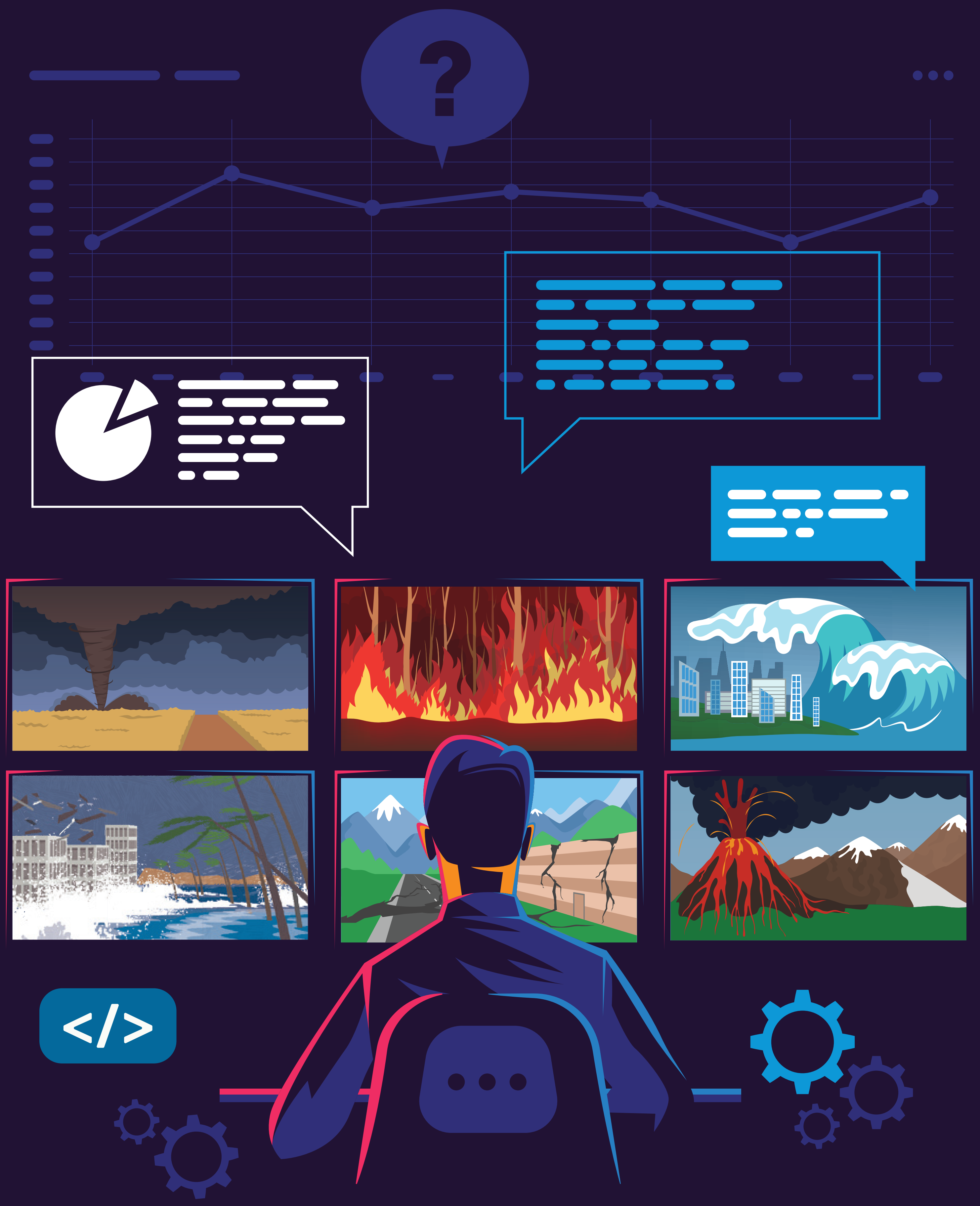
journal
OF GOVERNMENT FINANCIAL MANAGEMENT®

SPRING 2021 VOL. 70, NO. 1

Connecting with Citizens

AGA®



Streamline Disaster Recovery with a Risk-Based Approach

By Daniella Datskovska, Stacey Floam, Ray Kulisch and Matt Lyttle

A community is ravaged by disaster. Schools, fire and police stations, municipal buildings are all gone, roadways impassable. The all-too-familiar scene in the aftermath of a catastrophe ignites a response in the United States from the Federal Emergency Management Agency (FEMA). Through its public assistance (PA) program, FEMA distributes critical funding to help jurisdictions rebuild public services and restore safety and normalcy.

FEMA's mission demands a balance of speed in grant disbursal with appropriate reviews and inspections to minimize fraud, waste and abuse. However, when COVID-19 health guidance created complications for on-site inspections, FEMA shifted to a virtual or desktop validation process to inspect damaged public facilities. As a result, fraud risk for PA disaster grants ballooned.

Desktop Validation

After a federally declared disaster, jurisdictions seeking reimbursement for repairs to public facilities must submit a list of damages to FEMA. Until COVID-19, FEMA staff visited each location to verify damage, cause and estimated repair cost. But the risk of the disaster workforce contracting coronavirus led FEMA to replace in-person site visits with virtual inspections. Called "desktop validation," the virtual process requires disaster relief applicants to inspect their facility, take photos of damage, collect repair receipts, and submit the evidence online. FEMA must rely on this information to validate the damage without a physical inspection.

Fraud has always been a risk in disaster relief. Inability to witness, evaluate and assess damage in person — unfiltered, unmanipulated, and with a complete set of physical data inputs — makes fraud detection and mitigation increasingly difficult. As FEMA considers ongoing desktop validations, fraud is of great concern. Decision-makers must consider and address root causes and elements of fraud, such as opportunity, pressure and rationalization. They must also leverage lessons learned from past instances of fraud, handled with traditional on-site inspections, with innovative solutions to streamline disaster recovery and PA grants management.

Decisions in favor of desktop validations over on-site inspections must take into account the risk of fraud, waste and abuse, the available technology solutions with "trust but verify" capability, and the processes for desktop validation. Efficiencies gained from decreasing on-site inspections should continue after the pandemic, but only with investment in standards and tools to prevent fraud, waste and abuse. If successful, the refined processes will speed up disaster recovery.

FRAUD IN NUMBERS

- In the Association of Certified Fraud Examiners (ACFE) *COVID-19 Benchmarking Report*, 77% of respondents said they had observed an overall increase in fraud, with one-third noting the upsurge was significant.[1]
- An estimated 1% of claims related to Hurricane Katrina, totaling more than $1 billion, were fraudulent.[2]

Lessons Learned from Disaster Relief

After a disaster, applicants seek as much funding as possible from the federal government. An applicant's share of eligible costs under FEMA's PA program, plus the ineligible costs, can run into millions of dollars. FEMA works with applicants to fund the eligible work but avoid paying for damages not caused by the federally declared disaster. The following examples of cases in which fraud was identified and mitigated involve instances noticed by a human being, not a system or technology. It is likely that for every example, many more fraud cases went undetected.

Example 1: Funds Requested for Damages not Caused by the Disaster

During 2017 hurricane recovery efforts, multiple representatives of one state attempted to pad their PA-funded permanent work projects with damages not caused by the disaster. The representatives pressured grant sub-recipients to claim additional damages that were actually the result of previous events or poor maintenance. They actively led recipients to enlarge the damage inventory by pointing to an item that was not listed and asking, "What about this? This *could* have been damaged by the disaster." FEMA site inspectors so frequently reported the scenario that the state organization required additional training. The attentiveness and diligence of the site inspectors saved the federal government millions of dollars in fraudulent claims.

Example 2: Duplicate Damage Claims

After Hurricane Sandy, one recipient was caught submitting damage claims for several police cars that had already been claimed as total losses and paid out in a previous disaster. Fortuitously, the insurance specialist working on behalf of FEMA on the grants application also worked the previous disaster for the same grantee, remembered the claim, and denied the duplicate claim.

RISK IN MASSIVE AID PROGRAMS

History has shown that immediate and direct access to massive amounts of federal aid brings with it the risk of fraud, waste, abuse and mismanagement. At least 10% of emergency aid could be lost to fraud, which could total tens of millions of dollars.[3]

Example 3: Fraudulent Claim for Poor Maintenance

Following Hurricane Harvey, an applicant claimed a fuel tank had been damaged by the storm. In fact, the contractor who performed the repair work indicated on the contract that the tank failed because of worn, cracked gaskets and seals. Also, the paperwork noted that an inspection performed immediately after the disaster showed no water intrusion into the fuel tank. The PA program delivery manager (PDMG) concluded the fuel tank damage was the result of poor maintenance, not flood damage, and removed it from the grant request.

In each example, people on the ground, bearing witness to the damage for submitted claims or trusting their personal experience, mitigated fraud. In desktop validation, these elements are limited or unavailable, and claims adjustors must depend on applicants' photographs, videos, and testaments to disaster damage. However, it is possible to develop and improve desktop validation to be comparable to on-site inspections by real people with working senses and instincts.

Viable Technology Solutions

Without doubt, the nation's current system of on-site inspections requires an enormous staffing footprint, significant data tracking, and extensive records management. If any of these components is lacking after a major disaster, the recovery process will slow, and economic impact will exacerbate. Even well-managed inspection processes can take months to begin and years to complete. When considering the complex and costly nature of the existing system, it is easy to see why desktop validations and other technology solutions would interest emergency managers.

INSPECTION DELAYS

An on-site inspection of a facility damaged by a hurricane can easily take an entire workday to complete, followed by hours of paperwork. In many instances, a site inspector conducts the initial visit 60 or more days after the disaster. The delay makes it difficult to discern disaster damage versus damage caused by other events or poor maintenance.

Aerial and Satellite Photography

Most jurisdictions maintain public facility data within their geographic information system databases. By overlaying this information with weather data, emergency managers can make high-probability assumptions on the damage status of facilities in their jurisdictions. This technology has long been applied in response to hurricanes, tornadoes and floods. By adding a third layer of data from post-event aerial and satellite photography, local officials and site inspectors can quickly validate earlier assumptions and begin the disaster claims process. Since this practice is already in use, the factor limiting widespread adoption in site inspections may be outdated policy rather than technology.

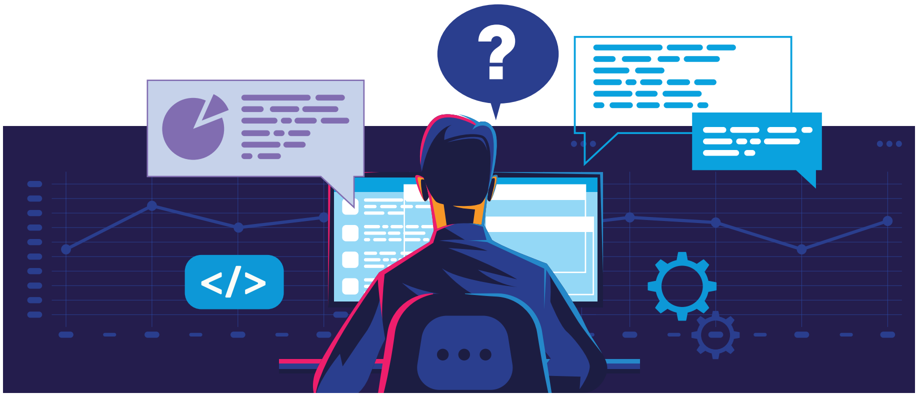
But when millions of dollars are on the line, is an aerial photograph enough to mitigate fraud risk? Local, state, tribal and federal officials may agree that a facility has been damaged in an event, but the cost of repair requires negotiation among several levels of government, further delaying the recovery process. Algorithms that combine local building material costs, labor rates, and disaster surge pricing can quickly produce an average reconstruction cost per square foot for virtually any public facility rebuilt with FEMA PA grants. When an average cost is settled, site inspectors can pair the aerial photography method with verification inspections to significantly reduce the number of site visits and still reduce fraud risk.

TECHNOLOGIES TO COMBAT FRAUD

- Geospatial data and remote sensing technology can be valuable tools for damage assessment and catastrophe response.
- Weather analytics and geospatial location data can help determine which policyholders were affected by an event and confirm the date of loss.
- Remote sensing can improve loss response times by communicating post-loss conditions directly to the inspector.
- Technologies, such as artificial intelligence, produce highly accurate claim scores and reason codes, necessary to detect questionable claims quickly and deliver critical insights to investigators.
- Screening data against prior applications for duplicates and against public databases for potential red flags, such as non-existent businesses, prior thefts, applicants involved in prior fraudulent activities, etc.

Smart Buildings

New "smart" or "connected" facilities are wired with sensors that routinely send data on building conditions to building engineers. Existing facilities can be retrofitted with similar technology to monitor conditions for humidity, temperature, air pressure, seismic activity, and even pests. If the technology could be tuned to monitor likely disaster damage, it could help site inspectors. For instance, just as firefighters gain immediate access to a fire alarm control panel when responding to an event at a commercial building, a site inspector could gain immediate access to a facility damaged by



disaster. Unlike the firefighter, the site inspector may be able to accomplish the mission from a desk five states away, if sensor data is accurate, secure and available remotely.

FIGHT FRAUD WITH TECHNOLOGY

According to an ACFE survey, only 30% of organizations use technology to fight fraud. Innovations permit inspections in a fraction of on-site time. When fortified with other fraud detection tools and applied in a balanced risk profile, they offer a path toward faster disaster recovery.

Set Risk Appetite to Prioritize On-Site Inspections

An example of the way risk appetite factors into everyday life and informs decisions is found in driving. Someone who drives a car every day implicitly accepts the risk of an automobile accident. The person has decided that the value of going to a destination is greater than the risk of being involved in an accident and accepted the risk.

The Committee of Sponsoring Organizations of the Treadway Commission defines risk appetite as the types and amount of risk an organization is willing to accept in pursuit of value. It applies throughout an organization and targets risk that must be taken toward long-term strategies. It is also connected to the creation and preservation of value in an organization.[4] Risk appetite is indifferent to industry and whether an organization resides in the private or public sector. It seeks answers to questions such as:

- What risks do we want to take and why?
- What risks do we want to avoid and why?
- Are uncertainties inherent in our business model that we need to understand?
- What future developments or emerging risks could alter the assumptions underlying our strategy?[5]

Although risk appetite is an invaluable decision-making and strategic capability, data suggests a low level of implementation in the public and private sectors. Many organizations like to think they have zero risk appetite, but it is not feasible. In FEMA, where inherent risk exists in its mission, defining risk appetite would boost the agency's effectiveness in achieving its mission. It would be the amount of risk FEMA is willing to take to increase efficiency and speed in disbursing grant funds and to enhance or sustain the protection of personnel through desktop validations.

RISK APPETITE STATEMENTS

- 42% of federal agencies have defined risk appetite statements. Only 8% of them communicate and integrate their statements into strategy and decision-making.[6]
- 31% of respondents in the "State of Risk Oversight" survey said they believe their organization has "mostly" or "extensively" articulated risk.[7]

FEMA might consider developing criteria to prioritize on-site inspections, based on its risk appetite. One approach would be comparing currently requested grant dollars to past requested grant dollars, based on disaster type, state, and other characteristics that may influence the cost of damage. FEMA could set a threshold of differential between the average past grant dollar amount and the currently requested dollar amount to determine if desktop validation is acceptable — or if an on-site inspection is warranted, as illustrated in **Figure 1**, which uses a 30% differential as the threshold for requiring an on-site inspection.

Risk appetite should not be a stagnant risk measure; it should be regularly reviewed to ensure organizations continuously maintain a risk appetite that supports strategy and business objectives. Using risk appetite as a tool to decide between desktop validation and on-site inspections may prove to not only mitigate fraud, but also expedite disaster relief.

Use Risk-Rankings in PA Funding

Individuals and businesses are risk-ranked each time they request a loan from a financial institution or apply for car insurance, for example. Factors such as credit history, location, employment, and other criteria determine whether funds or a policy are awarded, as well as the terms, rates and overall cost of the product. FEMA could use a risk-ranking approach for jurisdictions that receive PA funds. It might focus on tracking instances of fraud in mitigation, identifying trends in jurisdictions, and deciding between desktop validation and on-site inspections in jurisdictions with an implied or increased likelihood of fraud.

The first step in risk-ranking would be tracking instances fraud — mitigated or realized — on a jurisdictional basis. When an adequate data set becomes available after one to two years, it could be analyzed by

Figure 1. Desktop Validation vs. On-Site Inspection, Based on Risk Appetite

DESKTOP VALIDATION AND ON-SITE INSPECTION CRITERIA FOR HURRICANE DISASTERS — CATEGORIES 1 – 3

Facility Type	County	State	Average Past Grant Dollar Amount	Input Current Requested Grant Dollar Amount	% Difference Between Average and Current	Desktop Validation or On-Site Inspection (On-Site Inspection required if % difference is greater than +/-30%)
School	1	LA	$500,000	$2,000,000	300%	On-Site
Police Station	1	LA	$200,000	$250,000	25%	Desktop Validation
Fire Station	1	LA	$300,000	$250,000	(17%)	Desktop Validation
Police Station	2	LA	$250,000	$500,000	100%	On-Site

jurisdiction for trends in frequency, dollar amounts, and scenarios. FEMA could flag jurisdictions with a higher implied likelihood of fraud risk and require on-site inspections. The solution could mitigate the overall risk of fraud and might increase the speed at which relief is awarded in jurisdictions with lower risk.

A New Normal in Disaster Relief

The risk of fraud in disaster relief may remain present and elevated in post-pandemic operations, but FEMA can take mitigation measures and continue to provide rapid relief to communities through innovation. FEMA could then increase financial, operational and staffing efficiencies yet remain protected from COVID-19 with desktop validation. By implementing other new technologies, creating a risk appetite statement, setting tolerance thresholds, and conducting risk-ranking, FEMA could develop a new normal in disaster relief.

Endnotes

1. ACFE. "Fraud in the Wake of COVID-19: Benchmarking Report," Sept. 2020.

2. Silverstone, H. et al. "Preventing Disaster Fraud: The Winds of Change," *FVS Eye on Fraud* (a quarterly publication of AICPA Forensic and Valuation Services) Winter 2020.

3. Guidehouse. "The Importance of a Robust and Proactive Controls Environment During a Time of Crisis," *Insights & Experience*, Apr. 10, 2020.

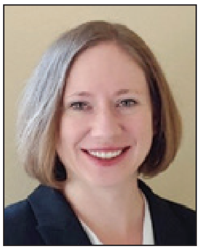
4. Martens, Frank and Larry Rittenberg. "Risk Appetite – Critical to Success: Using Risk Appetite to Thrive in a Changing World," Committee of Sponsoring Organizations of the Treadway Commission, May 2020.

5. Protiviti. "Defining Risk Appetite: Integrating Corporate Performance Management and Risk Management," Early Mover Series, 2012.

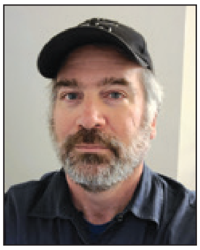
6. Guidehouse and Association for Federal Enterprise Risk Management. "Federal Enterprise Risk Management 2020 Survey Results," https://www.aferm-survey-results-2020.com

7. Beasley, Mark S., Bruce C. Branson & Bonnie V. Hancock. *The State of Risk Oversight: An Overview of Enterprise Risk Management Practices*," (11th Edition), North Carolina State University Poole College of Management, Apr. 2020.

Daniella Datskovska, PMP, CISA, CFE, RIMS CRMP-Fed, is a director in the Guidehouse Advanced Solutions practice with 20 years of consulting experience, leading organizations through change. Her expertise includes enterprise risk management (ERM) to meet complex organizational, governance, operational, compliance, and risk management challenges. She is President-Elect of the Association for Federal Enterprise Risk Management (AFERM).



Stacey Floam is a senior consultant in the Guidehouse ERM Advanced Solutions group. After a decade in risk management and compliance roles for financial institutions, she now supports public and private sector clients with ERM and general risk assessments. She holds the COSO ERM Certificate, Lean Six Sigma Yellow Belt, and serves as treasurer of International Social Service-USA.



Ray Kulisch is a managing consultant in the Guidehouse National Security segment and supports federal, state and local clients responding to federally declared disasters. He has deployed to more than a dozen disasters in support of FEMA's Individual Assistance, PA, and Continuous Improvement programs and managed FEMA systems development. He now manages the FEMA PA Technical Assistance Contract contract and serves as a subject matter expert on several FEMA and related projects, including COVID-19 response.

Matt Lyttle, an associate director in the Guidehouse National Security segment, supports federal clients with strategy and transformation projects to build disaster resilience. Matt has deployed to lead disaster response, recovery, and capacity-building activities throughout the U.S. and Latin America over the past 15 years. He held various positions in FEMA's National Preparedness directorate and supported the U.S. Senate Homeland Security and Government Affairs Committee.