THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND
HOMELAND SECURITY

JANUARY 2014
RESILIENCE

VOLUME 12 NUMBER 7

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

Follow us on Twitter here
Like us on Facebook here

The CIP Report begins the year with another issue focusing on **Resilience**. Last month saw the U.S. Department of Homeland Security's (DHS) release of *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, and our authors discuss its potential impact, as well as other aspects of resilience implementation and measurement.

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

First, Bob Kolasky, Senior Advisor and Director of Strategy and Policy at the DHS Office of Infrastructure Protection, introduces NIPP 2013. Dr. Wayne Boone of Carleton University then explains functional resilience as an essential component of organizational resilience, and Jeff Gaynor, Founder of American Resilience Consulting, stresses the need to move towards resilience implementation and measurement. The Government Accountability Office's John F. Mortin next reports on DHS' Regional Resiliency Assessment Program, and Frederic Petit, Kelly Wallace, and Julia Phillips of Argonne National Laboratory present a bottom-up approach to characterizing critical infrastructure resilience. Finally, Ronald Bearse, CIP/HS Senior Fellow and President of Nauset National Security Group, and Ann Coss, Founder and President of Personal Recovery Concepts, follow up on their article in last month's edition, examining the return on investing in personal resilience.

We would like to take this opportunity to thank this month's contributors. 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

Partnering for Critical Infrastructure Security and Resilience

by Bob Kolasky, Senior Advisor and Director of Strategy and Policy,
Office of Infrastructure Protection, U.S. Department of Homeland Security

The President's National Infrastructure Advisory Council estimates that $1 billion or more is invested in infrastructure across the Nation daily. Much of this infrastructure that was once managed through physical controls now relies on information and communications technology to operate, and we have seen growing use of infrastructure beyond its design considerations, either because of age, lack of upkeep, or change in demographic patterns.

This changing environment can exacerbate the complex risks infrastructure faces from a variety of hazards, including climate change and extreme weather, aging and failing components, cyber threats, pandemics, and acts of terrorism. In an increasingly interconnected world of global supply chains, where critical infrastructure crosses national and state borders, the potential consequences of an incident are complicated by cross-system dependencies and interdependencies. While great progress has been made in securing these vital systems and assets, our national approach for ensuring infrastructure resilience must recognize the evolving environment in which infrastructure operates.

Policy Direction

In February 2013, President Obama issued Executive Order (EO) 13636 on Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) 21 on Critical Infrastructure Security and Resilience. These policies highlight the need to augment our existing focus on managing critical infrastructure risk through physical protective measures with additional emphasis on strengthening security and resilience across interrelated systems.

As stated in the National Preparedness Goal, a secure and resilient Nation maintains "the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk." In his article, "Beyond the Storms," Dane Egli notes that to achieve these policy aims there is a "need for more innovative thinking that goes beyond simply investing in more 'guns, gates, guards, and locks' in order to protect physical structures. We must identify the capabilities needed to mitigate the impact of, and respond to, *inevitable* hazards."[1]

The Plan

The critical infrastructure community includes a broad range of stakeholders that are motivated by different business drivers—some foster innovation and contribute to new capabilities via research and development, while others focus on implementing security measures and managing resources to ensure continuity of operations. The National Infrastructure Protection Plan (NIPP) guides efforts across these stakeholders to enhance the security and resilience of critical infrastructure across the country in conjunction with national preparedness policy. First released in 2006, and most recently updated in 2013, the NIPP was developed by infrastructure partners including private sector entities, state and local governments, Federal departments and agencies, non-governmental organizations, and academia.

The *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* is informed by the evolution of infrastructure risk, policy, and operating environments, as well as experience and lessons learned from exercises and real-world events, such as Super Storm Sandy and cyber incidents. The updated plan lays out an

(Continued on Page 3)

[1] Dane S. Egli, "Beyond the Storms: Strengthening Preparedness, Response, & Resilience in the 21st Century," *Journal of Strategic Security* 6, no. 2 (2013): 32-45, 39.

(Continued from Page 2)

enterprise approach to risk management that incorporates cyber and physical security and resilience measures. It builds on previous plans by emphasizing how security and resilience complement efforts to reduce critical infrastructure risk.

To achieve enhanced security and resilience solutions, the plan embraces a collaborative partnership based on comparative advantage and reinforces the importance of efficient information sharing. It calls on partners to pursue shared goals and priorities—and employ tools that facilitate actionable and relevant information sharing regarding emerging threats, vulnerabilities, and consequences—to move toward identified markers of success in the future.

Partnerships in Action

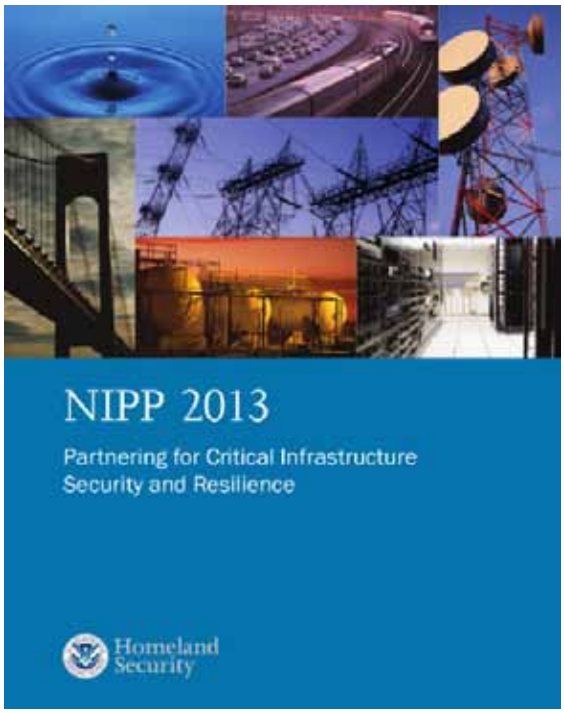
NIPP 2013: Partnering for Critical Infrastructure Security and Resilience validates the existing partnership framework, the value of which has been seen across various examples of collaboration within sectors, spanning regional entities, bridging corporate executive leadership, and across government agencies.

One example of sector-specific collaboration is within the financial services sector, which has employed actionable information sharing for more than a decade. The Financial Services Information Sharing Analysis Center (ISAC), in collaboration with the Department of Treasury and the Financial Services Sector Coordinating Council, works to enhance the ability of the financial services sector to prepare for and respond to cyber and physical threats and incidents. Because the Financial Services ISAC continuously gathers information from financial services providers; commercial security firms; government agencies; law enforcement; and other trusted resources, it is uniquely positioned to quickly disseminate threat alerts and other critical information to sector partners.

At the regional level, the All Hazards Consortium is a partnership across North Carolina, the District of Columbia, Maryland, Virginia, West Virginia, Delaware, Pennsylvania, New Jersey, and New York focused on homeland security, emergency management, and business continuity issues. The Consortium was founded in 2005 to help states collaborate and has evolved into a network of thousands of stakeholders. Working to facilitate regional planning and system integration between governments and the private sector infrastructure owners and operators, the Consortium has engaged with companies in the power, transportation, telecommunications, medical, food, water, banking and finance, information technology, commercial facilities, and chemical industries. During Super Storm Sandy, the Consortium quickly leveraged its partnership to collect information on infrastructure disruptions and operations to help government officials prioritize restoration efforts and encourage resource-sharing across industry.

Another partnership initiative focuses on bringing together private sector decision makers in the infrastructure community. Recognizing the criticality of certain energy sector functions, Chief Executive Officers (CEOs) across the electrical industry formed an executive-level Sector Coordinating Council (SCC), which is sponsored by the Secretaries of the Department of Energy and Department of Homeland Security, to work on risk management solutions. Through this partnership, electricity CEOs collaborate to utilize available technologies for securing cyber systems and test response plans addressing potential incidents.

Finally, coordination across government agencies following the recent attack at the Westgate Mall in Nairobi, Kenya has demonstrated the value of the partnership approach. The Federal Bureau of Investigation, State Department, and Department of Homeland Security joined together to analyze the tactics, techniques, and procedures utilized in the attack. Insights from this



(Continued on Page 4)

(Continued from Page 3)

analysis were used to share lessons learned and develop preparedness material in coordination with the nation's mall owners. While government agencies joined together to analyze the attack, the private sector played a central role by providing expertise on the types of information that would most readily allow malls to undertake augmented security measures to secure facilities against similar attacks in the future.

There is no single model for effective partnerships. Real world collaboration validates the NIPP's combined approach of encouraging standing bodies–such as SCCs, ISACs, and regional consortiums–to build trust networks and promote innovative partnership solutions to solve high-priority problems in an adaptable manner. However, there are certain attributes that make a partnership more likely to succeed. In 2013, DHS conducted an evaluation of public-private cooperative initiatives and identified a set of key attributes that are central to successful partnerships: defined purpose, clearly articulated goals, measurable progress, leadership involvement, clear and frequent communications, flexibility, and trust.

Seven Core Tenets

In addition to reaffirming the partnership approach, the NIPP 2013 articulates seven core tenets, which are intended to inform infrastructure planning efforts:

1. Risk should be managed in a coordinated and comprehensive way across the critical infrastructure community to enable the effective allocation of security and resilience resources.

2. Understanding and addressing risks resulting from cross-sector dependencies and interdependencies are essential to enhancing critical infrastructure security and resilience.

3. Gaining knowledge of infrastructure interdependencies, consequences, and risk requires information sharing across the critical infrastructure community.

4. The partnership approach to critical infrastructure security and resilience recognizes the unique perspective and comparative advantage of the diverse critical infrastructure community.

5. Regional and state, local, tribal and territorial partnerships are crucial to developing shared perspectives on gaps and actions to improve critical infrastructure security and resilience.

6. Infrastructure critical to the United States transcends national boundaries, requiring cross-border collaboration, mutual assistance, and other cooperative agreements.

7. Security and resilience should be considered during the design of systems, assets, and networks.

With the above tenets in mind, the *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* supports the prioritization of security and resilience strategies to ensure government and private sector resources are applied where they provide the most benefit. It focuses on a set of lifeline functions—communications, energy, transportation, and water management—and emphasizes that, while these strategies need to be executed across the national, regional, state, and local level, they must be cost-effective and demonstrate a clear return on investment to be sustainably incorporated into the market environment.

The Path Forward

To support efforts to enhance security and resilience, the updated NIPP includes a call to action identifying strategic direction for national efforts in the coming years. It calls on partners to build on existing efforts by developing joint priorities, engaging in collective actions, and leveraging incentives to progress toward a national focus on security and resilience. It likewise emphasizes the need for innovative risk management to enable informed decision making based on identified dependencies, interdependencies, and potential cascading effects. Finally, the plan focuses on the importance of measuring progress toward identified goals and adapting to emerging threats to ensure we are progressing toward desired outcomes.

The NIPP is not intended to provide a solution to every security gap that exists across the critical infrastructure community. Instead, it is a plan to bring together unique capabilities of the public and private sectors to find solutions to emerging risks and manage the consequences of incidents that occur. In doing so, it provides the connective tissue and clear priorities to bring together varied stakeholders in a collaborative approach to enhancing the security and resilience of our Nation's critical infrastructure. ❖

Functional Resilience: The "Business End" of Organizational Resilience

by Wayne Boone, CD* Ph.D., Masters Program in Infrastructure Protection and International Security (IPIS), Carleton University, Ottawa Ontario*

Introduction

Like any suite of Asset Protection and Security (AP&S) safeguards, those implemented within a resilience-related protection model must work in a deterministic, consistent, complementary, and trusted manner. Trust in individual safeguards is based on evidence that they are "tamper proof … always invoked … [and] small enough to be subject to analysis and tests [i.e., verified as working correctly], the completeness of which can be assured."[1] The trust earned in individual safeguards must be validated again when they are implemented in an integrated manner to achieve "defense in depth" and "interlocking arcs of defense." Once both of these are attained through implementation of physical and technical safeguards, a security perimeter may be said to have been established, which in turn provides a solid foundation for additional technical, procedural, and personnel safeguards. When all AP&S safeguards in a facility are functioning in harmony to support business or operational success, organizational resilience may be considered to have been achieved. As Leflar and Siegel make clear, "Organizational resilience is a multidisciplinary systems approach … [and] a collaborative process [among] [t]he risk stakeholders within the organization (security, business continuity … asset management, human resources, business leaders, etc.)."[2] Many pieces must work together to achieve organizational resilience, as described below.

Problems with Resilience in a Critical Infrastructure Environment

Critical infrastructures (CIs) represent the "worst case" of the protection challenge for risk stakeholders, since the consequences of an unacceptably long[3] interruption in the provision of services or commodities supported by a CI are even more pronounced than those for other enterprises. As examples, the assurance requirements of CIs to provide an assured flow of oil through a pipe across the country, timely electronic transactions in banking, on-time and in-place food supply chains, on-demand fresh water for domestic and commercial use, or on-time actions by first responders (fire, police, and medic personnel) elevate these activities to National Critical Infrastructure (NCI) status[4] since they contribute to "the assurance of the four national objectives of sovereignty, national security, economic prosperity, and the health and safety of [in our case] Canadians."[5] Resilient CIs are necessary to minimize disruptions to valued services.

The problem is four-fold: citizens have high expectations of assured provision of goods and services from NCIs; untimely interruptions to the flow of goods and services are likely to have strategic implications;

(Continued on Page 6)

[1] U.S. Department of Defense, *Trusted Computer System Evaluation Criteria*, DoD Directive 5200.28 (August 1983), 65. While somewhat dated and applied to the Trusted Computing Base (TCB) concept of a security kernel to protect sensitive electronic information, these concepts apply equally well in assessing the utility of AP&S safeguards implemented in critical infrastructures to achieve both robustness and resilience, as will be explained further.

[2] James J. Leflar and Marc H. Siegel, *Organizational Resilience; Managing the Risks of Disruptive Events; a Practitioner's Guide* (CRC Press, 2013), 13.

[3] This time period is determined though a business impact analysis and confirmed by authorized senior management under Business Continuity Planning methodology.

[4] Public Safety Canada, accessed December 30, 2013, http://www.publicsafety.gc.ca/index-eng.aspx.

[5] Wayne Boone, "Bridging the CIP Capability Gaps: An Interdisciplinary, Multi-Modal Model for Advanced Education," *Homeland Security Review* 5, no. 3 (Fall 2011): 298, http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=72084700&site=ehost-live.

(Continued from Page 5)

there are myriad natural, deliberate, accidental, or deterioration threats that can impact those NCIs, necessitating an all-hazards approach to protection;[6] and the protection posture necessary to achieve organizational resilience is complex, requiring collaboration among risk practitioners and integration of personnel, physical, technical, and procedural safeguards.

It is suggested that organizational resilience is best achieved through a systematic decomposition of its components based on discernible criteria. This breakdown isolates each of the components and facilitates identification of key attributes or characteristics. Risk stakeholders or AP&S practitioners will be able to apply appropriate safeguards to individual components and then, more importantly, integrate component protection postures into an enterprise-wide, resilient critical infrastructure protection (CIP) program that is gap-free. This bottom-up approach will best contribute to mission success of our NCIs.

Functional resilience is a key but often overlooked component of overall system or organizational resilience. Safeguards implemented within this component must be especially trusted and deterministic in order to contribute to organizational resilience, since even the best plans executed incorrectly will likely lead to mission failure. Functional resilience may be considered the "business end" of the protection program, where the AP&S practitioners "get things done."

What Constitutes Organizational Resilience and Where Does Functional Resilience Fit?

In their useful book *Critical Infrastructure System Security and Resiliency*, Biringer et al. devote over four pages to definitions of resilience, concluding that it is a "positive concept that systems would desire. All [definitions] include … withstanding change … many mention the system's ability to 'adapt' or 'absorb' the impact of that change or to 'recover' as a means of withstanding change … faster."[7] A resilient CI system or facility responds to change more easily, requiring fewer additional resources, and acting "essentially on its own" to return to *status quo ante* (or however closely this is possible in the short-, mid-, and longer-term).[8] Further insight is gained in both Hyslop, who describes resilience as the ability to recover from (or to resist being affected by) some shock, insult, or disturbance (essentially being able to 'bounce back' to an original form),[9] and Manyena, who uses the term "bounce forward," acknowledging that any disaster will permanently change the status quo.[10] In a NCI context, this could mean returning post-interruption to the quality and quantity of goods and services expected by citizens, within their expected time-frame. AP&S practitioners often argue whether organizational resilience is a process to be achieved, or is a resultant state achieved through the integrated implementation of safeguards. This author favors the latter and suggests that the several components of resilience identified below may comprise the process through which the resultant state is achieved.

Figure 1 (p. 8) depicts organizational resilience and identifies its four components. They are differentiated briefly as follows. Personal resilience could describe what stakeholders *are*. This could refer to the prescience and motivation of individuals to learn as much as possible regarding the threats to, and vulnerabilities of, the CI that they operate or protect, as well as an inner fortitude, tenacity, and adaptation[11] to "shake off an interruption" and get back to activities

(Continued on Page 7)

---

[6] E. Wayne Boone and Steven D. Hart, "Full Spectrum Resilience," *Homeland Security Review* 7, no. 1 (Winter 2013): 1-21, accessed January 14, 2014, http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=85821494&site=ehost-live.

[7] Betty Biringer, Drake E. Warren, and Eric D. Vugrin, *Critical Infrastructure System Security and Resiliency* (Hoboken: CRC Press, 2013), 83.

[8] Ibid.

[9] Maitland Hyslop, *Critical Information Infrastructures: Resilience and Protection* (New York: Springer, 2007).

[10] Siambabala Bernard Manyena, "The Concept of Resilience Revisited," *Disasters* 30, no. 4 (2006): 417, accessed January 14, 2014, http://resolver.scholarsportal.info/resolve/03613666/v30i0004/434_tcorr.

[11] E. Grafton, B. Gillespie, and S. Henderson, "Resilience: The Power Within," *Oncology Nursing Forum* 37, no. 6 (2010): 698. This excellent article applies to nurses and describes personal resilience as an "innate resource" (p. 698), especially for those in oncology.

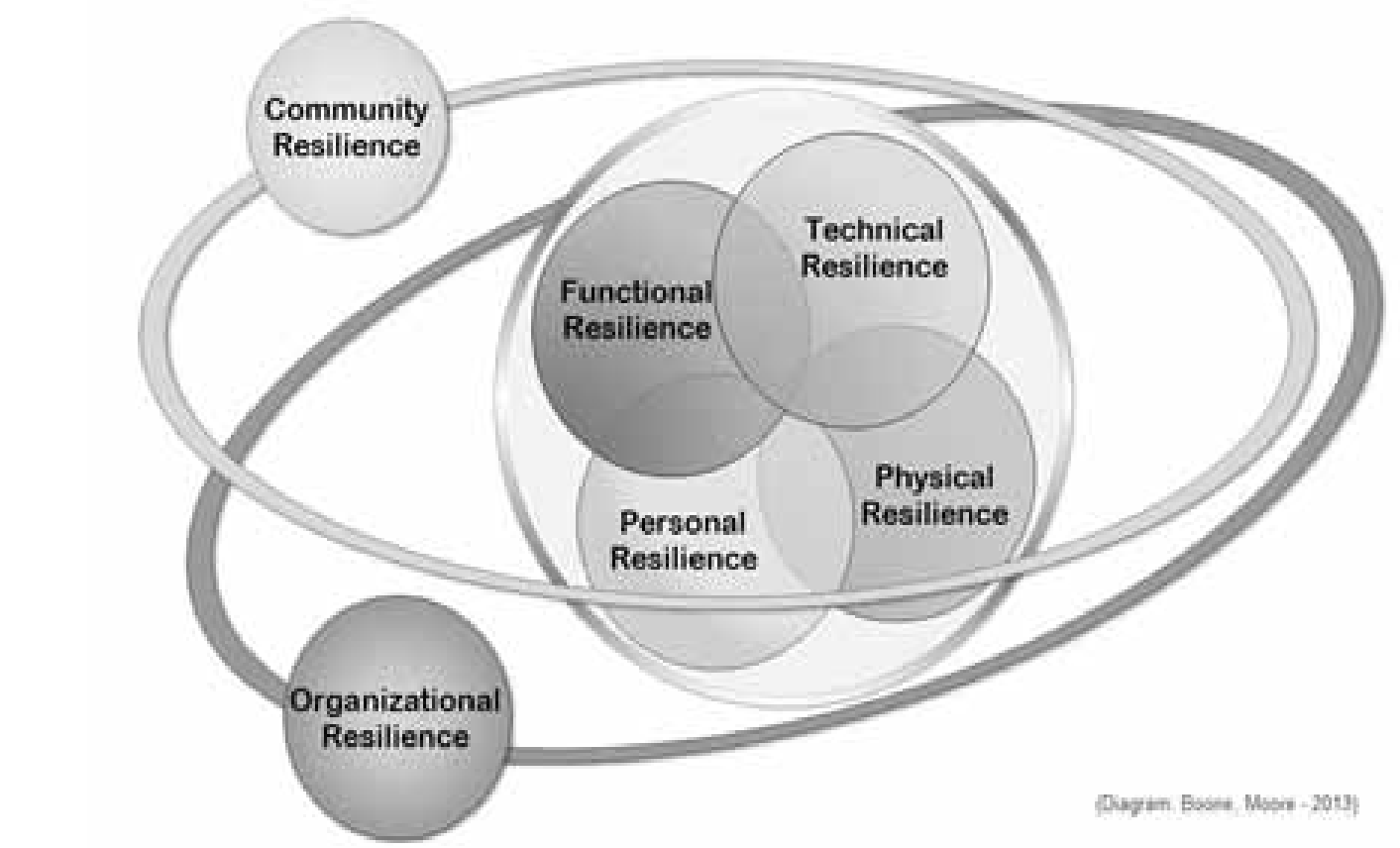


Figure 1: Resilience Component Model

(Continued from Page 6)

for which they are trained and equipped. Included is "the force that drives a person to grow through adversity and disruptions."[12] Physical and technical resilience could describe what the CI *has*, in terms of implemented tangible safeguards to deter or slow down an adversary (fences, locks, bars, etc.), detect an attack (guards, sensors, electronic access control systems, etc.), and/or mitigate vulnerabilities (shortcomings or weaknesses in the security posture). Functional resilience comprises what the stakeholders *do* to establish and maintain the necessary resilience or ability to "bounce back into the business." This can include the trusted, predictable, and consistent execution of operational AP&S plans in emergency response, evacuation, incident management, continuity of operations, disaster recovery, or investigations. Implicit in effective functional resilience are trusted and deterministic actions taken by adequate numbers of motivated, trained, skilled, educated, competent, and properly-equipped practitioners, all working collaboratively toward a common goal.

The "orbital nature" of Figure 1 reflects the dynamic and interactional nature of resilience processes. Both organizational resilience (i.e., the CIs) and community resilience (i.e., the municipal-level arrangements of citizens for protection and provision of minimal services) operate simultaneously; community resilience ensures that the required personnel, materials, and other resources are available, while organizational resilience ensures that the critical services that define a CI are provided. Within the central orbit, the spheres of resilience overlap to provide all-round defense (robustness) and the agility to respond effectively along the appropriate

(Continued on Page 8)

[12] Glenn E. Richardson, "The Metatheory of Resilience and Resiliency," *Journal of Clinical Psychology* 58, no. 3 (2002): 307, accessed January 14, 2014, http://resolver.scholarsportal.info/resolve/00219762/v58i0003/307_tmorar.

(Continued from Page 7)

attack vector.

What Part Does Functional Resilience Play in Achieving Organizational Resilience?

Figure 2 provides a temporal model for functional resilience. Consistent with the 80/20 rule of CIP, major activities in achieving functional robustness are conducted prior to a disaster or major interruption. Proactive efforts, such as establishing relationships among the resilience actors (the orbital spheres from Figure 1) to manage the resilience program and implementing physical, technical, and operational safeguards to achieve robustness, contribute to functional preparedness. Post-incident, those same relationships will provide the command and control, coordination, trust, and teamwork necessary to respond and thereby contain, isolate, and stabilize the impacts of that interruption. Such functional deployment will permit the organization to bounce back (or forward) and recover quickly to meet minimum service levels, as well as set the conditions for restoration of all services within the CI to *status quo ante* or *mutatis mutandis*. The act of *doing* that defines functional resilience exploits the personal, physical, and technical resilience spheres to achieve organizational resilience.

Conclusions

This short paper has provided a workable model to unpack organizational resilience into components that can be analyzed more readily and then reconstituted to provide the integrated, collaborative all-round defense-in-depth that befits a National Critical Infrastructure. Effective functional resilience integrates the other components and assures the continuous, correct, and appropriate implantation of safeguards. Functional resilience thus provides the "business end" in achieving agile organizational resilience to meet an adversary where and when required. ❖

**Since July 2009, Dr. Wayne Boone CD, CISSP, CPP, CBCP, CISM, PCIP has developed and taught in Carleton University's applied, interdisciplinary Master of Infrastructure Protection and International Security (MIPIS) program. Wayne brings to the classroom over 35 years of experience in providing reasoned advice, guidance and instruction to government, private industry and academia in corporate security, InfoSec, Business Continuity Planning and Critical Infrastructure Protection. He is a retired Canadian Forces Military Police Officer, having specialized in operational and information security. Dr. Boone consults regularly in Asset Protection and Security (AP&S), often utilizing his students in support of their professional development.*

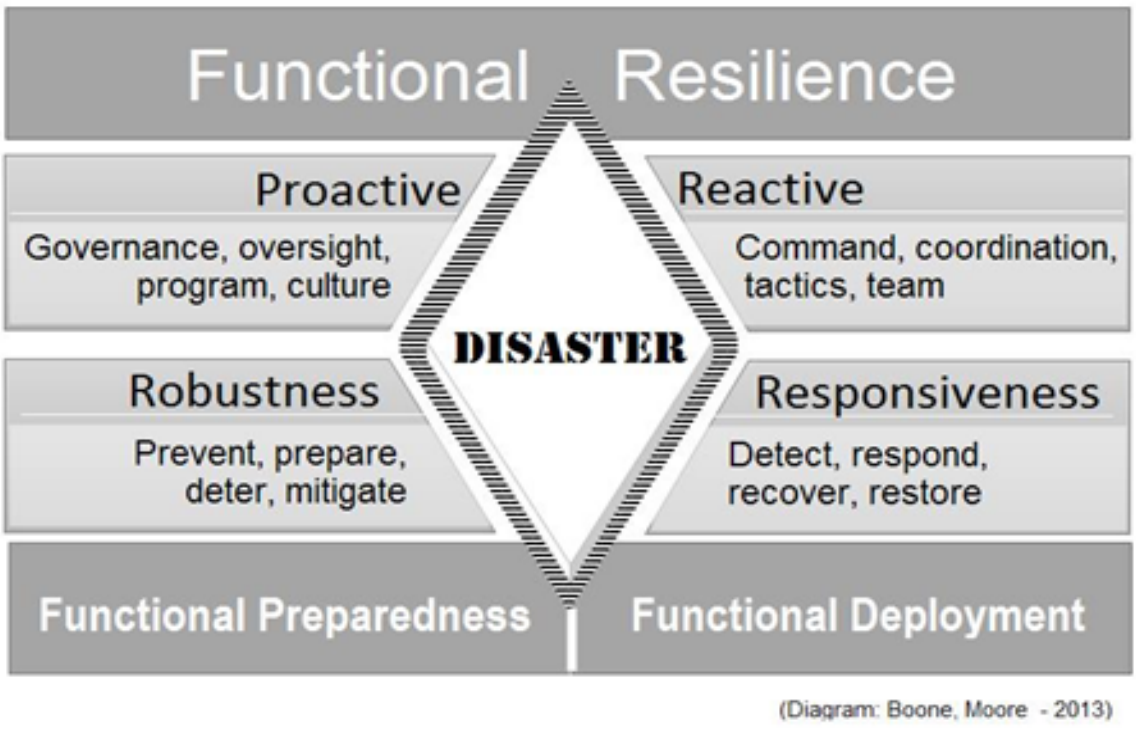


Figure 2: Temporal Characteristics of Functional Resilience

Quantifying and Implementing Critical Infrastructure Resilience (CIR): Building and Sustaining a Certifiably Resilient America

by Jeff Gaynor, Founder and Managing Member, American Resilience Consulting, LLC*

Conventional wisdom equates the resilience of American people with the resilience of the critical infrastructures essential to their safety, security, quality of life, and futures. While Americans have consistently proven themselves strong, adaptable, innovative, and resilient, America's critical infrastructures have not. The consequences of "all-hazards" events, combined with continuous, highly-successful attacks upon the Nation's interdependent and protected cyber and physical infrastructure(s) have made them America's Achilles Heel—and increasingly, single points of national failure.

As captured in headlines, when tested, America's protected critical infrastructure(s) prove themselves brittle, overstressed, and lacking in reserve components and capacities. America's intensifying Internet dependency has additionally made the Nation's critical infrastructure low risk and high payoff targets for a rapidly growing collection of dedicated and highly-sophisticated adversaries. Moreover, and quite inexplicably, America's infrastructures have become publicly accepted vectors for inflicting grave and lasting harm upon the Nation and all those residing within its borders. Without dramatic change in their operational resilience and preparedness the Nation's critical infrastructures will provide foreign and domestic predators the means to hold the Nation hostage to their aims without firing a kinetic shot.

Addressing these truths and synchronized with the drafting of the first National Infrastructure Protection Plan, in early 2005, the Homeland Security Advisory Council (HSAC) was directed to create a Critical Infrastructure Task Force (CITF). Its charge: review critical infrastructure protection (CIP) history, policies, and programs and propose immediately actionable advancements to them. On January 10, 2006, amidst the continuing horrific consequences resulting from the long-predicted failure of a single point of community failure, the New Orleans levee system, the HSAC publicly and formally recommended the Homeland Security Secretary raise the [infrastructure preparedness] bar and: "Promulgate Critical Infrastructure Resilience (CIR) as the top-level strategic objective—the desired outcome—to drive national policy and planning."[1] Eight years later and while the word resilience is increasingly seen and heard, critical infrastructure preparedness efforts remain almost exclusively focused on essential but clearly inadequate iterations of Cold-War CIP policies and programs.

Despite common misunderstanding, CIP does not provide the equivalent of police and fire protection. America's inextricably interdependent critical infrastructures make CIP to CIR what a frame is to an automobile—a foundation upon which to build. While essential to protecting largely static infrastructure sites, CIP cannot "protect" the as yet uncounted (and perhaps uncountable) number of infrastructure nodes and interdependencies required to ensure the ultimate objective of assuring the timely, nationwide delivery of critical infrastructure products and services. Despite the continuing lessons of history, a steady stream of ominous warnings of infrastructure-driven dangers, the very slow pace of CIR implementation has made America's critical infrastructures far more attractive, exploitable, and consequence-amplifying targets

(Continued on Page 10)

[1] Homeland Security Advisory Council, *Report of the Critical Infrastructure Task Force*, January 2006, accessed January 14, 2014, www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf.

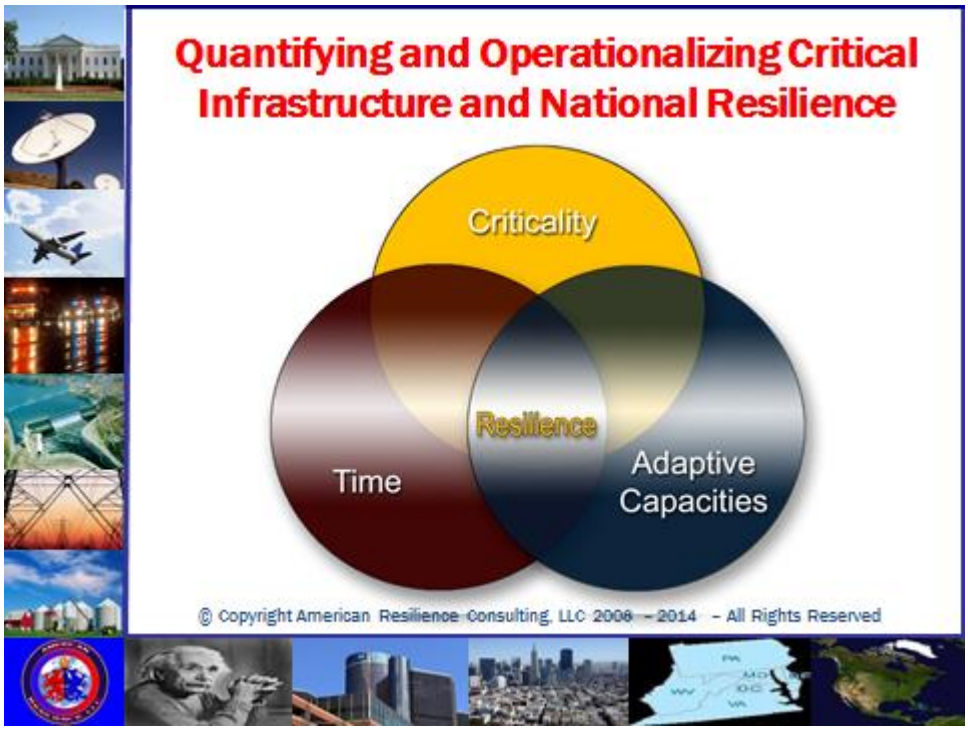
(Continued from Page 9)

than they were in January 2006.

In recognizing CIP as an enabler of CIR, PPD-21 and NIPP 2013 correct two fundamental flaws found in their predecessors. The new documents change from CIP to CIR "—the desired outcome—," and CIR provides an objective metric of infrastructure preparedness CIP/security cannot. No one can answer the question: How much CIP is required to protect/secure [keep from harm] critical infrastructures.

CIR has an objectively measurable, universally understood and accepted success metric—**time**, specifically the risk-based, consequence circumventing, continuity empowering **time** any entity is willing to be without infrastructure services. As a result of being collected from where all infrastructure services naturally merge—in American communities—performance-based, sector-spanning, individual, enterprise, community, and regional CIR requirements, coherently and comprehensively address the long-standing infrastructure interdependency issue. The collection of CIR requirements is not complicated. They empower all Americans to act in their best interests ultimately to the benefit of all. CIR requirements are captured and subsequently triaged and fulfilled and kept timely and accurate by any entity's response to three fundamental questions:

- What Critical Infrastructure services are essential?



- How long is any entity willing to be without them?

- What alternatives are available or must be created to provide essential infrastructure services within the time an entity is willing to be without them?

Leveraging the essentials of Occam's Razor[2]—complex problems with multiple solutions are best solved by the most simple of answers—below (p. 11) is a depiction of CIR requirements as they apply to critical infrastructure and the spectrum of national life.

As **time** applies to the resilience of "America's Nervous System," its increasingly compromised information infrastructure, CIR-driven technologies provide an advanced, preemptive, time-based dimension in cyber/information infrastructure preparedness—Cyber Indications and Warning (CI&W). Private sector-developed, operationally tested, and proven and patented CI&W technologies that are fully compatible with all existing network defense systems, and prior to reaching any network's Internet Point of Presence, instantaneously detect, neutralize, record, and, without endangering privacy, report all forms of anomalous activity and malware occurring simultaneously on all 56,535 Microsoft Operating System Ports, have been presented to appropriate private sector organizations and Federal agencies.

(Continued on Page 11)

[2] Josh Clark, "How Occam's Razor Works." *How Stuff Works*, accessed January 14, 2014, http://science.howstuffworks.com/innovation/scientific-experiments/occams-razor.htm.
[3] Homeland Security Advisory Council, *Community Resilience Task Force Recommendations*, June 2011, accessed January 14, 2014 http://www.dhs.gov/xlibrary/assets/hsac-community-resilience-task-force-recommendations-072011.pdf.

(Continued from Page 10)

The methodology to capture community-based infrastructure performance requirements and coherently build, achieve, and sustain CIR is captured in the HSAC's Community Resilience Task Force Recommendations.[3] A graphic depiction leveraging the Venn diagram above illustrates execution of the Main Street to Pennsylvania Avenue "American Resilience Assessment." In summary, CIR is the most fundamental of Homeland and National Security imperatives. Its continuing absence makes individual, enterprise, community, regional, and national resilience impossible to achieve. Despite this and repeated lessons of history, CIR advancement from recommendation to reality has been a long and unnecessarily consequence-filled road. The continuing decay and increasing exploitability of America's critical infrastructures and the Nation's preparedness trajectory is intolerable and yet correctable. CIR is not "a threat" to CIP. It is natural, straightforward, pragmatic, proven in the most stressful of environments, and at worst (given the guaranteed consequences of continued failure to implement it), cost neutral. America has the experience and means to both leverage CIP and realize an advanced state of national preparedness through implementation of CIR mindsets, metrics, methodologies, and technologies. The goal of resilience established by PPD-21 and NIPP 2013 can and should be immediately translated into action by new Homeland Security Secretary Jeh Johnson, transforming CIR to reality by fast-tracking comprehensive implementation of it as the foundation and success metric of American preparedness.

It's long-past time America advance national preparedness to the prevention and continuity side of the event curve. It shouldn't require another otherwise avoidable infrastructure-enabled and amplified disaster to do so. While time is no longer on America's side, the right time to do the right thing—continuously question the critical infrastructure status quo; empower people, enterprises, and communities; and institutionalize continu-

(Continued on Page 12)

(Continued from Page 12)

ous innovation and improvement in the operational preparedness and resilience of America's critical infrastructures and by extension, the Nation's safety, security, quality of life, and future—has always been and remains now. ❖

**Jeff Gaynor is a nationally recognized resilience advocate, innovator, and practitioner having better than four decades of national and homeland security experience. Jeff directed the Homeland Security Advisory Council's (HSAC's) Critical Infrastructure Task Force and was a principal contributor to its Community Resilience Task Force. Jeff is a member of InfraGard–the FBI's public-private infrastructure preparedness partnership–and is a retired U.S. Army Colonel and Defense Intelligence Senior Executive who directed DoD Year 2000 (Y2K) Operations, and served as the Communications Security Officer and as an Alternate Military Aide to Presidents Ronald Reagan and George H. W. Bush.*

GAO Report Calls for the Department of Homeland Security (DHS) to Strengthen the Management of its Regional Resiliency Assessment Program

by John F. Mortin
U.S. Government Accountability Office, Washington, D.C.*

The Department of Homeland Security's (DHS) 2009 update to the National Infrastructure Protection Plan (NIPP)[1] and recent White House policy initiatives[2] highlight the government's increased emphasis on critical infrastructure resilience, which according to DHS is the ability to adapt to changing conditions, and prepare for, withstand, and rapidly recover from disruptions.[3] The extensive damage and long recovery required from natural disasters like Superstorm Sandy demonstrates the importance of infrastructure resilience. The storm caused widespread damage to infrastructure across multiple states and affected millions of people. Damage included flooding that affected major transportation systems and caused widespread and prolonged power outages.

Over the past several years, the U.S. Government Accountability Office (GAO) has completed various studies of DHS's efforts to incorporate the concept of resilience into its critical infrastructure (CI) policies, procedures, and practices.[4] In July 2013, GAO completed a study that examined DHS efforts to develop and implement Regional Resiliency Assessment Program (RRAP) projects, which are to analyze a region's ability to adapt to changing conditions, and prepare for, withstand, and rapidly recover from disruptions.[5] GAO's study assessed DHS efforts to work with states to select and conduct RRAP projects, as well as measure project results and share them with CI partners. GAO reported that DHS has taken important actions to enhance the management of the RRAP, but further actions would enhance these efforts.

DHS's Regional Resiliency Assessment Program

DHS's National Protection and Programs Directorate's (NPPD), Office of Infrastructure Protection

(Continued on Page 14)

[1] DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resilience* (Washington, D.C.: January 2009), accessed January 6, 2014, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf. The NIPP provides the overarching approach for integrating the Nation's CI protection and resilience activities into a single national effort. DHS has overall responsibility for leading and coordinating the Nation's efforts to protect CI.

[2] On February 12, 2013, President Obama signed Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience. Barack Obama, *Presidential Policy Directive/PPD-21* (Washington, D.C.: February 2013), accessed January 6, 2014, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. PPD-21 advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

[3] DHS, Risk Steering Committee, *DHS, Risk Lexicon* (Washington, D.C.: September 2010), accessed January 6, 2014, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf. DHS developed the risk lexicon to provide a common set of official terms and definitions to ease and improve the communication of risk-related issues for DHS and its partners.

[4] GAO, *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*, GAO-10-296 (Washington, D.C.: March 2010), assessing DHS efforts to incorporate the concept of resilience into the NIPP, accessed January 6, 2014, http://www.gao.gov/assets/310/301494.pdf; GAO, *Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened*, GAO-10-772 (Washington, D.C.: September 2010) examining DHS efforts to build resilience into its critical infrastructure programs and assessment tools, accessed January 6, 2014, http://www.gao.gov/new.items/d10772.pdf; GAO, *Critical Infrastructure Protection: An Implementation Strategy Could Advance DHS's Coordination of Resilience Efforts across Ports and Other Infrastructure,* GAO-13-11 (Washington, D.C.: October 2012), focusing on DHS efforts to develop a resilience implementation strategy, accessed January 4, 2014, http://www.gao.gov/assets/650/649705.pdf.

[5] GAO, *Critical Infrastructure Protection: DHS Could Strengthen the Management of the Regional Resiliency Assessment Program*, GAO-13-616 (Washington, D.C.: July 2013), accessed January 6, 2014, http://www.gao.gov/assets/660/656344.pdf.

(Continued from Page 13)

(IP) developed the Regional Resiliency Assessment Program (RRAP) in 2009 to assess vulnerability and risks associated with dependent and interdependent infrastructure clusters and systems in specific geographic areas or regions.[6] RRAP projects—collaborative projects that rely on the voluntary participation of various stakeholders, including states and asset owners and operators—identify situations where failures at facilities or sectors would lead to failures at other facilities or sectors. They are intended to identify characteristics that make the assets and the region resilient and any gaps that could promote or foster disruptions. From Fiscal Year 2009 through Fiscal Year 2012, DHS conducted 27 RRAP projects in various locations throughout the country. These projects included one covering the financial district in Chicago; three covering commercial facilities in Minneapolis, Atlanta, and Las Vegas; and one covering energy production facilities managed by the Tennessee Valley Authority.

According to DHS, the process for conducting a RRAP project can take from 18 to 24 months from start to finish. The process includes selecting and scoping projects from proposals; assembling and preparing teams of Federal, state, and local stakeholders; meetings with asset owners and operators; analyzing vulnerability and security assessments at facilities; preparing a draft report for state review; and establishing a process to follow-up on progress making RRAP-related enhancements. The final RRAP report typically describes vulnerabilities in the sectors and regions under study, a hazard or risk analysis, and an analysis of dependencies and interdependencies. The final report also includes options or suggestions to address key findings and a list of organizations or possible funding sources to provide support in making enhancements.

Documenting Final RRAP Project Selections

GAO reported that DHS had developed criteria that consider various factors—such as the willingness of asset owners and operators to participate and the region's concentration of high-risk assets—when identifying possible locations for RRAP projects. DHS used these criteria to develop a list of project candidates and officials used this list to make final project selections, but did not document why some projects were selected over others. DHS officials stated that projects that appeared equally feasible were not selected for various reasons, including the availability of DHS personnel to conduct the RRAP and resource constraints facing stakeholders.

GAO reported that documenting the rationale for making project selections would provide (1) DHS managers and others responsible for program oversight valuable insights into why one project was selected over another, particularly among proposals that appear equally feasible and worthy and (2) a basis for defending its selections or responding to queries about them, particularly given the desirability of the program among states and budgetary constraints facing states and other stakeholders. Knowing why a RRAP proposal was not selected might provide stakeholders information they need to make decisions about dedicating additional resources to refining future proposals, or adjust the scope of their involvement in future RRAPs based on anticipated budgetary increases or decreases.

GAO recommended that DHS document decisions made with regard to individual projects. DHS concurred and stated that it would develop a mechanism to more comprehensively document the decision-making process and justifications that lead to the selection of each project.

Working with States to Improve RRAPs and Sharing RRAP Reports

GAO reported that DHS has worked with states to improve the process for conducting RRAP projects and is considering an approach for sharing resilience information with its CI partners, including Federal, state, local, and tribal officials. Since 2011, DHS has worked with states to improve the process for conducting RRAP projects, including more clearly defining the scope of projects. DHS officials stated that actions taken include setting expectations early on to inform stakeholders when particular RRAP

(Continued on Page 15)

[6] DHS works with certain Federal Agencies—known as Sector Specific Agencies—that represent 16 industry Sectors, such as Commercial Facilities, Communications, Energy, and Transportation.

(Continued from Page 14)

events are scheduled to occur and group discussions among the various stakeholders participating in the RRAP. According to DHS officials, these efforts have been viewed favorably by states.

GAO also reported that DHS is considering an approach to more widely share resilience lessons learned with its CI partners, including a possible resiliency product or products that draw from completed RRAP projects. DHS officials stated that they engage CI partners in meetings and conferences where partners' resilience information needs are discussed and have been incorporating this input into their efforts to develop a resilience information sharing approach. DHS officials cautioned that a planned resilience product was in its conceptual stages and had not yet been funded. However, DHS officials said that they envision that a resilience product would leverage RRAP data, findings from DHS security assessments, and open source information to communicate collective results, lessons learned, and best practices that can broadly contribute to efforts to strengthen the resilience of critical infrastructure.

Measuring Results Associated with RRAP Projects

GAO reported that DHS has taken action to measure efforts to enhance security and resilience among facilities that participate in the RRAP, but faces challenges measuring results associated with RRAP projects. DHS performs security and vulnerability assessments at individual CI assets that participate in RRAPs projects as well as those that do not participate. DHS also performs follow-ups among asset owners and operators that participate in these assessments with the intent of measuring their efforts to make enhancements arising out of these surveys and assessments. However, DHS does not measure how enhancements made to individual assets that participate in a RRAP project contribute to the overall results of the project. DHS officials stated that they face challenges measuring performance within and across RRAP projects because of the unique characteristics of each, including geographic diversity and differences among assets within projects.

GAO reported that it recognized that measuring performance within and among RRAP projects could be challenging, but stated that DHS could better position itself to gain insights into projects' effects if it developed a mechanism to compare facilities that have participated in a RRAP project with those that have not, thus establishing building blocks for measuring its efforts to conduct RRAP projects. One approach could entail using DHS's assessment follow-up process to assess whether participation in a RRAP project influenced owners and operators to make related resilience enhancements.

GAO recommended that DHS develop a mechanism to assess the extent to which individual projects influenced participants to make RRAP related enhancements. DHS concurred and stated it would review alternatives, including the one discussed by GAO, and would provide additional details on how it will address this recommendation in the near future.

Conclusions

GAO concluded that DHS has taken important actions to standardize the selection process for RRAP project locations by developing criteria for selecting projects. It has also worked with state stakeholders to better communicate the scope of projects, consider how it can share resilience information with CI partners, and gather information on CI partner actions to enhance resilience after the RRAP project is completed. However, further actions could strengthen these endeavors.

First, with regard to selecting RRAP locations, GAO concluded that documenting why specific recommendations were or were not made would help ensure accountability, enabling DHS to provide evidence of its decision-making. This would not only provide insights into why decisions were made and enable DHS to defend its selections among competing projects. Recording why decisions are made is particularly important if senior managers or staff move to other positions and new managers and staff are responsible for understanding the basis for their decisions.

Second, GAO concluded that DHS faces challenges developing performance measures to gauge results among and across RRAP projects, but could benefit from assessing

(Continued on Page 16)

(Continued from Page 15)

how participation in an RRAP project may or may not influence change. Doing so would enable DHS to compare the extent to which facilities that participate in a RRAP project made enhancements with those facilities that do not. This comparison could serve as a building block for measuring DHS's efforts to conduct RRAP projects thereby providing measures to establish accountability, document actual performance, and promote effective management. It would also provide key insights about how RRAP findings may have affected facility resilience. ❖

**John F. Mortin, is an Assistant Director responsible for Critical Infrastructure Protection Issues with the Homeland Security and Justice Team at the U.S. Government Accountability Office. He can be reached at mortinj@gao.gov.* *For more information on the GAO report cited, please see GAO,* Critical Infrastructure Protection: DHS Could Strengthen the Management of the Regional Resiliency Assessment Program, *GAO-13-616 (Washington, D.C.: July 2013) at www.gao.gov/cgi-bin/getrpt?GAO-13-616.*

An Approach to Critical Infrastructure Resilience

by Frederic Petit, Kelly Wallace, and Julia Phillips
Infrastructure Assurance Center, Decision and Information Sciences Division,
Argonne National Laboratory*

Introduction

In proclaiming November Critical Infrastructure Security and Resilience Month, President Obama addressed the need to work together to further enhance the security and resilience of critical infrastructure and reiterated that it is one of his top priorities.[1]

The need for a consolidated approach, based on core capabilities, for the protection and resilience of critical infrastructure is already the main purpose behind two Presidential Policy Directives, National Preparedness (PPD-8) and Critical Infrastructure Security and Resilience (PPD-21). In 2011, PPD-8 underscored national preparedness for strengthening the security and resilience of the Nation.[2] A strategic imperative outlined in PPD-21 is the implementation of an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.[3] In parallel to these two directives, Executive Order 13636, Improving Critical Infrastructure Cybersecurity, issued in February 2013, reinforces the need to "enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."[4]

A resilience assessment methodology for critical infrastructure must therefore be comprehensive enough to apply to all types of critical infrastructure, consider all kinds of threats, and integrate physical and cyber components.

Critical Infrastructure Resilience

Enhancing the resilience of critical infrastructure requires determining the ability of an entity—such as an asset, organization, community, or region—to anticipate, resist, absorb, respond to, adapt to, and recover from a disturbance.[5] Thus, a resilience assessment methodology requires consideration of all of the components of resilience that apply to a critical infrastructure system. In addition, accounting for the dependencies and interdependencies among critical infrastructure becomes a necessary and crucial component of system resilience.

It is possible to assess the resilience of a critical infrastructure system by using a top-down or a bottom-up approach.[6] A top-down approach consists of characterizing a system

(Continued on Page 18)

---

[1] Barack Obama, *Presidential Proclamation – Critical Infrastructure Security and Resilience Month,* The White House, Office of the Press Secretary, Octber 31, 2013, accessed December 9, 2013, http://www.whitehouse.gov/the-press-office/2013/10/31/presidential-proclamation-critical-infrastructure-security-and-resilienc.

[2] Barack Obama, *Presidential Policy Directive/PPD-8, Subject: National Preparedness,* The White House, March 30, 2011, accessed December 9, 2013, http://www.dhs.gov/xlibrary/assets/presidential-policy-directive-8-national-preparedness.pdf.

[3] Barack Obama, *Presidential Policy Directive/PPD-21, Subject: Critical Infrastructure Security and Resilience*, February 12, 2013, Office of the Press Secretary, accessed Dec. 9, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[4] Barack Obama, *Executive Order 13636 – Improving Critical Infrastructure Cybersecurity*, in Part III (Title 3), The President, Presidential Documents, of the Federal Register, Vol. 78, No. 33 (2013), pp. 11739–1174.

[5] L. Carlson, et al., *Resilience Theory and Applications*, ANL/DIS-12-1 (Argonne National Laboratory, Argonne, Ill.: January 2012), accessed December 9, 2013, http://www.ipd.anl.gov/anlpubs/2012/02/72218.pdf.

[6] D. Verner and F. Petit, "Resilience Assessment Tools for Critical Infrastructure Systems," *The CIP Report, Resilience*, Vol. 12, No. 6 (CIP/HS, George Mason University: December 2013).

(Continued from Page 17)

at a large scale (e.g., global or national level), then identifying and characterizing all its components. A bottom-up approach identifies and characterizes the individual base elements of the system and then combines these elements into larger-scale systems. These two approaches are complementary and must be combined to assess the resilience of critical infrastructure and ultimately regional resilience.

The U.S. Department of Homeland Security's (DHS's) Protective Security Coordination Division, in collaboration with Argonne National Laboratory's Infrastructure Assurance Center, has developed a bottom-up approach for characterizing the resilience of critical infrastructure. Information is collected at the facility level, using a question-and-answer web-based format called the Infrastructure Survey Tool (IST); the resulting data are then used to characterize the level of resilience at a given facility by calculating a Resilience Measurement Index (RMI). The IST also collects information on facility dependencies (e.g., electric power or water) that can be used to generate facility dependency curves. These curves can provide insight to emergency preparedness agencies, DHS, and critical infrastructure owners and operators on the impacts that could result from the loss of given resources (e.g., electric power, water, communications).

Resilience Measurement Index

The RMI is calculated based on answers collected via the IST. The IST question set was based on business continuity and resilience standards (British Standards Institute [BSI] Standard BS 25999, *Standard on Business Continuity*,[7] National Fire Protection Association [NFPA] Standard 1600, *Standard on Disaster/Emergency Management and Business Continuity Programs*,[8] American National Standards Institute/ASIS International [ANSI/ASIS] Standard SPC.1-009, *Standard on Organizational Resilience*,[9] and International Organization for Standardization [ISO] Standard ISO 22301:2012, *Societal Security – Business Continuity Management Systems – Requirements*[10]).

The RMI is organized into four major resilience-related components: preparedness, mitigation measures, response capabilities, and recovery mechanisms. It uses the principles of decision analysis and multi-attribute utility theory to define an indicator of resilience ranging from 0 (low resilience) to 100 (high resilience).[11] When all else remains equal, the RMI will increase as additional resilience measures (e.g., planning or dependency backups) are implemented by a facility.

The data on resilience collected at a facility are presented in an interactive, web-based tool called the IST RMI Dashboard (Figure 1). The Dashboard is configured to allow facility owners to examine their specific resilience posture in comparison to the postures of similar facilities. The Dashboard is an interactive tool that allows users to create scenarios based on different answers to the IST questions related to resilience and then compare a scenario's RMI value to their facility's existing RMI value to see if resilience has improved as a result of implementing different resilience measures (e.g., backup generator fuel supply versus improved resilience plans) and to see by how much it has improved. The Dashboard displays (as Facility: Scenario in light blue) the impact of resilience component modifications on the RMI values overall and displays each individual component of resilience compared to the original RMI (Facility: Existing in dark blue) and to the nationwide average RMI (Sector average in gray) for similar facilities.

(Continued on Page 19)

---

[7] BSI, 2010, *BS 25999 Business Continuity*, 2010, accessed December 9, 2013, http://www.bsiamerica.com/en-us/Assessment-and-Certification-Services/Management-systems/Standards-and-Schemes/BS-25999/.

[8] NFPA, *NFPA 1600 – Standard on Disaster/Emergency Management and Business Continuity Programs*—2010 Edition, Quincy, Mass., accessed December 9, 2013, http://www.nfpa.org/assets/files/pdf/nfpa16002010.pdf.

[9] ASIS, *The Organizational Resilience Standard [ASIS SPC.1-2009]*, 2009, accessed December 9, 2013, http://organizational-resilience.com/OrganizationalResilienceStandard.htm.

[10] ISO, *ISO 22301:2012 – Societal Security – Business Continuity Management Systems – Requirements*, 2012, accessed December 9, 2013, http://www.iso.org/iso/catalogue_detail?csnumber=50038.

[11] F. D. Petit, et al., *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*, ANL/DIS-13-01 (Argonne National Laboratory, Argonne, Ill.: 2013), accessed December 9, 2013, http://www.ipd.anl.gov/anlpubs/2013/07/76797.pdf.

(Continued from Page 18)

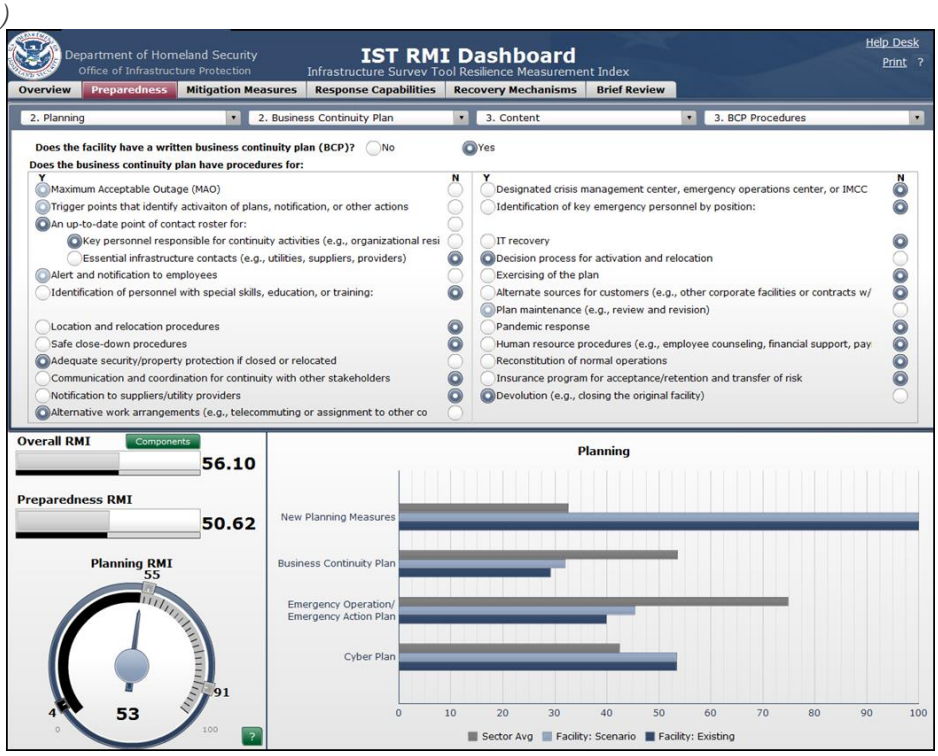


Figure 1 – Illustrative Example of RMI Dashboard

The IST RMI Dashboard allows critical infrastructure owners and operators to utilize information collected during a facility visit and develop alternative scenarios for day-to-day operations that can support investment decision making and strategic planning.

Dependency Curves

Dependencies are a fundamental consideration when assessing the resilience of critical infrastructure assets and, ultimately, the resilience of a region. Dependencies are the linkages between two critical infrastructure assets, through which the state of one infrastructure influences or is influenced by the state of the other (e.g., the resilience of a transportation control center is influenced by the resilience of its electric power provider). It is important to thoroughly characterize the amount of dependency between infrastructure systems when seeking to assess the extent to which the resilience of a facility is directly affected by the missions, functions, and operations of other critical infrastructure assets.

The facility-specific dependency information collected by using the IST is incorporated within the RMI and also allows for the creation of dependency curves, which represent the impact of the loss of a given resource over time (Figure 2). Specifically, information is collected on dependency redundancy and backups, on the impact of the loss of the dependency with and without backups, and on the time needed to restore the facility back to full operations, as displayed in Figure 2.

(Continued on Page 20)

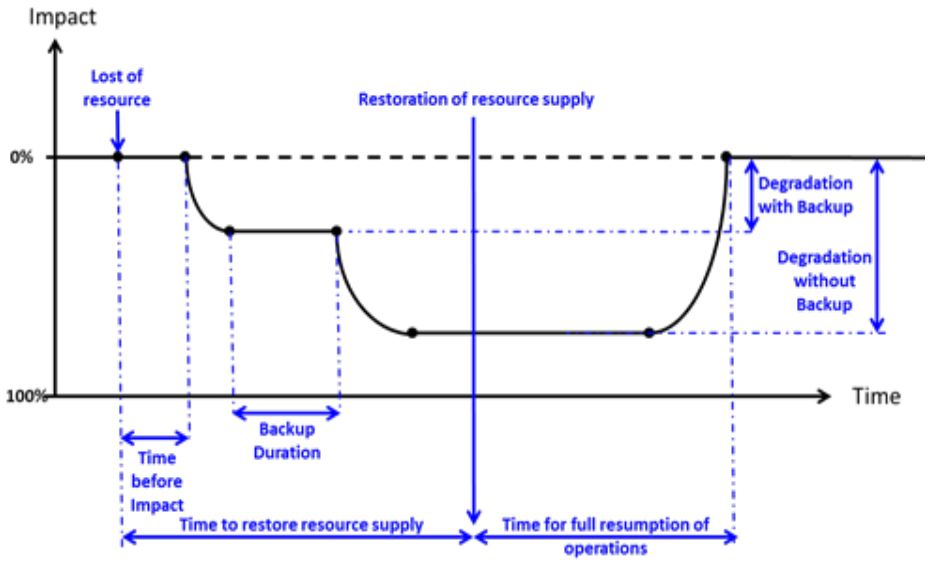


Figure 2 –Dependency Curve Components

(Continued from Page 19)

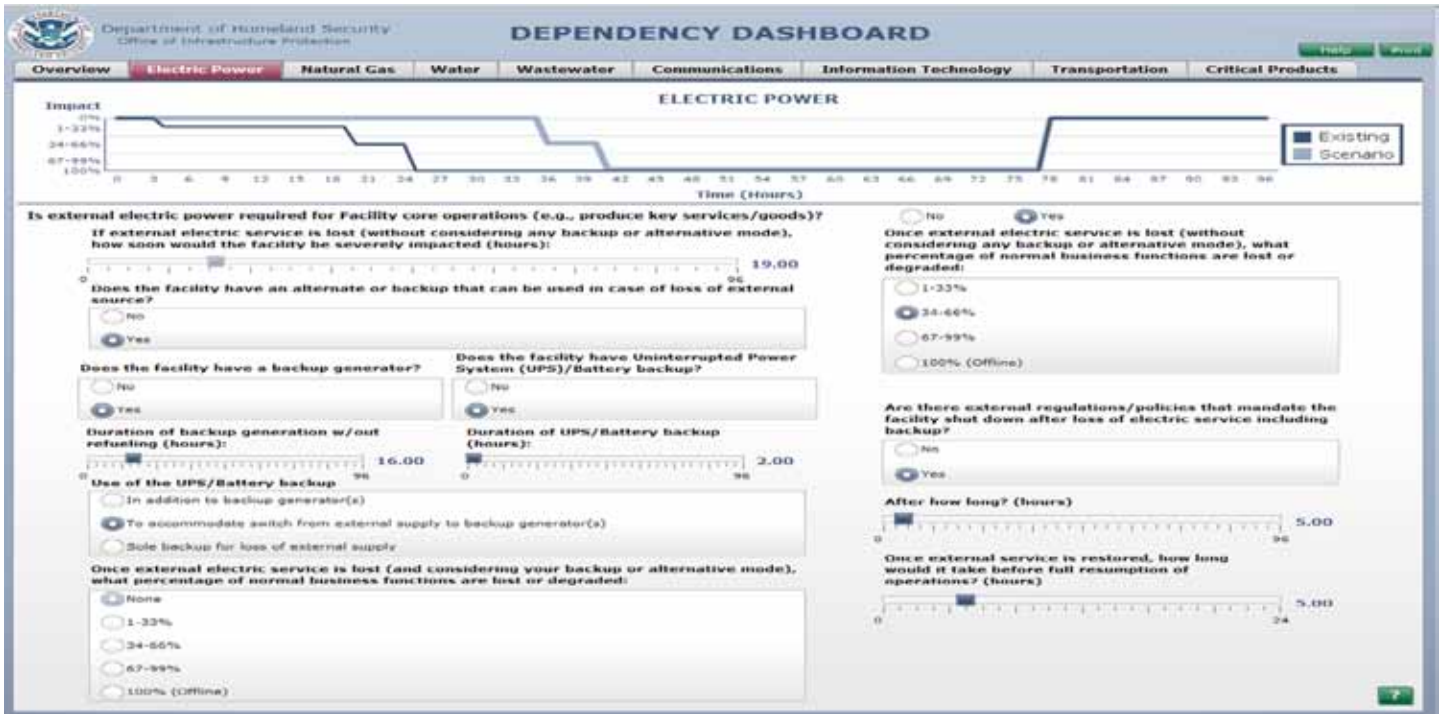


Figure 3 – Illustrative Example of Dependency Dashboard

Similar to the RMI, the dependency information can be displayed in an interactive Dashboard that allows the user to test different dependency mitigation scenarios (e.g., changing the duration of backup generation by increasing the number of hours that fuel is available) and to observe the effect on the degradation of the facility's core operations over time. Figure 3 is an example of the Dependency Dashboard for electric power.

The facility RMI and dependency curves can then be used to define the resilience of connected infrastructures. The RMI defines the resilience of critical infrastructure assets (the nodes of the system), and dependency curves characterize the connections between critical infrastructure assets (links between the nodes). Ultimately, as more critical infrastructure information is collected, it can be used to more completely characterize cascading and escalating failures among critical infrastructure assets and systems.

Conclusion

The RMI and dependency curves have been in use since January 2013, and more than 1,000 sites have been assessed with these tools. They are currently used in several DHS programs (e.g., Enhanced Critical Infrastructure Protection, Site Assistance Visit, and Regional Resiliency Assessment Programs). The RMI and dependency curves comprise possible first steps of developing a bottom-up approach for characterizing the resilience of a system of critical infrastructure assets. This approach can be combined with top-down approaches that characterize global interactions among several subsystems (e.g., critical infrastructure, population, economy, and government) in order to characterize the resilience of a region. ❖

Acknowledgment

The submitted manuscript has been created by UChicago Argonne, LLC, Operator of Argonne National Laboratory ("Argonne"). Argonne, a U.S. Department of Energy Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. The U.S. Government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government. The development of the tools presented in this paper has been funded by the U.S. Department of Homeland Security Protective Security Coordination Division under Contract No HSHXDC-13-X-00223.

The Return on Investing in Personal Resilience

by Ronald Bearse, CIP/HS Senior Fellow and President of Nauset National Security Group, LLC
and Ann Coss, Founder and President of Personal Recovery Concepts, LLC*

In last month's edition of *The CIP Report*, we wrote about personal resilience being the foundation of national resilience and we discussed the consequences of the following facts:

- Most Americans are not prepared for a disaster or an emergency.

- Less than 10% of Americans have documented or safely stored personal, financial, emergency, household, medical, and legal information.

- Everyday workforce disruptions are costing our nation tens of billions of dollars due to the lack of personal preparedness for events such as home fires, identity theft eldercare, childcare, unexpected death, and personal emergencies.

- A sizeable percentage of businesses with emergency preparedness and business continuity plans have not adequately accounted for human resiliency.

- There is a link between personal and family preparedness and organizational readiness and resilience, and it is vital to building a national culture of resilience.

We also mentioned the need for government and industry to invest in helping individuals see themselves as capable, connected, adaptable, and self-sufficient, rather than dependent, victimized, or helpless. This will affect their decisions, actions, and ability to cope in the face of disaster, emergency, or crisis. We also stated that the collective return on the investment made in this regard can be enormous for our country. Let's take a further look at the return on investing in personal resilience.

People are the first line of defense against disasters and emergencies–they become a force multiplier when prepared. People are the real key to improving the nation's ability to absorb, recover from, and adapt to disasters and emergencies. The more prepared people are, the lower the cost and time of recovery to the individual, the community they live in, and the organization they work for.

The lack of personal resilience adversely impacts organizations every single day. Things like home fires, divorce, elder- and child-care, urgent home repairs, accidents, bankruptcy, and other personal issues cause lost productivity and unscheduled absenteeism and presenteeism which cost the nation over $268 billion annually.[1]

Presenteeism is defined as an employee that has come to work, but is not fully engaged. Presenteeism accounts for 61% of an individual's total lost productivity and medical costs. What's particularly illuminating is that 60-70% of all Employee Assistance Plan requests are legal services to cover estate planning, family law, divorce, real estate, and bankruptcy. Nearly 30% of employees come to work at least 5 days when they are too distracted to be effective. Roughly 28% of workers take time off for care giving and 25% took at least 1 hour/day to deal with personal issues. With respect to absenteeism, roughly 60% of all unscheduled absences are related to personal issues other than illness. Unpreparedness for these everyday disruptions becomes magnified during an emergency, costing industry millions of dollars for every hour it takes an employee to be available to their employer. In order to improve daily productivity and survivability, particularly in times of crisis, emergency, or disaster, there must be a shift from readiness to resilience.

Organizational resilience becomes evident when employees have

(Continued on Page 22)

[1] Paul Hemp, "At Work, But Out of It," *Harvard Business Review*, 2004, accessed January 15, 2014, http://hbr.org/2004/10/presenteeism-at-work-but-out-of-it/ar/1; *2007 CCH Unscheduled Absence Survey*, accessed January 15, 2014, https://www.cch.com/Absenteeism2007/.

(Continued from Page 21)

addressed the highest priority they have in a threatening situation—the safety and security of themselves, their family, and other loved ones—and that they have developed the means to restore critical life information in order to reduce recovery time when bad things happen. This is particularly important for employees, such as first responders, emergency managers, and continuity planners and owners and operators of critical infrastructure if they or other family members are also impacted by an event.

All risk management plans—whether housed in a business, an agency of first responders, or community support agencies—rely on a single common asset: people. Yet conventional approaches to emergency management and continuity plans assume, all too often, that people will be available to execute emergency plans and procedures. Although some organizations have rosters of 2-3 (and perhaps even 4) people deep who can perform critical roles and responsibilities in the event of crisis, emergency or disaster, the fact of the matter is that if the most experienced people on the roster are not available, it puts extra strain on the organization and produces sub-optimal effectiveness unless, of course, the organization has developed a robust cross training program to ensure everyone on an emergency roster knows how to perform the roles and responsibilities of the position they may have to assume when the balloon goes up. The real issue in a major event will be if the number 1 and 2 person on an emergency roster are impacted by the event. This is why it's vitally important to ensure employees have a personal and family emergency plan, as well as the critical personal and family information they will need to recover more quickly from the event and be ready to assume their emergency responsibilities for their employer.

If the entire U.S. workforce of 140 million people had a personal resilience plan to help them cope better and recover more quickly from a personal or community crisis, emergency, or disaster, there would be a much higher probability that employees would be able to provide their employers at least an additional full day of focused work on the job each year. In fact, availability for just one extra day per year would save $32 billion dollars on an annual basis (140M x $29.18/hr. x 8 hours (or $233/day)). For a company employing 5,000 employees, yearly savings could be $1.165 million. For a 1000 employee organization, the savings could be nearly a quarter of a million dollars. Over time, a more resilient workforce can save the nation hundreds of billions of dollars. This fact alone should motivate people, industry, and government to examine the issue of personal resilience much more closely.

We know that less than 10% of people have emergency preparedness and recovery plans, but why haven't organizations invested more in providing enterprise-wide solutions to improve personal resilience? Why do so few companies offer their employees resilience planning tools either directly or through their Employee Assistance Program (EAP)? It seems like a no-brainer—particularly when the ROI is not only self-evident, but in the nation's economic best interest. The reason why a large majority of organizations have not taken a serious look at how personal and family preparedness impact their organization's bottom line must be because they are not aware of the tools that can increase employee resilience.

We do know that virtually all HR offices offer specific programs to help employees who are sick, or have family emergencies, or need legal or other help to solve important problems. These problems account for a lot of workplace stress and low productivity. Human resources managers are only now learning the real value of investing in personal resilience. Emergency management and security professionals need to spend some quality time meeting with HR and other organization officials to explain this issue, raise awareness, and assist them in institutionalizing viable personal resilience solutions.

When over 90% of people and families do not have a preparedness plan, they have to scramble to respond and recover from unexpected events. Simply being "ready" for an unexpected event misses the opportunity to plan for recovery. This effectively delays the amount of time an employee needs to be available to his/her company or organization in the event of an emergency—personal or otherwise. This is why national guidelines are evolving from readiness to resilience. The challenge is getting both individuals and organizations to realize that investing in personal resilience is vital to both their and

(Continued on Page 23)

(Continued from Page 22)

their employer's success.

Beyond specific plans that ensure the safety and security of family members *during* an emergency, the largest impact to employee availability after an event is the restructuring of the employee's life (or that of the employee's family)—from securing alternate shelter to the rebuilding of personal records. Concern for what it takes after an event for an individual to recover must be recognized and communicated more widely. A 2009 Citizens Corps National Survey, Personal Preparedness in America, indicated that only 2% of respondents had stored financial documents in a restorable format or alternate location. Only 9% had recorded the names, dosage, and frequency of the medications their family members have to take, and only 1% had made arrangements to copy and store personal identification. How long would it take you to find critical information if you lost it in a fire, flood, or simply couldn't find it in short order if you needed it quickly?

If we are now convinced about the efficacy of strengthening personal resilience, what do we need to invest in? Beyond investing time to raise awareness, communicating the possible savings, and fostering momentum in building personal and family plans, there are a number of free and relatively inexpensive tools on the market to help people and families prepare for and recover from an unexpected event. However, many of these tools and the zillion checklists that can be found on the internet provide an overwhelming amount of information that can leave the average individual exhausted in trying to apply this information in a relevant, coherent manner. The paper-based family emergency plan can be lost. Many personal preparedness planning tools and checklists are not designed to address both an individual's resilience and how it actually relates to supporting his/her employer's business continuity, disaster recovery or workforce preparedness challenges—particularly if the individual has to perform specific roles and responsibilities in an emergency in support of his or her employer.

More importantly, many tools available for free or in the marketplace address preparedness, but not personal recovery. Again, this is critical for employees that have specific emergency or continuity roles and responsibilities in the organization. Many tools are too expensive for the average worker, have low levels of security, and do not offer customer support to help the user when questions arise. Very few, if any, are focused on simplifying the information needed to recover from a wide array of disruptive events, organizing this information in simple, highly restorable formats, and guiding the individual through a personal risk assessment that examines prevention, preparation, and recovery from commonly occurring emergencies to natural disasters—particularly as they relate to individual's specific job or geographic location. In summary, few tools available today:

- Provide understanding for why individual and family preparedness is needed
- Actually guide the individual through the process of preparing an adequate plan
- Acknowledge the benefits of self-reliance
- Make it simple and easy to gather the information needed for themselves, their family, or employer
- Shorten the time required to achieve demonstrable resilience
- Provide proper security of the individual's personal data, and ensure access to it when needed

There is absolutely no question that strengthening the protection of the nation's critical infrastructure is vital to our national security. Owners and operators of U.S. critical infrastructure have been working smartly to strengthen their ability to prepare for disasters in ways that reduce or eliminate long-term effects to people and property and improve response and recovery capabilities. New design structures and systems are enabling critical infrastructures to withstand disruptions and mitigate both direct and indirect (cascading) consequences. Redundant systems are being built to ensure continuity of critical functions, and critical operations are being decentralized to reduce vulnerability to single points of failure or disruption.

However, only by focusing more intently on personal (human resources) resilience, can we truly increase our nation's ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from emergencies and disasters that

(Continued on Page 24)

(Continued from Page 23)

interrupt productivity and revenues.

The safety and security of American families can be significantly improved if more citizens and organizations commit to becoming more resilient to unexpected events—be they personal tragedies, public threats, or the "won't happen here" natural disaster that could occur later today. National resilience is a shared responsibility. While government and industry have played a role in strengthening the nation's critical infrastructure and making communities more resilient, focus on individual and family preparedness remains a continuing challenge.

In proclaiming last November as "Critical Infrastructure Security and Resilience Month," the President of the United States stated: "…*as we recognize that safeguarding our critical infrastructure is an economic and security imperative, let each of us do our part to build a more resilient Nation*."

We applaud the President for penning his proclamation and call to action, and we penned this article to bring closer attention to the owners and operators of critical infrastructure the importance of making their companies more aware of the need to strengthen the personal resilience of their employees. By doing so, all of us can "*do our part*" to help achieve and maintain a demonstrably effective national resilience posture. The faster we work to help make this happen, the faster Americans will: (1) better understand the risks they face; (2) work together before, during, and after emergencies to ensure resilience activities are informed by local knowledge and capabilities and are thus undertaken more safely; (3) complement the work of first responders and other disaster response and recovery agencies; and (4) know what to do, who to call, and what to expect when disaster strikes.

We urge all readers of *The CIP Report* to take time out to think more critically about the safety and security of the people in your organization or your own loved ones. Unfortunately, someday they are very likely to experience some type of an emergency, disaster, or other terribly disruptive event. The likelihood of their lack of preparedness and ability to quickly recover from such an event is a clear and present predicament, *but it does not have to be that way*. ❖

**Ronald Bearse is the president of Nauset National Security Group, LLC, a security consulting and technology services company based in Hyannis, MA. Ron served in a variety of analytical, managerial and leadership positions within the national security emergency preparedness community during his 20+ year career with the Departments of Defense, Homeland Security and the Treasury. He can be reached at: rbearse@nnsgllc.com.*

Ann Coss is the CEO of Personal Recovery Concepts, LLC and a leader in personal resilience planning for individuals, families and public, private and non-profit organizations. She can be reached at: ann@personalrecoveryconcepts.com.

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison University 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 here:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1