Agencies Should Add Carrier and Network Redundancy to Disaster Recovery Planning

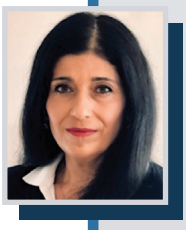
FEATURED CONTRIBUTORS:

- **Rob Sears**
  Director, Enterprise Network Program, NOAA

- **John Leon**
  President & CTO, ORock Technologies & *Founder, Chairman, & CEO*, Hidataics

- **Danielle Marcella**
  Director, Strategy & Product Line Management, PS & PC, Communication Systems, L3 Harris

- **Jim Westdorp**
  Chief Technologist, Ciena Government Solutions Inc.



- **Shaden Shorrosh**
  Sr. Sales Engineer, Federal, Windstream Enterprise

Network failure is simply not an option—it's always been true of government services, but it's an idea that has become soberingly urgent as the landscape of government has shifted. Government agencies are increasingly reliant on digital infrastructure to drive internal development activities, serve their constituents, execute critical operations and remain on mission. To that end, most federal agencies have developed detailed Continuity of Operations Plans (COOP) as a safeguard in the event of a failure or disruption. While many COOP plans involve backups for data, networking and physical locations, agencies may not have considered carrier diversity, which is becoming increasingly critical as a key to maintaining a modern communications infrastructure and supporting complex operations during a crisis.

INTRODUCTION

The environment in which government must function is evolving, in many cases, faster than policies and procedures can be (re)written. Still, no matter the circumstance or operational challenges that may exist, government must adapt and is expected to maintain vital civic and bureaucratic functions. In an effort to mitigate any disruption to public service or interagency accessibility, many federal agencies have enacted Continuity of Operations Plans (COOP) to ensure their most important operations remain intact, whether disrupted by a minor, localized event or a national disaster. Most federal COOP planning is guided by the Federal Emergency Management Agency (FEMA) in the National Continuity Policy Implementation Plan (NCPIP) and the National Security Presidential Directive 51/ Homeland Security Presidential Directive 20 (NSPD-51 / HSPD-20).

ciena | WINDSTREAM ENTERPRISE

For most agencies, the most recent deployment of COOP plans has been in response to the COVID-19 pandemic, where thousands of government workers have been unable to go to their physical work location to carry out the business of government. While most agencies had robust COOP strategies in place, many of those plans were too narrowly focused on the technical aspects of operations, and generally assumed that most of their agents and employees would still be together in a secondary office somewhere, as with other disasters. Few agencies, if any, had a roadmap for across-the-board telework or a long-term decentralized federal workforce.

Agencies had to work up new plans on the fly, revising their COOP policies overnight. By all accounts, they did a great job, as is evident by the federal government still functioning and offering services even as most of the workforce telecommutes, participates in online meetings and generally continues operations in a very different way than anyone thought was possible or even considered just a few months ago.

The pandemic has been disruptive on a foundational level, and it has shone a bright light on disaster planning for federal agencies, making business continuity planning a mission-critical exercise. As agencies develop new plans and examine what went wrong or right in their initial responses to the pandemic, it presents an opportunity to continuously assess gaps in their COOP planning and add new elements to increase resilience and agility of government in previously unimagined realities.

Any new elements added to agency COOP plans must help to account for newly identified potential threats, the totality of agency network operations and supporting technology, and any policy and compliance mandates such as National Security Presidential Directive 51. It should also strongly consider the agency's reliance on telecommunications and remote operations during their pandemic response. As the pandemic has clearly demonstrated, many agencies can operate effectively using a fully remote workforce, but only if they have the ability to connect those employees back to their supervisors, colleagues and shared data sources. For many agencies, safe methods of contact with the public, as well as public access to information are also critical.

To enable and add resilience to these channels of communication, it's very important to consider carrier redundancy and diversity in any COOP plan within government. Some branches of government, such as the military, already have these factors built into their communications and network design, because of the inherent volatility of active military operations. But as the pandemic has laid bare, even the most routine government processes must be built to withstand widespread, prolonged disruptions to their normal operations.

One of the most effective ways to safeguard continuity of communications and vital technical infrastructure is to add carrier redundancy to network designs. This fortification ensures reduced interruptions in the event the primary network carrier's service is disrupted or damaged, by enabling an agency to quickly re-route traffic to their backup.

WHAT IS CARRIER AND NETWORK DIVERSITY?

In an increasingly unpredictable environment, the resilience and reliability of government agencies and the vital programs they administer has never been more important. As portions of the government's workforce have become decentralized, and routine interactions and processes have transitioned to a virtual environment, network connectivity and reliability are now two of the most important aspects of continuity of government. Network failure is simply not an option, and experts at Windstream Enterprises and Ciena Government Solutions say smart techniques like carrier redundancy and diversity can keep agencies up and running, even when primary networks are down.

In a decentralized working environment, the most important tool is the communications network. Without it, nearly all operations for agencies would grind to a dark, devastating halt. Duplicating network infrastructure with alternate connections and having diverse carriers can reduce the risk of a single point of communications failure and ensure another path to network connectivity. Plus, these methods can help agencies meet scalability and security requirements.

For Ciena Government Solutions, carrier diversity is achieved by constructing a network that can overcome the types of failures that drop the primary network. It's important that carriers are truly diverse, meaning they also provide the networking equipment capable of sensing and redirecting traffic when there's a failure among the available paths.

"If you're trying to build critical infrastructure or a high-availability network, you really want something that's geographically diverse," says Jim Westdorp, chief technologist at Ciena Government Solutions. "You want to make sure that you're routing traffic in ways that the same major geographically-affecting event—such as a fire, earthquake or hurricane—doesn't take down your traffic."

Carrier diversity also includes factors like route and conduit diversity. If a train derails and wipes out a conduit, for instance, simple redundancy may not be enough to keep an infrastructure connected if redundant circuits include common conduits.

"You'd still be down the entire conduit," Westdorp explains, and as a result, an agency would still experience complete network failure. "Having carrier diversity can actually mitigate many of these risks."

Ciena Government Solutions helps carriers like Windstream Enterprise find capacity on fiber-optic cables and designs flexible network solutions. Ciena also partners with Windstream Enterprise to provide equipment for route automation and orchestration that allows end enterprises, including government customers, to optimize their network with route and carrier diversity.

The solutions provided by Windstream Enterprise can also help agencies meet those goals while minimizing costs, modernizing their IT infrastructure and enhancing reliability. Windstream Enterprise boasts approximately 170,000 miles of local and long-haul dark fiber.

With a rich history as a trusted primary and diverse provider to over 150 federal agencies, Windstream Enterprise brings a deep understanding of the federal space, and the dynamic demands of COOP planning.

Their government solution experts meet federal agencies at the whiteboard with custom solutions that leverage nationwide data network connectivity, managed services, cloud services and voice/unified communications. What's more, they're able to accommodate carrier diversity within their own network.

"When we're asked to design a solution to avoid certain carriers, we leverage Windstream Enterprise's state-of-the-art network. In many cases, we do so by completing fiber builds, if we have to trench or bore to provide the avoidance, we will," remarks Shaden Shorrosh, senior sales engineer for federal at Windstream Enterprise.

NETWORK RESILIENCE FOR IT MODERNIZATION

Carrier diversity is part and parcel of IT modernization. The journey for federal agencies has at times been incumbered by regulatory roadblocks, but the Federal Information Technology Acquisition Reform Act adopted by Congress in December 2014 to overhaul government technology has set government on a clear path to IT modernization.

"IT infrastructure relies on the underlying network infrastructure just to operate," Westdorp expresses. "If that infrastructure is not reliable enough, you don't have a worthwhile IT service."

In turn, having carrier diversity and network redundancy will ensure the network is reliable enough to support IT modernization. Internet protocol networks and IT networks must be diverse and redundant in order to have a high survivability rate within the carrier's network and operating system.

"At Windstream Enterprise, we've built our backbone IT network to support redundancy and diversity and survivability. That's what really helps us keep our customers up and running and helps them throughout any outages," states Shorrosh.

Windstream Enterprise also provides secure cloud application delivery solutions and managed services that can help agencies reach and maintain IT modernization goals. Their modern data and network solutions, managed services and unified communications empower agencies with reliable, adaptive and secure connectivity in a dynamic technology environment.

TAKE RESILIENCE A STEP FURTHER WITH SOFTWARE-DEFINED NETWORKS

From a network communications provider standpoint, having a software-defined network (SDN) allows for ease of programming services and speedy response times to customer requirements. SDN also allows agencies to efficiently use a diverse carrier, choosing which path to take for lower latency.

"We're able to provide agencies the services they need with just programming instead of rolling trucks or having to go out to their customer sites and install equipment," Shorrosh adds. "We can deliver services almost immediately."

Windstream Enterprise's software-defined wide area network (SD-WAN) solution is built for resilience and performance because it enables multiple connections. SD-WAN helps users take advantage of carrier and route diversity, sending the data over the best-performing connection—a critical capability in the event of a failure.

Ciena's Adaptive Network™ supports these smart network environments, creating a dynamic backbone infrastructure comprised of programmable network elements, software analytics and orchestration—core competencies of an agency network environment fully optimized with SD-WAN and other programmable network functions.

With this advanced level of resilience baked in, users can connect any underlying provider, including existing multiprotocol label switching (MPLS) routing techniques, broadband carriers and cellular broadband. Users can connect to the carriers they want and integrate their access so that there's automatic failover with a seamless user experience in the event of a primary network outage.

CARRIER DIVERSITY IN PREPARATION FOR AN UNPREDICTABLE ENVIRONMENT

Agencies are still working to meet 2002 Federal Information Security Management Act requirements and to support the national policy on the continuity of federal structures and operations during national emergencies. During instances of increased remote work and natural disasters, bandwidth can increase and networks can become congested.

By investing in carrier diversity, network redundancy and network optimization, agencies can maintain their operations while also adhering to necessary cost structures—they don't have to rely on just one carrier.

Additionally, by adopting solutions like those offered by Windstream Enterprise and Ciena, agencies can ensure constant network uptime with redundant MPLS route reflectors, and rely on fixed wireless access when wireline diversity isn't readily available. Even with these solutions in place, agencies must have a backup circuit and network, along with the right security to protect their infrastructure.

KNOW YOUR NETWORK, PLAN FOR THE FUTURE

Some agencies are already benefiting from the advantages of having multiple carriers. In just one instance, Windstream Enterprise worked with one defense agency to provide two completely diverse end-to-end solutions with separate fiber paths, and separate equipment—all while maintaining 50 meters of separation between them, which ensures network failover if one circuit is compromised.

As agencies move to fortify their networks with carrier diversity, agency IT leaders must first understand the network they are running on. When evaluating proposing carriers, it's important to understand how the carriers will provide service, and if it's truly diverse from what the agency already has. Agencies should also ensure carriers share the exact proposed route of the agency's traffic so it can be compared with other carriers to identify any common points of failure. Plus, agencies should consider the way the network is built and the level of service the additional carrier provides, especially during disaster recovery.

Government is entering a new era of connectivity and dynamic accessibility, and network reliability and performance is key.

CIENA GOVERNMENT SOLUTIONS

Ciena is a networking systems, services and software company. We're driven by a relentless pursuit of network innovation—enabling our customers to adapt within ever-changing environments to deliver richer, more connected experiences for their business and users.

WINDSTREAM ENTERPRISE

With extensive expertise in providing services to organizations of all sizes, Windstream Enterprise can help with your complex communications and networking needs. Every customer is a valued customer. Every aspect of your service is supported by a knowledgeable staff to deliver a superior experience.

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300

Info@FedInsider.com
FedInsider.com
@FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

Ciena Government Solutions Inc (CGSI)
7031 Ridge Road
Hanover, Maryland 21076

(800) 921-1144

jwestdor@ciena.com
Ciena.com/government
Facebook.com/CienaCorp
Linkedin.com/company/Ciena
Twitter.com/Ciena

Windstream Enterprise
4001 North Rodney Parham Road
Little Rock, AR 72212

(786) 428-9470

shaden.shorrosh@windstream.com
windstreamenterprise.com/fed-gov
Linkedin.com/company/windstream-enterprise
@windstream