



# **Unmanned Aircraft Systems: Benefits & Consequences – Part 1**

## **Proceedings of Roundtable**

*By Charles J. Guddemi & Catherine L. Feinman*

*Note: All comments provided in these proceedings reflect the opinions of the individuals and do not necessarily represent the views of their agencies, departments, companies, or organizations. Quotes within the report without acknowledgment were made anonymously by roundtable participants.*

# **UNMANNED AIRCRAFT SYSTEMS: BENEFITS & CONSEQUENCES – PART 1**

## **PROCEEDINGS OF ROUNDTABLE**

Fifty-five years ago, Bill Hanna and Joe Barbera created the cartoon, “The Jetsons,” which depicted the family of the future. Debuting in 1962, the imaginative creators provided futuristic comforts for their characters, which included: people movers, tube travel, vehicles that folded up into brief cases for parking purposes, home computers, internet, microwave ovens, CT x-ray for medical purposes, cellphones, and speed limits of up to 2,500 miles per hour. Fast-forward to today, the nation seems to be on a path to become the Jetsons. As roadways become more congested, one logical alternative is to go up. The National Aeronautics and Space Administration (NASA), coordinating with the Federal Aviation Administration (FAA), currently serves as the lead agency in developing the Unmanned Aircraft Systems (UAS) Traffic Management system to facilitate low-altitude UAS operation.

Since they were developed, UAS (commonly known as drones) have transitioned from very large, very expensive products (reserved for military and spy agencies for weapon delivery or reconnaissance purposes) to much smaller, less expensive, commercially available models (used by hobbyists, industry, scientific research, and the first responder community). Today, UAS are affordable, come in different shapes and sizes, and have different capabilities, which have made them one of the hottest gift ideas for the past couple years. With many benefits and requests for them to be integrated into the national airspace, this trend is expected to continue well into the future. In addition, individuals or groups can use UAS as disruptive technology for nefarious purposes such as invading privacy, advancing criminal enterprises, or conducting terrorist activity.

Still, for many, UAS are seen as toys, something to play with in the backyard or at the local park. For others, this is a new threat to personal security, corporate assets, and critical infrastructure that will force those on the ground to always look up. Two key events sparked debate for further regulation and mitigation of this technology and its capabilities: the UAS incursion onto the south lawn of the White House in January 2015; and the

manned, small, low- and slow-flying gyrocopter that landed on the U.S. Capitol's West Lawn in April 2015.

U.S. families may be on the path to becoming the Jetsons of the year 2062, but a lot still has to happen in terms of regulation, policy, counter capabilities, education, and continued development of the UAS Traffic Management. A roundtable discussion addressed the benefits and threats the nation faces as this technology evolves and becomes integrated into the daily operations of various industries.

#### **Four Key Discussion Points**

On 6 June 2017, 28 senior subject matter experts representing various communities of interest – defense; first responder (law enforcement, fire, emergency medical services); intelligence; science, technology, and industry; critical infrastructure; and legal – convened for a roundtable discussion to address the benefits and threats of unmanned aircraft systems (UAS). While discussing this evolving technology, which is rapidly becoming integrated into the daily operations of various industries, four key discussion points emerged.

First, before discussing how to approach the issue of UAS, participants shared the history behind this technology and identified the threats UAS pose and the existing capabilities they offer to jurisdictions. By understanding the threats and capabilities UAS technology introduces, emergency management and public safety personnel can take steps to mitigate the threats and leverage the capabilities.

Second, regulations and technology will continue to evolve. Therefore, participants addressed the ongoing need to review emergency preparedness and response plans and procedures to reduce any potential policy gaps at all levels of government. By recognizing technological developments related to UAS, emergency management and public safety personnel can stay current on changes in regulations, or become drivers for regulation changes to address their operational needs.

Third, participants shared their knowledge of current and potential threats, capabilities, and current legislation that emergency preparedness and public safety professionals can

leverage to reduce security gaps and promote resilience in a changing threat environment. By knowing how to enforce current rules and mitigate existing threats, these professionals can better protect the communities they serve.

Fourth, participants agreed that UAS technology is in a rapid growth mode that is unlikely to slow in the foreseeable future. By examining existing research and understanding how this technology can facilitate operations, public safety and emergency management agencies are improving search and rescue, damage assessments, and other critical operational tasks to minimize threats and maximize public safety and security.

### **Understanding Threats & Capabilities**

Since the late 1990s and early 2000s, threats from the air and from remote-controlled devices have existed. These threats range from benign to catastrophic. For example, United States Park Police (USPP) officers stationed in New York when the 9/11 attacks occurred encountered a series of incidents that raised great concern. Within a six-week span in 2001: (1) a paraglider crashed into the Statue of Liberty torch on 23 August; (2) four airplanes crashed into the twin towers in New York City, the Pentagon in Washington, D.C., and a field in Shanksville, Pennsylvania, on 11 September; and (3) a remote-controlled aircraft with a four-foot wingspan washed up on the beach area on the backside of Liberty Island on 1 October. Although the remote aircraft was not found to have been involved in any wrongdoing, the incident sparked new public safety concerns from law enforcement officials in the wake of the 9/11 terrorist attacks.

Although UAS was not a significant issue during 9/11, the threat and potential benefits of [such technology have evolved](#) since that time. At the Washington, D.C., branch of the USPP, officers respond to many incidents and special events. On 16 September 2013, for example, a multi-aviation response to the Washington Navy Yard shooting required careful coordination to ensure the safety and security of everyone involved. Helicopters certainly played a critical role that day, and remain the best option for some operations (e.g., hoist rescues, medical evacuations, and SWAT insertions). However, under some circumstances, UAS could provide safer, more efficient, and less costly alternatives. In the “fog of war,” an overhead perspective offers several benefits:

- Helps clarify communications between many mutual aid assets;
- Identifies the “good guys” and “bad guys”;
- Operates when vehicle gridlock on the ground occurs; and
- Conducts building searches through windows and on rooftops.

On 19 June 2014, it became illegal to launch, land, or fly over any National Park Service (NPS) property (under 36 CFR 1.5(f) “[Violation of Closure and Public Use Limits: Launching, Landing, or Operation of Unmanned Aircraft](#)”). In collaboration with FAA, U.S. Department of Homeland Security (DHS), United States Capitol Police, and other agencies, USPP recognized the growing threat that UAS could pose and the agency’s need to develop plans to mitigate these potential threats. For example, restricted airspace enables USPP to safely operate its aviation assets during large-scale events, but these assets are limited (e.g., helicopter limits ability to get too close to concerts and venues where acoustics can be affected and weather can restrict flight plans).

Despite NPS restrictions, UAS continued to operate on NPS sites in Washington, D.C., New York City, and San Francisco, California. Following is a list of just some of the incidents that occurred in 2015. All of these events highlighted the need for further planning, coordination, and mitigation efforts:

- 26 January – UAS landed on the White House south lawn;
- 15 April – a gyrocopter landed at the U.S. Capitol;
- 12 June – a UAS flew into the chamber of the Jefferson Memorial;
- July – a British national launched a UAS from Liberty Island, circled the Statue of Liberty, took high-resolution video, and landed undetected;
- July – a week after the Liberty Island video, the same British national flew the UAS over the Washington Monument;
- 19 July – a toy quadcopter crashed into the Statue of Liberty; and
- 16 August – a quadcopter flew from Liberty State Park to Liberty Island (after park closure) then to Ellis Island (individual was arrested after NPS personnel saw the aircraft overhead).

Identifying the reasons for these security breaches have helped officials thwart other UAS attempts, but more is still needed. Several reasons that require ongoing planning efforts include the need to:

- Define roles and responsibility for airspace;
- Develop stronger deterrents for violating laws (e.g., in D.C., the fine is only \$110);
- Provide screening staff with proper training and education (e.g., screeners at Battery Park are busier than many airport terminals); and
- Ensure that security personnel recognize potential threats (e.g., the UAS taken onto Liberty Island went through an x-ray machine, but was considered a toy).

## **National Plans**

The federal government currently faces the challenge of securing the skies, safely and securely integrating UAS into the national airspace system, and countering UAS use by potential attackers – whether criminal, terrorist, or hostile foreign government. Another challenge the government faces is ensuring community safety as the commercial industry continues to expand (e.g., delivering packages with UAS). The Obama and Trump administrations have both emphasized the need to safely integrate UAS technology into the National Airspace System, while ensuring privacy, civil rights, and civil liberties.

On 15 February 2015, The White House released “[Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems](#).” That memorandum addressed two key topics: (1) UAS policies and procedures for federal government use – privacy protections, civil rights and liberties protections, accountability, transparency, and report; and (2) multi-stakeholder engagement process. On 2 August 2016, the administration made “[New Commitments to Accelerate the Safe Integration of Unmanned Aircraft Systems](#)” and announced \$35 million for new UAS research funding through the National Science Foundation over the next five years. To address issues related to the integration of UAS into the National Airspace System, the White House Office of Science and Technology Policy and the Association for Unmanned Vehicle Systems International brought together key stakeholders of the public and private sectors as well as academia for a workshop on “[Drones and the Future of Aviation](#).” Breakout sessions focused on three areas: (1) low-altitude airspace management/UAS Traffic Management; (2) expanded operations for small UAS; and (3) comprehensive integration to create a smarter National Airspace System.

The current administration has also expressed plans to expand the integration of UAS as well as to enact legislation that counters the illicit use of this technology by malicious actors. On 22 June 2017, the White House Office of Science and Technology Policy held another event that brought together industry leaders and federal agencies to address [“American Leadership in Emerging Technology.”](#) Legislation has been proposed to help close the gap between what the law currently allows and what law enforcement officers require to effectively counter these systems when misused. On 7 September 2017, in a statement of administration policy in response to the [National Defense Authorization Act for Fiscal Year 2018](#), the administration addressed concern that counter UAS was not included. The statement noted the need to develop a legal framework to guard against misuse and enable effective oversight and privacy protections. The new proposed legislation has a federal focus, but also recognizes that state and local law enforcement agencies may need countermeasures as well. The best and most appropriate way to build capabilities beyond the federal government is still not certain. However, current legislation does not preclude the delegation of their use to appropriate local authorities if used for official use, with federal oversight, and with properly trained operators.

On 25 October 2017, The White House released a [“Presidential Memorandum for the Secretary of Transportation,”](#) which focused on the establishment of a [pilot program for UAS integration](#) within 90 days, with proposals being accepted by the FAA by that time. The three-year program has three key objectives: (1) to test and evaluate models for involving state, local, and tribal governments in developing and enforcing federal regulations for UAS; (2) to encourage UAS development and safety testing for new and innovative concepts of operation; and (3) to develop federal guidelines and regulatory decisions for UAS operations. This document expresses the federal government’s commitment to promote the following: promote innovation and economic development; enhance transportation and workplace safety; improve emergency response as well as search and rescue functions; and use the radio spectrum competitively and efficiently.

The White House National Security Council also plans to coordinate federal-level working groups on how to look at this emerging technology. The working groups will examine how UAS technologies may be applied effectively from a research and development aspect and

from an ethical standpoint. One of the biggest challenges, though, is how to build response policies relevant to federal, state, local, and private actors. To address this challenge, more dialogue is needed with all key government and nongovernment stakeholders.

### **Legal Considerations**

During the roundtable, Brendan Groves represented the Department of Justice (DOJ). He serves as a Senior Counsel in the Office of Legal Policy. He also serves as the chairperson of the DOJ UAS Working Group, and the chairperson of the Interagency Legal Working Group on Countering UAS. Groves noted that, although UAS technology and its uses involve many “thorny legal issues,” it is important that security and innovation move forward together.

Before law enforcement agencies take action against malicious uses of UAS within their jurisdictions, they should become familiar with a variety of laws that may apply to counter-UAS activities. The “dozens” of laws that may apply include, but are not limited to the following:

- [Wiretap Act](#), which restricts interception of electronic communication;
- [Pen/Trap Act](#), which restricts interception of non-content information;
- [Computer Fraud and Abuse Act](#), which restricts unauthorized access to protected computers; and
- [Aircraft Sabotage Act](#), which criminalizes acts that damage or destroy aircraft.

***Dozens of laws apply to counter-UAS activities, including the Wiretap Act, Pen/Trap Act, Computer Fraud and Abuse Act, and Aircraft Sabotage Act.***

Another roundtable participant added the importance of creating a new working group with regard to keeping civil liberties, civil rights, and privacy at the forefront. The authority enacted by Congress must be consistent with the Constitution and must include other stakeholders into the conversation. Although executive privilege limits inclusion of industry in some federal working groups, private sector partners could contribute by participating in roundtables, advisory committees, and other outreach efforts that federal agencies use to reach vendors.

Groves emphasized that these potential legal issues may affect both the public and private sectors. For that reason, both sectors could potentially benefit from legislation providing

relief from problematic statutory constraints. Congress has already granted limited relief to the Departments of Defense and Energy, authorizing them to protect nuclear and space-related assets from malicious uses of UAS. However, that legislation does not apply to other federal departments and agencies. The private sector similarly lacks any sort of statutory relief at this time.

There was consensus among participants that it is unclear how and when Congress will address the need for counter-UAS legislation, in part because the issue implicates the jurisdiction of a variety of different congressional committees. Thus, even if one committee exercises leadership with respect to a particular aspect of this issue, the underlying legislation may still require approval from, or consultation with, another committee. However, one participant stated that it is conceivable that Congress could take a stair-step approach: authorize federal departments and agencies to execute counter-UAS activities, then analyze the lessons learned, and use those lessons to extend the authority in some form to state and local governments and private industry.

Another participant asked Groves what latitude state and local governments have to regulate UAS flights, if any. He explained that this was an issue for FAA, rather than DOJ, and mentioned the [FAA's public paper](#) on the issue. In general, the FAA has taken the view that some state and local laws regulating UAS operations may impinge on the FAA's authority to regulate flight within the national airspace. If state and local laws are challenged, a court would determine their legality on a case-by-case basis. As UAS technology and use cases continue to develop, the federal government and state and local governments will need to arrive at a shared understanding of the types of laws permissible to make at that level.

### **National and International Security and Intelligence Concerns**

The global terrorist threat has become more complex with the introduction of UAS technology. David Cohen, retired deputy commissioner of intelligence for the New York City Police Department and retired Central Intelligence Agency (CIA) deputy director for operations, pointed to an example where the Islamic State group effectively used an unmanned aerial vehicle (UAV) to attack Mosul by dropping bombs. This threat, though, is not new. He described how the United States and other countries became aware of this

technology and began developing it for reconnaissance purposes as early as the 1980s. Then-Director of the CIA James Woolsey brought in the private sector to develop the technology in order to reduce cost and time. As with many new technologies, oversight and bureaucratic concerns arose over the program. The first significant UAV deployment by the U.S. government was in Bosnia.

Since 2013, Tom Hewitt, chief of the UAS Threat Integration Cell at the U.S. Department of Homeland Security's Office of Intelligence and Analysis, has been working on the UAS threat environment and examines how adversary intent and capabilities are changing. The diverse and increasing legitimate uses for UAS (e.g., emergency response, media and surveillance, disaster response, pest control, terrorist propaganda), as well as related safety and security concerns, have evolved over the past decade. With both legitimate and nefarious uses, UAS technology poses opportunities and challenges as federal, state, local, and private sector partners strive to integrate UAS into the national airspace system. At the federal level, whole-of-government partners are focusing on ways to promote safety/resilience and address emerging security concerns.

Brandon Sasnett, who was previously the director of unmanned systems at TechINT Solutions Group LLC, provided insight on the defense industry and the growing threat that UAS pose to military defenses and critical infrastructure. He described ways in which the U.S. Department of Defense is addressing threat groups that have used UAS technology, with the Islamic State group having the most sophisticated technology and most confirmed kills using UAS. A significant concern is terrorist organizations weaponizing UAS, so government efforts must examine the full system, which includes the human component, the ground control station, and the unmanned aerial vehicle (UAV). The type of threat a UAV poses can rapidly change depending on what it is carrying (e.g., a custom-made fixed wing aircraft carrying explosives or other weapons). With the low-cost, very effective deployment of UAVs, countermeasures must be implemented now even though such measures have not yet been perfected.

Other points that were made clear at the roundtable were the need to engage and prioritize intelligence, exploit actionable intelligence, experiment with various technologies, and

educate/train staff to better understand threats and their full capabilities. Since it is not possible to protect everything, low-cost, no-cost countermeasure plans should be implemented for resilience. Terrorist organizations often prefer commercially available UAS rather than military grade or high-end technology because they are inexpensive and easily available. As such, defense agencies must stay current on what commercial vendors are doing. With each new technology, the process of engaging, exploiting, experimenting, and educating must be repeated.

***Since it is not possible to protect everything, low-cost, no-cost countermeasure plans should be implemented for resilience.***

### **Controlling the Airspace**

The mission of the FAA's Law Enforcement Assistance Program ([LEAP](#)) is to prevent persons from committing actions against the National Airspace System and threatening national security. The FAA's Senior Technical Advisor Andy Nahle and LEAP Manager Janet Riffe described the functions of LEAP (e.g., law enforcement liaison, intelligence dissemination, investigations, operations) and the FAA's role in protecting the nation's airspace from UAS (e.g., assistance with drafting local ordinances, outreach and training, technical assistance). However, the FAA's success in this area depends on law enforcement notification of incidents to ensure that proper action is taken. The FAA plans to expand its outreach through webinars and training videos to be distributed widely among law enforcement agencies. In addition to "no drone" campaigns to prevent the use of UAVs in certain locations, outreach information also includes how law enforcement agencies can set up their own UAS programs.

***Roundtable participants discussed the confusion over the rules and laws that exist, how they are implemented and enforced, and by which agency or jurisdiction.***

Participants discussed topics related to "no drone zones," which currently apply only to the takeoff and landing sights. In addition, several participants noted that it is not well established or practical for local agencies to set up their own no drone zones because of resistance from local communities. Although the FAA has authority over all airspace, the authority to take off and land remains at the local level. This division of authority thus creates a poor

environment for people to be compliant with UAS usage. Roundtable participants discussed the confusion over the rules and laws that exist, how they are implemented and enforced, and by which agency or jurisdiction. One participant described how these discrepancies can actually create a “sense of lawlessness.” For example, although UAVs are aircraft, there is currently no federal statute for how to enforce their use. If someone shoots down a UAV that he or she feels is a disturbance or infringement of privacy, there may be no legal ramifications or deterrents for others to take similar actions. FAA enforces civil regulations, and it is up to law enforcement agencies to take action on criminal violations.

Another discrepancy addressed involved incident scene management. Incident commanders still do not have control of the airspace over the scene – despite some incident command documentation claiming otherwise. To avoid hindering response efforts in such scenarios, Charles Raley, senior attorney for the Enforcement Division of the Office of the Chief Counsel at the FAA, stated that local agencies and the FAA should discuss preemptive measures to answer the question about who is in charge of the airspace. Also, although there is no set altitude, the FAA’s Drone Advisory Committee is looking into the roles and responsibilities of state and local jurisdictions and the types of arrangements that can be implemented. He stated that FAA’s national airspace system includes protection of people and property on the ground and includes operations of aircraft in any airspace. However, there are no set parameters for regulatory authority.

***Incident commanders still do not have control of the airspace over the scene – despite some incident command documentation claiming otherwise.***

The discussion highlighted problems that can arise without a clear line between the FAA’s airspace control and local law enforcement’s ability to protect privacy. For instance, property owners and local municipalities can use no drone zones, but have no authority once UAVs are launched. In another instance, temporary flight restrictions require prior FAA approval and are enforceable by the FAA. In yet other cases, such as the Super Bowl, no drone zones and temporary flight restrictions may be implemented in tandem. Local actions allowed by law are still unclear in cases where protecting local privacy would require controlling airspace. To address the many lines of ambiguity, the FAA has a federal

framework to move aircraft efficiently and safely, while considering preemptive measures as needed. Different entities have different interests, so the FAA must analyze preemptive issues on a case-by-case basis.

Of course, there is no such thing as a clear line on any of these issues. With the rules being incredibly complicated, operators and law enforcement agencies have trouble understanding them. Justin Towles, vice president of regulatory and legislative affairs at the American Association of Airport Executives (AAAE), warned this could create a “culture of noncompliance,” where recreational operators may not provide the required notification to airports when flying in areas at heightened risk for air-to-air collisions. He recommends a change in policy and in the law. By clearly defining the roles and responsibilities of key stakeholders, a collaborative effort would avoid assumptions about what law enforcement needs and wants from their local and federal partners. AAAE, which represents over 6,000 airport executives, has taken steps toward building new UAS policy. These activities are related to safety, security, and expanded use of UAS, which include: serving on UAS rulemaking committees; serving on the FAA Drone Advisory Committee Subcommittee and task groups; co-chairing the 26 Coalition for UAS Safety; managing an annual UAS Policy Conference; and offering UAS enforcement training to airport operators and law enforcement officers.

Participants agreed that additional guidance from the FAA would help address issues that arise from people operating UAVs illegally or nefariously, but they also need the authority to control such operations and ensure appropriate decisions are made. More support from governance for law enforcement is needed. Without that support, law enforcement agencies must respond to incidents, but without having anything in the “toolbox” to disable a UAV in the airspace. Some effort is being made from the National Institute of Standards and Technology (NIST) and other key stakeholders to assist with tracing UAVs back to the owners. Measures that could be implemented include adding serial numbers to all UAVs, requiring registration for purchases, and establishing safety statements to be included in sales of UAS. Although such measures would help law enforcement officers conduct threat assessments and prevent incidents before they occur, wording of documents related to

UAVs limit enforcement abilities even when the constitutionality of registration is not questioned.

*The conclusion drawn from roundtable participants is that policies and legislation is needed to address two components: (1) clear legal enforcement authority; and (2) understanding of liability.*

The conclusion drawn from roundtable participants is that policies and legislation is needed to address two key components: (1) clear legal enforcement authority; and (2) understanding of liability. Without these components, there will be either hesitation or overreach to enforce UAV use at the local level.

### **Technological Developments**

In the early 1960s, when the animated sitcom “The Jetsons” debuted, the creators had foresight that technology would make life a lot easier. Their imagination for industry and commercial developments in technology introduced the possibilities that could exist, and in some ways now do. Like “The Jetsons” creators, emergency planners and responders now need to imagine the possibilities that UAVs introduce.

Diana Marina Cooper, senior vice president of policy and strategy for Precision Hawk, described the company and how it collaborates with commercial enterprises and government agencies as an end-to-end UAS solution provider. Cooper shared the company’s goal of developing a scalable framework to support full and safe integration of UAS into the national airspace. Cooper also shared NASA’s vision that [UAS Traffic Management](#) infrastructure development and deployment is necessary to enhance safety and security while increasing access to airspace. Precision Hawk developed its LATAS platform in response to market need for solutions that could lower operating risk by providing situational awareness, airspace information, tracking, and detect-and-avoid features.

Public-private collaborative efforts such as the FAA Pathfinder Program and the NASA UAS Traffic Management program are beneficial for addressing UAS integration and safety challenges. The research conducted by Precision Hawk under Pathfinder culminated in the company receiving a waiver to conduct commercial beyond-line-of-sight operations and will serve as a critical resource for the FAA in developing the regulatory framework for

beyond-line-of-sight operations. Cooper recommended increasing communication between industry and law enforcement agencies in order to adequately address the public safety and security aspects of UAS. She noted that, as UAS become more pervasive, public education efforts surrounding safe operations of UAS also need to increase.

A representative from the aircraft industry expressed concern on multiple fronts – from the unintentional consequence of a UAV entering a plane’s engine air intake to a deliberate strike on the plane’s structure. Many changes have occurred over the past three years, but counter-UAS technology is a potential solution to prevent a UAV and other aircraft from occupying the same space at the same time. The aircraft manufacturing industry’s primary areas of focus include: the global regulatory framework that it works within; safety control measures for aircraft (e.g., cybersecurity and air traffic management); and standards and regulations that support certified aircraft. The promulgation of UAS in the global airspace raises concern for commercial aircraft carriers on multiple fronts: controls in place; transfer of protection overseas; ability to clear the airspace in an emergency; and roles and responsibilities of stakeholders. Although aircraft are designed to prevent cyberattacks, companies continue to address counter efforts and controls needed to mitigate potential threats.

Jonathan Hunter provides counter-UAS solutions at Department 13 Inc. The company’s counter-UAS efforts include “protocol manipulation” technology that provides the ability to take over and control the threat. This control and/or non-jamming technology can be useful in the entertainment industry, where UAVs can disrupt sporting, concert, and open-air venue events, where protecting airspace is critical for the safety and security of participants and host organizations.

Ramin Baseri, a program manager at CACI-BIT Systems, described another form of technology (SkyTracker™) that can intercept signals to identify and mitigate UAS threats. This technology has evolved over the past decade and works by monitoring the RF spectrum in the area, sounding an alarm if a UAS is present, and mapping the UAS activity. Demonstrations have shown effective interoperability without affecting airport operations. It can be difficult to stay ahead of threats and technology, but technology companies are

advancing counter-UAS capabilities to address the threats. UAS threat is not a simple problem to solve, it introduces potential issues that must be addressed.

Craig Marcinkowski, director of strategy at Gryphon Sensors, described how his company is addressing both sides of the UAS debate: UAS security (i.e., public safety, airports, critical infrastructure, and stadiums) and UAS integration (i.e., deliveries, disaster relief, agriculture, and mapping). In New York State, Gryphon's Project U-SAFE (awarded at the end of 2015) acknowledges that UAS use will continue to expand and considers four primary areas of focus: a 50-mile "validated" UAS Traffic Management corridor; beyond-visual-line-of-site (BVLOS) commercial UAS operations; critical infrastructure protection applications; and the need for a National UAS Standardized Testing and Rating facility (NUSTAR). Phase I of this project was just been completed (including mobile UAS Traffic Management capability [Mobile Skylight™] – launch date in June 2017). Phase II will include a dynamic and interactive 50-mile corridor to validate UAS-enabled safety cases and protect critical infrastructure (will be completed by end of 2018).

Gregory Walden, formerly served as FAA chief counsel, now serves as aviation counsel with the Small UAV Coalition and teaches aviation law. He shared the mission of the coalition and its top policy priorities. The coalition advocates for a regulatory framework that permits commercial and philanthropic consumer UAS operations beyond line of sight, autonomous, and to scale, but that cannot happen unless these operations can be done safely and reliably with security protections in place. This will require legislation, registration of all UAS operators, as well as identification and tracking capabilities to provide real-time accountability to FAA and law enforcement. He added that a UAS Traffic Management system will deliver enormous benefits to safety, security, reliability, and privacy, and thus working to test and deploy UAS Traffic Management should be a high priority. He also noted that the administration's [National Defense Authorization Act](#) proposal is a move in the right direction and, with certain revisions, could enlist the UAS industry's support.

John Resnick, policy lead for UAS manufacturer DJI, shared some historical information about UAVs and the importance of knowing what this technology can and cannot do. A unique quality of this technology is its flight-controlling ability. Early versions of this

technology required a lot of skill to operate but, with global positioning systems, advanced flight controllers, stabilized cameras, and other sensors, these aircraft can achieve a high level of stability and ease of operation. As a result, people outside of traditional aviation are adopting UAS as a valuable tool and platform for accomplishing a broad variety of tasks. This means, though, that the threat pool could also expand. With the combination of technology and its varied uses and users, it is critical that people operate these systems in a responsible manner. However, Resnick further stated that this ongoing continuous process is only as effective as the regulations that are put in place.

Participants concluded that, despite information systems, geofencing, and technological deterrents, the pilot is ultimately responsible for the aircraft. Information systems are not enforcement systems, and geofencing only deters those who are not authorized to fly in specific areas. UAS technology and UAS deterrents will continue to evolve, with a trend toward smaller UAVs. Resnick ended with a warning to be careful about expectations that UAS operators have less rights than people using other technologies.

### **Enforcing Rules and Mitigating Threats**

Law enforcement agencies regularly face enforcement challenges when there is no clear law behind their actions. Sergeants Kenneth Burchell and Mark Varanelli of the United States Park Police (USPP) described these challenges in the context of UAS. For example, in January 2013, someone saw a homemade UAS being operated on National Park Service property, but the operator did not think he was doing anything wrong because some officers saw the operator in the past and said nothing. Since then, the reporting process has improved, with 60 documented incidents, 21 UAS platforms identified, and 22 citations issued. Of the 48 operators contacted by the USPP, most were males with an average age of 33. The transient base of visitors to National Park Service properties makes enforcement more difficult because many visitors do not understand why the restrictions are in place. The USPP are undergoing the long process of educating its personnel, with the main goal of stopping the UAS nuisance problem because it is taxing on the resources of small agencies like the USPP. Burchell, who is the assistant commander for the USPP helicopter unit, operates multiple helicopters. The USPP's responsibility for responding to incidents includes the following necessary steps:

- *Coordination* (e.g., multiple aircraft from multiple agencies operating together in close quarters) – None of the UAS on Park Service property were spotted by aircraft, but rather by officers on foot or in automobiles.
- *Reconnaissance* – There is a need to provide information to the incident commander, which may include foot, automobile, and aerial options.
- *Containment* – The incident should be confined to a specific area.
- *Rescue and Medivac* – A rapidly developing incident requires fast response (e.g., use of different aircraft, radios).

With 122 federal prisons and 185,000 inmates, counter-UAS is also a concern for prisons, as described by Todd Craig, chief of the Office of Security Technology (OST) for the Federal Bureau of Prisons. UAS offers operational use cases for contraband interdiction, threat detection, and tactical response, but this technology is also being widely used for criminal and gang activities and as a way to circumvent more traditional physical security measures. Intelligence reports and criminal investigations indicate that UAS are now a security threat to federal prisons. As such, there is a need for countermeasures to mitigate this threat. Measures the OST has taken to address the UAS security threat include: engaging technical experts in government and industry; participating in UAS working groups; and conducting market research to evaluate UAS technologies. By having legislative authorities in place and a whole of government approach, law enforcement agencies can better protect against and mitigate potential UAS threats. In addition, Craig noted that, once counter-UAS technology is legal, funded, and deployed, the technology could be effective and cost effective.

The Federal Bureau of Investigation (FBI) also is taking steps to counter UAS when it presents a threat to safety and security, which currently includes passive detection systems. James Price, supervisory special agent and program manager of the Counter-UAS Program for the FBI, agreed with other participants that the confusion over law enforcement's authority needs to be addressed on all sides to ensure mutual understanding. Although electronic identifications could be helpful in protective systems, those with nefarious intent would likely find ways around such systems. However, having some type of beaconing or operator identifying system, as well as UAS Traffic Management, set up would still help to point out any anomalies. As terrorists adapt, so too must the response. This includes reexamining laws and definitions on the books that are lagging behind the technology.

## **Leveraging New Technology**

It is critical for emergency preparedness professionals to develop an understanding of the threats and capabilities that UAS technology has to offer, as well as how to ensure safety and security when the technology is being used. However, this evolving technology also offers beneficial tools that agencies and organizations can leverage to facilitate both daily and emergency response operations. The roundtable participants finished the discussion by addressing the planning and useful applications related to UAS integration into their operations.

## **Manufacturers**

Before purchasing a UAS product, as with any new technology, agencies and organizations must consider their organization's operational needs (e.g., clarity in expectations, requirements, scalability, flexibility), the key features of the UAS (e.g., site survey, tactical kits, autonomous mode, protocol manipulation), and the cost benefits for integrating this new technology. In terms of detection techniques, participants recommended developing an understanding of the main uses, their drawbacks, and the markets to determine individual needs, for example:

- Software-based systems facilitate system updates;
- A multi-sensor approach provides more clarity;
- Detection techniques offer different ranges of detection, with acoustics being shorter range versus electronic detection; and
- A layered sensing approach provides greater detection and identification capabilities.

Challenges arise when there is not a comprehensive set of operational requirements, or there is a lack of understanding or appreciation of cooperative and non-cooperative UAS operations. Participants also pointed out that UAVs do not always behave as designed, so lacking this knowledge makes it more difficult to counter the technology when it is not behaving as designed. To date, a fundamental understanding of the technology is still lacking in the operational community. Information can be fed into the machine, but it will only work if the machine is performing as designed.

Roundtable participants expressed concern about the federal government not yet properly defining what is allowed and not allowed. Despite the government being involved at the front end of defining UAS requirements, industry and response agencies must be better informed about these requirements, so industry can meet these needs and response agencies can leverage the capabilities. In addition, there need to be realistic expectations of what is considered “successful” when developing and using UAS. One participant stated that systems do not need to be 100% fail proof to be extremely useful, but the level of acceptable risk has not yet been defined. He concluded that, although legislation is important for driving requirements, requirements actually should be leading the legislation.

Another participant urged that, before identifying requirements, it is critical to identify the risk that people are willing to take. UAS raises concern because of its use by terrorists or by people with minimal knowledge of how to safely operate the technology. Fatalities from a physical strike are just one risk, but others include information transfer (where it is going), storage (where and how the information is being stored), and protection (how the information is being guarded from bad actors). Experimentation can start to build an understanding of how the technology can be and is being used.

The challenge for UAS manufacturers is to make technology that consumers want to buy, but they cannot control how this technology will be used outside the designed purpose.

***Industry worries about 99% of users, whereas law enforcement officers must worry about the other 1%. No solution can be designed that will satisfy every eventuality.***

UAVs can facilitate law enforcement to locate or track criminals, but they can also help criminals spot law enforcement. As mentioned earlier, the end users are ultimately responsible for their own actions, regardless of which tools are used to carry out those actions. The growing ease of access makes UAS a growing threat, but preventing its use is not a viable solution. An aircraft manufacturer summed up the challenge, “At some point, you have to make assumptions. We have to assume that all pilots are good actors [to ensure the functioning of aviation operations].” He further explained that industry worries about

99% of users, whereas law enforcement officers must worry about the other 1%. No solution can be designed that will satisfy every eventuality.

### **Private Sector/Large Venue Facilities**

The FBI and other federal agencies have taken steps to work with and educate the private sector on how to secure their assets and address the problem of distrust and privacy concerns (e.g., FBI's Project Touchstone). One law enforcement participant described the challenge of using UAS technology because of the public trust issue. He suggested placing high priority on using telemetry systems to provide proof of surveillance efforts and operating hours to better inform the public about where the camera was pointed and where/when it was flying. On the question of surveillance, laws should be based on the violation rather than the technology being used.

From the perspective of Dan Delorenzi, vice president of safety and security services for Metlife Stadium, UAS are almost entirely viewed as a homeland security threat. When manufacturers of costly detection and interdiction systems approach him, it is his responsibility to do the research and obtain financing, but he also needs to consult DHS. However, he has found that DHS does not want to give advice about what does and does not work. To address this issue, Metlife Stadium has proposed a memorandum of understanding with DHS to make the stadium a live test bed for detection and interdiction methods. Delorenzi's frustration is that the federal government has capabilities to protect people, but those same capabilities are not being recommended for protecting people who regularly fill stadiums. Law enforcement agencies are encountering similar issues.

UAS technology could be beneficial for private sector and large facilities, but potential customers like those involved in the roundtable discussion become frustrated without definitive answers from federal authorities. Although more is being done in Congress at the federal level than even a year ago, a lot more still needs to be done. Todd Craig of the Federal Bureau of Prisons has been part of a working group with the Department of Justice for about 18 months on legislative authority. He asserted that new legislative authority that they are working toward would grant the Department of Justice, DHS, and other federal agencies the authority to better detect and mitigate potential threats.

Michael Hopmeier, president at Unconventional Concepts Inc., countered some of the roadblock arguments by stating that it is not entirely true that testing cannot be done because of laws or that systems cannot be used because of regulations. Waivers could be granted and testing can be done in some areas, but he has seen a lack of will to make these efforts. DHS's Tom Hewitt acknowledged that testing of UAS detection and mitigation technology has occurred and is ongoing across the whole of government, but reiterated that near-term, widespread use of these systems in the homeland environment is constrained by statute and the emerging nature of UAS detection and mitigation technology. Although the majority of UAS reports are non-malicious in nature, encounters over critical infrastructure, such as outdoor events, can present an unacceptable risk to public safety.

***“We aren’t integrating drones, drones are integrating us,” said DHS’s Tom Hewitt.***

Whether communication, messaging, or gaps between local and federal stakeholders, frustrations certainly exist on both sides of the end user/private sector and government discussion. UAS integration is a complicated long-term process, with many unknown or unclear components to consider. This technology has taken on a life of its own, so the government and users are now faced with learning how to manage rather than control the process. Hewitt summed the need for continued collaboration across federal, state, and private sector partners by saying, “We aren’t integrating drones, drones are integrating us.”

### **Emergency Management/Public Safety**

Despite frustrations from many stakeholders, some emergency management and public safety agencies have found ways to leverage UAS technology within their operations. Harry Humbert, deputy assistant secretary of public safety, resource protection, and emergency services at the U.S. Department of Interior (DOI), described success stories of UAS across disciplines. In 2016, the White House’s Office of Science and Technology identified DOI as a leader in aircraft systems for government services: science, safety, savings, and service. The DOI uses UAS for various interests (e.g., detection, classification, interdiction over public lands) and concerns (e.g., wildfires, sensitive areas, growing recreational desire). In addition to spreading UAS operation awareness, DOI has identified the cost effectiveness of UAS use versus manpower for tasks such as fire reconnaissance, mapping, and search and

rescue, especially in areas where it is dangerous to send helicopters or rangers. [DOI's goals for its UAS program](#) include plans to increase its collaboration as well as number of pilots and other personnel across the nine DOI bureaus.

In many jurisdictions, first responder agencies are implementing UAS into their operations. Charles Werner, acting deputy state coordinator for Virginia Department of Emergency Management (VDEM) and Charlottesville, Virginia, fire chief (retired), described VDEM's UAS team structure. Each of Virginia's regional teams will have remote pilots, which provides greater technology and capabilities across the region and state (including regional state teams like the combination team of the York County, Virginia, Sheriff's Office & Fire Department). Werner's extensive involvement in national UAS committees and public safety organizations (including chair of the [National Council on Public Safety UAS](#), where stakeholders can register to participate) have given him varied opportunities to explore the possibilities as well as the potential problems associated with UAS. However, the commonality for all stakeholders is public safety, with four critical guidelines: safety, security, reliability, and legality. The number of uses for UAS in the public safety realm is almost limitless. As more agencies (e.g., public safety, media) implement this technology, though, there need to be protocols or standards in place to manage multiple agencies flying UAVs simultaneously through an effective UAS Traffic Management system.

Werner appreciates the FAA's movement forward, but would still like to see more templates to guide the Certificates of Authorization ([COA](#)) process and bridge gaps between the COA and [14 CFR Part 107](#) (Title 14 Code of Federal Regulations) requirement (there are things that can be done in one but not the other). Additionally, Werner hopes that applications for COAs and Special Government Interest applications (SGI, formerly known as eCOAs) will be automated for faster processing and to reduce inconsistencies. Flexibility and expeditious processing in an emergency are necessary. Also, geofencing limitations with some UAS for public safety have proven problematic if validation is needed each time. He stated that the public safety sector is presently working with industry. Public safety is also interested in working with industry to know more about emerging technology and to share public safety needs. More research could help answer questions such as, "Which sensors are best in

certain functional areas?” This dialogue will bring public safety and industry together for the development of mutually beneficial products.

From a public safety perspective, Werner pointed out that UAS has become an *essential* tool for public safety. UAS provides situational awareness that enhances incident management decisions, resulting in better and safer outcomes for citizens and responders. The [National Council on Public Safety UAS](#) website serves as a repository of UAS policies and procedures from local, state, and federal agencies for the purpose of information sharing/collaboration and advancing UAS in public safety.

Darren Price, who is employed in emergency management at the state level, shared his Naval Postgraduate School thesis research on, “[Unmanned Aircraft Systems for Emergency Management: A Guide for Policy Makers and Practitioners](#),” as well as his experience in emergency management, to highlight the many benefits of UAS for emergency management. Situational awareness, including damage assessments, is critical to emergency management, but emergency management is all too often an afterthought when introducing new technologies and FAA rules. As a supporter of UAS integration, Price advocates for local/regional UAS capabilities and advances the cost effectiveness of UAS from a public safety and emergency management perspective (e.g., rapid and deployable UAS technology within minutes, rather than waiting for aerial support missions via conventional fixed and rotary winged aircraft).

Price noted that public education is needed to increase understanding of how UAS technology can be used for public safety and emergency management missions. Funding is an issue for local and state agencies, as current funding sources (e.g., State Homeland Security Program and the Emergency Management Performance Grant) consider UAS to be part of the controlled equipment list. As such, these funding sources require different grant management and monitoring processes that limit the ability to leverage funds for the development and sustainment of local and state emergency management-based UAS programs. As part of his Naval Postgraduate School thesis research, Price developed a decision guide to lead decision makers and practitioners through the steps of developing and sustaining a UAS program. This decision guide has been advanced via professional

publications such as the *DomPrep Journal* and briefed at local and national UAS conferences, as well as to a North Atlantic Treaty Organization (NATO) Specialists' Meeting.

In the emergency management and public safety spaces, testing, education, exercising, and public engagement are critical areas for the establishment and sustainability of UAS that will establish a recognizable threshold for the acceptance of public safety UAS activities. The benefits of UAS programs for emergency management are evident. However, as with any new program, a consideration of liabilities, public perception, and cost analyses are needed before program implementation to ensure long-term operation and sustainability. The use of UAS will not replace the need for conventional aircraft missions for disaster response, but will rather serve as another tool in the toolbox for emergency managers.

#### **Academia/Research: The Studies and Finding**

With a wealth of different perspectives on the topic of UAS and how it can be used or misused, more research would help close the knowledge gaps. As a technical advisor to the D.C. Continuity of Government Counter-UAS Working Group and member of numerous national panels, Michael Hopmeier of Unconventional Concepts Inc. has conducted research on UAS, including helping to rapidly design and deploy a noncooperative system for a detect-track-kill exercise. The drone sniper program could track and hit UAS 1,000 feet away. The counter-UAS hit-and-kill rate rose from 30-40% (with three-four hours of training on flight simulators and a trained spotter) to 95% after just a few days. Hopmeier's research showed that most companies that have counter-UAS technology rely on radio frequency detection, but do not have third-party validation. As such, significant deficiencies were found in the range, size, and height of detection and lack of discussion about liability. Despite leaving the consumer responsible for evaluation of products, there are no or limited: procedures and practices to validate performance; algorithms of how data was collected and what was collected; and information about what was happening inside the control loops of the devices due to protection of proprietary data. His research focused not on evaluation of the technology, but what was needed to do the testing (report available on request).

Arthur Holland Michel, co-director of Center for the Study of the Drone at Bard College, helps stakeholders address the opportunities and challenges of UAS. As an “observer” without a direct stake in the UAS industry, the Center is an inquiry-driven organization (without a policy agenda) that supports a broad range of stakeholders and serves as a common ground for discussion based on reliable resources. [“Weekly Roundup”](#) newsletters on Mondays provide industry stakeholders with a common standard portrait of the UAS landscape. Key studies conducted by the Center include, but are not limited to:

- A broad survey of publicly listed localities that have adopted some form of ordinance (many ordinances typically restrict private UAS use);
- Study of about 350 public safety agencies around the country that operate UAS;
- Review of incidents that resulted in legal actions against use of UAS technology, as well as inconsistency in these rules; and
- Report on close encounters and intrusions of UAS, which was divided between “sightings” and “close encounters.”

Michel acknowledged two important caveats to UAS research. First, controversial topics such as UAS can skew results as perspectives differ. Second, studies today address today’s technology, but technology is constantly changing (e.g., better endurance, better autonomy). As such, futuristic thinking is needed to predict what could exist even a year or more from now. He closed by urging roundtable participants and other key stakeholders to try to understand the perspectives of those around them, “You have a lot more in common than is obvious.”

The roundtable discussion exposed the needs of both those in favor of and those opposing UAS technology. Federal stakeholders are concerned about how to create regulations and policies that can be effectively implemented by various stakeholders. Security personnel protecting large venues and critical infrastructure are concerned about weaponization of UAS technology. Manufacturers are concerned about restrictions and criminal uses that could hinder technological development. First responders are concerned about policy gaps to address UAS. From all perspectives, forward thinking is needed to keep pace with this rapidly evolving technology.

## **Key Takeaways & Recommendations**

The community stakeholders represented at the UAS roundtable are split between two viewpoints: (1) unmanned aircraft systems (UAS) represent threats to privacy, security, and public safety that need to be controlled; and (2) UAS are effective tools for public safety and disaster response. Both sides must be heard in order to bridge the preparedness gap that could otherwise widen as this emerging technology continues to evolve.

At the federal level, participants recommended that agencies should review and update the regulatory and statutory frameworks for UAS. They should clearly define agency responsibilities and requirements, and change any policies and laws to minimize confusion at the operational level. They should develop control systems to mitigate malfunctions or nefarious use, which includes requiring UAS equipment to be registered and electronically identifiable. In addition, federal agencies should designate a lead committee to address all UAS-related issues to ensure the safe integration of UAS into the public space, ensure civil rights and privacy are protected, and bridge gaps between federal and state/local legislation to increase compliance.

Participants recommended that preparedness and public safety leaders should be able to identify threat indicators that could lead to criminal activity and determine acceptable levels of risk. They also should be able to balance public safety response and private sector's right to use UAS through education and realistic expectations. This can be facilitated through collaboration with research institutes, mutual aid agreements, whole community roundtables and discussions, and working groups to discuss, test, and evaluate new technologies. By identifying agency requirements and removing reporting inconsistencies for UAS incidents, preparedness and public safety leaders can better adapt to a rapidly changing operational environment.

## **Roundtable Participants**

A special thank you to all the participants who contributed to this important discussion:

*Ramin Baseri, Ph.D., CACI*

*Ken Burchell, Sgt., Assistant Commander, Aviation Section, USPP*

*David Cohen, Retired NYPD Deputy Commissioner*

*Diana Marina Cooper, Senior VP of Policy & Strategy, Precision Hawk*

*Todd Craig, Chief of the Office of Security Technology, Federal Bureau of Prisons*

*Daniel Delorenzi, Vice President, Security and Safety Services, Metlife Stadium*

*Brendan Groves, Senior Counsel, Office of Legal Policy, U.S. Department of Justice*

*Charles Guddemi, Deputy Chief (Ret.), United States Park Police (USPP)*

*William (Tom) Hewitt, Chief of the UAS Threat Integration Cell, U.S. Department of Homeland Security's DHS Office of Intelligence and Analysis*

*Michael Hopmeier, President, Unconventional Concepts Inc.*

*Harry Humbert, Emergency Management, Department of the Interior, Deputy Assistant Secretary*

*Jonathan Hunter, CEO, D13*

*Craig Marcinkowski, Director of Strategy, Gryphon Sensors*

*Arthur Holland Michel, Co-Director, Center for the Study of the Drone, Bard College*

*Andy Nahle, Senior Technical Advisor, Unmanned Aircraft Systems (UAS), Office of the Deputy Administrator, Federal Aviation Administration (FAA)*

*Darren Price, State-Level Emergency Manager*

*James Price, SSA, Counter-UAS Program Manager, FBI*

*Charles Raley, Senior Attorney, Enforcement Division, FAA Office of Chief Counsel*

*Jim Remik, Security Supervisor, Skadden LLP*

*Jon Resnick, Industry – DJI Phantom*

*Janet Riffe, Program Manager, FAA Law Enforcement Assistance Program*

*Brandon "Sas" Sasnett, former Director of UAS Intel, Training, and Fabrication, TechINT*

*David Silver, Vice President, Aerospace Industries Association (AIA)*

*Justin M. Towles, Vice President, Regulatory and Legislative Affairs, American Association for Airport Executives (AAAE)*

*Mark Varanelli, Sgt., Assistant Commander, Intelligence and Counter Terrorism, USPP*

*Gregory S. Walden, Senior Advisor, MWC, McGuireWoods Consulting LLC*

*Charles Werner, Acting Deputy State Coordinator, Virginia Department of Emergency Management (VDEM); and Charlottesville, Virginia, Fire Chief (Retired)*

## **Roundtable Observers**

*Rebecca Adamcheck*, Unconventional Concepts Inc.

*Mark Adamchik*, Captain, United States Park Police

*Dennis Bosak*, Department of the Interior

*Robert Boyd*, Executive Director, Secure Schools Alliance

*Tim Butters*, WMD/CCA Coordinator, Virginia Department of Emergency Management  
Region VII/NCR

*Philip Cecere Jr.*, Captain, Prince William County Police Department

*Stephen M. Clark*, Superintendent, Flight 93 National Memorial

*Joseph Dolan*, Sgt., Metropolitan Police Department

*Robert Ehrich*, CEO & Founder, Slipstream Strategies

*Andrew Goldblatt*, Geospatial Information Unit Leader, Office of National Capital Region  
Coordination, FEMA

*Noel Goldstein*, CACI

*Kirk Griffin*, CTO, WGS Systems

*Elliott Grollman*, Commander, Special Operations, Federal Protective Service, DHS

*David Ihrle*, Chief Technology Officer, CIT

*Paul Joyal*, Managing Director, Public Safety, Homeland Security, Intelligence Practice, NSI

*Dave Matsuda*, Principal, Matsuda & Associates LLC

*Robert Mendenhall*, DTRA Contractor (Watermark Risk Management International LLC),  
J10NSE, Defense Threat Reduction Agency (DTRA)

*Gregory Monahan*, Major, United States Park Police

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

*Toni Palmer*, Portfolio Manager, Admiral Security

*Dave Parrish*, Director of CBRNE Programs, JGW

*Greg Pass*, Lt., Prince William County Police Department

*Chris Runde*, Director, Airport Innovation Accelerator, American Association of Airport  
Executives (AAAE)

*Andrea Schultz*, Strategic Security Policies and Programs, National Football League (NFL)

*James Shieder*, Special Agent, Amtrak Police Special Operations Unit

*Michael Stewart*, DHS SOPD, Commercial Facilities

*Dawn Thomas*, Associate Director, CNA's Safety and Security division

*Michael Tierney*, The MITRE Corporation

*David Tolson*, Sgt., Aviation Section, U.S. Park Police

*Wayne Wylie*, MPA, Disaster Response and Recovery Officer, Virginia Department of  
Emergency Management Region VII/NCR

[DomesticPreparedness.com](http://DomesticPreparedness.com)

IMR Group, Inc.

Severna Park, MD 21146 US

+1410/518-6900

[info@DomPrep.com](mailto:info@DomPrep.com)

© Copyright 2017, by IMR Group Inc. Reproduction of any part of this publication without express written permission is strictly prohibited.