

DRAFT 1

A White Paper

On

Fortifying Telework: An “All Hazards” Secure, Scalable, and Survivable Option

Office of the National Capital Region Coordination
Department of Homeland Security (DHS)

And

General Services Administration

May 23, 2006

Introduction

With the emergence of broadband internet access and wireless network, the federal government has implemented telework¹ to reduce traffic congestion, conserve office space, and recruit and retain qualified, productive employees. In addition, the federal mandate requiring all federal agencies to formulate a continuity of operations (COOP) plan has contributed to the awareness of telework as a viable option to augment the COOP plan.² However, a number of agencies are not identifying critical mission functions that can be accomplished through telework and are not planning for how telework can be effectively used in emergency situations. The stakes are even greater as potential threat conditions (e.g. pandemic influenza) may force an unprecedented number of government employees in the National Capital Region (NCR)³ from accessing their primary work locations. In short, telework in the federal government requires a well-coordinated effort to bring about government wide acceptance of telework to meet current and future mission requirements. The aforementioned effort should yield a standards-based model that can be replicated across the various agencies and jurisdictions within the NCR. This paper will outline fundamental attributes of a sound telework communications model and discuss possible implementation strategies for future discussions.

- **Survivable Network Architecture**

The public internet, the most popular medium among those practicing telework, can be vulnerable during an “all-hazards” event from potential and actual physical

¹ an umbrella term, for all Federal alternative worksite arrangements, regardless of the location of the alternative worksite

² "Should take maximum advantage of existing agency field infrastructures and give consideration to other options, such as telecommuting locations, work-at-home, virtual offices, and joint or shared facilities." *Federal Preparedness Circular 65, June 15, 2004.*

³ The National Capital Region is comprised of over 200 federal government agencies, all three levels of government, and 19 jurisdictions, and well over 1 million federal, state, and local government employees.

DRAFT 2

threat imposed on its various server and intranet nodes. Moreover, the increased internet traffic during an “all-hazards” event may significantly reduce web performance to the point that no appreciable tasks can be conducted via the web. The web is also vulnerable indirectly since its content providers, end terminals, and nodes depend on a power source which has either experienced a dramatic increase in per-unit demand or suffered physical damage itself. Even during a time of crisis, the network supporting telework must maintain a level of performance that allows teleworkers to access and share information in text, voice, and for some, rich video formats.

It would be neither practical nor feasible to construct a separate ‘standby’ network; such a network would be cost-prohibitive. A standby network which is not integrated into the daily business function would also present significant challenges for those workers not accustomed to using it. The existing network must be fortified to support user and network surge capacity.

- **User Authentication and Information Presentation**

Federal Information Processing Standards 201 (FIPS-201) calls for the use of strong authentication⁴, among other requirements, when verifying personal identity. The alternate workplace should mirror the standards that are being implemented in the primary workplace to ensure interoperability and compliance. When properly vetted by the identification process as outlined in FIPS-201, those granted logical access have the same level of privileges as would the first responders or contingency workers at an incident site. The use of strong authentication not only facilitates access control, but it also enables the various stakeholders to align their physical and logical access protocols.

- **Scalability**

There must be enough bandwidth allocated to first ensure communication among those who plan and execute emergency support functions, then among those who provide necessary but non-essential public services. Finally, both permanent and ad hoc remote workers are granted access to perform their duties. The system must have capacity to accept an unusually large number of teleworkers (worst-case-scenario). What is implied in this situation is articulating and enforcing access priority and user discipline. This calls for policy implementation and training in addition to technology implementation.

⁴ Any authentication protocol that requires more than one independent way to establish identity and privileges. This contrasts with traditional password authentication, which requires only one factor (knowledge of a password) in order to gain access to a system. Common implementations of two-factor authentication use 'something you know' as one of the two factors, and use either 'something you have' or 'something you are' as the other factor

DRAFT 3

- **Security (sensitive or classified information)**

The most vulnerable point of entry is at the individual teleworker level. Telework platforms at home are not as secure as the government machines used in the primary workplace. Physical security is at risk, because unauthorized users, including family and friends, can access sensitive data. The risk of unauthorized access to sensitive information is much higher unless there exists a mechanism to protect the privacy of both the worker who uses home-based platforms extensively and citizens whose sensitive information may be displayed or stored in these platforms. In addition, many agencies that routinely deal with sensitive information often use additional layers of security. This calls for a review of security policies and coordination among federal agencies for possible mutual use provisions should the primary workplace become inaccessible, necessitating cross-departmental sharing of data and facilities.

- **Technical Support**

With a drastic increase in the number of teleworkers, technical support staff cannot possibly provide adequate services to teleworkers unless its capacity and mobility increase proportionately. Software and hardware acquisition should examine “thin client” alternatives that require minimal installation and maintenance support. IT support desk must have the ability to correct as many problems remotely as possible, reducing the need for on-site assistance or equipment turn-in.

- **Funding**

It is not possible to implement telework using a single, centralized approach. Not only does each stakeholder have a unique set of practices and traditions, but the stakeholder has also attained a level of interoperability that may or may not facilitate immediate participation. Each stakeholder must conduct gap analysis and leverage on its current funding efforts to achieve interoperability. Moreover, telework can augment each agency’s COOP preparation and planning and should be part of its COOP budget. In addition, it is possible to acquire “telework-friendly” equipment as part of the routine equipment refresh. While each agency’s unique business needs drive the acquisition of applications and hardware, multi-agency coordination can certainly facilitate the purchases of hardware and software universal to all teleworkers and take advantage of economies of scale.

Further Discussion on Implementation

The burden of proof must shift to determine not “who is eligible to telework” but “who is not eligible to telework.” This shift is critical on two accounts. First, it creates an atmosphere conducive to telework and non-traditional work arrangements. Second, it

DRAFT 4

allows for critical capability analysis, both procedural and technological, to account for agency-specific shortcomings.

While each agency or department is responsible for implementing telework on a larger scale, it is important to leverage common attributes of telework implementation to streamline the process. The fundamental framework may not vary too much from one agency to another; i.e., modes of communication and work distribution schemes. The content and delivery preference may vary. However, sufficient common attributes exist to allow for the derivation of a general model. In fact, an adaptable model is what needs to be implemented in the NCR. The conception, building, testing, and implementation of this telework model must involve a wide variety of entities in the NCR to ensure that the model is truly representative of the population it purports to accommodate. Specifically, telework policy development and engineering process must converge; policy, while providing direction and boundaries, must permit the incorporation of technology to the greatest extent possible. The objective is to create a tested, standards-based, well-documented model that can be easily replicated across the various jurisdictions of the NCR.

Conclusion

As discussed above, fortifying telework involves both improving communications infrastructure and policy-making. While no specific evidence points to the insufficiency of the current infrastructure and provisions, no one would argue that any one of the most frequently discussed threat conditions can affect an unprecedented number of government entities and workers for a significant period of time. The task ahead requires a well-coordinated effort among organizations that do not have habitual working relationships but are inextricably tied to one another because of shared interests and responsibilities of serving the public. In the end, the problem presented herein is not just a technology issue but is a multi-faceted problem set that requires discussions and actions from managers, subject matter experts, and practitioners.