

“WORKING THROUGH AN OUTBREAK: PANDEMIC FLU PLANNING AND CONTINUITY OF OPERATIONS” TESTIMONY TO UNITED STATES CONGRESS

Mr. Scott Kriens, chairman of Juniper Networks, Inc. offered a private sector assessment of federal government agencies' progress in developing Continuity of Operations plans, and specifically made four key recommendations regarding telework for the federal government to consider while planning and preparing for a potential pandemic or other national emergency.¹

1. Technology is Available Today — For Effective Continuity of Operations Through Telework

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

First, there needs to be an integrated and intelligent infrastructure that provides for the ready transmission of data, through close “integration” of all the components of the system and the right “intelligence” to help make this happen. Data flow is the essential requirement, and whether it moves through wires, fiber, or the air, it will have to be robust enough to function through a crisis.

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

For example, a telework system for COOP will require virtually 100 percent confidence that the system can remotely authenticate who is accessing and using what information, and ensure that they access and use only information for which they have authorization. Users must be able to access files securely and share information from a headquarters location anywhere, anytime, on multiple products operating on multiple platforms.

2. Focus on Critical Employees

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

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

3. Maintain the Integrity of the Network—by Authenticating and Authorizing End Users

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

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

4. Open Standards Allow Use Of Best-of-breed Technologies and Lower Costs

In an emergency, communications necessarily will come from many sources. Technologies that govern information access and authentication must be able to recognize and interoperate with a spectrum of these technologies. The governing technologies themselves should be as interoperable as practicable with

¹May 2006 testimony

technologies from any number of manufacturers. This not only allows implementation of the best-of-class solutions and increases operational efficiency, but also leads to lower operating cost.

Conclusion

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

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.



Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin,
Ireland
Phone: 35.31.8903.600
Fax: 35.31.8903.601

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.