THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 9 NUMBER 10
AND HOMELAND SECURITY

APRIL 2011
COOP/COG

21st Century Planning 2
COOP/COG Challenges 5
EMI 6
Personal Resilience 7
Legal Insights 10
WEIS 12
WOCI 13

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

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.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

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
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.

Personal Resilience *(Cont. from 8)*

has been taken to mitigate these known factors. Such care may shield the organization from litigious activity following a disaster. Both the United States v. Caroll Towing Co.8 and Conway v. O'Brien cases (see below) offer examples for the responsibility of an organization to take reasonable care for the actions taken by the personnel that act on their behalf.

The common law standard of care can be wide ranging and is based on probability, gravity and burden: The essence of reasonable care was set out by Judge Learned Hand in United States v. Carroll Towing Co.8 as a calculus of three factors: the probability of an accident occurring, the gravity of the resulting injury, and the burden of adequate precautions.99Id. at 173.

See also Conway v. O'Brien, 111 F.2d 611, 612: *The degree of care demanded of a person by an occasion is the resultant of three factors: The likelihood that his conduct will injure others, taken with the seriousness of the injury if it happens, and balanced against the interest which he must sacrifice to avoid the risk. All these are practically not susceptible of any quantitative estimate, and the second two are generally not so, even theoretically. For this reason a solution always involves some preference, or choice between incommensurables, and it is consigned to a jury because their decision is thought most likely to accord with commonly accepted standards, real or fancied.*[8]

Table 2

Family and personal resilience
• Zip-code specific family and pet evacuation and shelter plan • Communication plan, including emergency code words and critical recovery contacts (i.e., insurance agent, lawyer, doctor, etc.) • Survival kits that plan for up to *three* weeks of self reliance – for home, work and school • Wallet-size portable emergency cards • Knowledge of utility shut off • Asset/property list • Copies of personal identification, medical information, key financial data and critical passwords and PINS
Workplace resilience
• Plan for the individual's personal recovery before establishing time-to-recovery objectives and dispensing duties. • Establish family communications systems and liaison support. • Clearly understand the risk mitigation and management plan and their individual roles and responsibilities within it. Have *individuals* create a continuity of operations plan for their own job. This provides a micro-level plan that links back to the macro-level plan, therefore solving for the complexities and interdependencies that characterize organizations. This answers the question, "Yes, but what do *I* do?" • Empower employees with authority to act upon an understanding of the business continuity plan objectives in a decentralized communications structure and/or where there is a lack of an authority figure; • Empower employees to react in an adaptable and flexible manner depending on the circumstances to best achieve the organization's objectives; • After a turbulent change, have employees document the environment and context under which decisions were made. This supports ongoing learning as well as protects from post-event litigation.

In Summary

Where continuity of operations have not accounted for the link to personal resilience, opportunities for effective response and recovery are missed. First responders and critical stakeholders in agencies, communities, business, and government must have prepared their families first to perform their duties in a timely and effective manner. They must also understand their workplace duties at granular

(Continued on Page 17)

[8] The Legal Obligation for Corporate Preparedness, Bill Raisch, M.B.A. – Director & Matt Statler, Ph.D. – Associate Director New York University International Center for Enterprise Preparedness, Denis Binder, S.J.D., Professor of Law Chapman University , October 16, 2006

Legal Insights

Top Choice: A Survey of Gubernatorial Succession Law

by Robin Jessica Clark*

When crisis hits, we need a clear answer to the question, "who is in charge?" and those in the line of succession for the office of Governor need to know and be ready to lead if needed. Continuity planning for a State's chief executive, however, is frequently complicated by State constitutional laws that predetermine the order. The varying qualities of these laws across the Nation may result in a patchwork of preparedness for the unexpected circumstances that trigger a gubernatorial succession. Additionally, the difficulty of modifying some of these legal instruments may delay changes or additions. This article explores the different constitutional provisions guiding succession for State governors to reveal their strengths and weaknesses. This article does not include statutes and executive orders which may expand upon the laws governing succession.[1]

Federal guidance for succession planning provides that, "[c]ontinuity of leadership during crisis, especially in the case of senior positions is important to reassure the Nation and give confidence to its citizens that the principal or appropriate successor is managing the crisis and ensuring the performance of essential functions."[2] A minimum of three positions for all orders of succession are recommended in FEMA's Continuity Guidance Circular-1, but for a leadership position like the Governor, a deeper succession is warranted. For comparison purposes, the order of presidential succession has a depth of 18.[3]

Despite Federal guidance, a survey of constitutional provisions of gubernatorial succession across the country recalls our States' distinct governance structures. While there are some commonalities, they vary widely, in the number of successors, in the successors themselves, and in the circumstances that are taken into account. The first successor is almost always the Lieutenant Governor, and the second successors may be the Attorney General, the Secretary of State, President pro Tempore of the Senate, or another official. While some States, such as Idaho, outline only one successor, Oklahoma has more than ten. Each provision has a slightly different way of describing the possible circumstances that may create a vacancy in the office and thus trigger the succession. While some detail the terms of temporary vacancy due to disability, others simply make mention of that possibility.

Amending the Order

Changes to constitutional

(Continued on Page 11)

[1] Many States have statutes expanding on their constitutional provisions for succession of the Governor, including Alaska, Arkansas, California, Connecticut, Delaware, Florida, Hawaii, Illinois, Kansas, Minnesota, Nevada, New Jersey, New Mexico, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, and Virginia. "State Gubernatorial Succession Law," The Council of State Governments available at http://www.nlga.us/web-content/LtGovernors/TIA_FF_Succession_Law_000.pdf.

[2] Continuity Guidance Circular - 1(CGC-1), Federal Emergency Management Agency, January 21, 2009.

[3] For the Presidency, the Constitution and statute establish the Order of Presidential Succession for officials who meet the constitutional requirements as follows: The Vice President, Speaker of the House, President Pro Tempore of the Senate, Secretary of State, Secretary of the Treasury, Secretary of Defense, Attorney General, Secretary of the Interior, Secretary of Agriculture, Secretary of Commerce, Secretary of Labor, Secretary of Health and Human Services, Secretary of Housing and Urban Development, Secretary of Transportation, Secretary of Energy, Secretary of Education, Secretary of Veterans Affairs, Secretary of Homeland Security. Presidential Succession Act of 1947 (3 U.S.C.19).

Legal Insights *(Cont. from 10)*

provisions may take time because of the rigidity intentionally built into these foundation documents. Depending on the State, there may be requirements for constitutional conventions, referendums, super majority, and voter initiatives. Such requirements may intimidate emergency managers from suggesting the changes. Even emergency managers who are accustomed to following legislation and building relationships with politicians to support statutes that affect emergency management may be reticent to seek a constitutional amendment. Before embarking on changes to a State constitution, emergency managers may explore whether orders of succession set out in a constitution may be added to by statutes or executive orders that do not require amending the constitution.

An intimidating factor to proposing new law in this area is the political sensitivity of the topic of gubernatorial succession. While the basis of the need for a Governor's order of succession is to support the State's emergency preparedness, because of the political process required to make the change, and the political nature of the office that is the subject of the succession, a change to the order may be seen as a political issue. When making recommendations for revisions, a focus on the positions rather than the persons currently holding them should help to separate the process from politics.

One way to accommodate or deflect political pressure may be to amend a State's constitution to provide that the Governor or the legislature has the power to determine successors themselves. Some constitutional provisions, such as those in Alaska, Delaware, Maryland, Florida, and New York leave determination of some successors up to the appointment by the Governor and a vote of the legislature. The concern of this approach from an emergency management standpoint is that it relies on a separate process that may be difficult to carry out during a time of emergency, and may be forgotten or delayed during political transitions. Also, the frequent changes to the order that would occur are less desirable than an established succession that can be practiced and exercised and become a known and accepted fact of government. While it may be difficult or daunting, amending the constitution to create a set order of succession, where one of sufficient depth does not already exist, is the best method of resolving this gap in a State's continuity planning.

Trigger Points

There are admittedly a variety of circumstances which should trigger activation of an order of succession. Enumerating all of these would be difficult to do in one statute. However, there are different ways of dealing with the need for coverage of all circumstances within the law, and States vary on the levels of specificity with which they treat this topic, and some take a short-cut by referring to other sections of their constitution. Death, disability, resignation, and removal are commonly enumerated while some statutes note specific instances, such as a governor who is convicted of treason,[4] or who refuses to take the oath of office.[5] In other cases, euphemisms for disability such as an inability to "discharge the duties of the office"[6] or an "unsoundness of mind" are used. Several constitutions mention an "absence from the state,"[7] and Alabama very specifically notes 20 days of absence as a trigger for succession.[8] Oklahoma and Virginia mention that disaster events may cause the Governor to be unable to exercise his duties.[9]

Determining Disability

While many State constitutions

(Continued on Page 16)

[4] Article IV, Idaho Constitution Section 12.
[5] Colorado Constitution, Article IV, Executive Department, "Succession to the Office of Governor and Lieutenant Governor."
[6] Iowa Constitution, Chapter 7 Governor and Lieutenant Governor, 7.14 Disability of Governor to Act; Kentucky Constitution Section 84, Hawaii Constitution Succession to Governorship, Absence or Disability of Governor, Section 4.
[7] Nevada Constitution, Article 5, Sec: 18, Vacancy in Office of Governor; Duties to Devolve Upon Lieutenant Governor; New Hampshire State Constitution, Executive Power - Governor, [Art.] 49. President of Senate, etc., To Act as Governor When Office Vacant; Speaker of House to Act When Office of President of Senate Is also Vacant.
[8] Alabama Constitution, Article V. Executive Department. 127.
[9] Oklahoma 63 Okl.St.Ann. § 685.4; Virginia Constitution, Va. Const. Art. V, § 16.

The Tenth Workshop on Economics of Information Security (WEIS 2011)

Tuesday, June 14, 2011 to Wednesday, June 15, 2011

at

The Mason Inn Conference Center and Hotel
4352 Mason Pond Drive
Fairfax, Virginia 22030

Registration is now open!!!

Early Bird Registration fees are as follows (additional $50 after June 1st):
Academic/government/post-doc -- $500
Student -- $200
Industry -- $600

For additional information and to register for this event, please visit:
http://www.regonline.com/builder/site/Default.aspx?EventID=960652.

Workshop on Cybersecurity Incentives

June 16, 2011

Mason Inn Conference Center and Hotel
George Mason University, Fairfax, VA

Workshop Objectives

This workshop brings together researchers, economists, policymakers and practitioners to discuss the technical models and incentives that could lead to an increase in the adoption of more secure cyber capabilities. The workshop is aimed at:

- ✓ Promoting the prioritization of security in risk management decision making
- ✓ Improving the understanding institutional designs which create incentives for security
- ✓ Exploring implementable cybersecurity governance mechanisms at the enterprise and national levels

Other presenters

Sean Barnum, MITRE Corp.
L. Jean Camp, PhD, Indiana Univ.
Joe Jarzombek, DHS
Brent Rowe, RTI International
Robert Sloan, PhD, Univ. of Illinois-Chicago
Richard Warner, JD, Chicago-Kent Law School

Workshop Co-Chairs

Daniel E. Arista, SRC, Inc.
Timothy P. Clancy, J.D., George Mason University

Keynote Speaker

Joel Brenner, JD, PhD
Of Counsel, Cooley, LLP

Before joining Cooley, Mr. Brenner held notable appointments such as the Senior Counsel at the National Security Agency, U.S. Counterintelligence Executive, Office of the Director of National Intelligence, Inspector General at the National Security Agency, and as a Prosecutor in the Justice Department's Antitrust Division. He holds a JD from the Harvard Law School, a PhD from the London School of Economics, and a BA from the University of Wisconsin – Madison

Opening Remarks

Bruce Schneier
Chief Technology Officer, BT

Mr. Schneier is the founder and CTO of BT Counterpane, formerly Counterpane Internet Security, Inc. As the inventor of outsourced security monitoring and the foremost authority on effective mitigation of emerging IT threats, Schneier is the author of eight books on the subject, and one of his earlier books, Applied Cryptography, is the seminal work in its field. He writes the free email newsletter Crypto-Gram, which has over 70,000 readers. He received his master's degree in computer science from the American University in Washington, DC.

The Workshop on Cybersecurity Incentives (WoCI) will discuss the history, present, and future of societal mechanisms and institutional designs that leverage incentives to bring an acceptable balance between security and other priorities in cyberspace. The agenda will focus on illustrating cyberspace as an ecosystem of actors and discuss their roles and responsibilities, and the dynamics of their interaction and interconnectivity. Scholarship in law, economics and other fields within the behavioral sciences inform stakeholders about how markets, incentives and legal rules affect each other and shed light on determinations of liability and responsibility. This is considered essential to achieving efficient accountability and a sound public-private order in cyberspace. Considerations of what is technologically possible and feasible will be included. Ongoing debate and research in this area will be presented in practical terms allowing for participants to immediately realize implementable options for governing cybersecurity at the enterprise and national levels. The workshop will discuss the legal, economic and technological facets of the topics presented.

Presented by
GEORGE MASON UNIVERSITY
Center for Infrastructure Protection and Homeland Security

Presented by
SRC

Promotional Partner
AFEI

For more details on the workshop visit
http://cip.gmu.edu/woci2011.html

21st Century *(Cont. from 4)*

stakeholders: Federal, State, local, territorial, and tribal governments; private sector critical infrastructure owners and operators; first responders; and the public to identify and protect our infrastructure from hazards or attack. These critical infrastructure partnerships continue to build their information-sharing capacity and develop actions that strengthen our Nation's preparedness, response capabilities, and recovery resources.

In his proclamation, the President continued:

My Administration is committed to delivering the necessary information, tools, and resources to areas where critical infrastructure exists in order to maintain and enhance its security and resilience. I have proposed a bold plan for renewing and expanding our Nation's infrastructure, including its critical infrastructure, in the coming years. Additionally, we must work to empower communities, an integral part of critical infrastructure security, to work with local infrastructure owners and operators, which will make our physical and cyber infrastructure more resilient. Working together, we can raise awareness of the important role our critical infrastructure plays in sustaining the American way of life and develop actions to protect these vital resources.[3]

We are heartened by *The CIP Report's* decision to dedicate this month's issue to COOP and COG because, as is clearly the case, there is an unequivocal symbiotic relationship between COOP, COG, and critical infrastructure protection.

It cannot be overemphasized enough that continuity planning must not only take its rightful place at the resilience planning table but also a permanent place at the governance table itself. Our policies in these areas are clear. Efforts to effectively implement them will increasingly be dictated by our collective ability to foster and facilitate the enterprise-wide communication, coordination, cooperation, collaboration, and concentration that define how world class continuity programs are built and maintained.

During the sobering days of having to think through the consequences of a nuclear weapons laydown (Armageddon) planning scenario, continuity planning was viewed on the basis of low-probability and ultra-high-consequence events if deterrence failed. Today, our adversaries, vulnerabilities, and low barriers to entry for mischief and malice are challenging us to think in terms of high-probability high-consequence events.

With this year marking the 20th Anniversary of the end of the Cold War and the 10th Anniversary of the attacks of September 11, 2001, it is time to assess the present condition of continuity, embrace the transilient opportunity before us, and engage the governance elements of every organization in building a world that is safer to live in, better prepared for the unexpected, and more resilient to the threats and risks it faces.

As this article was being finalized, the Japanese earthquake of March 11, 2011 became a mega-disaster with four distinct components — each of which is catastrophic by itself: (1) earthquake; (2) tsunami; (3) flooding; and (4) radiological emergency. What clearer signal could we possibly have for the urgent need to take stock of our current business continuity and emergency preparedness capacities and capabilities for addressing catastrophic events? ❖

[3] Presidential Proclamation--Critical Infrastructure Protection Month, http://www.whitehouse.gov/the-press-office/2010/11/30/presidential-proclamation-critical-infrastructure-protection-month (November 2010).

EMI *(Cont. from 6)*

(CGC 1) for Non-Federal Agencies to offer guidance. While the guidelines in the CGC 1 are similar to the FCD 1, this document focuses on State, local, tribal and local governments, as well as private-sector organizations.

The third objective pertains to the Continuity Program Management Cycle. This cycle entails a four-step process, including: planning; training; evaluating; and developing corrective action plans. The planning procedure includes tasks such as assigning a Continuity Program Manager; selecting the planning team; determining essential functions; and identifying resources required for continuity planning. The training task involves developing and conducting test, training, and exercises, or TT&E. The third task in the Continuity Program Management Cycle pertains to the evaluation, including after-action reports and lessons learned of TT&E. The last task in the cycle is to develop a Corrective Action Program (CAP), a tool used to identify requirements, assign responsibilities, and develop corrective actions as a way to resolve deficiencies and weaknesses in continuity plans. If an action is applicable, it is then incorporated into the continuity plan.

The fourth and final objective describes the elements of a viable continuity program. This portion of the course describes ten items and/or tasks that are fundamental to a practicable continuity plan. These elements are identified in the FCD 1. They include 1) essential functions; 2) orders of succession; 3) delegations of authority; 4) continuity facilities; 5) continuity communications; 6) vital records management; 7) human capital; 8) test, training, and exercise (TT&E); 9) devolution of control and direction; and 10) reconstitution operations.

FCD 1 and CGC 1 set in place four support functions to help ensure that the continuity managers and planners posses the necessary resources to form a viable continuity program. The first function, program plans and procedures, generally entails the development of a "pre-planning plan." The second function, risk management, in the context of COOP, pertains to identifying, weighing, controlling, and minimizing the impact of an all-hazards event. The third function, budgeting and acquisition of resources, is an important aspect of not only supporting infrastructure, but also supporting people. It is essential to secure funding for resources for appropriate use in a continuity plan. Finally, the fourth function relates to developing a family support plan. While this may not be an obvious task to ensure a viable continuity plan, this task is essential to allowing employees to continue to do their job during an all-hazards event. This plan recommends that employees work with their families to prepare for an evacuation. The plan is also intended to ease the mind of family members through the use of an emergency information line and personal and office "go kits." After all, the psyche of both employees and family members involved in an all-hazards event is extremely important. If employees are concerned for their family members, it will be difficult for them to function, thereby creating unintended and disastrous consequences.

This course is well organized in content and effectively delivers information. It presents helpful information on the definition of continuity of operations and its history with Federal initiatives. It also discusses the elements of a viable continuity plan. This course is just a sample of the many courses that EMI provides to the public and private sectors as well as the general public. In the wake of the tragedy in Japan, free, online courses such as these are valuable tools for the public and private sectors as well as the general public to ensure that life continues, even in the face of insurmountable destruction. ❖

For more information about this course, please visit the following website: http://training.fema.gov/EMIWeb/IS/IS546A.asp.

Legal Insights *(Cont. from 11)*

describe disability as a temporary condition that will result in an ultimate reversion of power back to the Governor,[10] few provide specific guidelines for determining the beginning and the end of that period. Disability and the procedures for determining it may be defined elsewhere in a State constitution or by statute, but there are also a few constitutions that treat it within the succession provision. While they may not be perfect, the following examples highlight some of the questions that may arise during a governor's disability, providing guidance for the procedural features that should be considered in any law on the subject.

Iowa's Constitution describes that a governor's ability to carry out the office may be questioned by either the person next in line of succession, or the Chief Justice of the State. A conference of the Chief Justice, the State Director of Mental Health, and the Dean of Medicine at the State University of Iowa is then held.[11] These three examine the Governor within ten days of their conference, and within seven days conduct a secret ballot and by unanimous vote may find that the Governor is temporarily unable to discharge the duties of the office.[12] In Kentucky, "[i]f the Governor, due to physical or mental incapacitation, is unable to discharge the duties of his office, the Attorney General may petition the Supreme Court to have the Governor declared disabled."[13] Before the Governor resumes his duties, the Chief Justice certifies to the Secretary of State that the disability has ceased. The Secretary of State enters the finding on the Journal of the Acts of the Governor.[14] Similarly, in Mississippi, "[s]hould a doubt arise as to whether a vacancy has occurred in the office of Governor or as to whether any one of the disabilities mentioned…exists or shall have ended, then the Secretary of State shall submit the question in doubt to the judges of the Supreme Court." A majority of the Supreme Court must investigate and determine whether or not a disability exists and deliver their opinion in writing to the Secretary of State. This opinion is to be considered "final and conclusive."[15]

Piecing Together

Governors have a pivotal role in our national security structure as a link between State governments and between State and Federal governments. The importance of establishing orders of succession of sufficient depth and definition for these executive positions outweighs the difficulty of constitutional amendment or political concern. While some diversity in succession planning is acceptable and even warranted, coming together to provide for sufficient depth and procedural specificity in gubernatorial succession laws nationwide will weave a stronger fabric of national preparedness. ❖

Robin Jessica Clark, J.D., Senior Law and Policy Analyst, University of Maryland Center for Health and Homeland Security. *I would like to thank Rahat Husain for his extensive research support on this topic.*

[10] Arizona, California, Colorado, Georgia, Hawaii, Idaho, Illinois, Michigan, Missouri, Nebraska, Nevada, New Hampshire, New Mexico, New York, North Dakota, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Texas, Utah, Vermont, Washington, West Virginia, Wisconsin, and Wyoming.

[11] Provided, if either the director or dean is not a physician duly licensed to practice medicine by this state the director or dean may assign a member of the director's or dean's staff so licensed to assist and advise the conference.

[12] Iowa Constitution, Chapter 7 Governor and Lieutenant Governor, 7.14 Disability of Governor to Act.

[13] Kentucky Constitution Section 84.

[14] Kentucky Constitution Section 84.

[15] Mississippi State Constitution, Article IV, Section 131.

Challenges *(Cont. from 5)*

requirements as they are contractually applied today, we find that there may be requirements, but they differ even within the same agency. The standards vary from COBIT (Control Objectives for Information and Related Technology) to ISO 27001 to no standard at all. Calling for different standards for preparedness will not provide the consistency required to affect an end-to-end recovery. Additionally, there is no proviso for ensuring that the vendor has indeed complied with the standard.

The challenge and opportunity are clear: all government agencies must insist on a consistent set of COOP planning standards for all vendors and ensure that the standard actually exists for all vendors. The solution may very well be that all agencies use the requirements in PL 110-53, Section 524, which is the Voluntary Private Sector Accreditation and Certification Preparedness Program passed into law and signed by President Bush in August 2007. The law allows DHS to designate recognized standards against which companies may certify. To certify against the standards, an organization must use a certifying body that has been trained by an accredited training organization and has demonstrated their knowledge by passing a structured examination. In essence, companies would be audited by trained and certified emergency/disaster and business continuity management professionals, all of whom would have been trained by similarly accredited institutions.

With this requirement in place, government vendors will be able to align their recovery responses to a consistent standard that will allow for a more manageable recovery response. This in turn will provide the foundation for Federal agencies to have a more dependable, predictable, and holistic response to an emergency situation.

PL 110-53 provides a means that will help deploy a better and more uniform response to emergency situations faced by the Federal government. The government should take advantage of this situation and create uniformity with the private sector entities that it is currently missing. ❖

Personal Resilience *(Cont. from 9)*

enough levels to be an empowered agent on behalf of the organization they represent. These steps toward resilience can help an organization move beyond surviving to thriving from inevitable turbulent events. As standards and litigation evolve, organizations stand not only to gain a competitive advantage by building resilience, but to meet requirements and to protect themselves from post-event lawsuits by demonstrating reasonable care has been taken to prepare the individuals who act on their behalf. ❖

Personal Recovery Concepts, LLC is a leader in the sector of people-continuity services for government, business and citizens. For more information, please visit www.personalrecoveryconcepts.com or call (866) 528-9186.

The Center for Infrastructure Protection works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link: http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1.