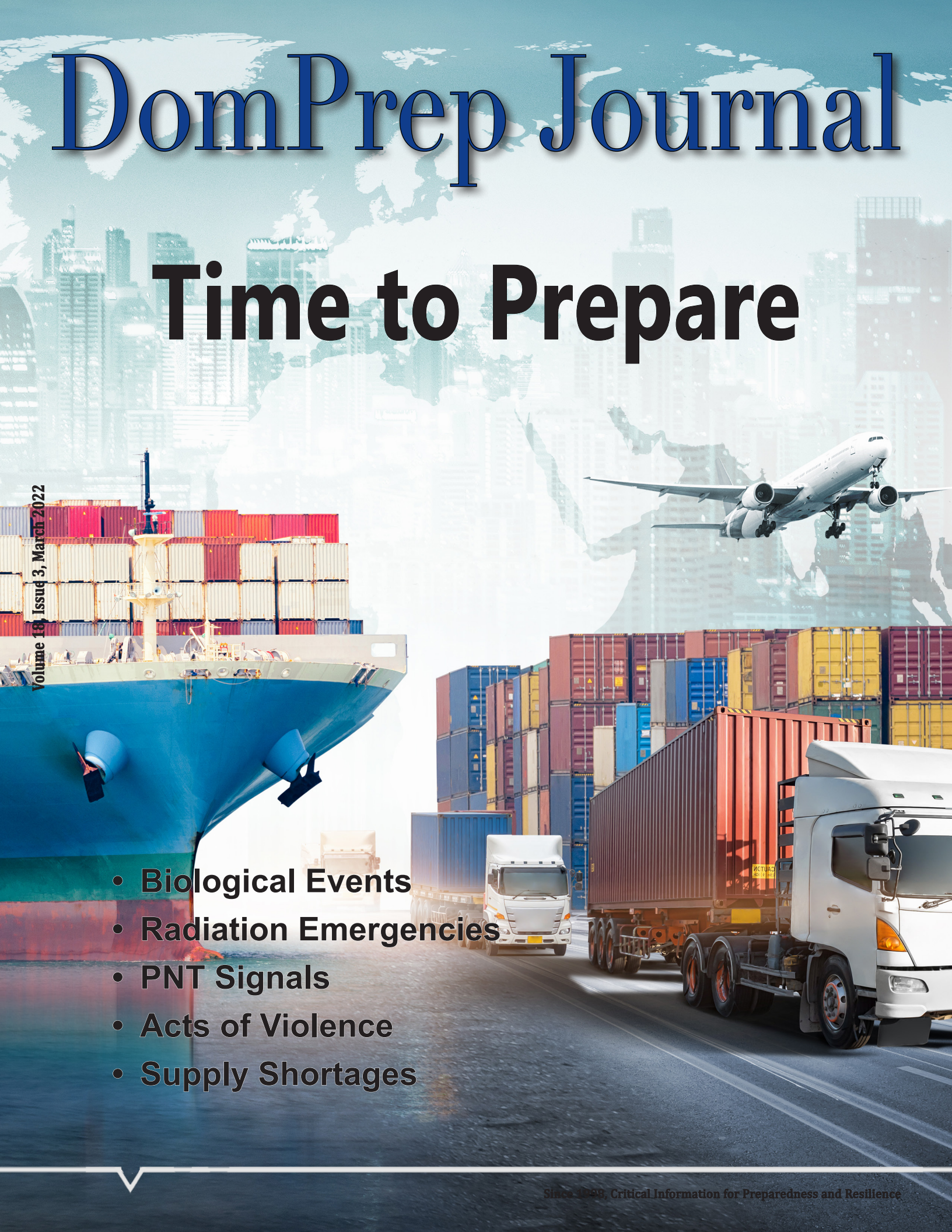
DomPrep Journal

Time to Prepare



Volume 18, Issue 3, March 2022

- Biological Events
- Radiation Emergencies
- PNT Signals
- Acts of Violence
- Supply Shortages

Since 2005, Critical Information for Preparedness and Resilience



Partner with the world-wide leader in emergency preparedness and response solutions

Juvare connects more than 95% of the U.S. population through its emergency preparedness and response technologies, including **WebEOC.** As the world's most widely-used, battle-tested emergency management software, WebEOC empowers users to prepare for and respond to emergencies with features built for any user, at any skill level.

- **Unrivaled flexibility** with built-in tools and an open API that enable you to customize the solution to your organization
- **Enables efficient collaboration** though data-sharing and common workflows across agencies, geographic boundaries, and both public and private sectors
- **Faster alerting** though WebEOC Alerts Plugin, with notifications that meet responders where they are most easily reached
- **Emergency preparedness expertise,** with a deep understanding of the needs of our partners across federal, state and local agencies, healthcare, corporate, non-profit and education

Visit *juvare.com* to learn more about WebEOC and other flexible solutions to meet your unique emergency preparedness and response needs.

JUVARE



Business Office
1033 La Posada Drive
Suite 135
Austin, Texas 78752
www.DomesticPreparedness.com

Staff
Texas Division of Emergency Management
Publisher

Catherine Feinman
Editor
cfeinman@domprep.com

Martin Masiuk
Founder & Publisher-Emeritus
mmasiuk@domprep.com

Advertisers in This Issue:

Juvare

Featured in This Issue

Pictured on the Cover: Source: ©iStock.com/Tryaging

ARTICLES OUT LOUD FOR YOUR BUSY LIFE

Emergency Preparedness Professionals are incredibly busy and often on the road. To give you more opportunities to benefit from the articles in the Journal, you now have access to Articles Out Loud that will be available for a trial period.

You can find our first Article Out Loud on our website under the Podcast channel, or in the iTunes store.

Don't forget about last month's Journal! Click **HERE** to download it now.

DON'T MISS ANOTHER ISSUE OF THE DPJ WEEKLY BRIEF OR THE DOMESTIC PREPAREDNESS JOURNAL

SUSCRIBE **HERE**

Closing Preparedness Gaps – Timing Is Everything

By Catherine L. Feinman

In some ways, communities are well prepared for emergencies. However, it is critical to continuously assess systems, structures, models, and procedures to identify even small weaknesses and gaps that can become significant impediments to effectively responding to threats, hazards, and risks. The authors in this March edition of the Domestic Preparedness Journal identify gaps and share possible solutions for various critical infrastructure, public health, and physical safety vulnerabilities and threats.

The The common phrase "timing is everything" takes on even greater significance when preparing for and mitigating future threats. For example, position, navigation, and timing signals are a necessary component for critical infrastructure sectors to function effectively. Any breakdowns in critical infrastructure can lead to negative cascading effects for daily lives throughout communities. Robust planning with built-in contingencies can help close gaps that would otherwise exacerbate response scenarios.

Being prepared for an emergency or disaster means having pre-incident plans in place to ensure incident response is effective and post-incident recovery is expedited. When communities are not prepared for known or emerging threats, it is difficult to coordinate efforts, allocate resources, and clearly communicate to all stakeholders when a disaster occurs. One type of threat that the United States is currently unprepared for is a biological event. The nation needs to be more prepared for the next pandemic or other biological event than it was for COVID-19.

Regardless of the type of incident, gaps can be identified and addressed by regularly assessing emergency plans and procedures, expanding learning opportunities, and applying lessons learned and best practices. Creating new models to proactively prevent incidents from occurring, training to address responses to medical challenges, and strengthening supply chain procurement processes are just three ways described in this issue to build resilience. There are so many ways that leaders are preparing for the next incident. The Domestic Preparedness Journal will continue to share best practices, lessons learned, emerging technologies, and other tips to better prepare communities today. Timing is everything, and the best time to prepare is now.

Catherine L. Feinman, M.A., joined Domestic Preparedness in January 2010. She has more than 30 years of publishing experience and currently serves as editor of the Domestic Preparedness Journal, www.DomesticPreparedness.com, and the DPJ Weekly Brief, and works with writers and other contributors to build and create new content that is relevant to the emergency preparedness, response, and recovery communities. She received a bachelor's degree in international business from University of Maryland, College Park, and a master's degree in emergency and disaster management from American Military University.

Biopartisan Commission Says Nation Unprepared for Biological Events

By Asha M. George & John T. O'Brien

On 17 February 2022, Dr. Asha M. George, executive director of the Bipartisan Commission on Biodefense testified as an expert witness before the U.S. Senate Committee on Homeland Security and Governmental Affairs at a hearing on addressing the gaps in the nation's biodefense and level of preparedness to respond to biological threats. In 2015, the Bipartisan Commission on Biodefense released its first report, A National Blueprint for Biodefense, to warn that the biological threat was rising and to inform the government that the nation was insufficiently prepared to handle a large-scale biological event. When COVID-19 emerged in early 2020, many of those findings proved to be true.

While some strides have been made before and during COVID-19, the United States and the international community are still insufficiently prepared to address the escalating biological threat. Last year, the Department of State released a report in which it stated clearly that Russia and North Korea possess active biological weapons programs, with China and Iran not far behind. The United States must assume that its enemies are actively paying attention to the vulnerabilities revealed during COVID-19 and must prepare for a biological weapons attack on the U.S. homeland.

U.S. biopreparedness is fractionated, multifaceted, and distributed across all levels of government and much of the private sector. The federal government's response to the pandemic has illustrated the broad swath of departments and agencies involved in biodefense. All 15 cabinet departments, 8 independent agencies, and 1 independent institution (see Table 1) are responsible for biodefense, including preparedness.

Since the release of the Blueprint, some improvements have certainly been made. For example, Congress required – and the Trump Administration released – a National Biodefense Strategy to align all existing policies and programs across the federal government. In many other ways, however, the United States has either made no headway or took steps backwards. For example, the United States has participated in exercises that frequently demonstrated that a large-scale biological event could quickly overcome the nation, yet leaders did not take decisive action to ensure that the lessons observed became lessons learned.

Many of the homeland security assets in place today are inadequate to meet the needs of the nation. The Department of Homeland Security's (DHS) BioWatch program, for example, is incapable of detecting biological threats effectively. Last year, the Commission issued a report, Saving Sisyphus: Advanced Biodetection for the 21st Century to describe

Table 1. The 15 Cabinet Departments, 8 Independent Agencies, and 1 Independent Institution Responsible for Biodefense		
Cabinet Departments	**Independent Agencies**	**Independent Institutions**
Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Interior, Justice, Labor, State, Treasury, Transportation, and Veterans Affairs	Central Intelligence Agency, Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Nuclear Security Administration, National Science Foundation, Office of the Director for National Intelligence, and U.S. Postal Service	Smithsonian Institution

concerns about BioWatch and make recommendations as to what can be done to achieve the vision for the program begun in 2003. Nineteen years is long enough for things to go on as they have. The Commission recommends that Congress either shut it down or replace it with a program that works effectively. States, localities, and taxpayers deserve no less and the good people working in the Department of Homeland Security deserve some relief.

In 2017, DHS created an Office of Countering Weapons of Mass Destruction (CWMD), which Congress subsequently authorized a year later. Though department officials envisioned the office to be a one-stop-shop to address weapons of mass destruction by the department, authorizing legislation did not reflect that mission. As Congress examines the department's Countering Weapons of Mass Destruction Office, they must clarify its role.

Since the release of the Blueprint, some improvements have been made. In many other ways, however, the nation has either made no headway or took steps backwards.

While preparing for the next biological event seems daunting, the nation has overcome grand challenges like this in the past. If going to the moon is achievable, so is establishing an Apollo Program for Biodefense to take all pandemic threats off the table in 10 years. The Commission recommended such a program and has developed other specific biodefense recommendations, including many for the Department of Homeland Security.

The United States cannot afford to focus on COVID-19 to the exclusion of all other biological threats. As the nation continues to respond to and tries to recover from this pandemic, leaders must prepare for biological attacks, accidental releases, and other infectious diseases with pandemic potential.

Asha M. George, DrPH, is the executive director of the Bipartisan Commission on Biodefense. She is a public health security professional whose research and programmatic emphasis has been practical, academic, and political. She served in the U.S. House of Representatives as a senior professional staffer and subcommittee staff director at the House Committee on Homeland Security in the 110th and 111th Congress. She has worked for a variety of organizations, including government contractors, foundations, and non-profits. As a contractor, she supported and worked with all federal departments, especially the Department of Homeland Security and the Department of Health and Human Services. She also served on active duty in the U.S. Army as a military intelligence officer and as a paratrooper. She is a decorated Desert Storm Veteran. She holds a Bachelor of Arts in Natural Sciences from Johns Hopkins University, a Master of Science in Public Health from the University of North Carolina at Chapel Hill, and a Doctorate in Public Health from the University of Hawaii at Manoa. She is also a graduate of the Harvard University National Preparedness Leadership Initiative.

John T. O'Brien, MS, is a research associate for the Bipartisan Commission on Biodefense. He is a public health security professional with a background in bioengineering and emerging infectious diseases. Prior to joining the Commission, he conducted research on the biosecurity implications of artificial intelligence with the Future of Humanity Institute at the University of Oxford. Before that, he worked at the Nuclear Threat Initiative where he supported work on the Global Health Security Index as a contributing author. He previously conducted laboratory research at George Mason University's National Center for Biodefense and Infectious Diseases on novel detection methods for Zika, Chikungunya, Venezuelan Equine Encephalitis, and Rift Valley Fever viruses. He holds a Bachelor of Science in Bioengineering, with a concentration in Biomedical Signals & Systems, from George Mason University and a Master of Science in Biohazardous Threat Agents and Emerging Infectious Diseases from Georgetown University. He is also currently pursuing his DPhil in Biology at the University of Oxford.

Radiation Emergency Medical Challenges and A Global Pandemic

By Ron Cain

It seems that every day over the past two years there are plenty of news stories covering the strain hospitals are facing in staffing shortages and the impacts from a global pandemic. Emergency medical services (EMS) are also dealing with their own similar issues across the nation. Many of these critical facilities and services are located in the proximity of nuclear power plants in which previous agreements were established to provide treatment, patient transportation, radiation monitoring, and decontamination in the event of a patient-generating event within a nuclear power plant's emergency planning zones.

Biennially, the Federal Emergency Management Agency (FEMA) grades Medical Services Drills (MSD) and requires training in the off year for designated hospitals and EMS systems. FEMA requires radiation response teams in both hospital and prehospital organizations with specialized training. It is possible due to the combination of staffing shortages and pandemic impacts that a gap in radiation emergency preparedness could lead to life-threatening problems that are much worse that a negative drill finding from FEMA.

A Solution for Meeting Training Requirements

A state level emergency management agency in the Southeast recently addressed these potential issues after it revised the MSD training it offers to hospitals and EMS systems. During a rehearsal of concept (ROC), the scenario included a county emergency management department in coordination with an affected hospital requesting state level training support for new emergency department staff with no previous radiation emergency experience or training.

The training content provided during the ROC included the following:

- Oak Ridge Institute for Science and Education's Radiation Assistance Center/Training Site (REAC/TS) standards are emphasized throughout the training. REAC/TS is considered the gold standard for radiation emergency medical treatment and patient decontamination.
- Training content focused on new and/or inexperienced EMS and hospital staff with didactic and practical learning outcomes.
- Reminder that the ongoing global pandemic has created some similarities in response and management of radiation emergencies for EMS and hospital responders and clinicians.
- Emphasis on the partnership between local EMS, hospitals, local, state, and federal level emergency management organizations.
- Comparisons and contrasts between a medical services drill and a real radiation emergency incident.

The Medical Services Drill (*Source:* Ron Cain, June 2021).

A didactic presentation was followed by practical training on dosimetry, patient monitoring, how to use detection instruments, patient packaging for EMS transport, and patient decontamination. This usually lasts two hours but can go longer depending on class size. No virtual option was available due to the critical need to teach the above listed skills in person for better learning outcomes.

Like many other issues the global pandemic has exposed, radiation emergency preparedness could become a vulnerability itself – if it has not already. The ROC scenario included a mix of travel nurses, new employees, and staff members that transferred from other hospital departments – all with no combined experience in radiation emergency medicine or in patient decontamination. With a graded MSD in the future and a gap in their preparedness, outside help in the form of state level training support was requested by the local emergency management agency.

REAC/TS offers excellent training at its site in Oakridge, Tennessee. The nuclear energy companies coordinate and support the attendance of hospital, EMS, and emergency management professionals that are involved in radiation emergency preparedness, but the courses seem to fill fast. In addition, like many other teaching institutions in the past two years, they have canceled in-person classes due to the pandemic. Subsequently and realistically, the option was not in the ROC scenario to send hospital and EMS employees to REAC/TS.

Key Takeaways From the ROC

With all the aforementioned issues with EMS and hospitals, the ROC included a discussion about the realities of an MSD versus real events:

- FEMA requires the demonstration of one patient for treatment, transportation, monitoring, and decontamination during its graded MSDs. In reality, there may be many patients calling EMS or driving themselves to the hospital.

- Nuclear power plant emergencies tend to develop slowly, and the hospital and community may have activated their emergency plans days before the first potentially contaminated patient arrives. Incident management for extended times should be considered.
- EMS and hospitals should evolve their radiation emergency planning for multiple patient transports from within contaminated zones and establish robust personal protective equipment resupply lines. Radiation emergencies, unlike a viral pandemic, can be rapidly detected using dosimetry and radiation monitoring instruments that are stockpiled in nuclear power plant emergency planning zones.
- Actual nuclear power plant emergencies will require the partnerships between local, state, and federal agencies who should already be coordinating well before any exercise or actual incident.

Trained radiation response teams that exist today could be non-existent tomorrow due to the staff turnover and other factors related to the global pandemic. This will negatively impact two of FEMA's community lifelines – the Health and Medical and the Energy (Power & Fuel) – and potentially impact even more community lifelines as the incident grows. The ROC scenario was built with these critical issues in mind.

While it is still important for EMS systems and hospitals to pass FEMA-graded medical services drills, it is far more important to adapt to the constantly changing operational environment and to continue to be prepared for real radiation emergencies that threaten the life safety of communities, however unlikely they may be.

Ron Cain is a radiological emergency preparedness coordinator for a state emergency management agency. He has previous experience as a hospital and small county emergency manager. He has over 25 years of experience as a paramedic in county, military, and private EMS systems. He is a graduate of the National Fire Academy's EMS Special Operations and Advanced Life Support for Hazardous Materials Incidents Course and a graduate from the REAC/TS Radiation Emergency Medicine Course. He is a state certified emergency manager and has earned undergraduate and graduate degrees in disaster and emergency management.

The REAC/TS class photo (*Source:* Ron Cain, February 2020).

PNT Signals as National Critical Infrastructure

By Nathan DiPillo

Several national critical functions and all 16 critical infrastructure sectors rely either directly or indirectly on functional and consistent position, navigation, and timing (PNT) signals. As such, fragility of weak and easily imitated global positioning system (GPS) signals could lead to catastrophic impacts on dependent and interdependent critical infrastructure systems. Designating PNT-signal-emanating assets as a standalone national critical function would bring resources, awareness, research, additional risk mitigation measures, and new solutions to help keep consistent and resilient PNT signals operational if threatened by natural and human-caused threats.

Imagine starting the day three hours behind, receiving a cellphone warning of identity theft, getting a call from a financial planner about retirement assets going missing, and learning that the Federal Aviation Administration (FAA) has grounded hundreds of planes – all potential scenarios following significant PNT disruption. These scenarios involve day-to-day functions and transactions that rely on PNT to operate. Many other local and national critical infrastructure depend on PNT signals for business operations, identity management, secure communications, and financial transactions.

Local critical infrastructure (such as water treatment plants, energy, and transportation) and financial institutions (such as banks and brokerage firms) conduct millions of transactions daily – all of which depend on authentic, accurate, and rhythmic PNT signals. For example:

- Water treatment plants rely on PNT systems to securely communicate between their operating technologies to manage daily water flow, balance chemicals, and monitor water quality.
- Banks validate customer authenticity and identity when completing transactions using phasor measurement units' synchronization from U.S.-based PNT and GPS systems.
- Some financial institutions and companies dealing with cryptocurrencies rely on proof of location in their blockchains.
- First responders rely on communication equipment like digital and analogue systems that operate with PNT signals from space-bound GPS satellite systems.

However, not all companies are relying on weak GPS signals to validate PNT data, obfuscating analysis of true impact of fragility in the national GPS network. Although cryptocurrencies rely on proof of location in their blockchains; not all blockchain startups are relying on GPS signals for identity management. Some companies opt for geotriangulations using low-power wide-area networks (LPWAN) or other Internet-of-Things gadgets to help validate locational data. Other companies are looking at terrestrial

unlicensed radio spectrum to help validate location due to not having confidence in current PNT space-based networks. This is still new in advancing industries. Although the solutions seem simple, like internal atomic clocks on servers or running parallel timing systems, there is no final process that is accepted industrywide. Foamspace Corp published a 2018 white paper on blockchain and a protocol for the decentralized geospatial data market:

> *Civil GPS is unencrypted, it has no proof-of-origin or authentication features, and despite dire warnings first raised in 2012, the system remains extremely susceptible to fraud, spoofing, jamming, and cyberattack…. A backup for GPS is needed because it can be easily spoofed, jammed, or falsified. This means that there is currently no truly secure way to verify location in blockchain-based smart contracts or decentralized applications.*

The white paper indicated that more research is needed to create a reliable non-satellite-based resilient PNT signal network for civilian use that is redundant and can be relied upon if other systems are compromised.

Critical Infrastructure Relies on Precision Timing Supported by Weak GPS Signals

Energy grid, transportation, emergency communications, health care, and local and national logistics systems are all critical infrastructure that rely on precision timing. These industries usually do not have the most recent technology due to bureaucracy or funding and take time to reach new industry standards. Any slight disruption, malfunction, or misdirection could impact information communication technology (ICT) and connected interdependent systems especially if they are linked truncated systems that operate or support national critical functions.

The PNT signals used in many of these industries depend on a space-bound GPS network for everyday validation of PNT data. Advancing business analytics are now more ingrained in industrial control systems and supervisory control and data acquisition (SCADA) systems that operate lifeline infrastructure. Failure of these systems would have devastating effects on business and culture impacting communities, family, and industries both nationally and internationally, some may be nearly impossible to recover from or even have the capability to rebuild due to aging or unsupported software and or hardware – ultimately delaying these systems from coming back online.

Dependency on Satellite GPS Systems for PNT Signals Creates a National Security Risk

According to the Resilient Navigation and Timing Foundation, "Thousands of disruption incidents have been reported throughout 2020, from China to California, and from the Arctic Circle to New Zealand" in the form of spoofing and jamming of GPS signals on aircraft, manufacturing equipment, and even pig farms. These jammers can be as small as a 12-volt item plugged into a cigarette lighter of a vehicle to foreign-based systems that are able to jam whole continents. Spoofing PNT signals is now standard procedure for some governments to evade sanctions on a grand scale. According to The Times of Israel, "Windward, a maritime intelligence company … said that since January 2020 it has detected more than 200 vessels involved in over 350 incidents in

which they appear to have electronically manipulated their GPS location." Enforcement actions rely heavily on location data to enforce violations.

Addressing a government advisory board in December 2021, National Security Council Director for Response and Resilience, Caitlin Durkovich said GPS remains "a single point of failure" for the U.S. Today, a lot of the critical infrastructure in California and other states are owned and operated by private/civilian sector entities, to include cities, counties, and special districts. Some of these entities use off-the-shelf ICT that rely on space-based GPS for their PNT signals. Consequently, when GPS signals are disrupted or interrupted, all 16 critical infrastructure sectors that partially or completely rely on GPS for PNT data for their ICT are at serious risk of being interrupted or completely disabled.

Dana Goward, president of the Resilient Navigation and Timing Foundation stated in 2018, "GPS signals have become essential to an incredible variety of services that everyone relies on: navigation, routing, common operational pictures, blue force, and asset tracking to name a few." Interdependencies of PNT signals connecting all 16 critical infrastructure sectors present more clear evidence of how important physical GPS systems – either space-bound or terrestrial – that produce PNT signals are to the U.S. strategic imperatives supporting sustainment of lifelines.

Due to the dependencies and interdependencies to all 16 sectors, it might be time that domestic physical assets like GPS satellites and terrestrial networks (fiber and tower based) become their own national critical function, which would allow access to Department of Homeland Security (DHS) information and security resources like monies and organizational support. Although the physical assets that produce PNT signals are not yet recognized as one of the 16 critical infrastructure sectors, DHS did list PNT signals as one of the 55 National Critical Functions, which highlights how vital PNT signals are. An official designation of the physical assets would provide an additional layer of protection and a more robust exchange of information and requests for advice or assistance from designated committees like the Critical Infrastructure Partnership Advisory Council and other special interest groups. These efforts and proper designation would help in keeping these systems relative and resilient and allow for other solutions for PNT signals to be analyzed like visualizing geolocational data from blockchain technology, fiber lines, and tower-based systems like eLORAN.

Priority System

A May 2021 Government Accountability Report on Defense Navigation Capabilities highlighted, "While GPS provides significant capabilities to both military and civilian users under normal conditions, it is subject to interference by adversaries." This is significant as it discusses the U.S. Department of Defense's role and civilian role in using and/or supporting alternatives to PNT signals that do not emanate from GPS-type systems.

Over the past two years, there have been physical delays in many day-to-day critical systems. Some of these delays are due to disruptions in ICT systems due to cyberattacks or national disasters. One priority system is the logistical or supply

chain system(s). Additionally, in response to the U.S. Department of Commerce in October 2021, the Resilient Navigation and Timing Foundation stated, "PNT services are used in transportation, logistics, telecommunications, SCADA, and other systems that support all supply chains, including those for ICT device production." These ICT systems are an integral part of the business analytics that manage everyday local, statewide, national, and international SCADA and industrial control systems. The National Institute of Standards and Technology Interagency or Internal Report 8323 states,

> *The national and economic security of the [US] is dependent upon the reliable functioning of the nation's critical infrastructure. [PNT] services are widely deployed throughout this infrastructure. In a government wide effort to mitigate the potential impacts of a PNT disruption or manipulation, Executive Order (EO) 13905, Strengthening National Resilience Through Responsible Use of Positioning, Navigation and Timing Services was issued on February 12, 2020*

COVID-19 has again highlighted additional vulnerabilities in critical infrastructure systems, one of them being the fragile PNT signals from space-bound systems. These vulnerabilities include but are not limited to cascading impacts from resource diversion or delays, unauthenticated business transactions, and a continuing barrage of cyber impacts, which all affect manufacturing, materials processing, energy grids, and other industrial functions. Some of these activities include spoofing, denial of services, jamming, or compete failure of whole systems and interdependent systems from natural hazards like solar flares. These threats are real and relevant today. According to Forbes in February 2022, "At least 40 of the 49 Starlink satellites launched by SpaceX last week have been destroyed by a geomagnetic storm."

Over time, these cascading impacts or snowballing effects will lead to devastating long-term challenges and open opportunities for adversaries to exploit vulnerabilities embedded within the supply chain and other interdependent systems that support local critical infrastructure and national critical functions. This will inevitability create catastrophic residual impacts to lifeline systems and could overwhelm emergency management agencies, first responders, and essential workers, especially when managing multiple incidents at the same time.

Defining GPS- and PNT-Signal-Producing Hardware as Critical Infrastructure

Executive Order 13905 Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services defines how to responsibly protect the use of PNT signals. This order highlights current efforts on PNT profile identification, testing, and categorization of navigation and timing services. It defines critical infrastructure as:

> *[S]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a*

debilitating impact on national security, national economic security, national public health or safety, or on any combination of those matters.

When these essential elements of information are defined as priority informational requirements used by intelligence agencies – and knowing the PNT signals rely heavily on only U.S.-controlled space-bound and/or terrestrial GPS interoperability networks – the country's current physical GPS assets undoubtedly fit within this defined criterion. Next, this sets a principle in understating that U.S. owned and operated GPS and dependent systems that produce a PNT signal are the nucleus of how national critical functions and other business cycle analytics operate every day of the year, keeping communities and industries thriving. According to Dana Goward, "GPS-based time stamps allow databases to know which is the most recent bit of information being stored. They also provide location data as a part of identity management and offender monitoring systems. The list is almost endless."

With the onset of 5G, automatous vehicles, precision agricultural systems, data cloud storage processes, and many other emerging industries, there will be greater dependency on a fully functional, operational, and resilient terrestrial and space-bound GPS infrastructure producing PNT signals in support of ICT systems across all 16 sectors.

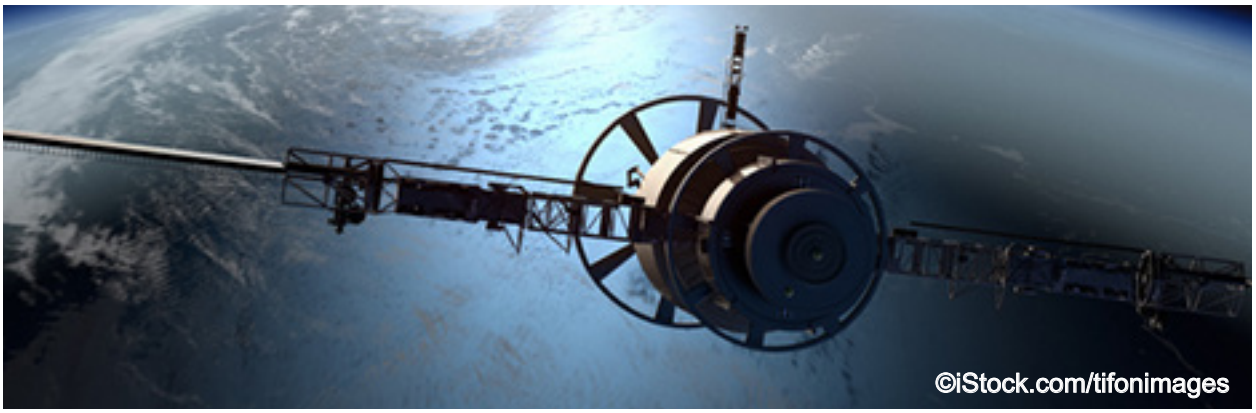
Defining National Critical Functions

In 2017, former DHS Secretary Jeh Johnson designated U.S. elections systems as a national critical infrastructure. This was significant as the U.S. electoral system was being exploited. The fact that elections have been designated as a national critical function is supportive of the concept that dependent and interdependent systems can have their own national critical function designation due to their national and international impacts if exploited or corrupted. This is true of PNT signal producing systems that are connected to encrypted cyber services and business operation cycles that manage critical infrastructure and lifeline systems

Even when compared with other countries' definitions of critical infrastructure, space-bound and terrestrial GPS systems seem to meet similar data points, further supporting the narrative it should be a standalone critical infrastructure sector. In 2008, the Council of the European Union defined critical infrastructure as:

[A]n asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or societal well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

This was further discussed in 2017 report by Canadian authorities who are exploring the idea of designating satellites as a critical infrastructure. Even though Canada has not accomplished this to date, the report stated:



> *In this connection, space assets fall outside what is currently considered national critical infrastructure. Not only is space an operational domain of increasing importance to the Canadian Armed Forces, space assets such as the Global Positioning System and Anik-series telecommunications satellites are critical to the security, safety and economic well-being of this nation as a whole.*

Even as recently as 2021, Edward Swallow, vice president of the civil systems at the Aerospace Corporation, stated:

> *[T]he Global Positioning System is vital for shipping and transportation, including ground, air traffic and marine navigation – anywhere in the world. Communication and information processing, including the world's developing 5G networks, rely heavily on space-based infrastructure…. It's time to protect our nation's space-based systems by designating them as critical infrastructure. Without adequate security, cyberattackers can cause them to malfunction, send false information or collide, potentially creating a debris field that could linger for decades.*

This is the cyber and physical side of how GPS satellites could be compromised. Evaluating vulnerabilities in both the physical and virtual spaces in which PNT signals emanate further links these assets and cyber vulnerabilities as pivotal to national security.

Clear and Present Efforts

When defining national critical functions, local critical infrastructure, sectors, and sub-sectors, there are many systems and networks that continue to depend on precise timing and locational information to make sound business and security related decisions. The President's Executive Order 13905 outlines how silent but valuable U.S. PNT signals are, "The United States made the Global Positioning System available worldwide, positioning, navigation, and timing (PNT) services provided by space-based systems have become a largely invisible utility for technology and infrastructure."

With emerging and advanced Internet of Things products coming online every day (both in the business and private spaces), identity theft, and the proliferation of cyberattacks on connected networks, there will be more demand to drive reliance on

validation of services starting with an authentic and organic PNT signal. Although private sector solutions (e.g., blockchain technology) are currently being developed, they are still in development and only parallel the widely relied upon strong PNT signals. Making GPS assets that emanate PNT signals a critical infrastructure sector would help codify investment in national risk resilience, furthering the importance on the public-private sector interdependency model. In 2021, Peggy O'Connor, director of communications and policy for INSA, summed up a white paper titled, "Designating the U.S. Space Sector as Critical Infrastructure":

> *Designating the space sector as the United States' 17th critical infrastructure sector would clarify government agencies' roles and responsibilities in protecting space infrastructure, make clear to U.S. adversaries that the United States is committed to defending its space infrastructure, contribute to the establishment of global norms regarding the safety and security of space systems, and accelerate development of best practices and technologies for ensuring cybersecurity and resilience of space assets.*

There is a clear and present herculean effort from private and public sectors to protect space-bound systems, which prioritizes satellites that produce PNT signals. At the same time, there is a continued need to protect, harden, and advance technologies by developing multiple approaches to securing PNT signals and/or creating separate and resilient system(s). The Department of Defense has taken this problem seriously and developed information assurance standards to increase cybersecurity protections for space and ground control systems. Fully implementing these standards, Raytheon Intelligence & Space plans to deliver the enhanced ground control segment – GPS Next-Generation Operational Control System (GPS OCX) – in 2022.

While an official designation will not solve all the problems with PNT signals or completely protect the physical aspects of GPS assets, this is a good step in the right direction in keeping awareness of GPS assets and PNT signals at the forefront of how critical infrastructure, the Department of Defense, and everyday business analytics depend on these systems for PNT signals. Preparing now under the opus of a defined effort both domestically and from a national defense posture is key to understanding how any failure or any small disruption in PNT signals could be catastrophic in nature and could cause cascading impacts to unknown areas of lifeline systems. Designating both space-bound and terrestrial PNT signal(s) producing assets as an official national critical sector is a vital step to keeping these systems operational and resilient.

Nathan DiPillo currently serves with the California Office of Emergency Services as a Critical Infrastructure Analyst in the State Threat Assessment Center. Prior to state service, he functioned as a Critical Infrastructure Specialist with the Department of Homeland Security and has 25+ years in the emergency management and security industry. In addition, he served as a non-commission officer (E7) with the California State Military Department, Army National Guard with the 223rdTraining Command. He continues to champion the public and private partnerships. He received a Master of Emergency Management/Homeland Security MSEMHS focused on Domestic Security Management and Leadership from National University.

A New Model for Proactive Prevention

By Rick Shaw

Shootings, acts of violence, crimes, abuse, suicides, overdoses, and other incidents and tragedies are increasing nationwide. Cities across the nation saw a surge of homicides in 2020 and many cities were at or near record levels for homicides in 2021. Cities also saw spikes in 2020 and 2021 with crimes, abuse, suicides, overdoses, and other incidents. Organizations, schools, and communities have continued to add more security solutions as well as more hotlines, safety/threat assessment teams, policies, trainings, and laws. However, violence and crime statistics do not reflect better safety.

Decades of post-incident reports from the U.S. Secret Service, Federal Bureau of Investigation (FBI), and other federal agencies have researched numerous incidents and tragedies and issued various documents regarding mass shootings and other acts of violence. Most post-incident reports routinely identify the presence of more than enough pre-incident indicators existing before a mass shooting occurred and a pathway to violence also existed for most attackers and shooters as they escalated and then executed their plans. But even with more than enough pre-incident indicators, proactive prevention actions still failed.

A Shift in Focus – Asking the Right Questions

Most after-action reports focus on how and why an incident occurred – the pathway that led to the violence and a profile of the attacker – in hopes of finding ways to prevent future attacks. However, when the focus of the research is shifted from the violence aspect to the prevention aspect, the research provides community leaders with new ways and new models to prepare for and prevent future threats. Shifting from validating a pathway to violence to identifying a profile of failed preventions is proving to be a game-changer, but this shift is only possible when leaders of communities and organizations start asking the right questions – and different questions – such as:

- Were pre-incident indicators observed and known by others before the attack?
- Were multiple incident reporting options available?
- Were resources/safety/threat teams available?
- Were trainings and policies provided?
- Were security solutions in place?
- Were laws and standards available?
- Were social workers and mental health resources available?
- Were law enforcement resources available?

Asking questions, especially different questions, is a good way to uncover what might be commonly overlooked or missing. The answers to the questions above can help to

reveal additional questions that need to be asked and answered. For example, when asking the above questions after incidents or tragedies occurred over the past several years, the answer to each of these questions is often "yes."

Because of the "yes" answers, follow-on questions are needed to better understand why prevention efforts still failed. For example, if pre-incident indicators were exhibited, observed, and even reported before an incident occurred, then:

- Where were they?
- Who were they reported to?
- Why were the pre-incident indicators not shared with the right people?

Research from hundreds of past incidents reveals that pre-incident indicators almost always exist. However, when the indicators were reported, numerous incident reporting options are being used. This causes the indicators to be scattered across multiple incident reporting options, across multiple entities, across multiple systems, and across multiple people and departments. Some of the incident reporting options include:

- Hotlines – including organizational, community, local law enforcement, state agency, federal (like See Something Say Something, Crime Stoppers, 9-11, etc.), nonprofit, or other specific hotlines such those established for bullying, weapons, suicide, gangs, domestic violence, workplace violence, fraud, ethics, or numerous others

- Electronic communications – including text lines, mobile apps, emails, websites, or social media
- Personal contacts – including trusted adults (such as teachers), supervisors, human resources, security, teams (threat, safety, risk, behavior, workplace violence, etc.), counselors, mental health workers, employee assistance, legal advisors, friends, or family

Closing Prevention Gaps – A New Model

There are many reasons why pre-incident indicators are not collected and not shared with the right people who have authority to take proactive intervention actions. In addition to incident reporting silos mentioned above, there are numerous other issues related to trust, confidentiality, and sensitivity that can create gaps in information sharing. For example, misunderstandings regarding the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), and other privacy guidelines are common. Personality traits and egos, departmental turf wars, and information not being shared and not assessed because those receiving the information do not believe it is their job are also common. Numerous other issues are also contributing factors, such as not knowing who the right team members are to share the information with or which other internal and external resources need to know about the information, especially as entities experience employee turnover or attrition.

When asking different questions, the different research path reveals numerous and dangerous gaps, silos, and disconnects that are making prevention difficult, if not impossible. Smart funneling and secure information sharing is critical to ensuring the right team members and resources are seeing the bigger picture surrounding individuals and situations of concern. Sadly, scattered pre-incident indicators, scattered team members, scattered community resources, and other scattered expertise are common reasons why proactive prevention efforts continue to fail.

Pulling together disparate information sources reveals the bigger picture surrounding individuals and situations of concern, which is vital for prevention.

Collecting and sharing indicators are just part of a comprehensive six-stage prevention model. Community leaders need to know what they do not know and know what others know on how to replace old and outdated models with the new research-based prevention model. Community leaders must understand:

- New strategies to build awareness of key indicators
- New ways to collect and funnel the warning signs into a central and secure platform
- How to share information with the right people
- How to empower the right people to assess the indicators/information

- How to connect the dots – connect at-risk individual(s) with community resources for intervention and monitoring, and ultimately how to proactively intervene, disrupt, and prevent escalation of at-risk behaviors

Preventing more incidents and tragedies is possible using the new First Preventers model to complement and help their first responders. The new model consists of innovative, research-based, and real-world proven strategies, templates, and tools that were created by asking the right questions, so the right people are seeing the bigger picture, connecting the dots, and proactively preventing more incidents and tragedies before they occur. Everyone can and must do better.

Rick Shaw founded Awareity in 2004 and founded First Preventers in 2019 and is a prevention expert, author, and prevention coach to organizations and communities. For the past 20+ years, he has been researching post-incident reports, lawsuits, and lessons learned to identify the profile of failed preventions involving terrorism, violence, shootings, suicides, sex abuse, human trafficking, and numerous other incidents. His unique research exposed a profile of failed preventions due to dangerous gaps, silos, and disconnects that conventional and old playbook practices have created. He utilized the research to develop the First Preventers Model.

Disaster Procurement: Navigating the Supply Chain

By Brian McGinley

There are moments during a disaster that something needs to be purchased. Depending on the nature of the purchase, it could be something small, perhaps something that can be purchased with a company credit card. On the other hand, it could be a purchase for millions of dollars and, not only do procurement laws come into play, but so could federal procurement laws if the organization is going to seek Federal Emergency Management Agency (FEMA) reimbursement after the disaster closes. In the moments of needing to spend large dollar amounts, the procurement office should be consulted, not because all purchases need to go through that office, but because they work year-round to establish relationships, contracts, and price lists with suppliers that could save time, money, and allow focus to be on the disaster at hand.

During COVID, the global supply chain was greatly disrupted. Organizations with enormous purchasing power seemed to be buying up all the supplies leaving smaller organizations to deal with price gaugers, brokers, and resellers, or to hope for some level of government to help them. However, organizations, even smaller ones, with established contracts and relationships with local firms had opportunities for small orders here and there based on the working relationship throughout the normal year. Those close ties, being on a first-name basis with the local medical or facilities supplier, allowed some organizations to remain stocked with the supplies they needed and the confidence in the local supply chain for leaders to make informed decisions about safety, reopening, or supply distribution.

The essential mission of procurement within an organization is to maintain the supply chain and facilitate the acquisition of goods and/or services. Strategic sourcing is a long-term solution using all the information that is available to make data-driven, forward-thinking sourcing decisions. Instead of waiting for purchasing requests to come through and merely fulfilling transactions, a strategic outlook will analyze the data available to see where value can be created by looking at what matters most to the organization. The value added to the procurement depends on what the end-user considers the highest priority. In some instances, it could be time to first use; perhaps it is the total cost of ownership, or it may be securing business continuity and financial health. This emphasis can be weighted in the evaluation process to avoid the traditional government procurement pitfall of having to award to the lowest bidder.

Benefits of Strategic Procurement

Some of the main advantages of strategic procurement for business continuity and disaster recovery is pre-negotiated pricing lists and satisfying all procurement rules prior to the incident. During emergencies, it is not uncommon for vendors to take advantage of the market disruption and increase prices. There are even instances where vendors with

pre-negotiated prices still try to take advantage of the crises to abandon their obligations. Penalties can be included by the Procurement Department into the pre-negotiated contracts for not honoring the pricing lists. With pre-negotiated contracts for goods and/or services in place, there can be a predetermined list of commodities and services with listed prices almost as a disaster catalog. This catalog of available resources would be a vital component to any disaster recovery or disaster risk management plans.

By taking a more proactive approach, the decision makers in partnership with procurement can set up a more resilient supply chain for the organization, including multiple vendors in case of disruption. By utilizing existing options, such as the U.S. General Services Administration (GSA) Multiple Award Schedule (if eligible), or state versions of the same concept, there can be a multitude of options available to order from existing pricing agreements monitored and awarded by government agencies. Individual organizations also have the option of awarding their own multiple award schedules by issuing a solicitation for a range of products and services and awarding contracts to multiple vendors to create a stable supply chain through multiple outlets. This is very difficult to do during an emergency and, by not having these agreements in place, organizations struggling to find product could be held captive to the fluctuations in supply, demand, and price.

The risk of disruption and price gauging is minimized simultaneously by using pre-existing agreements. Diversification is key to dispersing the potential impact and risk to the organization. Suppliers/vendors are just as susceptible to the forces of the marketplace during an emergency. In serious or widespread disasters, some of these suppliers will be unable to deliver under their agreements or be subject to bottlenecks within the supply chain that limits availability. Working with vendors before the emergency can provide an understanding of their business model and how resilient the business is under normal circumstances.

Questions about operational resiliency, especially surrounding the supply chain, and business continuity plans can be requested and reviewed during the request for proposal or request for qualifications. This information informs the stakeholders about the suppliers' capabilities and limitations and provides worthwhile insight into the strengths and potential liabilities of a supplier/partner. This vital information can be much more valuable than just a price list. Deploying a strategy of redundancy and having multiple suppliers to choose from reduces this risk, but having suppliers spread out geographically (even internationally) could also reduce the risk during localized events.

Action Items

Here are some steps to discuss with the procurement office within the organization:

- **Supply chain assessment** – An assessment of the supply chain used by an organization will include things such as spend analytics (looking at where the dollars go) to identify the suppliers that are most integrated into the organization's

business processes. These suppliers will be the most crucial for business continuity and identifying critical functions for supplier diversification. When all the various internal departments involved with the procure-to-pay process are involved and made aware of the critical role played in the business continuity plan, proactive approaches can be made (in conjunction with business impact analyses) to make internal processes resilient.

- **Strategic development** – Value creation is important for every department or unit within the organization. Procurement Departments and all the members of the supply chain have the capability to shape a sourcing strategy for overall productivity and business continuity. Contingency plans, disaster recovery plans, and business continuity plans, including those that require alternative or emergency suppliers, are established, along with key performance indicators (KPIs) for internal process efficiency, vendor performance and compliance, etc.
- **Performance management** – To hold suppliers accountable for the goods and/or services being provided, KPIs are closely monitored and utilized to adjust the sourcing strategy should suppliers no longer add value to the organization's supply chain. Contracts and agreements drafted for suppliers should include the expectations for performance as well as communication frequencies and standards to keep the relationship trending in a positive direction for the mutual fulfillment of each organization's goals.

Disaster purchasing does not in itself need to be a disaster. The mechanisms and relationships established for day-to-day operations can be leveraged during disasters to cooperatively add value to the acquisition of required goods and/or services. The goal of supplier management is being able to call the local sales representative, refer to them by their first name, and tell them any challenges. Then, two organizations with sufficient resources work together to solve a mutual problem, not solely for the sales commissions but to help a business partner. Global supply chain challenges and opportunities will continue to evolve and change at an ever-increasing frequency, and organizations with secure and resilient supply chains have a distinct advantage in the future global marketplace.

Brian McGinley, DBA, is the Section Chief, Finance and Administration for the Texas Division of Emergency Management and came to work for the agency in July 2021 from another Texas A&M University System member, Texas A&M University-Commerce. There he served as the contracting officer for the organization and worked as a business analyst to help department streamline business processes for efficiency and automation. Prior to joining the university, he began his career as a procurement specialist at the National Aeronautics and Space Administration (NASA) Shared Services Center at Stennis Space Center in Mississippi and became a lead for the NASA Small Business Innovation Research and Small Business Technology Transfer Program, processing over 1,000 contracts and purchase orders with an annual program spend of over $100 million.

Domestic Preparedness Journal

EDITORIAL ADVISORS

Bobby Baker
Hazmat-WMD Specialist

Nathan DiPillo
Critical Infrastructure Analyst, California Governor's Office of Emergency Services

Michael Breslin
Director, Strategic Client Relations, Federal Law Enforcement, LexisNexis Special Services Inc.

Gary Flory
Agricultural Program Manager, Virginia Department of Environmental Quality

Bonnie Butlin
Co-Founder and Executive Director, Security Partners' Forum

Kay C. Goss
Senior Advisor, VS4S

Kole (KC) Campbell
Executive Advisor, Enterprise Security Risk Management (ESRM), Bolante.NET LLC

Charles J. Guddemi
Statewide Interoperability Coordinator, Operations Division, DC Homeland Security and Emergency Management Agency

Timothy Chizmar
State EMS Medical Director, Maryland Institute for Emergency Medical Services Systems

Robert C. Hutchinson
Director, Black Swans Consulting LLC

Domestic Preparedness Journal

EDITORIAL ADVISORS

Rodrigo (Roddy) Moscoso
Executive Director, Capital Wireless Information Net (CapWIN)

Melissa Hyatt
Chief of Police, Baltimore County Police Department

Kyle R. Overly
Advisory Specialist Master, Deloitte

Joseph J. Leonard Jr.
CDR, USCG (ret.)

Laurel Radow
Chair, Transportation Research Board (TRB) Standing Committee on Critical Infrastructure Protection

Ann Lesperance
Director, Northwest Regional Technology Center at the Pacific Northwest National Laboratory and Northeastern University Seattle

Daniel Rector
Emergency Planner, "I Love U Guys" Foundation

Anthony S. Mangeri
Assistant Vice President, Mitigation and Resilience, The Olson Group Ltd.

Richard Schoeberl
Program Chair & Director of Graduate Studies, Criminology and Homeland Security, The University of Tennessee Southern

Audrey Mazurek
Director, Public Health Preparedness, Homeland Security, and National Resilience, ICF

Lynda Zambrano
Executive Director and Founder, National Tribal Emergency Management Council