THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

VOLUME 9 NUMBER 10

APRIL 2011
COOP/COG

EDITORIAL STAFF

EDITORS
Devon Hardy
Olivia Pacheco

STAFF WRITERS
M. Hasan Aijaz
Shahin Saloom

JMU COORDINATORS
Ken Newbold
John Noftsinger

PUBLISHER
Liz Hale-Salice

Contact: dhardy1@gmu.edu
703.993.8591

Click **here** to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

GEORGE MASON UNIVERSITY

School of Law

CENTER
for
INFRASTRUCTURE PROTECTION
and
HOMELAND SECURITY

In this month's issue of *The CIP Report,* we highlight Continuity of Operations (COOP) and Continuity of Government (COG). In light of recent events in Japan, it is evident that COOP/COG is essential to delivering critical services and resources in the aftermath of a disaster.

First, the Director of Emergency Management and Continuity Planning at Nova Datacom, LLC and the President of the InfraGard Nations Capital Members Alliance and CEO of Pi2 Strategies, LLC discuss the transilient nature of early 21st century continuity planning. The Executive Director of DRI International then expounds upon the challenges involved with COOP/COG. The next article examines the important link between personal resilience and continuity of operations plans. Finally, we provide information about a course offered by the Emergency Management Institute (EMI) Independent Study Program (ISP) on continuity of operations awareness.

This month's *Legal Insights* analyzes gubernatorial succession, an important process both during and after an emergency.

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

The Transilient Nature of Early 21st Century Continuity Planning

by Ronald Bearse, CIP/HS Senior Fellow and Director of Emergency Management and Continuity Planning at Nova Datacom, LLC, and
Paul Byron Pattak, President of the InfraGard Nations Capital Members Alliance and CEO of Pi2 Strategies, LLC

Transilient (tran zil' yent) adj – passing abruptly or leaping from one thing, condition, etc. to another.

21st century continuity planning will increasingly depend on transilient thinking at the governance table simply because it is now impossible to separate thinking about enterprise continuity from thinking about mission-critical operations — and this applies to every level and unit of society and every type of organization — from the individual household to our Republic itself.

A transilient approach to continuity planning requires accepting the following:

- In an era of accelerated processes, just-in-time business paradigms, quickly-evolving technologies, and growing inter-connectedness, it is vitally important that continuity planning fully reflects the speed at which our modern society operates and allows for future (next generation) growth.

- Continuity planning contributes to resilience and the full spectrum of continuity activities: Enduring Constitutional Government (ECG); Continuity of Government (COG); and Continuity of Operations (COOP), and their equivalents in business, must be seamlessly integrated with critical infrastructure protection and emergency preparedness to mutually support and reinforce each other.

- In a fast-paced world where risks can present themselves in shorter and shorter timeframes, continuity must have a seat at the governance table and transcend the moniker of "something that's happening in the basement or somewhere in Bob's shop," and become an integral and valued element of mission-critical operations — whereby enterprise success directly results from good continuity planning.

As participants in, and practitioners of, the full spectrum of continuity activities, the authors have between them over 50 years of experience. In the beginning of their careers, continuity at the Federal level reflected the assumptions and realities of the Cold War, and was complemented by a robust Civil Defense program to address State and local needs. In those relatively simple days, the threat was easily understood, our adversaries were few, and government had significant monopolies on relevant information, tools, and resources. With respect to our national infrastructure, banking, transportation, and energy seldom overlapped and none of them relied on telecommunications to the extent we take for granted today. Government and business, more or less, knew their respective boundaries and they overlapped in clear and defined ways. Continuity planning, while often challenging, was a straightforward proposition — and frequently done either very discreetly or entirely behind the walls of highly-classified programs.

Within the span of a career, all these assumptions have completely changed. Urgency was always present in the old system, but today it manifests much differently. Today, our Nation has never been so dependent on so many different technologies, any of which, if compromised or disrupted, could seriously impact the continuity of essential functions. Clarion calls for national, regional, organizational, and even personal resilience have been issued by government and industry alike (and rightfully so), yet much remains to be done.

At the Federal level, national continuity planning is fairly straightforward. National Security Presidential Directive-51/Homeland

(Continued on Page 3)

21st Century *(Cont. from 2)*

Security Presidential Directive 20 (NSPD-51/HSPD-20), National Continuity Policy was signed by President George W. Bush on May 9, 2007 and defines ECG, COG, and COOP as follows:

- "Enduring Constitutional Government," or "ECG," means a cooperative effort among the executive, legislative, and judicial branches of the Federal Government, coordinated by the President, as a matter of comity with respect to the legislative and judicial branches and with proper respect for the constitutional separation of powers among the branches, to preserve the constitutional framework under which the Nation is governed and the capability of all three branches of government to execute constitutional responsibilities and provide for orderly succession, appropriate transition of leadership, and interoperability and support of the National Essential Functions during a catastrophic emergency;

- "Continuity of Government," or "COG," means a coordinated effort within the Federal Government's executive branch to ensure that National Essential Functions continue to be performed during a Catastrophic Emergency; and

- "Continuity of Operations," or "COOP," means an effort within individual executive departments and agencies to ensure that Primary Mission-Essential Functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies."

NSPD-51/HSPD-20 further states that: "Federal Government COOP, COG, and ECG plans and operations shall be appropriately integrated with the emergency plans and capabilities of State, local, territorial, and tribal governments, and private sector owners and operators of critical infrastructure, as appropriate, in order to promote interoperability and to prevent redundancies and conflicting lines of authority."[1]

Three months after signing out NSPD-51/HSPD-20, President Bush approved the National Continuity Policy Implementation Plan which states:

- "Continuity requirements shall be incorporated into daily operations of all executive departments and agencies. As a result of the asymmetric threat environment, adequate warning of potential emergencies that could pose a significant risk to the homeland might not be available, and therefore all continuity planning shall be based on the assumption that no such warning will be received. Emphasis will be placed upon geographic dispersion of leadership, staff, and infrastructure in order to increase survivability and maintain uninterrupted Government Functions. Risk management principles shall be applied to ensure that appropriate operational readiness decisions are based on the probability of an attack or other incident and its consequences."

- "The following NEFs are the foundation for all continuity programs and capabilities and represent the overarching responsibilities of the Federal Government to lead and sustain the Nation during a crisis, and therefore sustaining the following NEFs shall be the primary focus of Federal Government leadership during and in the aftermath of an emergency that adversely affects the performance of Government functions:

1. Ensuring the continued functioning of our form of government under the Constitution, including the functioning of the three separate branches of government;

2. Providing leadership visible to the Nation and the world and maintaining the trust and confidence of the American people;

3. Defending the Constitution of the United States against all enemies, foreign and domestic, and preventing or interdicting attacks against the United States or its people, property, or interests;

4. Maintaining and fostering effective relationships with foreign nations;

5. Protecting against threats to the

(Continued on Page 4)

[1] National Security Presidential Directive-51/Homeland Security Presidential Directive 20, National Continuity Policy, available at http://www.dhs.gov/xabout/laws/gc_1219245380392.shtm (May 9, 2007).

21st Century *(Cont. from 3)*

homeland and bringing to justice perpetrators of crimes or attacks against the United States or its people, property, or interests;

6. Providing rapid and effective response to and recovery from the domestic consequences of an attack or other incident;

7. Protecting and stabilizing the Nation's economy and ensuring public confidence in its financial systems; and

8. Providing for critical Federal Government services that address the national health, safety, and welfare needs of the United States."[2]

In February 2008, the U.S. Department of Homeland Security (DHS) issued Federal Continuity Directive 1 (FCD 1) to provide direction for the development of continuity plans and programs for the Federal executive branch. For national continuity planning to be transilient in nature, it must be complemented with strategy and action directed by governance elements in an enterprise.

Armed with the latest iteration of national continuity policy and guidance, continuity planners have been very busy over the last three years building continuity plans, procedures, teams, systems, and facilities as well as conducting the equally decades-old practice of conducting tests, training, and exercises to determine the extent to which their continuity programs are meeting, falling below, or exceeding requirements and, more recently, increasingly stringent stakeholder expectations. Experienced continuity planners clearly see the "transformative, game-changing continuity opportunity" which stands before them, and they are now in the process of taking decisive, irrevocable steps to achieve a quantum leap in continuity planning by embracing a variety of technologies such as cloud computing, virtualization, telework, social media, unified communications, enterprise governance, risk and compliance solutions, interoperable platforms, super-equipped continuity teams, readiness reporting dashboards, and other very exciting tools and technologies. The really good news is that others around the governance table also see these technologies as "must-haves" for growing and operationally optimizing their organizations.

With an unprecedented transformative, game-changing continuity opportunity before the Nation, it is time for a comprehensive national, multi-level, cross-sector assessment of the progress that has been made in implementing the 75-plus critical actions identified in the National Continuity Policy Implementation Plan for ensuring the effectiveness and survivability of our national continuity capability under any adverse conditions.

Such an assessment would:

- Evaluate continuity program readiness to ensure the adequacy and capability of continuity plans and programs by transcending the process of "self-assessment;"

- Support the 2010 Quadrennial Homeland Security Review objective of ensuring the continuity of essential services and functions;

- Identify the deficiencies, gaps, and unmet challenges that must and can be urgently addressed;

- Help ensure that the executive branch's COOP and COG policies in support of ECG efforts are appropriately coordinated, synchronized, and integrated with those of the legislative and judicial branches to achieve non-negligible economies, ensure operability and allocate national assets efficiently to maintain a functioning Federal Government at all times; and

- Help define and resource continuity requirements.

National policy continues to be very clear. On November 30, 2010, in a statement during Critical Infrastructure Protection Month, President Barack Obama issued a proclamation that stated, in part:

The Department of Homeland Security leads an unprecedented national partnership dedicated to the security and resilience of our critical infrastructure. The National Infrastructure Protection Plan integrates a multitude of diverse

(Continued on Page 14)

[2] National Continuity Policy Implementation Plan, available at http://www.fema.gov/pdf/about/org/ncp/ncpip.pdf (August 2007).

Facing the Challenges of Continuity of Operations Planning and Continuity of Government (COOP/COG)

by Al Berman, Executive Director
DRI International

In a perfect world, the ability to respond to a disruptive incident would involve a single controlled source marshalling its resources in a linear, precise, and coordinated manner. Alas, so much for the way we would like the world to operate. Consider reality: an organization which relies on tens of thousands of suppliers to help perform day-to-day activities. At any given moment, an incident may affect this organization or any number of its suppliers preventing them from completing their mission.

In general, this concept is what COOP looks like for the U.S. government. "Partnership between the public and private sectors is essential, in part because the private sector owns and operates approximately 85% of the nation's critical infrastructure."[1] Combine this with the need for inter-agency, inter-jurisdictional complications and the need to create a well-grounded COOP process becomes essential to effectively dealing with major disruptions.

In 2008, the Federal government implemented Federal Continuity Directive 1: Federal Executive Branch National Continuity Program and Requirements and Federal Continuity Directive 2: Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process. These directives created the operational guidance for the creation of COOP and COG planning. The clear objectives of these documents were to create a planning and operational process that would preserve our form of government under any circumstances. While the documents create a specific and detailed process for planning and response to disruptions, they fail to take into account the need for coordination with the 85percent of critical resources that are outside of the government sector. The only mention that there may be outside resource requirements is in the vital records sections, which require "[l]ists of records recovery experts and vendors."

The issue becomes how COOP can be effective without the inclusion of specific recovery requirements for the private sector components. Clearly, without well coordinated and integrated planning, consistency and reliability of recovery efforts cannot take place. Think of dozens, if not hundreds, of key recovery components (analogous to a supply chain), each with a different set of rules for planning and implementation of recovery operations, each working apart from all the other components. The probability of affecting a successful recovery certainly is in doubt. The problem is analogous to issues that have been a part of private sector preparedness and the many vendors that must be in alignment to be able to provide the ability to continue to provide services and goods to its customers. While this is certainly a good business practice, it is also dictated by regulations that require due diligence be performed upon all critical components necessary to effect a recovery.

In embarking on the creation of an integrated COOP process where all the components work in concert with the governmental operation, the logical place to create the synergy is at the time of contractual inception. Ensuring that the private sector entity adheres to the same standard of care as does the government entity to which it provides a good or service is essential. In order to achieve this at time of procurement would require that all government entities adhere to the same standard for preparedness and compel the vendor to create plans around such standard. Given that we have reviewed the preparedness

(Continued on Page 17)

[1] U.S. Department of Homeland Security, Critical Infrastructure Sector Partnerships, Overview, http://www.dhs.gov/files/partnerships/editorial_0206.shtm.

The Emergency Management Institute: Awareness in Continuity of Operations and of Government

by Farshad Broumand, CIP/HS Intern

The Emergency Management Institute (EMI) is steadily working towards its goal of enhancing the skills of United States government officials. EMI strives to achieve its goal by providing a variety of emergency management programs, including more than 400 courses offered to the integrated emergency management community. This group of practitioners includes Federal Emergency Management Agency (FEMA) staff and disaster employees; Federal partners; State, Tribal, and local emergency managers; volunteer organizations; and first responders from across the Nation. Furthermore, EMI supports the international emergency management community. More than 50 countries, both in residence and through internationally organized training groups, participate in EMI's training and educational activities.

The EMI Independent Study Program (ISP), a web-based distance learning program available to the public, provides extensive online training. In 2007, ISP offered 62 courses and trained more than 2.8 million individuals. In 2011, 19 courses were added to their already vast curriculum.[1]

The Continuity of Operations Awareness Course (IS-546.a) course, updated in November 2010, is designed for public sector employees, and based on the course description, takes approximately one hour to complete. It consists of four lessons and provides an overview of continuity of operations, its function, and terminology. The four objectives of the course include: 1) defining continuity of operations; 2) identifying the legal basis for continuity of operations; 3) explaining the Continuity Program Management Cycle; and 4) describing the elements of a viable continuity program.

As described above, the first objective of the course is to define continuity of operations. Similar to discussions in previous articles, the course states that COOP is essential to ensuring that agencies have the capability to "continue performance of essential functions under a broad range of conditions."[2] More specifically, a COOP plan describes: what will occur in a continuity situation; how and how quickly continuity actions must occur; where continuity operations will occur; and who will participate in continuity operations.

The course further explains that there are four phases to implementing continuity plans: readiness and preparedness; activation and relocation (0-12 hours); continuity operations (12 hours–30 days or until resumption of normal operations); and reconstitution (recovery, mitigation, and termination). According to the course, in order to effectively implement a plan, or perform its "essential functions," an organization must possess sufficient leadership; train its staff to perform in a continuity environment; provide adequate, separate facilities locations; and develop and maintain reliable communication systems and technologies.

The second objective of the course is to identify the legal basis for COOP. The National Security Presidential Directive-51/Homeland Security Presidential Directive-20, National Continuity Policy, mandates that certain requirements for continuity plans be developed. Additionally, FCD 1 provides guidance to all Federal executive branch agencies, as well as State, local, and tribal governments, for developing continuity plans and programs. However, given that FCD 1 does not require non-Federal organizations to develop continuity programs, FEMA developed the Continuity Guidance Circular 1

(Continued on Page 15)

[1] For more information on ISP, please visit the following website: http://training.fema.gov/IS/.

[2] http://training.fema.gov/EMIWeb/IS/is546a.asp.

Personal Resilience is at the Core of Effective Continuity of Operations Plans

by Irma Clark,
Personal Recovery Concepts, LLC

People have become the focus for COOP as catastrophic events have highlighted weaknesses in conventional systems for emergency response. New questions have emerged, driving significant shifts in the approach to continuity of operations. These include: Can first responders perform duties if they too are victims of the threat they are asked to respond to? Should COOP focus beyond readiness to resilience? Is personal resilience linked to organizational resilience? Are organizations responsible for building personal resilience?

The First Priority for First Responders is Family

During Hurricane Katrina, 70 percent of Coast Guard personnel in the Gulf lost their homes to the storm.[1] It was also reported by the Louisiana Commission on Law Enforcement that officers left their duty assignments to check on and evacuate their families.[2]

In a 2003 report, the Joint Commission noted that 62 percent of nurses at St. Vincent's Catholic Medical Center's Emergency Department are spouses or partners of first responders in the New York City region. During the events of September 11, 2001, it must have been both professionally and personally anguishing to perform duties on that tragic day.[3]

Following these harrowing incidents, the debate became whether first responders could answer the call of duty when they were also victims of the catastrophe. The conclusion drawn by the Louisiana Commission states that:

> *[e]vacuating and sheltering families ahead of time, or having a preset plan when the disaster is of such a nature as to provide no advance warning, is, therefore, critical to the first responder role.*[4]

A Shift from Survival to Thriving from Turbulent Events — Readiness to Resilience

The focus on first-responders identified weaknesses in response. However, weaknesses in recovery soon followed as businesses grappled with the same issues surrounding lack of employee availability, effectively delaying their time-to-recovery and return to revenue-producing activities. Here too, the degree of personal and family preparedness became a key contributor to the degree of availability that individuals were able to provide to the businesses, organizations, or agencies that relied on them.

In New Orleans, job losses plummeted 30 percent one year after Hurricane Katrina. In addition, 26 percent of businesses had not re-opened. By the five year anniversary post Hurricane Katrina, New Orleans had been scourged by ensuing hurricanes Ike and Gustav, the devastating oil spill in the Gulf of Mexico, as well as The Great Recession. Despite these setbacks, job losses had recovered to a 10 percent decline and business closings had recovered to a 15 percent decline over the pre-Katrina state.[5] Under dramatic conditions,

(Continued on Page 8)

[1] Firehouse.com, *Katrina Response Sparks Review of Federal First Responder Role* http://cms.firehouse.com/content/article/printer.jsp?id=44564 Page 2 of 2 (January 30, 2009).

[2] Carle Jackson, Criminal Justice Policy, Advisor for the Louisiana Commission on Law Enforcement, *Managing Catastrophic Events: The Lessons of Katrina* (April 2006).

[3] The Joint Commission for the Accreditation of Health Care Organizations (JCAHO), *Health Care at the Crossroads: Strategies for Creating and Sustaining Community-wide Emergency Preparedness Systems* (2003).

[4] Carle Jackson, Criminal Justice Policy, Advisor for the Louisiana Commission on Law Enforcement, *Managing Catastrophic Events: The Lessons of Katrina* (April 2006), 21.

[5] Hurricane Katrina Anniversary Data for Louisiana, 2006, and Brookings Metropolitan Policy Program & Greater New Orleans Community Data Center , The New Orleans Index at Five (August 2010).

Personal Resilience *(Cont. from 7)*

Louisiana had come to the conclusion that recovery was not the end goal any longer. Rather, resilience was the capability the region developed and recognized as its critical strength.

Resilience as a strategy acknowledges risk as inevitable and manages an organization's capability to overcome any disruption. The definition for resilience has changed since it became an emergent philosophy. Table 1 (see below) describes the evolution for the definition of resilience in the supply chain.[6]

Personal Resilience Determines the Level of Organizational Resilience

The evolution for the definition of resilience is significant in that now it not only seeks to survive, but also to benefit from turbulent change. The latest definition does not view turbulent change as just something to mitigate, but a force that improves an organization's adaptability and spurs opportunity. Importantly, resilience looks beyond operations and infrastructure to include the role people have in achieving true adaptability:

More than education, more than experience, more than training, a person's level of resilience will determine who succeeds and who fails (Coutu 2002).

Therefore, creating resilient leaders is the best way to ensure that your organization will prosper in a very chaotic and uncertain future, and those resilient organizations consistently outlast their less resilient competitors (Stoltz 2004).[7]

To achieve personal resilience, an organization must therefore comprehend both a family emergency plan and a clear understanding of an individual's workplace roles and responsibilities during a turbulent event. The basic tenets for each are described in Table 2 (see page 8).

Table 1	
Rice and Caniato (2003)	***Ability to react*** to an unexpected disruption and ***restore normal operations***
Sheffi (2005)	***Containment of disruption*** and ***recovery*** from it
Christopher and Peck (2004a)	Ability of a system to ***return to its original state*** or ***move to a new, more desirable state*** after being disturbed
Fiksel (2006)	Capacity for complex industrial systems to ***survive, adapt and grow*** in the face of turbulent change

Evolving Standards and Legal Precedent are Driving an Organizational Responsibility for Personal Resilience

Lessons learned from actual events prove the link between family/personal resilience and workplace resilience. In response to these lessons, the numbers of standards and presidential directives that include recommendations or mandates for family and personal preparedness have increased over time. These include:

- Federal Continuity Directive 1
- HSPD-8: Homeland Security Presidential Directive 8
- HSPD-21: Homeland Security Presidential Directive 21
- National Preparedness Guidelines
- ASIS - American National Standard. Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use
- NFPA 1600 - National Fire Protection Association

Moreover, because case studies and precedence exist that demonstrate a predictable pattern of human behavior under duress that places concern for family above duty, an organization that takes steps to build a resilient workforce that may demonstrate that "reasonable care"

(Continued on Page 9)

[6] Timothy J. Pettit. Dissertation for The Ohio State University, *Supply Chain Resilience: Development of a Conceptual Framework, an Assessment Tool and an Implementation Process* (2008), 14.
[7] Timothy J. Pettit. Dissertation for The Ohio State University, *Supply Chain Resilience: Development of a Conceptual Framework, an Assessment Tool and an Implementation Process* (2008), 11-12.