UNMANNED AIRCRAFT SYSTEMS FUTURES SEMINAR

11-12 JULY 2017

UNMANNED AIRCRAFT SYSTEM FUTURES SUBCOMMITTEE

2017 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

TABLE OF CONTENTS

ACKNOWLEDGEMENTS **3**
BACKGROUND **4**
EXECUTIVE SUMMARY **5**
UAS PRESENTATIONS **6**
SCENARIO DRIVEN DISCUSSION (SDD)-OVERVIEW **13**
SDD, VIGNETTE 1: OUTDOOR EVENT / MASS GATHERING /SPORTING EVENT **15**
SDD, VIGNETTE 2: AREA SECURITY OPERATIONS – POWER GRID **18**
SDD, VIGNETTE 3: LARGE SCALE DISASTER RESPONSE **20**
APPENDIX 1: SEMINAR SCHEDULE DAY 1 ..... **22**
APPENDIX 2: SEMINAR SCHEDULE DAY 2 ..... **23**
APPENDIX 3: UAS COORDIANTION CELL CONCEPT **24**
APPENDIX 4: GLOSSARY **25**

ACKNOWLEDGEMENTS

The 2017 Analytic Exchange Program, Unmanned Aircraft Systems Futures Subcommittee would like to thank all the speakers and participants for generously offering their time, insights and experiences as part of the 2017 UAS Futures Seminar. The success of this effort is in no small part due to their willingness to contribute to ongoing discussions of safety and security aspects of UAS integration. A special thanks to the staff of the Department of Homeland Security Science and Technology Directorate's National Urban Security Training Laboratory in New York City for providing the venue and their willingness to host and support the UFS Seminar. This event would simply not have been possible without their assistance aiding in the near-endless and often-thankless administrative tasks that often go unnoticed.

Alas, there is nothing we can do about the commute in the New York-New Jersey metropolitan area.

BACKGROUND

The UAS Futures Subcommittee[i] is part of the Department of Homeland Security-Director of National Intelligence sponsored 2017 Analytic Exchange Program. The seven-month long program brings together private and public-sector partners and is intended to provide a range of perspectives to a range of challenging problems. Based on initial and ongoing discussions with 13 members of the Subcommittee over a six-month period, we chose to focus on small UAS (sUAS) capabilities in the near to midterm (out to 2020) for legitimate applications and explore areas which offer the potential crossover to malicious use.[ii]

The Subcommittee identified the integration of sUAS into security operations, as an avenue of identifying future use of sUAS capabilities and security concepts. Based off discussions with various US Government, academic and private sector partners, the Subcommittee assesses within the next three years sUAS will likely be part a routine part of security operations, multijurisdictional response, or large-scale disasters, and their overt presence these activities will require security managers to identify their requirements-both in terms of tasking public-use sUAS and managing compliant operations over their respective areas of operation. In preparing for this seminar, we sought out organizations that are using sUAS in their operations, as well as security managers and private sector partners to identify future planning requirements, and help inform future information needs.

To facilitate open discussion amongst participants, the Seminar was conducted under Chatham House rules.

[i] The UAS Futures Subcommittee is alternative referred to as "the Subcommittee" or simply "we "for the remained of this document.

[ii] See Appendix 4, Glossary for definition of small unmanned aircraft system (sUAS). For the remainder of this document the term UAS is used in lieu of sUAS.

EXECUTIVE SUMMARY

The Security Components of UAS Integration

As the integration of unmanned aircraft systems for legitimate commercial purposes moves forward in both global and domestic airspace, reports of UAS encounters across multiple critical infrastructure sectors challenge the ability to characterize benign, suspicions or malicious intent. While most reported UAS sightings within the United States are likely non-malicious in nature, they still typically require initial and investigative activities by security and law enforcement partners. In some instances, unauthorized UAS operations represent a risk to public safety and hinder or disrupt emergency response operations and occur across a range of security operation and critical infrastructure.

The security element of UAS integration is focused on minimizing the physical risk, either thru education, visual recognition, enforcement, or thru technical detection systems. In addition, the data security protocols for UAS operators within the public and private domain has emerged as a topic of interest.

Seminar Observations and Identification of Best Practices:

Over the course of the two-day Seminar, the Subcommittee noted best-practices for UAS integrated operations and their security planning considerations. Public and private sector security responders are a source of best security practices as these entities are encountering UAS during emergency response, public events or sensitive sites. These are summarized below, and expanded upon in greater detail throughout this document.

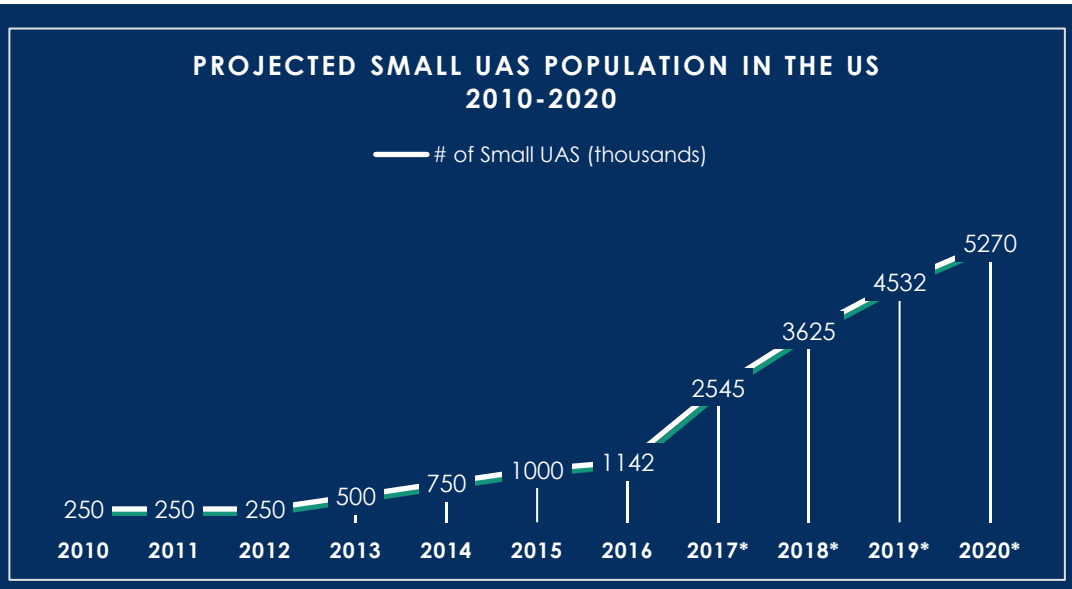
- Ensure user agreements are in place before UAS operations to avoid exposing propriety or sensitive information.
- Local-level UAS encounters and public safety UAS operators represent a wealth of lessons-learned, best-practices.
- Develop methodologies for characterizing reports of UAS near critical infrastructure.
- Understand organizational requirements and expectations for UAS operations.
- UAS detection operations include planning, require integrated data, established communications, to inform technical capabilities.
- There is no single system to counter malicious use of UAS, it's a layered activity requiring multiple technologies and planning.
- Develop and implement immediate actions and communication protocols for ground personnel sighting a potentially unauthorized UAS operation
- UAS capabilities are relying less on radio-frequency (RF) data links and sustained human-interaction.
- Future special-event planning considerations will likely include a UAS coordination cell to de-conflict public safety and commercial operations.

UAS PRESENTATIONS

Overview:

Day 1 was intended to provide all participants an opportunity to engage with various UAS operators and security personnel, and to share their experiences or perspectives on UAS integration. Over 40 participants and speakers were present for the day, including private sector partners from aviation, defense, professional sports, academic researchers, and public safety responders and emergency managers from the New York City area, as well as federal partners.[iii]

Global and Domestic Small UAS Overview:



Projected small UAS population, based off a combination of FAA reporting and possible systems resident within the US prior to 2015, and the start of small UAS registration. The includes both recreational and commercial use platforms.[iv]

[iii] Final presentation provided by a private sector UAS service provider was proprietary. The focus was on UAS solutions to enable Department of Defense, law enforcement, first responders and commercial customers to support tactical employment, security operations, emergency response, natural disasters and urban/rural search and rescue. While not summarized here, this presentation effectively segued into scenario driven discussions on day 2, focusing on integration into security operations.

[iv] Chart of potential UAS platforms is derived from USF research, publically available market research and FAA projections released in early 2017. We acknowledge that this data is likely the low end of the scale, and that actual number of all small UAS are likely much higher than represented here. This is intended to provide a baseline to measure the fidelity of assumptions over the scope of research, out to 2020.

Best Practice: Develop methodologies for characterizing reports of UAS near critical infrastructure. UAS reports and studies is maturing field and contain high uncertainty. Through and logical study of UAS reports can provide revealing data such as UAS capabilities, and trends that will support threat analysis and risk mitigation planning.

The initial briefing included an overview of domestic UAS regulations, global and domestic threat environments, examples of incidents of security concern, UAS consolidated reporting and trends out to 2020 and an overview of planning considerations, and countermeasures. Some key points include:

- Growth in the UAS market is likely the main factor behind increased reports of encounters and sightings over critical infrastructure facilities since 2012. Most of these sightings are likely non-malicious, but a portion could pose a risk to public safety or meet suspicious reporting criteria.
- Market forces are driving greater range and payload for a variety of legitimate applications. Depending on the specific application, the demand for smaller systems for specialized applications (e.g. confined space applications) are emerging.
- UAS have been integrated into criminal and terrorist operations across a range of tactical applications, this is likely to continue in the near-term.
- Current retail UAS are incorporating low-speed collision avoidance, and redundant data links for routine operations. It is likely that future systems will not require dedicated radio-frequency links for operation.
- In addition to physical security concerns, UAS operators and security planners should implement measures means to protect data collected during emergency and pre-planned security operations.
- There is no single physical countermeasure to deter or prevent unauthorized UAS encounters. Effective deterrence of unauthorized UAS operations include sustained outreach, education, development of safety and training standards, deliberate planning, as well as integration of technical detection capabilities.

Resources for UAS Integration or Best Practices:

- Federal Aviation Administration, "Law Enforcement Guidance for Suspected Unauthorized UAS Operations", March 2016
- Austin Fire Department, Robotics Emergency Deployment, "White Paper: Using Unmanned Aerial Systems During a Natural Disaster in Texas", 15 July 2015
- International Fire Chiefs Association, "Unmanned Aircraft Systems (USA) Toolkit", UAS Tactics, Policy, Technology and Regulations.

- National League of Cities, "Cities and Drones, What Cities Need to Know About Unmanned Aerial Vehicles", December 2016.
- National Council on Public Safety UAS, "Public Safety Resources" [Tab located at top of page]
- National Interagency Fire Center, "Drones & Wildfires Outreach Materials", July 2017

Small UAS in Fire Response Operations:

Best Practice: Understand Organizational Requirements. Unmanned aircraft systems can aid in supporting operations, but only if the organization has thoroughly considered their operational environment, as well as training, and sustainment requirements.

In March 2017, the Fire Department of the City of New York (FDNY) (link to video) began using a purpose-built, eight (8) pound tethered small UAS in response to a fire in the Bronx. The system allowed the on-scene commander to make informed decisions of firefighting operation on the roof of the structure, and aided the management of response operations. The tether provides continuous power and data links, preventing interference with radio frequency signals and is piloted by specifically trained FDNY firefighters. The FDNY platform has high-resolution and infrared video capabilities. FDNY works with the FAA prior to UAS operations for permission to deploy at night or in Class B airspace.

FDNY UAS Operations

Member of FDNY provides and overview of the concept of operations, planning considerations and real-world UAS support to firefighting operations.

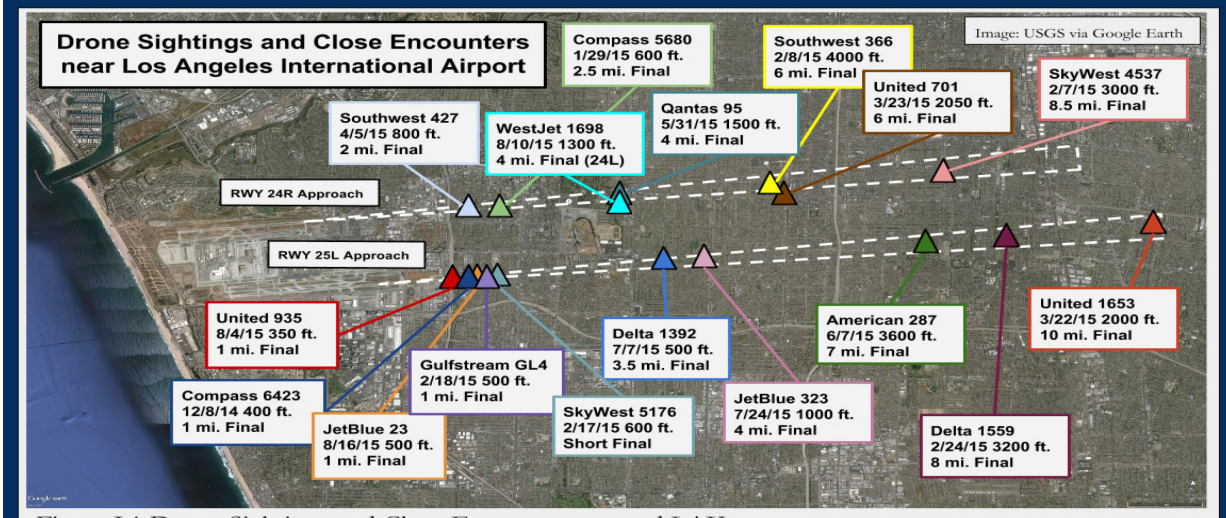
Public safety users, per Federal statue, can self-certify their UAS operators. At this time, there are no national training standards for public safety UAS operations or UAS capabilities. Each locality is responsible for conducting its own training, and select systems that are either purpose built or commercial-off-the-shelf.

UAS Academic Research:

Observation: UAS integration will require addressing of safety and security elements. These elements will be vital for commercial UAS users to transition from UAS integration to non-segregated airspace sustainment, with unmanned and manned systems operating in concert with each other.

Bard College Center for the Study of the Drone is an interdisciplinary research institution that examines the novel and complex opportunities and challenges presented by unmanned systems technologies in both the military and civilian sphere. The Center for the Study of the Drone (CSD) seeks to furnish stakeholders, policy-makers, and the public with the resources to engage in a robust public debate and develop policies that best address those opportunities and challenges. A full discussion of UAS and public safety/security are inextricable from the broader discussions concerning UAS integration. The dimensions of UAS integration include: nature of incidents; enforcement and countermeasures; regulations and collaboration/information sharing.

UAS Academic Research Presentation



Presentation from Bard College, UAS encounters by commercial aircraft[1]

As part of this effort, the CSD produces numerous in-depth studies, based off publically available information to provide a qualitative basis for discussion. For

example, an extensive review of Federal Aviation Administration, and other data sources as part of a 2015 study, "Drone Sightings and Close Encounters: An Analysis", approximately 35.5% of the 921 reviewed reports involving UAS met the criteria for a possible near-midair collision. A number of these incidents occurred on approach and outside of the five-mile exclusion area that should be observed by commercial and recreational UAS operators.

As part of a three-part series titled "Drones at Home", CSD researchers examined public safety users to determine the extent to which UAS are used to support emergency response operations. Key takeaways from the April 2017 publication:

- At least 347 state and local police, sheriff, fire, and emergency units in the U.S. have acquired drones.
- Local law enforcement departments lead public safety drone acquisitions.
- Consumer drones are more common among public safety units than specialized professional drones.
- A single manufacture, Dà-Jiāng Innovations (DJI), accounted for 80% of all public safety applications.

The March 2017 of publication "Drones At Home: Local and State Drone Laws" focused on the emergence of state and local UAS-specific regulations. A study of the statutory landscape found that 133 localities across 31 states applied additional rules, generally focusing on privacy, operations over private property and public safety. These rules may contravene federal authorities and may result in legal conflict between Federal and State authorities.

Turing the focus to technical measures to detect/defeat malicious use of UAS: there are no national standards for this technology, or how to measure its effectiveness; best practices are emerging at the local and tactical level, but have yet to emerge as a national set of best practices. A final paradox was offered for consideration: UAS integration cannot occur without security, but security is much easier with a properly integrated airspace.

UAS Data Security and Recovery:

Best Practice: Ensure user agreements are in place before UAS operations to avoid exposing propriety or sensitive information. UAS are collection systems. They not only contain data, but reveal what the operator is interested in. Retail UAS used by public and commercial operations may use off-site servers either thru user-agreements, and be supported third-party software, or hardware to store data obtained during UAS operations.

UAS are essentially collection platform. Video recorded by UAS receive a great deal of public attention via online aggregation of footage. Besides photo and videos, UAS's capture metadata, mission planning information, and flight logs. All this information has value by identifying and documenting intellectual property, critical infrastructure, new construction, emergency response operations. This has a two-fold consideration within the security space: data management policy and controls; and collection of UAS data for safety or investigation purposes

UAS users, particularly those who are utilizing 'turn-key' or off-the-shelf retail solutions, should be aware of third party collection and retention of data collected during UAS operations and develop appropriate policy to ensure protection of intellectual property or sensitive operations.

UAS Data Security Considerations

A UAS Futures Subcommittee member from Kovar & Associates provides an overview of UAS and data security considerations.

Suggestions for development of such policy include:

- Develop an explicit written policy: the supported agency maintains control of all data collected by a UAS service provider.
- UAS service providers turn over all data and metadata to the supported agency or can only use data collected during support operations with the express permission of the supported agency.
- Require approval of Chief Information Officer for in-house UAS procurement.
- For investigators or researchers, establish a process to access data from damaged or recovered UAS to aid in safety and security investigations.

In 2016, the National Telecommunications and Information Administration (NITA) convened a series of multi-stakeholder meetings resulting the publication May 2016 publication (hyperlink): "Voluntary Best Practices for UAS Privacy, Transparency and Accountability".

UAS Countermeasures: UAS Traffic Management & Counter-UAS

Observation: Detection and tracking technology is necessary to support UAS integration. No single system can perform all these functions. Information sharing mechanisms, data sharing processes planning, and communications will be essential elements to support development of UAS detection and tracking technology.

A private sector aerospace and defense company provided an overview of the development of Unmanned Aircraft System Traffic Management (UTM) and technical solutions to counter adversary use of UAS. The goal of UTM is to interface with traditional air traffic management systems ensuring interoperability and information sharing by leveraging highly automated, state-of-the-art technologies. Databases for registration, airspace maps, UAS flight planning, and regulations are necessary to provide an ecosystem for the fulfillment of manned-unmanned integrated airspace. An operational roadmap for UTM integration calls for UAS management in urban areas by 2020, with high density management by 2022 or beyond. This assumes that there are no roadblocks or regulatory frictions, and standardized UAS operations and safety cases can be developed to build requirements.

UTM and development of technical countermeasures to deter/defeat adversary use of UAS share a common theme: integration. Effective defense and countermeasures result from the convergence and interoperability between multiple technical and physical protection measures. An additional requirement of effective countermeasure development is that either electronic ID for UAS and geo-fencing must be standardized to facilitate reliable detection and categorization of complaint and non-compliant UAS. [Subcommittee note: Current concepts appear to be focused on electronic ID for commercial use-UAS. Recreational use-UAS do not appear to be part of this effort at this time.]

Finally, there is no single sensor solution to address the totality of countering malicious or unauthorized use of UAS. Instead, counter-UAS is a system of systems, ranging from standardized immediate response planning, complementary sensors; smart fusion and immediate notification; and decision-making tools that enable users to select the best means to mitigate or defeat potential threat UAS.

SCENARIO DRIVEN DISCUSSION (SDD)-OVERVIEW

Concept and Objectives:

UAS encounters, both malicious and non-malicious, within the Homeland Security Environment are centered on the assessment that UAS are expected to increase in the near-to-midterm. Members of the Subcommittee that participated in table-top exercises centered on UAS futures noted that the primary focus was on the physical security aspects, typically to inform regulation and technical solutions to detecting/deterring potential adversary use of UAS. We approached this scenario centered on the planning, information sharing and preparedness requirements to execute integrated UAS operations at a local, regional and national level. The intent was to identify information sharing needs, inform policy development, and identify training and technology requirements.[v]

To achieve this, we assumed that UAS integration in the near-to-midterm will incorporate UAS into security events and activities and minimized the role of technical detection solutions. The scenario based discussion had the following objectives:

Best Practices Emerging for Response to Unauthorized UAS During Fire Fighting Operations

UAS incursions over firefighting operations, National Interagency Fire Center[2]

Firefighting operations continue to be hampered by unauthorized UAS incursions. While the number of these incidents continue to rise nationwide, fire services have a set of best practices for interdicting unauthorized UAS operations. **These include a sustained public information campaign, knowledge of immediate actions on the part of ground and aircrews, established communication protocols with local law enforcement, and imposition of temporary flight restrictions and fines for unauthorized operations.**[3, 4]

[v] Scenario-based discussion is used in lieu of table-top exercise (TTX). While the format is comparable to a TTX in terms of design, the training audience was not specifically identified and no plans or procedures were being evaluated.

- Discover potential planning and response gaps
- Inform best practices for information sharing, security and integration efforts
- Explore possible future security applications and concerns

Assumptions:

The following scenario assumptions were provided to participants in order to frame a realistic future environment.

- Timeframe is mid-late 2020
- Unmanned Aircraft Traffic Management: in testing, but not deployed
- Beyond-line of sight operations in daylight hours authorized (video applications only); experimental corridors authorized
- Registration requirements reauthorized in late 2017
- Over six (6) million systems in operation
- Countermeasure employment limited to detection/tracking at National Special Security Events; Special Event Assessment Rating 1 & 2; limited use at outdoor sporting events and entertainment venues
- Significant incidents involving UAS near aircraft or as a weapon have occurred. This included one disrupted domestic plot involving a small unmanned aircraft with an explosive payload, and two confirmed collisions with aircraft.

SDD, VIGNETTE 1: OUTDOOR EVENT / MASS GATHERING /SPORTING EVENT

Vignette 1, actions during unknown UAS encounter

Outdoor Event: A weekend-long activity, Special Event Activity Rating-4, with over 100,000 expected attendees including a concert, fireworks show, and sporting exhibition match. No temporary flight restrictions were imposed. A local UAS service provider was contracted to provide footage of the event. Additionally, public safety UAS assets were on site.

Discussion and Exploratory Questions:

Security Planning Requirements

- Intelligence
- Operations/Operating Conditions
- Communications
- Additional Support Requests
- Liability
- Emergencies

Drone Service Provider Requirements

- Weather Information
- Safety Protocols
- Communications
- Additional Support Requirements
- Liability
- Emergencies

Exploratory Question: Can current airspace planning for manned aircraft integration be leveraged?

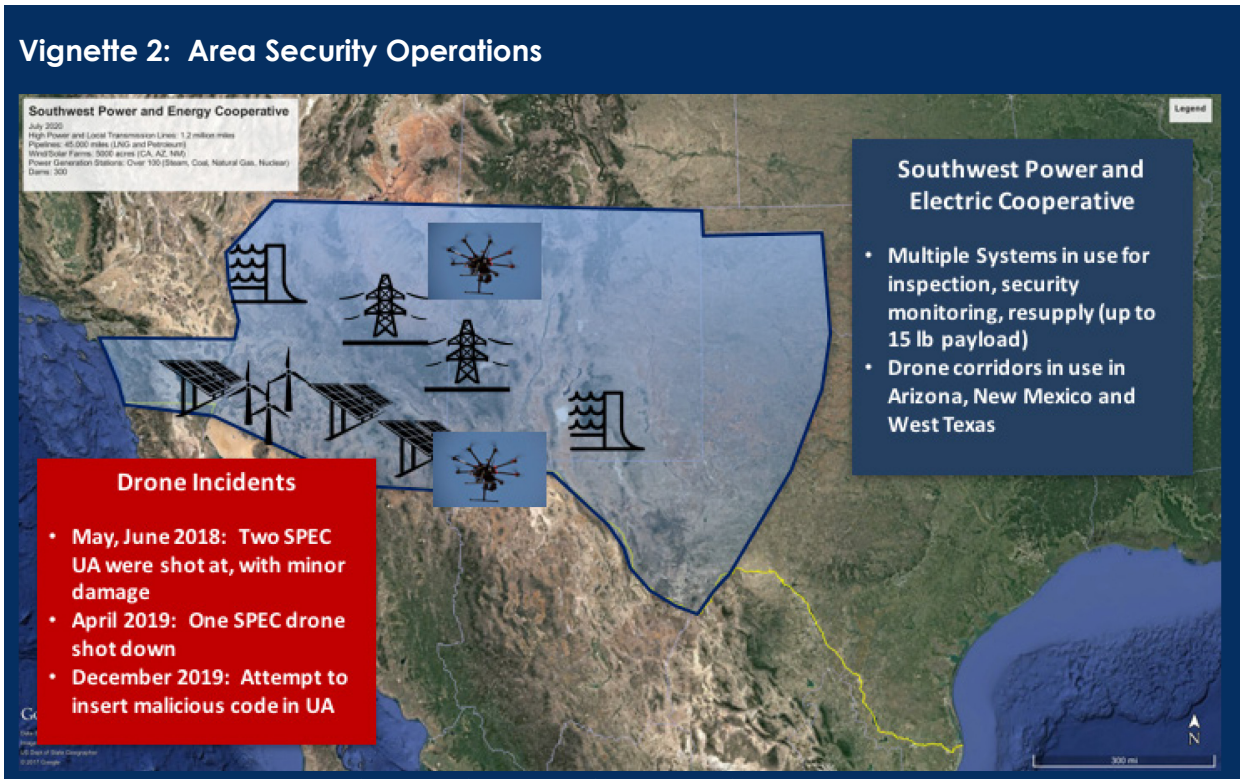
Vignette 1 Observations:

Participant engagement was high during this vignette, due to the broad crossover (e.g. outdoor events/public gatherings). The use of detection measures outside of visual was minimized during this vignette to allow for focus on development of security plans and requirements for integrating UAS into outdoor events.

- An 'air boss' or UAS coordination center (UCC) was discussed as necessary within an integrated command system. The likely location was co-located or under the air operations component. The UCC would be responsible (See Appendix 3, UAS Coordinating Cell Concept):
    - Authorizing all UAS operations with the approval of the incident commander.
    - Notifying ground elements of UAS scheduled operations, locations, and identifying features.
    - Coordinating with federal, state, local and private authorities for emergent tasking's, safety notifications, reports of non-complaints UAS operations, coordination of UAS detection or other technical assets.
    - Setting conditions for flight operations.
    - Publishing written standards for UAS operations (insurance, training certification, etc).
- What is less clear is the amount of new resources (personnel, equipment, and facilities) would be required to accommodate a UCC within the Incident Command System. One participant suggested that a public safety official be on-site at all UAS operations to ensure communications with UCC.
- Intelligence preparation of the security area should include:
    - Plotting of previous UAS incidents to determine trend and most likely system.
    - Based on likely system: determine most likely frequency, range, and description.

    - Determine most likely launch locations, to inform allocation of response and technical assets.
- Public engagement and implementation of local ordinances.
    - Outreach to known commercial and recreational user organizations should occur on a routine basis, but within 60 days of a large outdoor event.
    - These entities (commercial/recreational UAS users) may be temporarily impacted by necessary security and safety restrictions in place during a special event.
    - Localities should consider implementation of short-term ordinance limiting UAS operation in the interest of public safety, as a public endangerment authority. While federal regulations currently prohibit operation of UAS over people, these may be difficult to immediately enforce to protect the public.
- Conduct a name/background check on all outside UAS service providers
- Develop and execute clear contractual obligations for UAS service providers, comparable to those imposed on any other vendor, in terms of providing trained personnel, property functioning equipment, establishment of liability limits.

SDD, VIGNETTE 2: AREA SECURITY OPERATIONS – POWER GRID



UAS as a target and during routine security operations

Area Security/Routine Operations: A notional power company uses UAS for inspections, security monitoring, grid lifecycle maintenance, resupply along established UAS corridors. This company has experienced attempts to either physically disrupt drone operations or in one instance, an attempt to 'hack' a UAS and insert malicious code.

Discussion and Exploratory Questions:

Exploratory Questions:

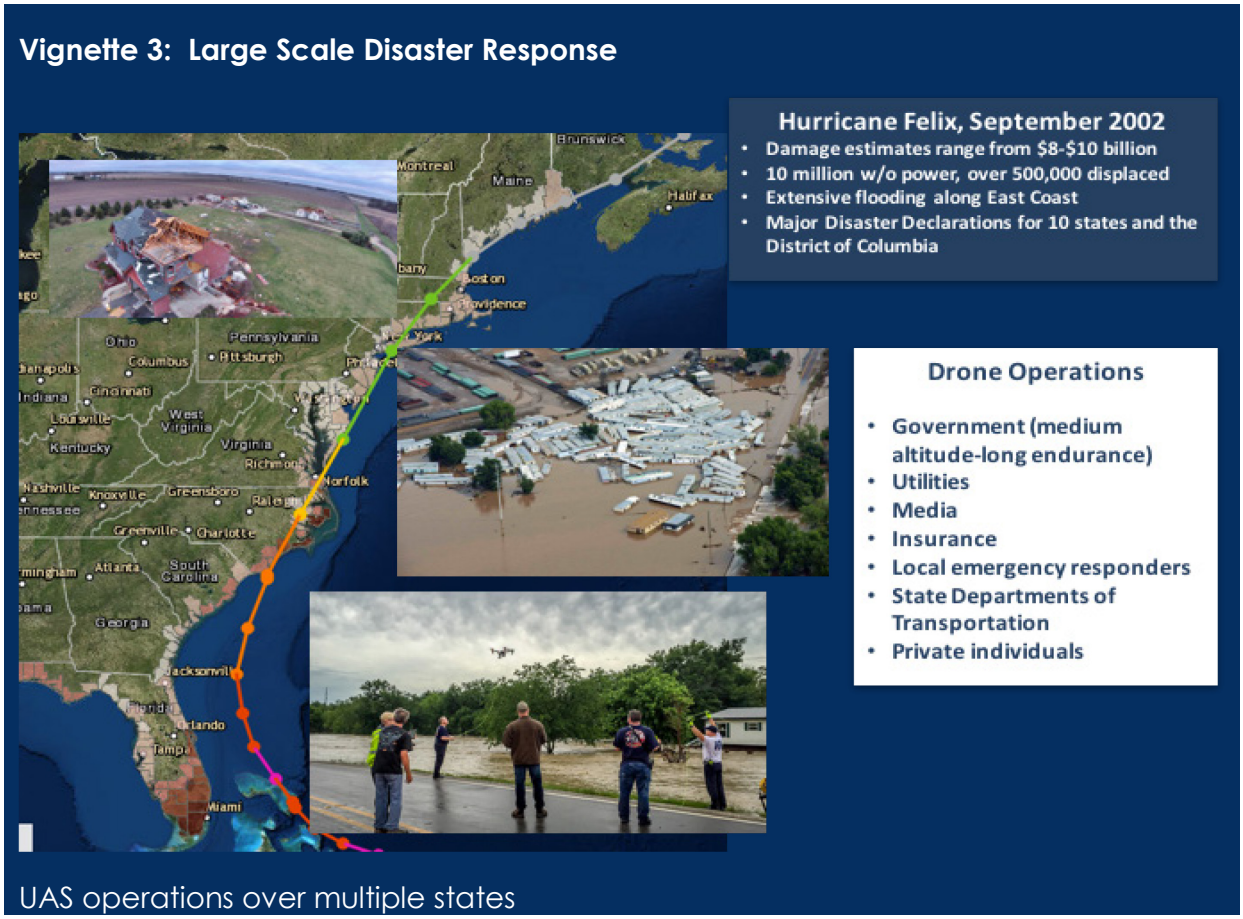
- What "countermeasures" can be employed for security?
- What are the data security considerations for UAS, and are they different from any other IT system?
- What information requirements (number of systems, markings, area of operation) are required by law enforcement to identify compliant systems? How do the ground response assets quickly access this information?

Vignette 2 Observations:

Observations were limited during this discussion, it was generally agreed that there was little difference in terms of security considerations between UAS used as a collection system and other IT systems. This would imply that a future requirement for sustained UAS operation is the development of data security requirement imposed by a chief information officer for any device that can connect and transmit data across the internet including UAS. As was noted during Day 1 presentations, the data collected by UAS in this vignette is likely specific, sensitive, company propriety information that could expose potential vulnerabilities within the notional power distribution system.

Countermeasures in this context were not focused on detection/disruption of UAS, but systems onboard the UAS which could evade ground disruption (e.g. low/high velocity projectiles), or communication disruptions. Another likely requirement of beyond visual line of sight UAS operations will be the reduction or elimination of RF control systems. Global positioning systems will still be a requirement, but future UAS operating without manned control could have backup mapping or rely on mesh networks with either cellular towers or other UAS in the fleet to establish their location and continue with their assigned mission.

SDD, VIGNETTE 3: LARGE SCALE DISASTER RESPONSE



Multi-Jurisdictional/Major Disaster: A late season hurricane moves across the East Coast, resulting in billions of dollars of damage, and millions of affected persons. In the wake of the hurricane, multiple UAS operations are ongoing-including utilities, insurance, federal, State and local response, and media.

Discussion and Exploratory Questions:

- Who is in charge of all of this?
- Is this manageable (from a UAS perspective)?
- What are the potential considerations for manned air response operations?

Vignette 3 Observations:

The general observation from all participants is that, like most major incidents, solutions will generate locally based off the specific needs and available resources in the wake of a major disaster. UAS management will likely not be high of the list of priorities within areas that were significantly or catastrophically impacted by the notional hurricane. Examples in support of local response that have already been observed or practiced by localities include search and rescue operations; flooding/site surveys; wildfires; weather monitoring; and tornado response. In addition to these public safety roles, commercial users ranging including but not limited to utilities; insurance companies and media will likely be in operation in various localities throughout the affected area.

The participants did note that manned operations would likely encounter conflicts with multiple UAS during this event; but reporting of such incident and subsequent investigation and enforcement will likely not be a high priority given the totality of circumstances. This scenario did highlight the scale of overall complexity regarding UAS traffic management, and could serve in future venues to highlight information needs and information sharing requirements necessary for integrated UAS operations.

APPENDIX 1: SEMINAR SCHEDULE DAY 1

TIME	TOPIC	ORGANIZATION
0800-0830	Welcome / Orientation	DHS National Urban Security Technology Laboratory
0830-0915	Global & Domestic Overview	DHS Office of Intelligence and Analysis
0915-0945	UAS in Fire Operations	Fire Department of the City of New York
0945-1000	Break	
1000-1100	UAS Research	Bard College Center for the Study of the Drone
0945-1000	Break	
1130-1145	TACTIC Program	DHS Science and Technology Directorate
1200-1300	Lunch	
1300-1400	UAS Data Recovery	Kovar & Associates
1400-1415	Break	
1415-1500	UAS Detection Technology	Private Sector
1500-1600	UAS Integration	Private Sector

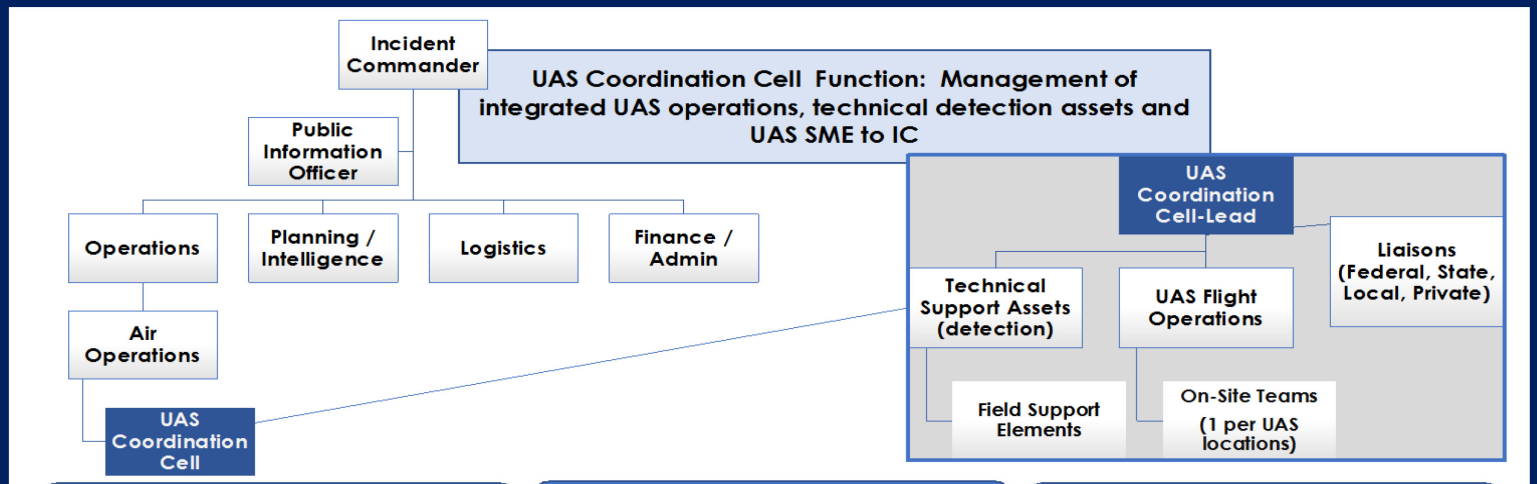
APPENDIX 2: SEMINAR SCHEDULE DAY 2

TIME	TOPIC	ORGANIZATION
0800-0815	Welcome / Orientation	National Urban Security Technology Laboratory
0815-0830	Scenario Overview	AEP-UAS Futures Subcommittee
0830-0930	Vignette 1: Sporting Event Integration	AEP-UAS Futures Subcommittee
0930-0945	Break	
0945-1045	Vignette 2: Routine Operations Integration	AEP-UAS Futures Subcommittee
1045-1100	Break	
1100-1130	Vignette 3: Multi-Jurisdictional Response-Disaster Response	AEP-UAS Futures Subcommittee
1130-1200	Break	
1200-1230	Observations Review	AEP-UAS Futures Subcommittee

APPENDIX 3: UAS COORDIANTION CELL CONCEPT

UAS Coordination Cell Concept

The function of UAS Coordination Cell (UCC) would be to manage compliant unmanned air operations and provide for expanded hosting of technical support assets (detection, tracking, mitigation) of unauthorized UAS operations over a security event.



Deliberate Planning & Preparation Phase

- Support to Training/Awareness of Ground Personnel for UAS recognition and response
- Develop and disseminate known flight times and systems
- Support development of contracts with known UAS service providers for data ownership, background checks, and liability.
- Support Operations: Integrate technical detection assets into IC
- Support Intelligence: development identification of high-risk launch locations and analysis of trends
- Support Planning: Establish environment (weather) conditions for UA flights, flight plans
- Support PIO: Develop outreach plan to inform public of UA operations during activity
- Support Logistics: Identify support requirements for UA operations and frequencies

Execution Phase

- Act as manager for IC for all UAS operations over venue.
- Maintain cleared UAS service provider list based off background checks.
- Track and manage all authorized UA operations during event
- Notify IC and ground personnel of compliant and unauthorized UA operations
- Persistent communication between IC and UAS operators
- Monitor fly/no-fly criteria
- Capture lessons learned/best practices
- Inform integrated UAS operations in future events
- Respond to RFIs from IC and other partners regarding UAS capabilities
- SME support to Plans/Intelligence as needed

Incident Response

- Immediate halt to all UA operations
- Shift to SME support advising IC, Ops, Air Ops and Ground Responders
- Consider available UAS platforms to aid in immediate response scenarios (suspicious devices, crowd management, search operations)
- Technical Support Team actions as defined by statue
- Other specific tasks as directed by IC

APPENDIX 4: GLOSSARY

The following lexicon is intended to aid in use of terminology related or directly applying to unmanned aircraft systems. When available, the entity used for a definition is indicated by name in parenthesis. Definitions specific to this document are indicated with an asterisk (*).[vi]

General Terminology

Aircraft: a device that is used or intended to be used for flight in the air.[5] (US Code, Title 14)

Airplane: an engine driven fixed wing aircraft heavier than air, that is supported in flight by the dynamic reaction of the air against its wings.[6] (US Code, Title 14)

Certificate of Waiver or Authorization (COA): Federal Aviation Administration grant of approval for a specific operation.

Fixed-Wing Aircraft: a heavier-than-air aircraft capable of flight using wings that generate lift caused by the vehicles forward airspeed and the shape of the wings. (*)

Helicopter: a rotorcraft that, for its horizontal motion, depends principally on its engine driven rotors.[7] See rotary-wing aircraft (US Code, Title 14)

Large aircraft: an aircraft of more than 12,500 pounds, maximum certified takeoff weight.[8] (US Code, Title 14)

Military operations area: airspace established outside Class A airspace to separate or segregate certain nonhazardous military activities from instrument flight rules traffic and to identify for visual flight rules traffic where these activities are conducted.[9] (US Code, Title 14)

Sense and Avoid: the capability of an unmanned aircraft to remain a safe distance from and to avoid collisions with other airborne aircraft.

Sense and Avoid: the capability of an unmanned aircraft system to remain a safe distance from and to avoid collisions with other airborne aircraft.[10] (FAA Modernization and Reform Act of 2012)

[vi] Portions of this glossary appeared in DHS Office of Intelligence and Analysis, "Reference Aid: Unmanned Aircraft Lexicon", dated August 2015.

Visual Line-of-Sight (VLOS): the distance at which the pilot is able to maintain visual contact with the aircraft and determine its orientation without enhancements other than corrective lenses. (Academy of Model Aeronautics)[11]

Unmanned Aircraft System Classifications

Drone: commonly used as an informal/shorthand term synonymous for unmanned aircraft system. Strictly speaking, a drone is a vehicle that is capable of operating autonomously without a human control element. (*)

Public Unmanned Aircraft System: a system that meets the qualifications and conditions required for operation of a public aircraft as defined in Title 49, US Code, Section 40102.[12] (FAA Modernization and Reform Act of 2012)

Remote Controlled Model Aircraft: a type of UAS that is produced commercially or are homemade; typically intended for recreational use; require a single person for operation, usually require operator control at all times, and generally have endurance of less than two hours. These platforms are also referred to as radio control aircraft/airplane. (*)

Remotely Piloted Aircraft (RPA): an unmanned aircraft which is piloted from a remote pilot station. (International Civil Aviation Organization, Annex 7)[13]

Remotely Piloted Aircraft System (RPAS): A set of configurable elements consisting of a remotely piloted aircraft, its associated remote pilot station(s), the required command and control links and any other systems elements as may be required, at any point during flight operation.[14] (International Civil Aviation Organization, Circular 328, AN/190)

Small unmanned aircraft means an unmanned aircraft weighing less than 55 pounds on takeoff, including everything that is on board or otherwise attached to the aircraft.[15] (FAA)

Small unmanned aircraft system (small UAS) means a small unmanned aircraft and its associated elements (including communication links and the components that control the small unmanned aircraft) that are required for the safe and efficient operation of the small unmanned aircraft in the national airspace system.[16] (FAA)

Unmanned Aerial Vehicle (UAV): see UAS. Note: UAV was defined prior to 2014 in Department of Defense, Joint Publication 1-02. This term has since been replaced with UAS.

Unmanned Aircraft (UA): a device used or intended to be used for flight in the air that has no onboard pilot. This includes all classes of airplanes, helicopters,

airships, and translational lift aircraft that have no onboard pilot. Unmanned aircraft are understood to include only those aircraft controllable in three axis and therefore exclude traditional balloons (FAA)

Unmanned Aircraft System (UAS): Within the United States, unmanned aircraft systems are classified as aircraft and regulated accordingly. The Federal Aviation Administration Modernization and Reform Act of 2012 defines an unmanned aircraft system as an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system.[17] (Public Law)

Unmanned Aircraft System Categories (FAA):

- Hobbyist: recreational use UAS for personal enjoyment.
- Civil: UAS used for or in support of commence, or for research purposes
- Public: UAS used by or in support of Federal, State, local government functions, including law enforcement or emergency response. See Public Unmanned Aircraft System

Unmanned Aircraft System Categories (Department of the Army):[18]

- Group 1: lightweight, man-portable systems with a maximum takeoff weight of 20 pounds or less, generally operating within line-of-sight at low altitudes generally less than 1200 feet above ground level, with limited endurance, with airspeed generally under 100 knots.
- Group 2: systems with a maximum takeoff weight from 21 to 55 pounds, operating at altitudes of less than 3500 feet above ground level, with airspeed of less than 250 knots.
- Group 3: systems weighing less than 1320 pounds, operating at altitudes of less than 18,000 feet above mean sea level, with no limitations on airspeed.
- Group 4: systems weighing more than 1320 pounds, operating at altitudes of less than 18,000 feet above mean sea level, with no limitations on airspeed.
- Group 5: systems weighing more than 1320 pounds, operating at altitudes of greater than 18,000 feet above mean sea level, with no limitations on airspeed.

Unmanned Aircraft System Encounter: interaction with a UAS where there is no obvious malicious intent, but based on particular circumstance (e.g. flights over critical infrastructure or near sensitive sites) may be sufficient to generate suspicious activity reporting. (*)

Unmanned Aircraft System Incident: interaction with a UAS where: 1) there is an inadvertent or intentional incursion of restricted airspace or 2) operation by a hobbyist operator which are not in compliance with FAA guidelines or 3) operation by a civil or commercial operator which are outside the limitations of a FAA issued certificate of waiver/authorization or 4) use of a UAS in furtherance of a criminal enterprise or violent activity. (*)

Unmanned Aircraft System Sighting: visual observation of a UAS by security officials that do not criteria of either an encounter or an incident. These are typically the result of an encounter by either concerned citizens or security personnel, however the operations of the UAS are in accordance with State, local and Federal requirements. (*)

Airspace Classifications

Controlled Airspace: a generic term that covers the different classification and defined dimensions within which air traffic control service is provided. Controlled airspace consists of Class A, B, C, D, and E.[19] (Federal Aviation Administration)

- Class A Airspace: generally the airspace from 18,000 feet above mean sea level, including the airspace overlying the waters within 12 nautical miles of the coast of the 48 contiguous states and Alaska.
- Class B Airspace: generally the airspace from the surface to 10,000 above mean sea level surrounding the nation's busiest airports in terms of airport operations or passenger enplanements.
- Class C Airspace: generally the airspace from the surface to 4,000 above an airport that have an operational control tower, are serviced by a radar approach control, and have a certain number of instrument flight rules operations or passenger enplanements. Class C airspace usually consists of a surface area surrounding an airport in a five-nautical mile radius, an outer circle with a ten-nautical mile radius that extends from 1,200 to 4,000 feet above the airport elevation.
- Class D Airspace: generally airspace from the surface to 2,500 feet above airports that have an operational control tower.

- Class E Airspace: airspace that does not fall into Class A, B, C, or D, which is considered control airspace. There are no specific pilot certifications or equipment requirements to operate in Class E airspace.

Prohibited area: airspace designated under US Code, Title 14, within which no person may operate an aircraft without the permission of the using agency. [20] (US Code, Title 14)

National Airspace System: The common network of U.S. airspace; air navigation facilities, equipment and services, airports or landing areas; aeronautical charts, information and services; rules, regulations and procedures, technical information, and manpower and material. Included are system components shared jointly with the military.[21] (Federal Aviation Administration)

Notice to Airmen (NOTAM): a notice filed with an aviation authority to alert aircraft pilots of hazards en route or at a specific location. The authority in turn provides means of disseminating relevant NOTAMs to pilots. .[22] (Federal Aviation Administration)

Special Use Airspace or Special Area of Operation (SAO): is a designation for airspace in which certain activities must be confined, or where limitations may be imposed on aircraft operations. Special use airspace usually consists of prohibited areas, restricted areas, warning areas, military operations areas, alert area, and controlled firing areas.[23] (Federal Aviation Administration)

Temporary Flight Restrictions (TFR). A flight data center notice to airmen is issued to designate a TFR. Purposes for issuing a TFR include protection of person and property in the air or on the surface from an existing or imminent hazard; provide a safe environment for the operation of disaster relief aircraft; prevent unsafe congestion of sightseeing aircraft above an incident or event which may generate a high degree of public interest; protect declared national disasters for humanitarian reason; protect the President, Vice President, or other public figures; provide a safe environment for space agency operations.[24] (Federal Aviation Administration)

Uncontrolled Airspace or Class G Airspace: the portion of airspace not designated as Class A, B, C, D, or E. Class G airspace extends from the surface to the base of the overlying Class E airspace. Although air traffic control has no authority or responsibility to control air traffic, pilots should remember there are visual flight rules minimums, which apply in Class G airspace.[25] (Federal Aviation Administration)

Sources:

[1] Bard College Center for the Study of the Drone; 11 JUL 2017, "UAS Research and Studies"; Date of Information (DOI): 2012-JUL 2017, Graphic used in presentation and originally published by CSD in December 2015, "Drone Sightings and Close Encounters: An Analysis", link: http://dronecenter.bard.edu/drone-sightings-and-close-encounters;
[2] National Interagency Fire Center; 7 JUL 2017; "2017 UAS Incursions", Date of Information: JAN 2014-7 JUL 2017; https://www.nifc.gov/drones/outreach.html; accessed 21 JUL 2017, Government information portal based off first-hand reporting from federal, State, local firefighters encountering UAS during operations.
[3] Department of the Interior-US Forest Service, "SAFECOM Aviation Safety Commuinque"; DOI: July 2017; https://www.safecom.gov/, accessed 27 JUL 2017, US Government sponsored portal hosting reports from federal, State and local firefighters, including UAS encounters, observations and actions.
[4] ; National Interagency Fire Center; accessed 7 JUL 2017, "2017 UAS Incursions', DOI: JAN 2014-7 JUL 2017; https://www.nifc.gov/drones/outreach.html, accessed 21 JUL 2017, US Government information portal based off first-hand reporting from federal, State, local firefighters encountering UAS during operations.
[5] United States Code, "Code of Federal Regulations, Title 14, Chapter 1, Section 1.1 General Definitions", http://www.ecfr.gov/cgi-bin/text-idx?rgn=div8&node=14:1.0.1.1.1.0.1.1, current as of 3 AUG 2017, retrieved 3 AUG 2017
[6] Ibid.
[7] bid.
[8] Ibid.
[9] Ibid.
[10] US Congress, Public Law 112-095, "FAA Modernization and Reform Act of 2012", February 2012, Section 331 "Definitions"
[11] Academy of Model Aeronautics, AMA Document #550, "Radio Controlled Model Aircraft Operation Utilizing "First Person View" Systems", Revision 12 January 2014.
[12] Ibid.
[13] International Civil Aviation Organization, "International Standards, Annex 7 to the Convention on International Civil Aviation", Sixth Edition, July 2012
[14] Ibid.
[15] United States Code, "Code of Federal Regulations, Title 14, Chapter 1, Section 1.1 General Definitions", http://www.ecfr.gov/cgi-bin/text-idx?rgn=div8&node=14:1.0.1.1.1.0.1.1, current as of 3 AUG 2017, retrieved 3 AUG 2017
[16] Ibid.
[17] US Congress, Public Law 112-095, "FAA Modernization and Reform Act of 2012", February 2012, Section 331 "Definitions"
[18] Department of the Army, "U.S. Army Unmanned Aircraft Systems Roadmap 2010-2035",
[19] Federal Aviation Administration, FAA-H-8083-25A, "Pilot's Handbook of Aeronautical Knowledge", Chapter 14, 2008, accessed 7 April 2015
[20] United States Code, "Code of Federal Regulations, Title 14, Chapter 1, Section 1.1 General Definitions", http://www.ecfr.gov/cgi-bin/text-idx?rgn=div8&node=14:1.0.1.1.1.0.1.1, current as of 3 AUG 2017, retrieved 3 AUG 2017
[21] Federal Aviation Administration, "Pilot/Controller Glossary"; 25 August 2011; http://tfmlearning.faa.gov/Publications/atpubs/PCG/N.HTM; accessed 1 AUG 2017
[22] Federal Aviation Administration, FAA-H-8083-25A, "Pilot's Handbook of Aeronautical Knowledge", Glossary, 2008, accessed 7 April 2015
[23] Ibid.
[24] Ibid.
[25] Ibid.