aep™ NETWORKS

Trusted. Certified. Secure.

WHITE PAPER

Preparing for Emergencies:
Secure Remote Working for Continuity of Operations

Teleworking has become an everyday occurrence for many organizations. Businesses use teleworking—or remote working—as a way to maximize employee productivity because it allows staff to work from home, from a conference center or while they're on the road. For government, however, teleworking plays a role above and beyond worker output. During an emergency, remote access becomes the communications backbone for government and emergency personnel. Military and civilian agencies, law enforcement, healthcare and emergency response personnel must all be able to work remotely to fulfill their duties in an emergency. Without remote access to key data, emergency personnel may be working without the critical information they need to successfully do their jobs.

This paper describes the key technology elements that contribute to running a fail-safe teleworking system for government. Using real-world examples–such as a field hospital set-up outside New Orleans for victims of Hurricane Katrina–we'll address technical requirements for implementing a disaster-ready remote access solution.

History of COOP: The Government's Role During a Disaster

Federal COOP Policy

It is the policy of the United States to have in place a comprehensive and effective program to ensure continuity of essential Federal functions under all circumstances.

As a baseline of preparedness for the full range of potential emergencies, all Federal agencies shall have in place a viable COOP capability which ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations.

– Federal Preparedness Circular 65

President Dwight D. Eisenhower was the first President to activate the 'Continuity of Operation Plan' (COOP) as a way to ensure that a constitutional government would remain in place in the US should a nuclear war occur. The demand for COOP dropped after the Cold War, but today the growing threat of terrorist attacks coupled with devastation caused by natural disasters, like Hurricane Katrina, has put COOP back on the table.

The term 'Continuity of Operations' no longer refers to just the protection of the US governmental system; it encompasses all aspects of Federal Preparedness. In 1999, the Clinton administration introduced the 'Federal Preparedness Circular 65', which required every federal agency to plan for the continuous performance of essential functions and operations in the event of an emergency. Part of an agency's plan for uninterrupted performance—Continuity of Operations—is to designate other locations and alternate facilities where work can be carried out. This is precisely where remote access comes into play. Teleworking gives governments access to important network information from any location so they can continue critical work in an emergency. In a crisis, having fast, secure access to network resources from any location could be the difference between continuity and catastrophe.

Remote Access Helps Doctors Do Their Jobs During Hurricane Katrina Disaster

In August 2005, New Orleans experienced full-scale tragedy. When Hurricane Katrina hit the city and surrounding area, everything was wiped out, including hospitals. With so many injured by the hurricane, temporary emergency hospitals were set-up in the surrounding area. The Thibodaux Regional Medical Center—55 miles from New Orleans—established one of those emergency hospitals to care for Hurricane Katrina victims.

Thibodaux Regional worked with the Red Cross, which had created a makeshift hospital in dormitory rooms at the local university. Doctors worked at the university 'hospital' to triage patients. Thibodaux used the AEP Netilla Security Platform SSL VPN solution to give doctors remote access in the emergency hospital. Having remote access meant doctors could sign-on to the network and applications from the makeshift hospital to access to patient information, laboratory results, etc. As a result, turnaround time for patient care was quick.

"Emergency response after the hurricane hit was critical. If it hadn't been for remote access from AEP, doctors and labs wouldn't have been able to connect with the hospital. By setting up remote access, we lessened the 'life or death' situation," said Terry Evans, CIO of the Thibodaux Regional Medical Center.

The temporary hospital created after Hurricane Katrina has been dismantled, but it was a great lesson on disaster recovery, says Evans. "We have the capability to establish access anywhere. Because there are other local hospitals using AEP Networks' NSP/ MEDITECH environment, we could quickly port our data and provide access through their network in the event our facilities are ever affected by other storms."

Teleworking Technologies

As AEP Networks specializes in teleworking solutions that grant off-site users secure access to applications and resources, this paper references AEP products in the larger discussion of general technologies that make up a fail-safe secure remote access system.

Authentication and Identity Management

Identity Management refers to technologies such as password management, user provisioning and access management. For government, robust authentication is a 'best practice' when accessing sensitive information from a remote location. Consider implementing trusted authentication options: software tokens, RSA tokens, USB authentication keys, etc. These authentication technologies have the advantage of focusing on authenticating actual users as opposed to devices, a definitive security advantage for sensitive teleworker environments.

AEP offers an integrated two-factor authentication system that provides better-than-password-only security and eliminates the need for resource intensive integration activities. In addition, AEP self-registration and provisioning capabilities can simplify administration and expedite the deployment process. Time is of the essence during emergencies.

Access Control Management

Blanket teleworker access raises the risk of unauthorized users accessing sensitive information; it can put privacy and confidentiality in serious jeopardy. Access Control Management builds on Identity Management by using identity to permit or limit the applications and data each user can access. For government deployments, granular access policies can be assigned based on agency affiliation or clearance levels. With AEP Networks' Policy Networking solutions, assigning users to various groups and adding and changing groups and roles is fast and easy.

The establishment of a granular access policy for network resources provides an equally beneficial advantage in audit capabilities. Audit logs that clearly illustrate what applications were accessed and what information was exchanged are becoming increasingly important to meeting regulatory requirements–whether or not an organization is operating under emergency conditions.

Compliance

Most organizations—public and private—struggle with compliance requirements. Many industries have their own compliance mandates, whether it's Sarbanes-Oxley in the private sector or HIPAA in healthcare. Because government compliance must be considered when implementing a teleworking solution, look for products that have received government approvals and certifications, such as FIPS and Department of Defense JITC, and have been designed to support FISMA, HIPAA and HSPD-12 compliance.

Data Encryption

Teleworker access solutions must maintain the privacy of data. Data encryption minimizes the risk of network intrusion by utilizing dynamic session keys, a technique that frequently changes the values used to encrypt the data between two points. Data encryption helps ensure that even in the unlikely event that a session key is compromised only a small fraction of the data being transmitted will be decipherable. 128-bit encryption may be suitable in some use cases, but those requiring stronger protection will need more robust solutions, like AEP's NIST approved 256-bit AES encryption.

Interoperability

A successful teleworking solution must operate within existing network architectures, applications and user environments. Many SSL VPN solutions only support certain browser versions with specified configurations. This almost always causes problems when users deviate from the required settings, use a shared Internet kiosk or unexpectedly download a browser patch or upgrade. This also becomes a problem when teleworking is extended to extranet users whose browser and operating environment can't be carefully managed. A teleworking solution must operate across a broad range of hardware and software environments and should provide seamless, high-performance secure remote access solutions over wired, wireless and satellite networks.

End-point Security

A compromised device can easily translate into a compromised network. If an endpoint becomes the victim of a keystroke-logging Trojan, then the URL of the gateway, the username, and the password can all be captured and used by the attacker. Popular endpoint security features include the ability to verify that firewall and/or anti-virus applications are running on the endpoint before establishing a session.

Using Remote Access for Emergency Response

Operation Respond® Institute (ORI) is a not-for-profit, public/private partnership serving the emergency response community. It provides software tools and training to first responders dealing with hazardous materials and incidents that occur on North American railroads and highways. One of ORI's key contributions to the emergency response community is access to its Operation Respond Emergency Information System (OREIS). The system provides emergency responders with critical information when an incident involving hazardous materials occurs.

For ORI, giving emergency responders remote, secure access to this system is essential. AEP helps ORI link more than 500,000 first responders to the information by offering a secure connection to the system through any wired, wireless or satellite-based device.

AEP's application layer VPN is installed on the user's computer and establishes a VPN connection to the system. AEP also offers a clientless access option for authorized users who might not be able to reach their primary computer during an emergency situation. The AEP SmartGate® solution includes a FIPS validated soft token for digital identity and strong authentication, and meets stringent US Government standards.

"Our selection of AEP SmartGate technology is a critical step to ensure that the sensitive Operation Respond Emergency Information System data is secure and protected. AEP technology will allow ORI to more securely share critical information and applications with OREIS users over the Internet," said Daniel M. Collins, President of Operation Respond Institute.

Remote Access and COOP

Secure, remote access is a requirement for an effective remote working program, especially for government implementations where COOP has become a Federal requirement. In a crisis, having fast, secure access to resources from any location can be the difference between continuity and catastrophe. Having the right set of network technologies in place will ensure a fail-safe teleworking system.

About AEP Networks

AEP Networks offers a comprehensive Policy Networking solution that provides complete security starting at the endpoints and working throughout a network – from the edge to the core. AEP's integrated portfolio of security products includes network admission control enforcement points, identity-based application security gateways, SSL VPNs, CAPS approved high assurance IPSec-based VPN encryptors, and FIPS certified hardware security modules for key management. Our products address the most demanding security requirements of public-sector organizations and commercial enterprises internationally. The company has design and development offices in its headquarters in Somerset, New Jersey, USA and Hemel Hempstead, UK.

Contact Us:

United States		**Europe**	**Email:**	sales@aepnetworks.com
Toll-Free:	1-877-638-4552	Tel: +44 1442 458 600	**Web:**	www.aepnetworks.com
Tel:	+1-732-652-5200			