facilitate telework for the acquisition workforce.**

## **References**

Are cited individually in the chapter above.

## **Appendices**

Government House of Oversight and Reform Committee Hearings/Reports  
GAO Reports  
Articles from the following News Publications  
    Washington Post  
    NY Times  
    GCN  
    FCW



**Authors:**

Roy Varghese, Director, Business Development, Cigital

Peter Tuttle, CPCM, Senior Procurement Policy Analyst, Distributed Solutions Inc.

Esther Burgess, PMP; VP GSA/GWAC Programs, SI International, Inc

## LIST OF AUTHORS & CONTRIBUTORS

### **Authors:**

Walt Grabowski, SI International, Inc.  
Rick Schrader, Appian Corporation  
Joe Brophy; ObjectBuilders, Inc,  
Mike Tiemann; EA Werks  
Thomas C. Evans, KMK Systems Technology  
Peter McDonald, CIPP Symantec  
David Edwards, Sprint  
Members of the Information Security & Privacy SIG's Privacy and Data Protection Committee  
Janis Keating, Constellation Inc.  
Bud Kinzer, NetApp  
Joi Greg, IBM  
Steve Charles, immixGroup  
Frank Ellmore, Verizon Business  
Julie Baker, Citrix Systems  
Mark Forsthoffer, Citrix Systems  
Carolyn Manetti, Advanced Technology Systems Corporation (ATSC)  
Roy Varghese, Cigital  
Peter Tuttle, CPCM, Distributed Solutions Inc.  
Esther Burgess, PMP, SI International

### **Editor:**

Judith Hasson

### **Overall Support and Coordination for this paper is attributed to:**

Faye Farah, GTSI  
Walt Grabowski, SI International, Inc.  
Janis Keating, Constellation Inc.  
David Shaw, SI International, Inc.