

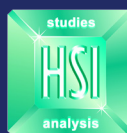


UNMANNED SYSTEMS IN HOMELAND SECURITY

January 2015



Homeland
Security



HOMELAND SECURITY®
STUDIES & ANALYSIS
INSTITUTE

An FFRDC operated by Analytic Services Inc. on behalf of DHS

HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE

The Homeland Security Act of 2002 (Section 305 of PL 107-296, as codified in 6 U.S.C. § 185) authorizes the Secretary of the Department of Homeland Security (DHS), acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. Analytic Services Inc. operates the Homeland Security Studies and Analysis Institute (HSSAI) as an FFRDC for DHS under contract HSH-QDC-09-D-00003.

HSSAI provides the government with the necessary expertise to conduct cross-cutting mission analysis, strategic studies and assessments, development of models that baseline current capabilities, development of simulations and technical evaluations to evaluate mission trade-offs, creation and evolution of high-level operational and system concepts, development of top-level system and operational requirements and performance metrics, operational analysis across the homeland security enterprise, and analytic support for operational testing evaluation in tandem with the government's acquisition process. HSSAI also works with and supports other federal, state, local, tribal, public, and private sector organizations that make up the homeland security enterprise.

HSSAI research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under Task 14-01.03.01, "Unmanned Systems and the Homeland Security Enterprise."

The results presented in this report do not necessarily reflect official DHS opinion or policy.



U.S. Army photo by Staff Sergeant John Etheridge / DVIDS

UNMANNED SYSTEMS IN HOMELAND SECURITY

January 2015

Matthew H. Fleming, PhD

Samuel J. Brannen

Andrew G. Mosher

Bryan Altmire

Andrew Metrick

Meredith Boyle

Richard Say¹



An FFRDC operated by Analytic Services Inc. on behalf of DHS

Subcontractor:
Center for Strategic and International Studies (CSIS)

¹ Fleming, Altmire, and Mosher are with the Homeland Security Studies and Analysis Institute, a not-for-profit federally funded research and development center operated by Analytic Services Inc. on behalf of the U.S. Department of Homeland Security. Brannen, Metrick, Boyle, and Say are with the Center for Strategic and International Studies, a bipartisan not-for-profit think tank. Corresponding author's e-mail address: matthew.fleming@hsi.dhs.gov.

For information about this publication or other HSSAI research, contact

HOMELAND SECURITY STUDIES AND ANALYSIS INSTITUTE

Analytic Services Incorporated

5275 Leesburg Pike, Suite N-5000

Falls Church, VA 22041

Tel (703) 416-3229 • Fax (703) 379-2556

www.homelandsecurity.org

Publication Number: RP14-01.03.01-03

Contents

Foreword	v
Acknowledgements.....	vi
Acronyms	vii
Executive Summary	ix
I. Introduction.....	1
II. Research Question, Methodology, and Scope	3
III. An Overview of Unmanned Systems	5
IV. Current Use in the HSE	17
A. DHS	17
B. Department of Defense	22
C. Other Federal Departments and Agencies ¹¹⁸	23
D. State and Local First Responders	23
E. Private Sector.....	24
V. Future Requirements	25
VI. Constraints	35
A. Privacy.....	36
B. First Amendment Rights.....	43
C. Safety	46
D. Cost	51
E. Other	51
VII. Implications	53
VIII. Conclusions and Thoughts for Future Research.....	57
Appendix I. State Laws on the Use of Unmanned Systems.....	59
Appendix II. Working Group Participants and Interviewees.....	65
Endnotes	69

FOREWORD

Unmanned systems are suited to a range of new and beneficial uses in homeland security. At the same time, a variety of legal, regulatory, and societal issues constrain these uses. To effectively weigh pros and cons, and to consider potential threats, careful and dispassionate study is essential. We believe that this report by the Homeland Security Studies and Analysis Institute and the Center for Strategic and International Studies is an important step in that direction. We have been happy to serve as the senior advisory committee during the compilation of this report, and we endorse its findings and recommendations.

John Hamre

President and CEO, Center for Strategic and International Studies

Michael C. Kostelnik

Major General, United States Air Force (ret.)

James M. Loy

Admiral, United States Coast Guard (ret.), Senior Counselor, The Cohen Group

Silvestre Reyes

Former U.S. Representative, Texas 16th District

Frances Fragos Townsend

Former Assistant to President George W. Bush for Homeland Security and Counterterrorism

ACKNOWLEDGEMENTS

The authors received invaluable input from a large number of individuals from government, industry, and academia, and for that they are truly grateful. In particular, the authors wish to thank the members of the study's senior advisory committee, as well as Philip Anderson and Richard Kohout (Homeland Security Studies and Analysis Institute) and Kathleen H. Hicks, Robert Wise, and Tracy Nelson (Center for Strategic and International Studies).



Acronyms

ABSAA	Airborne sense and avoid
ADS-B	Automatic Dependent Surveillance-Broadcast
AUVSI	Association for Unmanned Vehicle Systems International
CBP	U.S. Customs and Border Protection (DHS)
CBRNE	Chemical, biological, radiological, nuclear, and explosive
CEO	Chief executive officer
COA	Certificate of Waiver or Authorization
COCO	Company owned, company operated
COTS	Commercial off-the shelf
CPFH	Cost per flight hour
CSIS	Center for Strategic and International Studies
CT	Counterterrorism
DHS	Department of Homeland Security
DoD	Department of Defense
DOJ	Department of Justice
DSCA	Defense Support to Civil Authorities
EO/IR	Electro-optical/infrared
EOD	Explosive ordinance disposal
FAA	Federal Aviation Administration (DOT)
FBI	Federal Bureau of Investigation (DOJ)
FEMA	Federal Emergency Management Agency (DHS)
FMRA	FAA Modernization and Reform Act of 2012
GAO	Government Accountability Office
GBSAA	Ground based sense and avoid
GOGO	Government owned, government operated
GPS	Global positioning system

HALE	High-altitude long-endurance
HD	Homeland Defense
HRI	Human-robot-interface
HSE	Homeland security enterprise
HSSAI	Homeland Security Studies and Analysis Institute
IMU	Inertial measurement unit
ISR	Intelligence, surveillance, and reconnaissance
LOS	Line of sight
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NICCP	National Interdiction Command and Control Plan
NIJ	National Institute of Justice (DOJ)
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
OAM	Office of Air and Marine (CBP)
OUSD AT&L	Office of the Under Secretary of Defense for Acquisition, Technology and Logistics
PIA	Privacy impact assessment
PED	Processing, exploitation, and dissemination
QHSR	Quadrennial Homeland Security Review
R&D	Research and development
RAPS	Robotic Aircraft for Public Safety project (DHS)
RPA	Remotely piloted aircraft
S&T	Science and Technology Directorate (DHS)
SAA	Sense-and-avoid
SAR	Search and rescue
SATCOM	Satellite communication
sUAS	Small unmanned aerial system
SWaP	Size, weight, and power
SWAT	Special weapons and tactics
UAS	Unmanned aerial system
UAV	Unmanned aerial vehicle
UGS	Unmanned ground system
USAF	U.S. Air Force
USCG	U.S. Coast Guard (DHS)



Executive Summary

Unmanned systems—unmanned vehicles and their associated control and communications infrastructure, including human operators—are being used extensively and to great effect in national security missions worldwide. To a lesser but growing extent, unmanned systems are also being used in homeland security missions in the United States. Much has been written about unmanned systems in the national security context. Less attention has been paid, however, to unmanned systems in a homeland security context, impeding effective decision making on the deployment of potentially disruptive technology. Accordingly, a research team from the Homeland Security Studies and Analysis Institute and the Center for Strategic and International Studies examined the use of unmanned systems in homeland security. This paper presents the findings of the research.

In sum, the research suggests:

- Overall, unmanned systems appear to hold promise for the homeland security enterprise (HSE). They comprise a rapidly developing and maturing technology that appears to offer effective and efficient (and sometimes unique) capabilities—while becoming more affordable and easier to use.
- Technologies that can be applied to homeland security are increasingly emanating from the commercial sector and not from the Department of Defense. The Department of Homeland Security (DHS) and others in the HSE should adapt to this opportunity to meet their requirements. Along these lines, DHS could make significant use of commercial-off-the-shelf small unmanned aerial systems (sUAS), which will outpace other unmanned systems in domestic quantity and use over the next decade. sUAS may not offer radically different capabilities than are already available in manned aircraft, but they can offer those capabilities in a more affordable way and potentially can be fielded and operated in far greater numbers.
- Advances in unmanned systems technology and use present both an opportunity and a threat for the HSE. They may increase the congestion of airspace, roads, and waterways and the likelihood of accidents, as well as misuse by bad actors.
- Constraints on government and civilian use of unmanned systems are significant; public perception and safety will continue to be the biggest obstacles. Fairly or not, unmanned systems in general and unmanned aerial systems (UAS, both large and small) specifically play a central part in the public discussion of mass

surveillance programs by the government. Concerns about the stealth and persistence that unmanned systems offer have spurred public fears that they will be used to infringe on Americans' privacy rights. As a result, users across the HSE must meet a high standard in demonstrating responsible use of unmanned systems, yet statutes and case law offer no clear indication of where that standard will be set. In addition, significant safety concerns regarding UAS must be overcome through rigorous testing and evaluation, leveraging Federal Aviation Administration UAS test sites.

- On balance, the HSE is not yet well poised to capitalize on, or to respond to widespread commercial and consumer use of, unmanned systems. While work is underway in DHS, for example, it appears to be largely reactive, siloed, focused primarily (though not exclusively) on the air domain, and limited to DHS vice the larger HSE. This is not sufficient for disruptive technology.
- Beyond DHS and its HSE partners, the broader U.S. government lacks overarching policy and strategy on the domestic use of unmanned systems, which creates public safety, public affairs, and economic risks. Domestic use of unmanned systems must be understood in all its complexity and broader context. That means cultivating an awareness and understanding of the capabilities of a technology that is evolving each day; dealing with (and tracking) legal ambiguities in a shifting statutory landscape; and understanding overarching threats and opportunities for homeland security, economic prosperity, and implications for civil rights and civil liberties.

The research team makes several recommendations:

- The Deputy Secretary of Homeland Security should convene a 12-month internal working group to assess how DHS should best organize and posture to respond to the existing and emerging opportunities and threats presented by unmanned systems. The Deputy Secretary would be optimally positioned to undertake such a task because the issues associated cut across the full scope of missions and functions in DHS. The Deputy Secretary would present findings to the Secretary of Homeland Security, who may wish to initiate an interagency conversation. The scope of the working group would be to:
 - assess current DHS use of unmanned systems;
 - identify potential additional uses of unmanned systems to meet high-priority requirements;
 - understand the threat of use of unmanned systems by terrorists or criminals and how to mitigate this threat;
 - discuss the national role DHS should play in regard to unmanned systems, including questions of greater cooperation with the Department of Transportation (not least the Federal Aviation Administration), Department of Justice, Department of Defense, and others; and
 - consider options for public-private dialog on privacy concerns relating to the use of unmanned systems.
- Additionally, and to support the proposed working group, DHS should seek to incorporate unmanned systems into virtually all of its exercises.
- Informed by expertise resident within the DHS Science and Technology Directorate (S&T) from its Robotic Aircraft for Public Safety program, U.S. Customs and Border Protection and U.S. Coast Guard should pursue more formal testing and operational evaluation of sUAS in the border security mission.

- The National Institute of Justice and DHS should collaborate closely going forward—working with relevant non-governmental organizations such as the International Association of Chiefs of Police—in helping to set standards for state and local operators of unmanned systems, particularly sUAS.
- DHS operators and DHS S&T technologists should (continue to) liaise with federal partners, such as the U.S. Navy; U.S. Army; the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics; and the Defense Advanced Research Projects Agency on research and development in unmanned ground systems and unmanned maritime systems.



I. Introduction

Unmanned systems—unmanned vehicles and their associated control and communications infrastructure, including human operators—represent a rapidly maturing, proliferating, and likely disruptive technology. Unmanned systems have existed for more than 50 years in small numbers, often at high cost, and with limited application. Over the past decade, due to wartime military investment, they have grown significantly in number and use, particularly in the air domain (from dozens to thousands), but also on land and at sea. Military research and development (R&D) and demonstrated utility have generated interest in broader civil and commercial use. In a growing global market, unmanned systems are becoming more affordable, more capable, and easier to operate.

Unmanned systems are being used extensively in national security missions worldwide. For example, U.S. Air Force (USAF) and U.S. Army Predator, Reaper, and Grey Eagle unmanned aerial systems (UAS) had flown more than three million flight hours as of October 2014.¹ The U.S. Navy has recently increased its experimentation and interest in a range of unmanned maritime systems (UMS), both for surface and subsurface use. The U.S. Army and U.S. Marine Corps are continuing to operate unmanned ground systems (UGS) in support of the explosive ordnance disposal (EOD) mission and are testing unmanned cargo vehicles. Not surprisingly, militaries around the world are similarly intensifying use and R&D.

To a lesser—but growing—extent, unmanned systems are also being used in homeland security missions in the United States. Within the Department of Homeland Security (DHS), U.S. Customs and Border Protection's (CBP) Office of Air and Marine (OAM), for example, employs a fleet of Predator B and Guardian (the Predator B's maritime variant) UAS, primarily for border security missions. The U.S. Coast Guard (USCG) is experimenting with offshore use of small UAS (sUAS) deployed from cutters. Certain state and local jurisdictions employ sUAS in search and rescue (SAR) and policing activities. And first responders nationwide often use UGS for EOD (i.e., bomb squad use) or other tactical purposes (e.g., special weapons and tactics [SWAT] missions).

Much has been written about unmanned systems in the national security context. Several government reports set forth R&D, acquisition, and operational road maps, describing the likely direction to be taken by the U.S. Department of Defense (DoD).² Numerous reports by research groups discuss facets of unmanned systems'

use, or issues therein,³ including the use of armed UAS in counterterrorism (CT) operations⁴ and so-called autonomous weapons systems.⁵ Beyond these sources, there has also been extensive coverage of unmanned systems issues in both the general and trade press and substantial work done by advocacy groups such as the American Civil Liberties Union and the Association for Unmanned Vehicle Systems International (AUVSI).

Less has been written, however, about unmanned systems in a homeland security context. Occasional media reporting discusses use of certain unmanned systems by federal law enforcement agencies in support of homeland missions.⁶ There have also been a small number of congressional hearings on the issue,⁷ as well as a handful of nongovernmental organization reports.⁸ DHS has issued various privacy impact assessments (PIAs) that discuss, for example, the privacy implications relating to sensors on UAS.⁹ Government Accountability Office (GAO),¹⁰ DHS Inspector General,¹¹ Department of Justice Inspector General,¹² and Congressional Research Service¹³ reports also exist on the subject.

Lesser attention on unmanned systems in the homeland security context impedes effective decision making. The use of unmanned systems in a domestic homeland security context is sufficiently different than use in an overseas defense or intelligence context—and understanding of defense/intelligence issues does not translate directly to homeland security. Filling this knowledge gap enhances policy decision making and improves dialogue between the government and the American public. In so doing, it facilitates use of emerging technology that might help to more effectively and affordably execute homeland security missions. And it also provides opportunities to adequately manage any downside risks posed by unmanned systems.

Accordingly, a research team from the Homeland Security Studies and Analysis Institute (HSSAI) and the Center for Strategic and International Studies (CSIS) examined the use of unmanned systems in homeland security. The research sought to capture—in a comprehensive, objective way—current understanding of technology, operations, requirements, and legal and policy considerations.

This paper presents the findings of the research. It is structured as follows: Following this introduction are the project's research question, methodology, and scope; an overview of unmanned systems; current use of unmanned systems in the homeland security enterprise (HSE); future requirements; constraints; implications; and a conclusion that summarizes and closes with thoughts for future research.



II. Research Question, Methodology, and Scope

Formally, the HSSAI-CSIS team sought to answer the following research question:

- *What are the requirements for, constraints on, and implications of the use of unmanned systems in the HSE?*

To answer this research question, the HSSAI-CSIS team:

- Reviewed the extant literature: The team reviewed the very broad literature from government, industry, academia, and the media on topics including unmanned systems, innovation, homeland security missions and mission needs, requirements and requirements setting, and legal authorities.
- Conducted semi-structured interviews: The team complemented the findings of the literature review with more than 50 interviews. These were held with experts from government, industry, and academia in fields including engineering, computer science, robotics, law, national security, homeland security, policy, and business. Interviews included those held during site visits in Pittsburgh, Pennsylvania, with the National Robotics Engineering Center and other Carnegie Mellon University spinoffs, and in Blackstone, Virginia, at a flight test center for UAS.
- Hosted invitation-only working groups: Four working groups examined topics including unmanned systems technology; border security, CT, and counter-weapons of mass destruction; public safety/emergency response and infrastructure security and resilience; and constraints. These working groups collectively captured the input of more than 50 additional experts.
- Vetted the early research approach and later emerging findings with a senior advisory committee: A five-member senior advisory committee provided context, counterpoint, and criticism.
- Validated findings through peer review: The team conducted an extensive peer-review process that sought to confirm findings and clarify outstanding issues.

In terms of scope:

- The research explored unmanned systems in the air, land, and maritime domains. The team examined UAS, UGS, and UMS, including those used both on the surface and subsurface. Notably, UAS dominate the

literature and broader discourse; while this paper addresses use of unmanned systems in the three domains, the paper similarly focuses more on the air domain than land and maritime.

- The team assessed requirements, constraints, and implications of unmanned systems in the broader HSE, not simply DHS.¹⁴ This implied focus on entities including DHS, other federal departments and agencies, state and local governments, and the private sector. The paper focuses primarily (but not exclusively) on DHS operational components and directorates (including CBP; USCG; and the Science and Technology Directorate [S&T]); DoD Homeland Defense (HD) and Guard forces; state and local first responders; and private-sector owners and operators of critical infrastructure.
- The paper focuses on HSE missions intended to counter terrorism; chemical, biological, radiological, nuclear, and explosive materials and devices (CBRNE); illegal migration; illicit narcotics; and natural hazards, such as hurricanes (i.e., forecasting, preparation), as well as missions to support critical infrastructure security and resilience and public safety and emergency response.¹⁵ The research did not explore in depth issues relating to cybersecurity, benefits administration by U.S. Citizenship and Immigration Services, customs and exchange under CBP, the protective mission of the U.S. Secret Service, or efforts to counter potential adversary use of unmanned systems. These latter issues, though within the HSE mission set, are either somewhat far afield from use of unmanned systems or sufficiently sensitive for treatment elsewhere.
- The paper was written to be a foundational document. The research team sought to capture the current state of affairs in a single document to inform policymakers, as well as operators, technologists, and other stakeholders. Each topic could be subject to deeper analysis to advise specific decisions. For example, while the paper discusses requirements for unmanned systems, it by no means represents the kind of full requirements analysis that would support deeply granular acquisition decisions. Developing such a product would require longer study with joint teams of operators, strategists, technologists, budget professionals, policymakers, and counsel.
- It was envisioned that the results of the research would be unclassified. The research team purposefully employed only open-source literature and interviews conducted at the unclassified level. This approach was chosen to inform ongoing public discussion in an area in which the existing body of literature is limited.
- The research was carried out between June and December 2014. This report represents a snapshot of a brief period in the evolution of a highly dynamic issue set.



III. An Overview of Unmanned Systems

This section provides context by defining unmanned systems; their uses, shapes and sizes; coming technological advances; and the global market.

An *unmanned system* is a mobile electro-mechanical machine that operates in the air, ground, or maritime domain, comprising an unmanned vehicle (a platform and mission payload), control station, communications infrastructure, and external human operator(s) and maintainer(s).¹⁶ These elements are addressed in turn.¹⁷

- The platform of an unmanned system (i.e., of its unmanned vehicle) includes a chassis and power, propulsion, and other subsystems. These subsystems provide mobility. In this regard, platforms typically carry global positioning system (GPS) receivers and inertial measurement units (IMUs) to capture orientation in time and space. Platforms also carry batteries or liquid (or other) fuel reserves to power the platform and mission payload, motors, control servos, and the like. Common to all platforms, and of relevance to the selection of mission payload, are constraints of size, weight, and power (SWaP). Tradeoffs are made among these: a larger platform with a bigger payload typically requires more power, which is typically heavier, requiring a larger platform, and so on. Improvements in battery capacity, miniaturization of electronic components, and reductions in the power they draw contribute to more capable platforms within set SWaP limits.
- The mission payload represents sensors and actuators designed to accomplish one or more missions, such as remote sensing, EOD, or logistics (uses of unmanned systems are discussed in greater detail below). Payloads are, of course, mission specific; they range from electro-optical cameras that allow for full-motion video in infrared and other spectra to radars of various kinds to physical actuators that allow for kinetic influence in the physical environment (e.g., a robotic manipulator arm for EOD). Payloads may also include physical cargo being moved from one location to another (e.g., for troop resupply). Note also that sensors and actuators are used in the platform, for its control; the line between a mission payload and platform control subsystem is blurring, such that they sometimes share elements (e.g., GPS is used for platform control as well as geotagging of mission payload sensor data).

- A control station allows human operators to control the platform (its location, speed, and bearing) and its mission payload. Control stations range in complexity and size from smartphones and tablet computers to mobile trailer-based stations to larger fixed command centers. Some control stations can hand off from one to another, including between geographically separate locations, allowing for “remote split operations.”¹⁸
- A communications infrastructure facilitates the transfer of control data to and from the platform, and mission payload data to and from the mission payload. In some cases, this implies radios providing line-of-sight (LOS) communications links between operator and vehicle. In other cases—for operations beyond LOS—data links may involve radios or more costly space-based satellite communications (SATCOM) and associated terrestrial infrastructure. Physical tethers are also occasionally used to transfer data (and sometimes power) between the control station and vehicle.¹⁹ Importantly, most current-generation unmanned systems rely upon a sustained (i.e., continuous) communications link for platform control and effective use of the mission payload. And most unmanned systems employ wireless connectivity—which is imperfect, especially in the crowded 900 MHz and 2.5 GHz spectrums, in which many commercial off-the-shelf (COTS) unmanned systems operate. Accordingly, use of wireless communications technology carries with it certain safety requirements, such as lost-link capability and sense-and-avoid (SAA) technology.²⁰
- External human operator(s) provide some element of control over platform and payload. The role of the human operator ranges from full remote operation (also known as “teleoperation”) of both platform and mission payload, to only limited guidance (“go here and execute this mission”); the latter approach requires some level of vehicle autonomy.²¹ Indeed, increasingly, unmanned systems are capable of a combination of autonomous function and human operator control. For example, common to many unmanned systems is waypoint navigation, in which a human operator selects several intermediate destinations via the control station; using geolocation, the unmanned vehicle automatically travels to these predetermined points without further operator input. Integrating full autonomy into unmanned systems has so far proven a difficult challenge, however.²² Note also that certain unmanned systems have long endurance and can fly, drive, or swim for a day or more, well beyond the endurance of a single human operator and requiring multiple operator shifts. Of course, swapping pilots and payload operators while an unmanned system is in use is easier than with a manned system, as the latter either needs to carry multiple crews or return to an operating base for crew changes. In this way, unmanned systems can yield cost savings, as there may be no need to pay for operator overtime or travel to different locations.
- Human maintainer(s) keep unmanned systems in operation. Like their manned counterparts, unmanned systems break (parts wear, chips fail, software crashes, and accidents happen). Larger, more complex systems, especially those operating in harsh conditions (e.g., all-weather maritime environments), carry a larger maintenance burden. And new technology becomes available periodically, requiring hardware and software upgrades.

Unmanned systems are used for military and civil purposes (i.e., missions). These include sensing (e.g., intelligence/surveillance/reconnaissance [ISR], mapping, SAR, meteorology); and acting (e.g., kinetic strike [via missiles or other weapons]; non-kinetic strike [electronic warfare]; target designation; defensive action, like EOD; logistics [cargo delivery or troop resupply]; communications relay [mobile Wi-Fi]; crop spraying; and firefighting).²³

Unmanned systems are commonly thought to offer greatest return on investment—greatest utility—when performing tasks that are dirty, dangerous, dull, or difficult. That is, while unmanned systems are often used like their manned counterparts—for many of the same missions—they appear to be most effective and efficient in select circumstances. For example, unmanned systems provide stand-off distance for human operators that prevents exposure to dirty or dangerous hazards, such as radioactivity from a nuclear incident or potentially unstable ordnance from an improvised explosive device.²⁴ Unmanned systems may also offer a degree of stealth, in that their size or operating characteristics may make them quieter or harder to spot, which is beneficial in contested environments. Further, unmanned systems offer persistence and patience; these allow for long and also repetitive missions, such as daily remote sensing to detect changes along long stretches of national borders.²⁵ And because there is no onboard human operator, unmanned systems can be very small, allowing them to be used in physical locations in which it is difficult for humans or manned vehicles to otherwise go. Unmanned systems are also thought to be advantageous when they can meet a mission requirement at significantly lower cost than existing manned systems.²⁶

Unmanned systems are sometime recognized as being among a handful of technologies with disruptive potential in the near future.²⁷ According to Harvard Business School professor Clayton Christenson: “Disruptive technologies bring to market a very different value proposition than had been available previously. Generally, disruptive technologies underperform established products in mainstream markets. But they have other features that a few fringe (and generally new) customers value. Products based on disruptive technologies are typically cheaper, simpler, smaller, and, frequently, more convenient to use.”²⁸ The Defense Advanced Research Projects Agency (DARPA) has played a crucial role in the development of disruptive unmanned systems technology. In addition to investments dating back to the 1970s that led to many current-generation UAS platforms, DARPA has encouraged robotics research at universities and startup companies through a recent competition series with prize money. These have included the 2004 and 2005 Grand Challenges and 2007 Urban Challenge that led to rapid progress in autonomous ground vehicles, and more recent events such as the 2013–15 Robotics Challenge series focusing on advanced UGS for SAR applications.²⁹




Deriving utility from unmanned systems, not least in executing ISR and other “sensing” missions, requires an ability to employ data. The mission payload produces data; these data undergo processing, exploitation, and dissemination (PED), most often at the control station. Mission payload data are often compared to data collected previously to provide insights, perhaps through change-detection software, which compares sensor (imagery, radar, or other) data files for the same location to observe differences over time. Data may also be fused from multiple disparate sources (e.g., imagery with synthetic aperture radar) to generate multiple-intelligence-source insights. Some unmanned systems allow for onboard PED, in which case only relevant data are transferred to operators; onboard PED can reduce communications bandwidth requirements. In certain circumstances, mission payload data may be used for legal purposes (e.g., as evidence to support prosecutions). In this case, PED must occur subject to proper chain of custody procedures, with attendant investment in infrastructure and personnel. Notably, PED is considered to be a difficult and misunderstood element of the effective use of unmanned systems.³⁰

Unmanned systems are available in a wide and growing variety of shapes and sizes (see table 1). Unmanned systems may resemble manned systems—and sometimes, they are one and the same—because they have

been purposefully designed to be optionally manned or because they have been retrofitted for unmanned operation.³¹ But unconstrained by the physical and life support requirements necessary to accommodate onboard human operators, unmanned systems may also take on new and novel form factors to allow for unique applications.³² Widely adopted designs unique to unmanned systems currently include “quadcopter” and “octocopter” sUAS, which maximize lift, stability, and control for a small platform. And researchers are experimenting with mimicking naturally occurring structures and approaches for motion in unmanned systems designs (in a field known as “biomimetics”). For example, Harvard researchers have created starfish-like rubber platforms that could be useful in SAR applications because they can crawl over uneven terrain and squeeze their flexible, fire, and acid-resistant “bodies” through small openings.³³ Carnegie Mellon University has created a modular snake that slithers, allowing for sensing of hard-to-reach areas, such as pipes inside a nuclear plant.³⁴




Current-generation unmanned systems face certain safety and operational challenges. As noted, unmanned systems that rely on wireless communications typically require lost-link and SAA functionality (some of which remains in development). SWaP limitations sometimes preclude use of redundant platform subsystems, which are common to most manned platforms. Additionally, safe operation of unmanned systems may require specific training and some type of certification for operator and vehicle. And adverse weather conditions often limit use of unmanned systems—especially smaller systems.

Table 1. A Typology of Unmanned Systems (UGS)

SIZE	MAIN ATTRIBUTES	COMMON APPLICATIONS	IMAGE	EXAMPLES
Light (0-350 lbs.)	<ul style="list-style-type: none"> Small, lightweight devices that can be carried and deployed by one or two individuals Smaller devices can be “throwable” Generally tele-operated, although some devices are capable of limited autonomous movement Manipulator arm strength: 7-15 lbs. Common sensors: Color video cameras, IR 	<ul style="list-style-type: none"> Increase tactical situational awareness in high risk or inaccessible environments (e.g. SWAT entry) Explosive/hazardous materials detection operations 		<ul style="list-style-type: none"> iRobot 310 SUGV Recon Scout Throwbot iRobot 110 FirstLook ARA Pointman Tactical Robot QinetiQ Dragon Runner 20 iRobot 510 PackBot
Medium (351-5,000 lbs.)	<ul style="list-style-type: none"> Larger, heavier devices that can carry a wide variety of payloads Can be transported in most vehicles Generally tele-operated, although some devices are capable of limited autonomous movement Manipulator arm strength: ≤100 lbs. Common sensors: Color video cameras, IR, Night Vision, chemical and explosive detection sensors 	<ul style="list-style-type: none"> Increase situational awareness in high risk or inaccessible environments Explosive/hazardous materials detection operations 		<ul style="list-style-type: none"> QinetiQ Talon ECA Robotics Cameleon ICOR Technology Caliber T5
Heavy (5,000+ lbs.)	<ul style="list-style-type: none"> More capable devices that vary greatly in size and function Larger vehicles may utilize an autonomy kit and can be reconfigured to allow standard human operation when needed Manipulator arm strength: >100 lbs. Common sensors: Color video cameras, IR, thermal cameras, chemical and explosive detection sensors 	<ul style="list-style-type: none"> Functions vary significantly based on modules attached and the vehicle itself. Examples include: Increase situational awareness in high risk or inaccessible environments Explosive/hazardous materials detection operations Transport Perimeter patrol 		<ul style="list-style-type: none"> Oshkosh TerraMax iRobot 710 Kobra ASI Chaos Robotic Platform QinetiQ MAARS Black-i Robotics Landshark G-NIUS Guardium QinetiQ Minotaur IAI /TLD TaxiBot

Sources: Various; see endnote.³⁵

Table 1. A Typology of Unmanned Systems, continued (UMS: Unmanned Underwater Systems)

SIZE	MAIN ATTRIBUTES	COMMON APPLICATIONS	IMAGE	EXAMPLES
Light (0-350 lbs.)	<ul style="list-style-type: none"> • Small, portable vehicles • Most can be carried and deployed by one or two individuals • Generally tele-operated, although some models are capable of semi-autonomous movement • Depth range: 320 ft. • Common sensors: Color video camera, sonar, other environmental sensors 	<ul style="list-style-type: none"> • Increased situational awareness • Research/data collection • Surveying/mapping 		<ul style="list-style-type: none"> • Hydroid REMUS 100 • ATLAS SeaFox Mk II • Indel Partner Ltd. GNOM • Bluefin Robotics HAUV
Medium (351-5,000 lbs.)	<ul style="list-style-type: none"> • Larger vehicles that sacrifice ease of portability for greater payload capacity, depth, and endurance • Generally tele-operated, although some models are capable of semi-autonomous movement • Depth range: 1,900 ft. • Common sensors: Acoustic modem, sonar, color video camera, other environmental sensors 	<ul style="list-style-type: none"> • Mine countermeasures • Research/data collection • SAR • Surveying/mapping 		<ul style="list-style-type: none"> • ATLAS SeaCat • ATLAS SeaOtter • Hydroid REMUS 600 • BAE Talisman M
Heavy (5,000+ lbs.)	<ul style="list-style-type: none"> • Larger, more capable vehicles that may utilize modules or be designed to conduct specific tasks • Some models are capable of semi-autonomous movement, with the largest vehicles generally having more autonomy • Depth range: 10,000 ft. • Common sensors: advanced sonar array, special mission packages 	<ul style="list-style-type: none"> • Anti-submarine warfare • Cable laying • Mine countermeasures • Research/data collection • SAR • Surveying/mapping 		<ul style="list-style-type: none"> • Boeing Echo Ranger • i-Tech 7 QX Ultra • Proteus • ISE Ltd. Theseus • USN Large Vehicle Class UUV (planned)




Sources: Various; see endnote.³⁶

Table 1. A Typology of Unmanned Systems, continued (UMS: Unmanned Surface Systems)

SIZE	MAIN ATTRIBUTES	COMMON APPLICATIONS	IMAGE	EXAMPLES
Light (0-350 lbs.)	<ul style="list-style-type: none"> Small, lightweight, portable vehicles Most can be carried and deployed by a small team of individuals Generally tele-operated, although some models are capable of semi-autonomous movement Payload capacity: 100 lbs. Common sensors: Color video cameras, weather instruments, hydrophones, Acoustic Doppler Current Profiler 	<ul style="list-style-type: none"> Increased situational awareness Research/data collection Surveying/mapping 		<ul style="list-style-type: none"> Clearpath Robotics Kingfisher Liquid Robotics Wave Glider SV3 Njord Works Pioneer SeaRobotics USV-450 Heavy Payload Catamaran
Medium (351-5,000 lbs.)	<ul style="list-style-type: none"> Larger vehicles that sacrifice portability for greater payload capacity Generally tele-operated, although some models are capable of semi-autonomous movement Payload capacity: 220 lbs. Common sensors: Color video cameras, IR, communications relay devices, CBRN detection equipment 	<ul style="list-style-type: none"> Harbor patrol Hazardous materials detection Increased situational awareness Research/data collection Training/target practice 		<ul style="list-style-type: none"> Saab Piraya ASV Ltd. C-Hunter ASV Ltd. C-Stat Mobile Buoy Systems ASV Ltd. C-Target 3
Heavy (5,000+ lbs.)	<ul style="list-style-type: none"> Larger, more capable vehicles that may utilize modules or be designed to conduct specific tasks Larger models are capable of semiautonomous movement, with the largest vehicles generally having more autonomy Payload capacity: > 220 lbs. Common sensors: Color video cameras, IR video system, special mission packages 	<ul style="list-style-type: none"> Anti-submarine warfare Harbor patrol Increased situational awareness Mine sweeping countermeasures Surveying/mapping Training/target practice 		<ul style="list-style-type: none"> Zyvex Marine Piranha Elbit Systems Silver Marlin ASV Ltd. C-Sweep ASV Ltd. C-Target 13




Sources: Various; see endnote.³⁷

Table 1. A Typology of Unmanned Systems, continued (UAS: Rotary Wing)

SIZE	MAIN ATTRIBUTES	COMMON APPLICATIONS	IMAGE	EXAMPLES
Small (Weight: <55 lbs. Altitude: <400 ft.)	<ul style="list-style-type: none"> Small, easily transportable aircraft that can be operated by one individual Typical flight time: 10-25 minutes Sensors: Color video camera 	<ul style="list-style-type: none"> Increased situational awareness Site survey General mapping Photography Industrial inspection 		<ul style="list-style-type: none"> 3D Robotics Iris DJI Phantom
Medium (Weight: <1,320 lbs. Altitude: N/A)	<ul style="list-style-type: none"> Larger aircraft that requires more than one individual to deploy, fly, and maintain Typical flight time: 45-60 minutes Common sensors: Color video camera, LIDAR, terrain mapping equipment 	<ul style="list-style-type: none"> Site survey Specialized mapping Industrial inspection Agricultural applications 		<ul style="list-style-type: none"> Yamaha RMAX
Heavy (Weight: >1,320 lbs. Altitude: N/A)	<ul style="list-style-type: none"> Large, highly capable aircraft that is comparable in size to modern helicopters and requires a significant infrastructure to deploy and maintain Typical flight time: 6-8 hours Common sensors: EO/IR sensor ball, Synthetic Aperture Radar 	<ul style="list-style-type: none"> Surveillance Multi-demand missions Anti-submarine warfare Logistics support 		<ul style="list-style-type: none"> Northrop Grumman Fire Scout (MQ-8C)

Sources: Various; see endnote.³⁸

Table 1. A Typology of Unmanned Systems, continued (UAS: Fixed Wing)

SIZE	MAIN ATTRIBUTES	COMMON APPLICATIONS	IMAGE	EXAMPLES
Small (Weight: <55 lbs. Altitude: <400 ft.)	<ul style="list-style-type: none"> Small, hand-launched aircraft that can be easily deployed and operated by one individual Typical flight time: 60-90 minutes Sensors: Color video camera, IR video system 	<ul style="list-style-type: none"> Increased situational awareness Site survey General mapping Photography Industrial inspection Wildlife survey 		<ul style="list-style-type: none"> AeroVironment Raven Silent Falcon
Medium (Weight: <1,320 lbs. Altitude: <18,000 ft.)	<ul style="list-style-type: none"> Larger aircraft that requires more than one individual to deploy, fly, and maintain the system as well as a launching mechanism or runway for takeoff Typical flight time: 2-8 hours Common sensors: EO/IR video system, miniaturized radar system 	<ul style="list-style-type: none"> Broad area survey Specialized mapping Wide area industrial inspection Agricultural applications Wildlife survey 		<ul style="list-style-type: none"> Boeing Scan Eagle AAI Shadow
Heavy (Weight: >1,320 lbs. Altitude: >18,000 ft.)	<ul style="list-style-type: none"> Large, highly capable aircraft that requires a significant infrastructure to deploy and maintain but offers significantly more capabilities than smaller systems Typical flight time: 18-24 hours Common sensors: EO/IR sensor ball, various synthetic aperture radars, atmospheric and environmental sensor, wide area surveillance sensors 	<ul style="list-style-type: none"> Persistent surveillance Multi-demand missions Atmospheric monitoring Aerial communication relay 		<ul style="list-style-type: none"> General Atomics Predator/Guardian Northrup Grumman Global Hawk

Sources: Various; see endnote.³⁹

Research, development, testing, and evaluation will likely overcome many of these safety and operational challenges, and next-generation (within five years) unmanned systems are likely to be safer and easier to operate. The USAF envisions next-generation UAS, for example, that “must be multi-mission, adverse weather capable, net-centric, modular, use open architecture, and employ appropriate levels of autonomy.”⁴⁰ These objectives are largely achievable. The most important near-term technology will be SAA to allow for safer operation. Greater inclusion of autonomous functions will also improve safety and address inherent challenges in sustained communications and will reduce the burden on the operator, including potentially reducing the requirement for sUAS to employ a dedicated operator to maintain LOS contact. Further, control of next-generation unmanned systems will likely be increasingly intuitive, allowing for non-expert operators to employ systems safely and with desired effect. Unmanned systems engineers are leveraging intuitive software interfaces through a range of control stations to enable simple control, or control of multiple platforms.⁴¹ Advances in human-systems interfaces, including wearable technology, and systems that autonomously follow a designated user⁴² will make the operation of systems seamless from other activities. And next-generation unmanned systems are likely to offer new modes of operation. There is growing experimentation in the use of groups of multiple unmanned systems interacting together and sharing sensor data to achieve a mission. This includes a concept referred to as “swarming,” in which multiple UAS move and surround items of interest as an insect swarm would do.⁴³ DoD and others are also exploring the concept of “manned-unmanned teaming,” which pairs unmanned systems with existing manned platforms to achieve a mission more safely or effectively.⁴⁴

As technology matures and experimentation continues, unmanned systems are expected to become broadly viable for a range of commercial purposes in the United States.⁴⁵ When Amazon announced in November 2013 its intent to deliver packages using UAS,⁴⁶ it seemed to many that achieving that goal could take far longer than the four-to-five-year timeline stated by Amazon chief executive officer (CEO) Jeff Bezos.⁴⁷ In August 2014, Google announced similar intent,⁴⁸ and even in the eight months between announcements, technological and other developments shaped the environment to make both companies’ plans appear more feasible. For example, the Federal Aviation Administration (FAA) has granted exemptions from current regulation for commercial experimentation with sUAS in the energy and entertainment industries, pushing forward proof of concept in use of the technology.⁴⁹ sUAS should substitute in some missions currently performed by existing manned aircraft (particularly rotary aircraft) and likely will create new industries and applications as well.

Hobbyist use of unmanned systems is growing rapidly, and the automotive industry will likely bring unmanned vehicles to the consumer market by 2020. There is a longstanding hobbyist community of radio frequency remote-controlled airplanes, boats, and cars that dates back to the 1930s.⁵⁰ However, availability of relatively affordable, preassembled, and easy-to-operate current-generation unmanned systems has led to significantly greater interest.⁵¹ The smallest and simplest unmanned systems have benefitted from global trends in the availability and relatively low cost of sophisticated microelectronics, and companies such as Parrot (based in France) and DJI (based in China) have produced capable sUAS for amusement, photography, and videography at consumer price points, opening a fast-growing market.⁵² The transition of automobiles from human-operated to unmanned, semi-autonomous operation is progressing. The first experimental Google autonomous vehicle was introduced to public streets in 2011. Commercial automakers are increasing the integration of so-called autopilot (limited autonomy)⁵³ and vehicle-to-vehicle (V2V) networking technologies in luxury vehicles.⁵⁴ In October 2014, CEO and chief product architect of Tesla Motors, Elon Musk, noted that “maybe five or six years from now, I think

we'll be able to achieve true autonomous driving where you could literally get in the car, go to sleep, and wake up at your destination."⁵⁵

Strong growth is forecast in the U.S. and global military and commercial markets for unmanned systems. The United States seems poised to enter a decade of rapid and sustained growth in the domestic use of unmanned systems, particularly UAS below 55 pounds (sUAS). The growth of that market segment will likely mirror the U.S. military's own UAS structure, in which more than 90 percent of 11,000 total UAS are sUAS.⁵⁶ Estimates vary on how dramatic overall domestic UAS growth could be, subject to constraints related to safety, laws (including ongoing FAA rulemaking), available technology, and societal perceptions (discussed in section VI, "Constraints"). The Teal Group Corporation forecasts that "the potential for civilian UAS will come, but it will take time to develop and will not be anywhere near the value of the military market anytime soon."⁵⁷ At the optimistic end of the spectrum, AUVSI estimates that in the first three years following FAA approval of UAS integration in the National Airspace System (NAS), more than 70,000 jobs will be created in the United States with an economic impact of more than \$13.6 billion. The association predicts growth out to 2025 of more than 100,000 jobs created and economic impact of \$82 billion.⁵⁸ Both forecasts agree that the fastest growth is likely to occur in civil government use (including a number of HSE mission areas) and precision agriculture, with potentially tens of thousands of sUAS coming into use.⁵⁹ Estimates for potential growth of UGS and UMS could also be significant. The research firm MarketsandMarkets reports that the global UGS market could increase to \$8.6 billion by 2020, up from \$1.5 billion in 2014, with a broad and growing range of applications.⁶⁰ The same firm has estimated that the subsurface UMS market (focused on scientific, oil and gas, and military purposes) could grow to \$4.8 billion by 2019.⁶¹ No reliable figures are available for surface UMS, though plans to field the technology in the \$375 billion-per-year commercial shipping industry by companies such as Rolls-Royce⁶² suggest potential large-scale growth.

Lastly, increased demand for unmanned systems is being met with a growing, global supply base. The United States, Japan, China, Israel, France, Switzerland, and Austria are generally considered the leading suppliers of unmanned systems, capable of producing both high-end military systems and less expensive (but often very capable) consumer products.⁶³ And almost all countries are engaged with some kind of formal R&D or informal experimentation of the use of unmanned systems for a range of applications. The international competitiveness of the industry is spurring innovation and driving down prices, with U.S. industry directly competing against a growing range of foreign producers.⁶⁴ And notably, the capability overlap can be significant between hobbyist-grade and professional-grade unmanned systems. In some cases, such as the adoption of widely available tablets and smartphones as control stations, hobbyist-grade UAS have been ahead of professional-grade systems. Online open-source communities also allow hobbyists to rapidly develop new platforms and share innovations, including controller software, platform and sensor firmware, and 3D-printable components.⁶⁵



IV. Current Use in the HSE

This section discusses current use of unmanned systems in the HSE. It sets forth use of unmanned systems by select federal government departments and agencies, state and local first responders, and the private sector (primarily critical infrastructure owners and operators).⁶⁶

In sum, the research suggests that current use is largely limited to deployment of UAS for border security missions by DHS and UGS for EOD missions by law enforcement at federal, state, and local levels. sUAS and UMS appear to be used infrequently at best. DoD, the largest owner and operator of unmanned systems worldwide, has rarely deployed its assets for homeland security use in CONUS (in part because such use requires approval from the Secretary of Defense). Current use is discussed in sections below.

A. DHS

DHS is the most sophisticated user of unmanned systems in the homeland security enterprise. It currently operates large UAS principally in border and maritime security missions. It also operates UGS for EOD missions and in tunnel investigations. Uses are discussed in turn, beginning with UAS.

DHS has operated UAS since June 2004,⁶⁷ primarily in support of border security missions.⁶⁸ DHS first experimented with an Israeli-made Hermes UAS in support of the Arizona Border Control Initiative, then in early 2005 with a Northrop Grumman RQ-5 Hunter.⁶⁹ Later that year, CBP announced its decision to acquire and operate the General Atomics Predator B UAS (an unarmed Predator variant) on the southern border.⁷⁰ In 2009, CBP's OAM (formed in 2006) acquired a second Predator B to base in North Dakota for northern border missions.⁷¹ In 2008, OAM and the USCG "formed a UAS Joint Program Office to identify and address common maritime UAS requirements, including sensors, command and control, data exploitation, logistics and training, and basing."⁷² That led to the acquisition in late 2009 of the Guardian, which is "modified from a standard Predator B with structural, avionics, and communications enhancements, as well as the addition of a Raytheon SeaVue Marine Search Radar and an Electro-optical/Infrared (EO/IR) Sensor that is optimized for maritime operations."⁷³ The maritime variant was to focus on the U.S. Southeast Coastal Border Region, the Great Lakes/

St. Lawrence Seaway, and the Extended Border/Transit Zone.⁷⁴ CBP had planned to acquire 24 total systems⁷⁵ dispersed at airbases across the country, enabling a flight time of only three hours to any major populated area in the continental United States for disaster response. However, due to budget considerations, DHS settled on a current force structure of nine aircraft (seven Predator B and two Guardian aircraft).

OAM currently operates Predator B UAS from Libby Army Airfield (Sierra Vista, Arizona) and Grand Forks Air Force Base (North Dakota) and, jointly with the USCG, operates Guardian UAS from Naval Air Station Corpus Christi (Corpus Christi, Texas).⁷⁶ These aircraft use interoperable ground control stations forward located at takeoff-and-landing facilities, as well as satellite links that allow sustained communications when the aircraft moves beyond LOS (terrestrial frequency range). Once the aircraft is airborne, control can be transferred to any of the control station locations in Corpus Christi, Grand Forks, or Sierra Vista. Through the use of a mobile ground control station, CBP can also leverage existing relationships with other airfields in the United States (such as Fort Drum, New York) to establish takeoff-and-landing operations elsewhere for certain contingency responses. As previously noted, this ability to control a UAS from multiple locations is referred to as remote split operations. Flight crews from any location can control any airborne aircraft, although takeoff and landing are handled at the local airfield. These aircraft have the ability to fly more than 20 hours, though CBP appears to typically operate them for approximately 16 hours per flight.⁷⁷

According to DHS, OAM UAS are used primarily “in support of law enforcement and homeland security missions at the nation’s borders.”⁷⁸ The UAS have also performed disaster relief missions in support of the Federal Emergency Management Agency (FEMA) and USCG. A recent GAO study found that “over 80 percent of CBP’s UAS flight hours were associated with airspace encompassing border and coastal areas,”⁷⁹ with the additional 20 percent of activity explained by the fact that “CBP also uses UAS in support of other federal, state, or local law enforcement activities and for emergency humanitarian efforts....”⁸⁰ In this regard, CBP may provide UAS capability to other DHS operational components, such as FEMA or Immigration and Customs Enforcement. Civil society groups such as the Electronic Frontier Foundation have criticized the use of UAS in non-border and maritime missions,⁸¹ derisively calling the practice “loan-a-drone.” GAO, however, found that current use of UAS is within the authorities of DHS.⁸² CBP officials often point to the flexibility in response to a broad range of contingencies that UAS can provide both within the continental United States and in international approaches, contributing to homeland “active, layered defense in depth.”⁸³ External operation of UAS includes routine monitoring of Caribbean locations and has included deployment to San Isidro Air Force Base in the Dominican Republic.⁸⁴


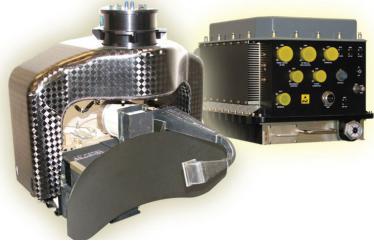


Since early 2013, the OAM Predator B fleet has been used to patrol remote sections of the border where officials suspect there is little illegal activity. The approach involves the deployment of a Predator B with high-resolution sensors to an isolated stretch of the border where there are no fences, Border Patrol agents, or other assets to detect illegal activity. Another flight is dispatched several days later to overfly the same terrain. Using advanced imagery software, analysts review the images from both missions to detect small changes, such as tire tracks. If any changes are detected, a team is dispatched to investigate the area and, if necessary, install cameras or other security infrastructure to deter illegal activity. According to CBP officials, only 8 percent of the missions indicated enough of a change in the terrain to dispatch ground personnel.⁸⁵ Some have observed that CBP is using these

UAS to “prove the negative” by ascertaining that there is not activity in remote areas, rather than supporting operations in high-traffic zones.⁸⁶

OAM has worked closely with the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD AT&L) to develop its UAS sensor capabilities. OAM has provided valuable test platforms and flight time for OSD AT&L and in return received sensor technology to meet its requirements, which it would not have been otherwise able to develop and field (see table 2, below, for a description of sensor capabilities). OAM continues to experiment with new sensors, including with Sandia National Laboratories and the USAF, to test a specialized sensor pod dubbed “Harvester” for nuclear forensics (post-detonation air sampling to identify the origin of an exploded atomic weapon) with test flights from Grand Forks Air Force Base.⁸⁷

Data collected from OAM UAS are fed into “Big Pipe,” a CBP/DHS video and image distribution network that shares live images and near-real-time video feeds to mission operators worldwide.⁸⁸ CBP also has operational cells for PED at the Air and Marine Operations Center in Riverside, California, and in Grand Forks.⁸⁹ These cells focus on the fusion of data from manned and unmanned aircraft, aerostats, FAA radars, and other sources. These fusion cells can compare time-series data and use change detection algorithms to highlight, for instance, patterns of activity in certain border sectors and determine where to direct manpower and on-the-ground assets, including confirming which areas are safe to lightly patrol.

Table 2. A Selection of Airborne Sensors

SENSOR	CAPABILITIES	IMAGE
Raytheon Multi-Spectral Targeting System (MTS-B)	The MTS-B provides multi-spectral imaging, including day television, low-light television, and infrared sensors for operations in day and night conditions. The sensor package also includes a laser ranger-finder/designator. This sensor is most likely to be used from the monitoring through apprehension phases of any mission.	
General Atomics Lynx Multi-mode Synthetic Aperture / Ground Moving Target Indicator Radar	The Lynx radar provides surveillance and imaging capabilities even in poor-visibility conditions and through cloud cover. This adaptable sensor may be used from detection through apprehension.	
Northrup Grumman Vehicle and Dismount Exploitation Radar (VADER)	VADER was originally designed to detect roadside bombs in Afghanistan and Iraq. This system can detect vehicles and individuals at long ranges and against a high degree of background clutter. This sensor is most likely to be used for broad-area surveillance and initial detection.	
Raytheon SeaVue Surveillance Radar	The SeaVue radar is used for maritime surveillance missions with its wide-area search capabilities optimized to detect small targets at sea. This sensor may be used during the detection and monitoring phases.	

Sources: Various; see endnote.⁹⁰

OAM has experimented with sUAS, but it is unlikely to acquire or field them until FAA sUAS rules are in place.⁹¹ OAM customers such as the CBP Office of Border Patrol (OBP) are interested in integrating sUAS into border missions, especially for OBP special operations units. OAM has experimented in the past with sUAS, such as the AeroVironment Battlefield Air Targeting Micro Air Vehicle, but did not feel the capability matched mission requirements and had concerns about airspace deconfliction with rotary aircraft. OAM has no specific plans in place to restart sUAS experimentation, but the issue is under discussion with OBP.⁹²

Beyond its partnership and cooperation with OAM on Guardian UAS, the USCG is waiting to move ahead with other UAS until FAA guidance on NAS integration is released and “the capability has sufficiently evolved (from a technological perspective).”⁹³ In particular, the USCG suggests that current-generation UAS are insufficient because they lack SAA and are not sufficiently all-weather.⁹⁴ The USCG has also partnered with the U.S. Navy on UAS, including investigation of the large rotary Northrop Grumman MQ-8B Fire Scout as a potential platform for the USCG national security cutter. The USCG had previously explored a large vertical-take-off-and-landing (tilt-rotor) UAS but abandoned it due to concerns about cost and capability. For the past several years, the USCG has conducted demonstrations of the Insitu ScanEagle tactical UAS, and it is also investigating the Insitu RQ-21A Blackjack that is being fielded by the U.S. Marine Corps. These UAS can be launched and recovered using a small pneumatic launcher and recovered using a “skyhook” (large pole with arresting cable).⁹⁵

In 2012, DHS S&T launched a field experimentation project for sUAS ... to volunteer their systems for assessment “under a wide variety of simulated but realistic and relevant real-world operational scenarios, focusing on response to situations where human lives are in imminent danger” at the U.S. Army’s Fort Sill training range near Lawton, Oklahoma.⁹⁶ Results from testing of technical capabilities are shared on FirstResponder.gov, along with information for HSE users on FAA guidelines and privacy considerations. RAPS is a “*Consumer Reports* for sUAS” and is viewed positively across the homeland security community, with its emphasis on identifying the right platform and right payload for specific mission requirements.⁹⁷ DHS S&T plans to continue the project in fiscal year (FY) 2015 and also to partner with the USCG on a new Robotic Aircraft for Maritime Public Safety program.

DHS S&T began specific investigation of unmanned systems for tunnel detection and investigation after 2010 and has fielded several systems for this purpose.⁹⁸ DHS has focused on meeting requirements along the Southwest border where nearly all tunnel attempts have been discovered.⁹⁹ OBP is the lead office for the CBP Tunnel Detection and Technology Program, supported by the CBP Office of Technology Innovation and Acquisition.¹⁰⁰ OBP Chief Michael Fisher named tunnel technology procurement a top priority in 2012, but DHS has lacked funding for prototype testing and has depended on industry to develop, test, and pitch new technology to meet the requirement.¹⁰¹ Because there is no unmanned system on the market designed specifically for tunnel exploration, DHS has experimented with various UGS for the tunnel environment. As of early 2014, CBP had deployed a small number of Inuktun 150 Pipe Inspection Crawlers (used commercially in sewer and storm drains, for mining purposes, and in oil and gas refineries) and ARA Pointman Robots (designed to support police, military, and SWAT operations in urban environments).¹⁰² Tunnels are usually first discovered by human intelligence, then investigated by a UGS to verify they are safe to enter, and finally inspected by a Border Patrol agent.¹⁰³

DHS S&T is pursuing additional unmanned tunnel detection systems through partnerships with industry and DoD.¹⁰⁴ One example is the Counter Tunnel System by the Space and Naval Warfare Systems Center Pacific and Air Force Research Laboratory. This program has focused primarily on providing a 3D localization, mapping, and characterization tool specifically built for tunnels. SSC Pacific held a test event of the Counter Tunnel Exploitation Robot and iRobot Packbot platforms with CBP in November 2013. The platforms performed well but have not yet been deployed in the border environment.¹⁰⁵

DHS S&T also maintains UGS research programs for EOD missions. For instance, the Semi Autonomous Pipe Bomb End-cap Remover offers EOD capability that additionally preserves forensic evidence.¹⁰⁶ And DHS S&T has contributed to standards for use by the manufacturers of UGS (and UAS/UMS) for various missions, including SAR and EOD.¹⁰⁷

The only HSE user currently known to operate UMS (including the USCG, which has no identified requirement) is DHS S&T, via its BIOSwimmer research program.¹⁰⁸ However, the U.S. Navy has recently increased its experimentation and interest in a range of surface and subsurface systems. This may eventually have spillover effects for broader U.S. domestic use, including for the HSE, in the same way that U.S. military research, development, and use of UAS and UGS have. Limiting factors to date for all users have been cost and relatively limited proven application.¹⁰⁹

B. Department of Defense

DoD unmanned systems can be used domestically as part of HD and Defense Support to Civil Authorities (DSCA) operations and military training and exercises, contingent upon approval by the Secretary of Defense.¹¹⁰ Any DoD capabilities provided for HD or DSCA purposes are done so based on mission requirements, not on a request for a specific platform or system. Unmanned systems are therefore only assigned when there is a unique requirement they are able to meet and they are available for such purpose (i.e., not engaged overseas). Use of UAS also requires an FAA Certificate of Waiver or Authorization (COA) and must take into consideration communications deconfliction and needs—a particularly important issue for smaller unmanned systems that may not use satellite links and were not designed for use in the United States. The use of armed DoD UAS in the United States for HD and DSCA is not authorized.

The Air National Guard has seven large UAS units: six MQ-1 Predators units (based in Arizona, California, North Dakota, Ohio, and Texas), and one MQ-9 Reaper squadron in New York.¹¹¹ These units have been heavily engaged in support of overseas contingency operations for several years, including “11 RPA combat patrols worldwide 365 days per year, totaling nearly 85,000 hours annually.”¹¹² Air National Guard UAS have only been used once to date for DSCA, in support of the National Interagency Fire Center’s response to the 2013 Rim Fire in Yosemite National Park, in which UAS persistence and sensors offered unique capability.¹¹³

The Army National Guard operates RQ-11 Raven B and RQ-7B Shadow UAS. The Army National Guard plans to have 982 Raven systems (with 3 aircraft each, equaling 2,946 platforms) by the end of FY 2016.¹¹⁴ Currently, the Army National Guard has 704 Raven systems (in theory equaling 2,112 airframes). The Army National Guard has 32 RQ-7B Shadow Tactical UAS in operation.¹¹⁵

As with all DoD assets, governors in states with UAS may not employ these UAS under Title 32 status¹¹⁶ without the approval of the Secretary of Defense. Also, any plans to use these assets must factor in the procedures and time required for FAA COAs.

DoD appears to provide only limited UGS or UGS-related support, such as training, for EOD missions. This is not necessarily surprising, as many entities across the HSE possess their own UGS. Note, however, that surplus DoD equipment, including UGS, is often provided to state and local law enforcement under the “1033 Program” under the National Defense Authorization Act of Fiscal Year 1997.¹¹⁷

C. Other Federal Departments and Agencies¹¹⁸

Within the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI) operates sUAS.¹¹⁹ The FBI Technical Surveillance Section leads the FBI UAS program and uses fixed-wing, COTS sUAS. It flies sUAS only within LOS, with an operator and a separate observer. The FBI considers sUAS a niche capability for specific missions in which persistence and stealth are at a premium and considers them extremely effective in this application.¹²⁰ The FBI treats specific information regarding platforms and sensors as highly sensitive. The Bureau of Alcohol, Tobacco, and Firearms is considering an operational capability but has not publicly elaborated on its plans.¹²¹ The Drug Enforcement Administration and the U.S. Marshals Service, also within DOJ, appear to have “acquired UAS for testing, but ... have no plans to deploy them operationally.”¹²²

DOJ’s National Institute of Justice (NIJ) has considered the use of sUAS for public safety and issues guidance and conducts analysis on the subject. NIJ has focused on practical matters for nonfederal law enforcement agency UAS use, including the negotiation of a memorandum of understanding with the FAA “to implement a streamlined training and authorization process to enable nonfederal law enforcement agencies ... to operate ... UAS ... within the United States safely, effectively, and lawfully.”¹²³

Federal departments and agencies operate UGS to perform EOD missions. These UGS typically employ a treaded platform able to negotiate stairs and rough terrain and possess a camera and a manipulator arm that allow remote operators to inspect a suspicious object and, in some cases, safely dispose of it. For example, the FBI maintains its own EOD teams with mission-specific UGS. In addition, the FBI runs the Hazardous Device School, which services as a training hub for state and local EOD technicians.¹²⁴

D. State and Local First Responders

State and local first responders have expressed interest in unmanned systems, including UAS and UGS, though barriers exist. State and local first responders have acquired a range of COTS sUAS through direct expenditures, donations, and DHS and NIJ grants.¹²⁵ Adoption, however, has been limited for reasons covered in depth in section VI, “Constraints,” including the legal complexity and ambiguity surrounding the use of UAS and public attitudes toward UAS.¹²⁶ For example, the Los Angeles Police Department acquired two sUAS but has not put them to use, awaiting the outcome of its police commission’s issuance of guidelines regarding UAS use, which was ordered in response to strong negative public reaction.¹²⁷ The sUAS were donated to Los Angeles by the Seattle Police Department, which abandoned plans to field them following local public outcry.¹²⁸ The

current shortcomings of sUAS technology and need for operator training also seem to have played a role in hindering adoption.

That said, first responders in certain jurisdictions have demonstrated the utility of UAS for applications such as SAR, crime scene documentation and accident investigation, and limited tactical use. The Mesa County, Colorado, Sheriff's Office, for example, is widely regarded as leading the way for state and local sUAS use.¹²⁹ FAA-approved test centers around the country are allowing state and local first responders to test UAS in certain settings alongside federal entities, academics, and industry.

State and local police and fire departments nationwide operate UGS to perform EOD missions. Large metropolitan police and fire departments, as well as state organizations, have operated such UGS for several decades. Since the mid-2000s, various federal grant programs (including those administered by FEMA) have also made these systems available to smaller municipalities.¹³⁰

E. Private Sector

The FAA has recently approved increased private-sector experimentation with sUAS for infrastructure monitoring, but use to date is extremely limited. The FAA issued a Special Airworthiness Certificate (SAC) for sUAS operation to Sempra's San Diego Gas & Electric to become the first utility in the country to "research, test and train flight crews on the UAS in a sparsely populated airspace in Eastern San Diego County."¹³¹ The FAA also approved AeroVironment and BP with a COA "to survey BP pipelines, roads and equipment at Prudhoe Bay, AK, the largest oil field in the United States."¹³² These are first movers in a field that has the potential for tremendous growth if a permissive regulatory and legal environment is created.

Lastly, on the ground, UGS have been used for many years for emergency response missions by critical infrastructure owners and operators. These missions include chemical or other toxic substance cleanup (not unlike what was seen after the Fukushima Daiichi nuclear plant incident in Japan, where UGS were employed for debris removal and decontamination).¹³³ UGS are also used for infrastructure inspection (e.g., for pipelines, bridges).¹³⁴ Emerging technology will facilitate use of UGS for mobile sentry applications (i.e., intrusion detection and fence-line patrol).¹³⁵



V. Future Requirements

This section examines requirements in the HSE for unmanned systems. Examination of such requirements allows decision makers to begin to understand those requirements that can be met with existing unmanned systems; requirements that might be met with such systems but that call for some focused R&D; requirements that are perhaps best met by manned systems; and gaps in need of policy or regulatory guidance or deconfliction. This, in turn, allows for development of policies and procedures to guide use of unmanned systems; acquisition strategies; methodologies to support apples-to-apples comparison of manned and unmanned systems on a cost-per-some-unit-of-analysis basis (for limited cost-benefit analyses or deeper analyses of alternatives); and R&D plans.

This section is intended to serve as a foundation for future decision making (i.e., it represents the beginning of a longer dialog) by framing the concept of requirements and, at a high level, the extent to which unmanned systems can meet those requirements. The section begins by defining requirements. It then presents an analysis of HSE missions to allow for consideration of the ability of unmanned systems to meet HSE requirements.¹³⁶

Per the Defense Acquisition University (DAU), a *requirement* is defined as “the need or demand for personnel, equipment, facilities, other resources, or services, by specified quantities for specific periods of time or at a specified time”; *operational requirements* are defined as “user- or user-representative-generated validated needs developed to address mission area deficiencies, evolving threats, emerging technologies, or weapon system cost improvements.”¹³⁷ Per DHS, requirements “define ‘the problem.’ In contrast, ‘the solution’ is defined by technical specifications.”¹³⁸ For the present paper, a requirement is defined as a “mission need.” Requirements are typically set by operators, with input from the acquisition and strategy/policy communities.

Requirements are guided by organizational strategies and plans and their associated goals and objectives, explicit or implicit.¹³⁹ For the HSE, this implies that requirements are guided by the QHSR and associated subordinate strategic documents. As noted above, the QHSR sets forth the HSE missions as follows: prevent terrorism and enhance security; secure and manage U.S. borders; enforce and administer U.S. immigration laws; safeguard and secure cyberspace; and strengthen national preparedness and resilience. Distilled to their essence, these missions may be described as:

- counter dangerous or illegal *people* (e.g., terrorists, illegal migrants, transnational organized criminals [TOCs]);
- counter dangerous or illegal *goods* (e.g., CBRNE; illicit narcotics; illicit contraband, including bulk cash, counterfeit goods, pests/animals);
- emergency (i.e., natural disasters, large-scale accidents, terrorist attacks) preparedness (including safety, such as the aids to navigation responsibilities of the USCG);
- emergency response;
- critical infrastructure security; and
- critical infrastructure resilience.¹⁴⁰

As stated in the 2014 QHSR, “homeland security is national risk management.”¹⁴¹ Risk is the “effect of uncertainty on objectives;”¹⁴² it is a function of threat, vulnerability, and consequence.¹⁴³ The HSE missions are risk management missions: each focuses on one or more elements of risk. That is, HSE missions relate to managing—identifying, assessing and treating—threat, vulnerability, and/or consequence. For example, the CT mission is a threat-focused mission, in that it requires identifying, assessing, and treating the threat posed by terrorist adversaries. Critical infrastructure security (i.e., preparedness) is a vulnerability-focused mission, in that it requires identifying, assessing, and treating vulnerabilities of critical infrastructure systems or assets, like a component of a region’s power transmission or distribution grid. Emergency response is a consequence-focused mission, in that it requires identifying, assessing, and treating consequences of an adverse event, like Superstorm Sandy. Table 3 categorizes the HSE missions depending on their focus on threat, vulnerability, or consequence management.

Table 3. Categorization of HSE Missions by Their Focus on Threat, Vulnerability, or Consequence Management

THREAT MANAGEMENT	VULNERABILITY MANAGEMENT	CONSEQUENCE MANAGEMENT
<ul style="list-style-type: none"> • Counter dangerous/illegal people • Counter dangerous/illegal goods 	<ul style="list-style-type: none"> • Emergency preparedness • Critical infrastructure security 	<ul style="list-style-type: none"> • Emergency response • Critical infrastructure resilience

Note: Certain HSE missions are outside the scope of this paper, including cybersecurity (though it is recognized that there is a cybersecurity element to unmanned systems).

Threat, vulnerability, and consequence missions each can be disaggregated into specific phases (i.e., activities). For example, DHS and others in the HSE seek to manage threats, such as terrorists and CBRNE, illegal migrants, or illicit narcotics. Threat management (often called interdiction) is a formal process with several phases, as noted in the *National Interdiction Command and Control Plan* (NICCP), and other sources; see box 1, below. Missions focused on managing vulnerabilities or consequences can be similarly disaggregated into specific phases; see boxes 2 and 3.¹⁴⁴ Note that the information presented in boxes 1 through 3 is notional.

Critically, these mission phases drive requirements. If threats must be interdicted in phases of cueing, detection, monitoring, and the like, then HSE entities need to be able to cue, detect, and monitor. In this example, HSE entities will require a surveillance capability with tracking. Of course, HSE missions and associated phases do not exist in a vacuum; rather, the missions are carried out in different places (e.g., continental United States or outside the continental United States, in source or transit zones), at different times (of the year, of the day), and to manage different threats, vulnerabilities, and consequences. Accordingly, the “what, where, when, who, why,

how” mission parameters—both tactical and strategic—will affect the requirements. For example, detection and monitoring of a threat likely to exist at unknown (or all) times of the day may call for persistent surveillance, whereas a threat likely to exist for a very specific time period may call for limited surveillance. Similarly, the “where” parameter may call for more robust all-weather capabilities if prevailing weather conditions in the operating environment are likely to be more harsh. Note that phases in italics in the boxes below were assessed by the research team to be those for which unmanned systems might play a role, either by sensing or acting or through archived PED output. The case for some phases is stronger than for others; the point, however, is that there are clearly some phases of threat, vulnerability, and consequence management that might benefit from the use of unmanned systems.

BOX 1. [THE PHASES OF THREAT] INTERDICTION (AS DEFINED BY THE NICCP, PRINTED IN DOD JOINT PUBLICATION 3-07.4, JOINT COUNTERDRUG OPERATIONS, APPENDIX J)

Interdiction: A general term used to describe the efforts focused on interrupting a specified activity. A completed drug interdiction [or an interdiction of other illicit flows or threats] normally consists of several phases, some of which may occur simultaneously.¹⁴⁵

- Cueing: Providing actionable intelligence to operating forces.
- Detection: *The initial acquisition of a contact.*
- Monitoring: *The tracking and/or interception of a contact.*
 - Tracking: *To maintain detection information (position, course, and speed) on a target.*
 - Intercept: *To direct the movement of an asset to the scene of a contact, either for purposes of identification or to position the asset to take further action.*
- Sorting/Classifying: *The process involved in identifying drug smuggling traffic [or that of other illicit flows] from legitimate traffic.*
- Handoff: *The act of shifting primary responsibility between forces or actors.*
- Disruption: *Halting an activity, usually the transportation of contraband, either permanently (by effecting an endgame) or temporarily (by causing an abort).*
- Endgame: The goal: in this case, usually the apprehension, causing the jettison of contraband, or arrest of offenders.
- Apprehension: The detention, arrest, or seizure of suspects, evidentiary items, contraband, and/or vehicles.

Note: **Phases in italics were assessed by the research team to be those for which unmanned systems might play some role**, large or small. Source: NICCP, as printed in DoD Joint Publication 3-07.4, Joint Counterdrug Operations, appendix J, J8, <http://www.fas.org/irp/doddir/dod/jp3-07-4.pdf>.

BOX 2. ACTIVITIES ASSOCIATED WITH VULNERABILITY MANAGEMENT (AS DEFINED BY FEMA AS PART OF A COURSE ENTITLED BUILDING DESIGN FOR HOMELAND SECURITY; UNIT IV: VULNERABILITY ASSESSMENT)

Vulnerability management process elements:¹⁴⁶

- Define site functions.
- Identify critical systems.
- Evaluate facility system interactions.
- Determine common system vulnerabilities.
- *Physically locate components and lines.*
- Identify critical components and nodes.
- *Assess critical nodes v. threats.*
- Determine survivability enhancements and options.
- *Document analytic processes.*
- *Treat identified vulnerabilities (e.g., fortify defenses).*¹⁴⁷

Note: **Phases in italics were assessed by the research team as those for which unmanned systems might play some role**, large or small. Adapted from source: FEMA, Building Design for Homeland Security course materials, Unit IV: Vulnerability Assessment, Slide IV-20 'Options to Reduce Vulnerability', 2008.¹⁴⁸

BOX 3. CAPABILITIES GUIDING CONSEQUENCE MANAGEMENT (ADAPTED FROM THE NATIONAL PREPAREDNESS GOAL DEVELOPED PURSUANT TO PRESIDENTIAL POLICY DIRECTIVE 8: NATIONAL PREPAREDNESS)¹⁴⁹

Shared by response and recovery: Capabilities spanning the entire consequence management time frame:

- Planning: Engage in a systematic process to develop executable strategic, operational, and community-based approaches to meet defined objectives.
- Public information and warning: *Deliver coordinated, prompt, reliable, and actionable information to the whole community.*
- Operational coordination: Establish and maintain a unified and coordinated operational structure and process and integrate stakeholders and support operations.
- Infrastructure systems: *Stabilize critical infrastructure functions, minimizing health and safety threats, and restoring and revitalizing systems.*

Response: Capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred:

- Critical transportation: *Provide transportation for evacuation and delivery of response personnel, equipment, and services.*
- Environmental response/health and safety: *Make guidance and resources available to address all hazards, including hazardous materials, terrorism, and disasters, such as relates to clean-up actions and assessments.*
- Fatality management services: *Provide body recovery and victim identification, collaborating with state and local authorities for temporary mortuary solutions, sharing information for reunification, and providing counseling.*
- Mass care services: *Provide life-sustaining services, including hydration, feeding, and sheltering and leading family reunification.*
- Mass SAR operations: *Deliver traditional and atypical SAR capabilities, including personnel, services, animals, and assets.*
- On-scene security and protection: *Ensure a safe and secure operating environment through law enforcement and related operations.*

(continued on next page)

BOX 3. CAPABILITIES GUIDING CONSEQUENCE MANAGEMENT (ADAPTED FROM THE NATIONAL PREPAREDNESS GOAL DEVELOPED PURSUANT TO PRESIDENTIAL POLICY DIRECTIVE 8: NATIONAL PREPAREDNESS)—CONTINUED

- *Operational communications:* Support timely communications in support of security, situational awareness, and operations, among and between communities in the impact area and all responders.
- *Public and private services and resources:* Provide essential public and private services to the affected community, including emergency power to critical facilities, fuel support to emergency responders, and access to community staples and response services.
- *Public health and medical services:* Provide lifesaving medical treatment via emergency medical services and related operations and avoid additional disease and injury through targeted public health and medical support and products.
- *Situational assessment:* Provide decision makers with relevant information regarding the nature of the hazard, cascading effects, and the status of the response.

Recovery: Capabilities necessary to assist communities affected by an incident to recover effectively:

- *Economic recovery:* Return economic and business activities to a healthy state and develop new opportunities contributing to a sustainable and economically viable community.
- *Health and social services:* Restore and improve health and social services networks.
- *Housing:* Implement sustainable and resilient housing solutions across the whole community.
- *Natural and cultural resources:* Preserve and rehabilitate natural and cultural resources and historic properties.

Note: **Phases in italics were assessed by the research team as those for which unmanned systems might play some role**, large or small. Source: Adapted from DHS, *National Preparedness Goal*, 2011, pp 12-18. (http://www.fema.gov/media-library-data/20130726-1828-25045-9470/national_preparedness_goal_2011.pdf)

Thinking about the HSE missions, their mission phases, and associated mission parameters allows for thinking about the requirements for unmanned systems. The following questions inform requirements setting and early thinking on meeting any requirements:

- Do these missions, phases, and parameters call for the use of either manned or unmanned systems?
- Do unmanned systems offer greater effectiveness or efficiency than manned systems in meeting requirements (as set forth in specific phases, given mission parameters)?
- Do missions, phases, and parameters call for neither manned nor unmanned systems (e.g., might an immobile pole-mounted camera be best)?
- Do they call for both (i.e., via manned-unmanned teaming)?
- Can requirements be met with the purchase of sensor data vice full use of unmanned systems?¹⁵⁰
- Are there missions or phases in which manned intervention is required (and are these limiting factors in the use of unmanned systems in earlier phases)?¹⁵¹
- Is unmanned systems technology currently capable of fulfilling requirements?
- Do other constraints on the use of unmanned systems exist?¹⁵²

As noted, unmanned systems offer perhaps greatest utility in dirty, dangerous, dull, and difficult missions or mission phases. Thus, an understanding of the marginal effectiveness or efficiency relative to manned or other systems should begin with consideration of missions, phases, and parameters and the extent to which they are dirty, dangerous, etc.¹⁵³ Notionally, dirty/dangerous/difficult missions and phases might include detecting, monitoring, sorting, classifying, handing off and disrupting threat interdiction; physically locating components, assessing critical nodes, and fortifying defenses in critical infrastructure security and emergency preparedness; and managing SAR operations and fatalities in emergency response. Dull missions and phases might include detecting, monitoring, sorting, classifying, handing off and disrupting threat interdiction; physically locating components and assessing critical nodes in critical infrastructure security and emergency preparedness; and managing SAR, cargo transport, and communications relay in emergency response and critical infrastructure resilience. Of course, comparisons between unmanned and manned systems must examine only marginal differences between them, and do so in an apples-to-apples, full-life-cycle-cost way.¹⁵⁴ Cost comparisons should also consider the extent to which unmanned systems would be capable of multi-mission/multi-phase/cross-parameter use, perhaps designed for full contingencies and to professional/military-grade specifications.¹⁵⁵ This has implications for cost, both pro and con.

As it happens, somewhat limited adoption in HSE of unmanned systems—discussed in the “Current Use” section, above—seems to make sense: requirements do exist, but the technology to meet at least some of those requirements is still in development, and certain regulatory constraints preclude full adoption (not least because of a lack of FAA guidance on UAS). In an era of tight budgets, entities in the HSE are taking a wait-and-see approach to the use of at least some unmanned systems.

That said, the technology is maturing rapidly, and policy may not be far behind. Prices for consumer- (and professional-) grade unmanned systems are such that they could be used in certain circumstances to meet more tactical requirements. Indeed, it is not difficult to envisage a time in which first responders’ vehicles are

equipped with sUAS that can autonomously deploy for a range of missions, allowing first responders greater efficacy or efficiency. Researchers at the Massachusetts Institute of Technology have created a prototype subsurface UMS smaller than a football that they say may one day help port authorities identify smugglers bringing in contraband. The UMS, which was largely made from a 3D printer and was originally designed to help engineers detect nuclear reactor leaks, could one day soon be fitted with an ultrasound device that experts say can be used to detect false hulls that typically carry illegal goods. Moreover, other next-generation unmanned systems will conduct a broad range of missions with application to the HSE. For example, significant experimentation is ongoing in high-altitude, long-endurance (HALE) aircraft that could remain in flight for weeks at a time. A USAF strategy document posits that “it is not difficult to imagine a day when specially equipped HALE aircraft can replace cellular towers over a natural disaster area or become part of the GPS constellation to help mitigate threat situations or constellation failures.”



VI. Constraints

The constraints on the use of unmanned systems in the HSE are arguably as important as the requirements that drive such use. While unmanned systems may satisfy a variety of requirements in compelling ways, constraints may present similarly compelling reasons to limit the use of unmanned systems. To understand the true value of unmanned systems in the context of homeland security, it is therefore essential to identify constraints, analyze them, and consider whether they should be accepted, rejected, mitigated, or shaped.

The research team identified several areas in which laws, regulations, practicalities, social mores, or other forces have constrained or will constrain such use:

- Privacy concerns, along with the legal ambiguity and public perceptions connected with them, constitute the greatest current and potential constraint. Public concern that government might use unmanned systems, specifically UAS, to compromise the right to privacy—and governmental efforts to address that concern—are already acting as a brake on the use of such systems by the HSE.
- First Amendment protections of the free flow of information are seen by some scholars and rights advocates as threatened by regulation of the use of unmanned systems—even regulation aimed at protecting privacy. This perceived tension between fundamental freedoms may present an obstacle to wider use of unmanned systems.
- Safety is one of the most basic reasons that governments seek to regulate unmanned systems. This constrains their use while policy makers and regulators seek to understand and mitigate safety risks, and may present a continuing constraint as new regulations are adopted.
- The cost of unmanned systems, widely touted to amount to a fraction of the cost of manned systems, is difficult to calculate. For some missions, unmanned systems may in fact be more costly to use than existing manned systems.

This section analyzes each of the identified constraints as follows: Each constraint is defined, and the ways in which advocates and critics view it are discussed. The laws and other forces that may impose that particular constraint are reviewed. Specifically, the effects of the U.S. Constitution; common law; federal laws, regulations,

and executive orders; state and local measures; societal concerns; and practicalities on each are investigated, as appropriate. Potential changes in the effect of the constraints are assessed—including, where appropriate, legal or policy proposals intended to mitigate or shape a constraint.

Discussion of constraints on UAS use dominates this section of the report; constraints on the use of UGS and UMS are discussed less frequently. There are several reasons for this ostensible imbalance. First, UAS use has generated considerably more public debate, and the literature on the subject is consequently more abundant. Second, at the end of 2014, concrete steps toward regulating UAS have been or are being taken at almost every level of government, from coast to coast; the same cannot be said with regard to unmanned systems on land or water. Third, as described in section IV above, use of UAS by entities in the HSE, while limited, exceeds use of other kinds of unmanned systems.

A. Privacy

Public concern about government's use of unmanned systems, specifically UAS, in ways that could compromise the privacy of individuals and groups appears to be the biggest potential constraint on the use of such systems by the HSE.¹⁵⁶ Abundant evidence of this public concern can be found in the mass media, among trade publications and websites, and in public opinion polls. Likewise, the research team heard the concern expressed repeatedly in working groups and one-on-one interviews—not only by privacy advocates and policy analysts, but by public- and private-sector officials from the HSE as well.¹⁵⁷

Privacy groups and other civil liberties advocates have articulated such concerns in numerous published reports and in testimony before Congress. A representative of the Electronic Privacy Information Center told a Senate panel that UAS “present a unique threat to privacy. Drones are designed to maintain a constant, persistent eye on the public to a degree that former methods of surveillance were unable to achieve.”¹⁵⁸ The Electronic Frontier Foundation contends that many UAS, “by virtue of their design, their size, and how high they can fly, can operate undetected in urban and rural environments, allowing the government to spy on Americans without their knowledge.”¹⁵⁹

Officials from the HSE and associated professional groups have stressed that they understand the privacy concerns that arise from their use of unmanned systems. DHS officials wrote in a 2012 memo that “DHS intends to take a proactive leadership role in ensuring that privacy, civil rights, and civil liberties are safeguarded by the lawful use of UASs by DHS components and grant recipients.”¹⁶⁰ In interviews and working groups conducted for this study, officials from throughout the HSE said that they had no intention of violating the rights of Americans.

Yet while acknowledging public concerns, officials have cited several reasons why the public should not see unmanned systems as posing a unique threat to privacy; three of those reasons were voiced repeatedly in interviews and working groups.

First, officials say they are using unmanned systems in more limited ways than privacy advocates suggest. As discussed above, agencies within the HSE have used UAS for a wide range of operations—not simply for law

enforcement, but also for firefighting, border patrol, disaster relief, SAR, military training, and other tasks. Yet after some experimentation, agencies generally have found UAS to be best suited to select tasks.

For example, DHS is the most prevalent user of UAS in the HSE, yet its current applications of the technology are largely limited to border security by CBP, as well as R&D.¹⁶¹ At the local level, police departments and other agencies say they have so far found that UAS are useful for surveying crime and crash scenes, monitoring so-called tactical situations, performing “quick look” reconnaissance, and SAR.¹⁶² These UAS are not being used to expand the surveillance activities of HSE agencies. One law enforcement official said in an interview that “we don’t see long-term surveillance or crowd control”—two uses that privacy advocates have called constitutionally objectionable—as roles for UAS.¹⁶³

Second, officials say that unmanned systems pose no greater or lesser threat to privacy than manned systems do. As noted in this report’s background section on unmanned systems technology, the technologically advanced sensors that can be mounted on UAS can also be put on manned airplanes and helicopters. In a PIA conducted for its aircraft systems, CBP’s OAM said: “All [CBP] aircraft, manned or unmanned, have some type of imaging capability such as video, still images collection, and/or radar. The UAS differ from CBP’s manned aircraft only in that the pilot controls the aircraft from the ground and the aircraft are capable of flying farther distances and longer hours continuously.”¹⁶⁴

Third, officials reason that if unmanned systems are no different from manned systems, existing statutes, regulations, and judicial opinions governing privacy and manned systems also apply to unmanned systems. Those legal rules, they say, are being obeyed. A law enforcement official said in an interview that “one of our core principles is rigorously holding to the Constitution.”¹⁶⁵

The debate over privacy and unmanned systems has focused not only on what those systems are capable of doing, but also on what is done with the data that those systems collect.

Law enforcement and HSE officials contend that data collected by UAS is no different than data collected by other means. Their PED, they say, is governed largely by the same laws that have controlled the way the government has handled data for years: the Privacy Act of 1974 and the E-Government Act of 2002¹⁶⁶ (discussed below in section VI.A.2, “Federal Statutes and Regulations”). One official said in a working-group discussion that management of data collected by UAS “is no different than managing data from a beat cop’s pocket camera.”¹⁶⁷

Privacy groups and other civil liberties advocates disagree, saying that UAS and other surveillance technologies have evolved to the point where existing laws cannot adequately address the scope and complexity of modern data collection. With HALE UAS capable of monitoring vast areas for days and weeks at a time, and with PED infrastructures capable of storing and disseminating ever-larger quantities of data, new laws are essential to preserve individuals’ privacy, these advocates say.¹⁶⁸

In the absence of specific legislation, regulations, or judicial decisions addressing privacy and the use of unmanned systems, the ambiguities inherent in existing law suggest a variety of possible outcomes.

1. THE U.S. CONSTITUTION AND THE SUPREME COURT

The Supreme Court has recognized a limited right of privacy that is implicit in several parts of the Bill of Rights. Those parts include the First Amendment, the Fourth Amendment, and the Due Process Clause and the Equal Protection Clause of the Fifth Amendment, as well as the Ninth Amendment.¹⁶⁹ The Fourth Amendment is most pertinent to discussions of privacy and law enforcement and thus to analysis of the use of unmanned systems in the HSE. The amendment guarantees in part that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.”¹⁷⁰

Rooted in British common-law concepts of real and personal property law,¹⁷¹ the Fourth Amendment has the effect of preventing Americans from having evidence used against them in criminal proceedings if it was unreasonably obtained by the government. The Supreme Court ruled in 1928 that police wiretaps did not violate the Fourth Amendment because they did not physically intrude on the defendant’s home.¹⁷² In similar rulings over the next few decades, the Court continued to judge the reasonableness of government searches on the basis of whether a defendant’s property rights were violated.¹⁷³

In 1967, however, the Court ruled that the Fourth Amendment “protects people, not property.”¹⁷⁴ The ruling in *Katz v. United States* held that the government, unless it obtained a search warrant, could not enter a place when (1) a person had “exhibited an actual (subjective) expectation of privacy” and (2) society would recognize that expectation as reasonable.¹⁷⁵

To date, the Supreme Court has not heard a dispute that specifically involved unmanned systems. It has, however, ruled in several cases arising from government searches that involved airplanes, helicopters, transponders, GPS devices, and cell phones. Legal analysts say these cases offer insights into how the Court might address Fourth Amendment challenge to a search in which an unmanned system was used.

In 1986, in the first of these cases, *California v. Ciarolo*, the court ruled that warrantless surveillance of a suspect’s back yard by a policeman in an airplane 1,000 feet overhead was not an unconstitutional search. Because the policeman was observing with his naked eye in publicly accessible airspace, the suspect’s expectation of privacy was unreasonable, the court ruled.¹⁷⁶ In another decision handed down the same day as *Ciarolo*—*Dow Chemical Company v. United States*—the Court also upheld aerial surveillance involving a sense-enhancing device: a mapping camera.¹⁷⁷ The majority held that “the mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems.”¹⁷⁸ But it noted that “surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public” may be unconstitutional.¹⁷⁹

Three years later, the Court held in *Florida v. Riley* that a defendant had no reasonable expectation of privacy from surveillance by police in a helicopter 400 feet over his greenhouse.¹⁸⁰ As in *Ciarolo*, the Court’s opinion said the police, under FAA air safety rules, had a right to be in such a craft at such an altitude, so the defendant had no reasonable expectation of privacy.¹⁸¹ In a concurring opinion, however, Justice Sandra Day O’Connor wrote that FAA regulations are designed “to promote air safety, not to protect ‘the right of the people to be secure in their persons, houses, papers, and effect, against unreasonable searches and seizures.’”¹⁸²

The Court returned to the issue of sensory enhancement in 2001 in *Kyllo v. United States*. The case turned on whether the government could use a technological device—in this case, a thermal imager—to gain information from inside a home that would otherwise have been unknowable without physical intrusion.¹⁸³ If “the technology in question is not in general public use,” the surveillance is a search, and presumptively unreasonable without a warrant, Justice Antonin Scalia said in the majority opinion.¹⁸⁴ A dissent, however, highlighted an ambiguity in the Court’s reasoning: The definition of “general public use is not even hinted at by the Court’s opinion.”¹⁸⁵

In *United States v. Jones*, decided in 2012, the Court held that when the government attached a GPS device to a suspect’s vehicle and monitored the vehicle’s movements for four weeks, it was conducting a search that, under the Fourth Amendment, required a warrant.¹⁸⁶ However, the Court’s opinion, again written by Justice Scalia, relied not on the *Katz* test for reasonable expectation of privacy, but on the fact that “the government physically occupied private property for the purpose of obtaining information.” Justice Scalia said his reasoning was consistent with *Katz*; some observers have suggested that the *Jones* decision returns discussions of privacy to the traditional realm of property law.¹⁸⁷

Two concurring opinions in *Jones* indicated that at least some of the justices recognized that the Court may not be keeping pace with surveillance technology. Justice Sonia Sotomayor noted that modern technological advances allow surveillance without intrusion, and she warned that refinements of government surveillance might eventually run counter to what society considers a reasonable expectation of privacy.¹⁸⁸ Justice Samuel Alito suggested that as technology advances, legislatures may be better equipped to address privacy issues than courts are.¹⁸⁹

Taken together, these cases offer at least some insight into—or, at least, allow inferences to be made about—how the Constitution might be applied to the use of unmanned systems.

The two aerial surveillance cases—*Ciaraolo* and *Riley*—suggest generally that warrantless searches are constitutional when surveillance is conducted in publicly accessible airspace in accordance with FAA safety regulations. Though both cases involved manned aircraft, it is difficult to imagine how courts would view UAS surveillance differently. At any rate, if a warrant were obtained in advance of a search—manned or unmanned—the search presumably would be considered reasonable and therefore permissible under the Fourth Amendment.

The two cases that focus primarily on surveillance technology—*Kyllo* and *Jones*—are somewhat more difficult to analyze, as both are fraught with ambiguity. Both cases indicate that surveillance conducted with devices “in general public use” would not violate a reasonable expectation of privacy and would therefore not be considered searches under the Fourth Amendment. Both cases, as well as *Dow Chemical* before them, also indicate that surveillance with devices that are less widely used might violate a reasonable expectation of privacy and therefore constitute a search—possibly an unreasonable one—under the Fourth Amendment. Neither case, however, specifies what “general public use” entails nor whether some sorts of technology might be more inherently intrusive than others.

The *Jones* decision, with its invocation of the Fourth Amendment's traditional property-based foundations and its mention of long-term surveillance, adds an extra layer of uncertainty. *Jones* declares that any time the government physically occupies private property to obtain information, it is a search—perhaps unreasonable, perhaps not—regardless of whether a suspect's expectation of privacy was reasonable. And, again, the procurement of a warrant before surveillance renders a search reasonable and therefore permissible under the Fourth Amendment.

The Constitution only protects Americans' rights from infringement by the government. Invasions of privacy by private parties are the subject of tort law, property law, and sometimes criminal law. They are also beyond the scope of this report because they do not present a homeland security issue.

2. FEDERAL STATUTES AND REGULATIONS

There is no single federal statute governing privacy; rather, several laws approach the issue from different directions. "Federal privacy law consists of a series of sectoral regulations, enacted somewhat haphazardly. One federal statute governs privacy in video watching, one governs drivers' license information, one governs health information, one governs financial privacy, and so on."¹⁹⁰

Federal law is silent on the specific subject of privacy and unmanned systems use, but several bills related to UAS were introduced in both houses of Congress in recent years. Three bills were put forth in the 113th Congress; none had moved beyond committee referral as the 113th Congress neared its adjournment at the end of 2014.¹⁹¹

Since 1974, however, the Privacy Act has regulated the ways in which the federal government can and cannot use the personally identifiable information that it collects.¹⁹² The Privacy Act limits agencies' collection, disclosure, and use of personal information maintained in systems of records. Whenever agencies establish or change a system of records, they must notify the public through a notice in the *Federal Register* that identifies, among other things, the categories of data collected, the categories of individuals about whom information is collected, the intended "routine" uses of data, and procedures that individuals can use to review and correct personally identifiable information.¹⁹³ In 2002, the E-Government Act enhanced protection of personal information in government information systems or information collections by requiring that agencies conduct PIAs. PIAs are analyses of how the federal government collects, stores, shares, and manages personal information.¹⁹⁴

DHS, the principal user of UAS in the HSE, said in a 2013 PIA that the Privacy Act and the E-Government Act do not apply to its aircraft systems, manned or unmanned.¹⁹⁵ DHS aircraft systems "and their associated devices are mechanical and operational systems rather than a distinct information technology system or collection of records pertaining to an individual," the PIA said.¹⁹⁶ However, the DHS Privacy Office has developed a set of Fair Information Practice Principles that are based on the Privacy Act and are intended "to encompass the full breadth and diversity of the information and interactions of DHS."¹⁹⁷ The PIA found that CBP's use of UAS was consistent with those principles.¹⁹⁸

Civil liberties groups have made a variety of recommendations regarding UAS legislation. The American Civil Liberties Union has urged Congress to ensure that any UAS legislation includes, at a minimum, usage limitations, image retention limitations, public notice requirements, democratic control, auditing and effectiveness tracking,

and a weaponization ban.¹⁹⁹ The Electronic Privacy Information Center has asked Congress to require commercial and public operators to submit detailed reports on intended UAS use and to require law enforcement agencies to secure a warrant for any surveillance conducted with UAS, among other proposals.²⁰⁰

For its part, the FAA in 2013 published privacy requirements to be followed at its six UAS test sites. While acknowledging that its mission “does not include regulating privacy,” the FAA acknowledged the public debate about whether UAS operations at the sites “will raise novel privacy issues that are not adequately addressed by existing legal frameworks.” The agency decided that setting the privacy requirements and requiring test site operators to abide by them would help “inform the dialogue among policymakers, privacy advocates, and industry regarding the impact of UAS technologies on privacy.”²⁰¹

The six requirements say that operators must have privacy policies that they publish, review, and regularly update, enact, and follow their own policies. They do not specify the nature or content of operators’ policies. The measure also requires operators to comply with “applicable privacy laws.”²⁰²

However, there has been considerable debate about whether the FAA should be issuing privacy regulations at all. As mentioned above, Justice O’Connor said in *Riley* that the FAA was empowered to promote air safety, not to enforce the Fourth Amendment. On the other hand, some commentators say that the FAA’s expertise in aviation makes it a natural choice to play at least some role in sorting out privacy issues that arise from UAS use. A Brookings Institution report written in 2014 posited that the federal government should “take advantage of the [FAA’s] small but growing competence in nongovernmental drones and privacy—and have the agency perform a kind of superintendence function.”²⁰³

In any event, Congress directed the FAA in the 2014 Consolidated Appropriations Act to conduct a study of the impact that UAS integration into the NAS will have on individual privacy.²⁰⁴ “The study should address the application of existing privacy law to UAS integration; identify gaps in existing law, especially with regard to the use and retention of personally identifiable information and imagery; and recommend next steps for how the FAA can address the impact of widespread use of UAS on individual privacy as it prepares to facilitate the integration of UAS into the national airspace.”²⁰⁵

In addition, the White House and DHS are preparing guidelines governing privacy considerations and UAS use.²⁰⁶ Several persons interviewed for this report confirmed that both agencies were close to releasing their documents. To date, however, neither had been released and their contents could not be ascertained.²⁰⁷

3. STATE CONSTITUTIONS AND STATUTES

Under the U.S. Constitution’s Supremacy Clause,²⁰⁸ if there is a conflict between federal and state laws, the state law is invalidated because the federal law is supreme.²⁰⁹ Under the 10th Amendment, any rights not specifically granted to the federal government by the U.S. Constitution are left up to the states.²¹⁰ Privacy, in particular, is one area where states have moved to establish their own rules. Ten states have written privacy guarantees into their constitutions.²¹¹ In addition, state legislatures regularly pass laws pertaining to privacy.

No state constitution directly addresses the use of unmanned systems, but nearly every state has considered some form of legislation addressing UAS in the past two years (see appendix I).²¹² The state measures range in

scope from comprehensive laws that regulate UAS and the data they collect to allotments of research funding in a bid to be awarded one of the six FAA test sites. (All of the laws address UAS. Four states have passed legislation addressing the use of driverless cars.²¹³ None has addressed maritime systems.)

Thirteen states have passed legislation regulating the use of UAS,²¹⁴ generally with the aim of protecting citizens' privacy or precluding UAS surveillance without a warrant.²¹⁵ As of September 2014, 27 states had UAS bills pending.²¹⁶

In April 2013, Virginia became the first state to enact a UAS law,²¹⁷ a two-year moratorium on UAS by any state law enforcement agency.²¹⁸ At least nine state measures generally require law enforcement agencies to obtain warrants before deploying UAS.²¹⁹ Many of these states have written exceptions into their laws that would allow UAS without a warrant in exigent circumstances, including CT operations, SAR operations, amber alerts, or recovery efforts after natural or man-made disasters.²²⁰

Some state UAS laws contain provisions governing how public agencies may retain or destroy data collected by UAS.²²¹ Many states have passed or are considering legislation that bans the attachment of weapons to UAS.

Legal analysts differ on whether the task of regulating the use of unmanned systems by private parties should be left to state legislatures or handled at the federal level, where Congress or an executive agency such as the FAA could craft rules for the entire nation.²²² One commentator suggested that the choice might not be that stark: "A federal, or mixed state and federal, approach to law enforcement drone use makes perfect sense. ... [F]ederal legislation on law enforcement drone use could establish a statutory core to be shared by the states, or a statutory floor, permitting state deviation towards more protection."²²³

4. LOCAL MEASURES

It is unclear exactly how many counties, cities, or other jurisdictions below the state level have enacted measures governing the use of unmanned systems. Likewise, an unknown number of individual public agencies, primarily police departments, have adopted such measures. The following are just a few examples of both:²²⁴

- Charlottesville, Virginia, was the first city in the country to formally pass an anti-UAS resolution in February 2013.²²⁵
- Iowa City, Iowa, banned most license plate readers, traffic enforcement cameras, and UAS in one bill.²²⁶
- Evanston, Illinois, banned UAS in May 2013.²²⁷
- St. Bonifacius, Minnesota, banned UAS from city airspace up to 400 feet, with exceptions for emergencies, issuance of a warrant, and when flying over one's own property.²²⁸
- A general order issued by the mayor of Lincoln, Nebraska, bans police from piloting UAS; this measure was part of a "comprehensive general order" governing how police officers monitor and record.²²⁹
- Syracuse, New York, in December 2013 barred police and other city agencies from using UAS until state and federal governments establish a legal framework that addresses privacy concerns.²³⁰

5. VOLUNTARY GUIDELINES

A broad range of organizations representing law enforcement, state governments, industry, and UAS users have published voluntary guidelines aimed at addressing privacy concerns and promoting air safety. The guidelines that contain privacy provisions include those drawn up by the International Association of Chiefs of Police. The association's 19-point proposal touches on such matters as community engagement, data retention, conditions under which a warrant should be secured, and weaponization ("Equipping the aircraft with weapons of any type is strongly discouraged.").²³¹ The association has said it hopes its guidelines will serve as a model not only for law enforcement agencies, but for local governments as well.²³² The Aerospace States Association and the Council of State Governments jointly list six "privacy considerations" that cover warrants, data, consent, and other issues.²³³ The AUVSI has published a voluntary industry code of conduct with multiple recommendations in the areas of safety, professionalism, and respect; the last area commits adopters to, among other things, "respecting the privacy of individuals ... (and) respecting the concerns of the public."²³⁴

6. SOCIAL MORES

In very broad terms, Fourth Amendment privacy protections are intended to ensure that when the government seeks to gather information, it does not do so by unreasonably violating a person's property or expectation of privacy. In practice, this generally means that information that is found to have been unreasonably gathered cannot be used to prosecute someone.

Those broad terms, however, describe something considerably narrower than the concept of privacy expressed by many people quoted in media coverage of UAS and privacy. To them, privacy protection means something more sweeping than making information inadmissible in court: It means preventing government from employing intrusive methods to gather that information. Judging from anecdotal evidence, an unquantified portion of society apparently sees government surveillance by UAS as the 21st-century embodiment of the Orwellian helicopter that "hovered for an instant like a bluebottle, and darted away again with a curving flight. It was the police patrol, snooping into people's windows."²³⁵

On the other hand, 21st-century society shows signs of having adapted to increased surveillance by government and the private sector alike, at least partly because it is seen as the price that must be paid for technological advancement. "New technologies have made it easier—and cheaper—to obtain information. Users willingly relinquish some of their privacy to avail themselves of these new devices. ... The prevalence of surveillance cameras capturing our images and our movements in public has changed attitudes about what is and should be considered an intrusion on one's expectation of privacy."²³⁶

B. First Amendment Rights

Privacy is not the only constitutional freedom that comes into play when assessing the use of unmanned systems in the HSE; analysts have noted that regulation of UAS use to ensure privacy must be weighed against the First Amendment's free speech and free press guarantees. "Laws governing civilian drone use risk restricting the ability of civilians to engage in legitimate and even essential information gathering," writes Yale Law School

lecturer Margot E. Kaminski. “These restrictions will be made in the name of privacy, but they are still restrictions on speech.”²³⁷

1. THE U.S. CONSTITUTION AND THE SUPREME COURT

The First Amendment states, in part, that “Congress shall make no law ... abridging the freedom of speech or of the press.” The Supreme Court has interpreted these guarantees in ways that have extended to various forms of expression²³⁸ and cover not only the publication of news but also the gathering and dissemination²³⁹ of it and the public’s right to receive it.²⁴⁰

Journalists and media companies have repeatedly cited rights regarding newsgathering and dissemination in their opposition to broad regulation of UAS. As they have begun to incorporate UAS into their newsgathering operations, they have urged that restrictions on their use not be allowed to constrain the media’s constitutional rights. For example, a 2014 court filing by some of the nation’s largest publishing and broadcasting companies contended that the FAA’s ban on commercial use of UAS had “an impermissible chilling effect on the First Amendment newsgathering rights of journalists.”²⁴¹

When making such arguments, journalists and civil liberties advocates point to the Supreme Court’s decision in *Branzburg v. Hayes*.²⁴² The Court said that “[n]ews gathering is not without its First Amendment protections”²⁴³ and that “without some protection for seeking out the news, freedom of the press could be eviscerated.”²⁴⁴ However, the Court’s ruling in *Branzburg* went against the media; in holding that a reporter could not resist a subpoena to disclose the identity of a confidential source, the Court said that “the First Amendment does not guarantee the press a constitutional right of special access to information not available to the public generally.”²⁴⁵ Nineteen years after *Branzburg*, in 1991, the Supreme Court ruled that “generally applicable laws do not offend the First Amendment simply because their enforcement against the press has incidental effects on its ability to gather and report the news.”²⁴⁶

The question, then, of whether restrictions on UAS or other unmanned systems could be applied to the press would appear to hinge on whether such restrictions were “generally applicable laws.” A neutral law of general applicability—a law that applies to all citizens and is not intended to restrict a specific class of people, type of action, or information content—is unlikely to be found to have violated the First Amendment.

When homeland security, law enforcement, or other public agencies bar access to specified areas in the name of public safety, journalists are typically required to obey. An example of this occurred during the civil unrest in Ferguson, Missouri, in 2014. In August, the FAA agreed to restrict about 37 square miles of airspace up to 3,000 feet over Ferguson in response to a request from the Saint Louis County Police Department. The restriction applied to the news media, and the FAA’s top official said no media outlets were known to have objected to it. In November, however, the Associated Press obtained voice recordings that indicated the restriction was aimed primarily at the media. A lawyer for the American Civil Liberties Union called the incident “extraordinarily troubling and a blatant violation of the press’s First Amendment Rights.” FAA Administrator Michael Huerta said that the “FAA cannot and will never exclusively ban media from covering an event of national significance, and media was never banned from covering the ongoing events in Ferguson in this case.”²⁴⁷

2. FEDERAL STATUTES, REGULATIONS, AND ORDERS

No federal statutes have yet been enacted to restrict the use of unmanned systems for any reason, so there is no statutory restriction on their use by media or any other commercial enterprise. However, as the federal agency responsible for establishing rules governing air safety, the FAA regulates the use of UAS.²⁴⁸ Private parties can operate UAS only after obtaining a Special Airworthiness Certificate (SAC), which the FAA has issued on a limited basis for flight tests, demonstrations, and training.²⁴⁹ In addition, the FAA Modernization and Reform Act (FMRA) of 2012 contains a provision that empowers the Secretary of Transportation to “determine if certain unmanned aircraft systems may operate safely in the national airspace system” before the FAA established formal rules and guidance regarding UAS use.²⁵⁰ These so-called Section 333 exemptions, named for the passage in the act that defines them, allow the Secretary to consider matters such as the size, weight, speed, and operational capability of a given UAS; proximity to airports and populated areas; and line-of-sight control when determining whether they “create a hazard to users of the national airspace system or the public or pose a threat to national security.”²⁵¹ (For a full discussion of FAA policies regarding UAS and the NAS, see section VI.B.3, “Safety,” below.)

The FAA has issued SACs or Section 333 exemptions for commercial UAS flights in only a few instances. The FAA granted a Section 333 for commercial UAS flights over land for the first time in June 2014, allowing the energy corporation BP to fly aerial surveys in Alaska.²⁵² In September, the agency allowed six aerial photo and video production companies, determining that they were exempt under Section 333 because they did not pose a threat to national airspace users or national security.²⁵³ In December, four companies were given a total of five exemptions to fly UAS for aerial surveying, construction site monitoring, and oil rig flare stack inspections.²⁵⁴

The FAA’s commercial restriction has been interpreted to apply to media outlets—or to anyone seeking to be paid for gathering news and information—on the grounds that the media are just one element of the vast commercial sector. For example, in February 2014, the FAA investigated whether a television photographer in Hartford, Connecticut, violated the commercial-use restriction after he flew a UAS over an accident scene.²⁵⁵

3. STATE CONSTITUTIONS AND STATUTES

While states may not adopt constitutional provisions or statutes that lessen the freedoms granted by the U.S. Constitution, states may provide greater protections. In the context of First Amendment press freedoms, state press shield laws offer a pertinent example. The Supreme Court’s *Branzburg* decision held that the First Amendment does not protect journalists who refuse to testify about criminal activity they have witnessed or who refuse to identify a confidential source. But 31 states and the District of Columbia have enacted shield laws that give journalists some form of privilege against compelled production of confidential or unpublished information.²⁵⁶

Just as states’ shield laws have created a limited right to newsgathering with regard to divulging information, states might expand newsgathering rights in ways that protect reporters’ methods, including the use of unmanned systems. However, the task team’s research has so far found examples of states moving in the opposite direction. Missouri, for instance, proposed banning the use of UAS by anyone “including a journalist, reporter, or news organization” for surveillance of a person or business without consent.²⁵⁷

C. Safety

With respect to safety, current-generation unmanned systems pose a variety of safety and operational challenges. For example, current-generation UAS lack key safety and operability features. Development of UGS for consumer use—the so-called driverless car—is in its infancy, leaving questions about safety largely unanswered but hardly unvoiced.²⁵⁸ UGS designed specifically for HSE and law enforcement missions by contrast, appear to have spurred less concern about safety, perhaps because they are used primarily in secured areas and away from public roads. And the use of UMS has so far been so limited that it has generated little debate in terms of safety.

The bulk of this subsection is devoted to UAS and how safety concerns continue to constrain their wider use. The primary reason for this narrow focus is that policy makers, homeland security actors, and the public are currently paying more attention to UAS than to other types of unmanned systems. In addition, the danger inherent in flying objects is widely seen to be more pressing than the risk posed by objects that operate on land or water (though advances in UGS development appear to be spurring greater concern about their use on the nation's highways).²⁵⁹ Also, the use of these systems is widespread enough by private entities, the military, and some private hobbyists that a basis for comparison exists with traditional manned platforms. As stated previously, this is not the case for UMS or UGS. Finally, the federal agency responsible for air safety—the FAA—is engaged in a high-profile process of opening the NAS to wider use of UAS.

The FAA's mission "is to provide the safest, most efficient aerospace system in the world."²⁶⁰ Since its creation in 1958, the agency has been responsible for regulating all kinds of civil aircraft, including UAS. But while the NAS accommodates more than 100,000 manned aircraft flights each day,²⁶¹ UAS flights are comparatively rare, because the FAA has authorized little more than 300 UAS COAs and SAC-Experimental Categories (ECs).²⁶² FAA officials have long contended that it must not put air safety at risk by acting with undue haste to introduce UAS into already crowded skies.

Most current-generation UAS lack redundant systems and, in the case of sUAS, a proven approach to setting the kind of airworthiness standards required for manned aircraft. UAS appear to be more sensitive to weather conditions such as high humidity, icing, and other inclement conditions. UAS are also uniquely vulnerable to losing link to the controller, dependent as they are on congested wireless spectrum. UAS operators can lose their communications link with their craft, a risk that is exacerbated by crowded radio frequencies. In such cases, most UAS are programmed to fly to a predetermined spot and either land or circle until they reestablish contact or lose power. But lost links can lead to crashes that result in property damage, injury, or death.²⁶³ In the absence of guidelines from the FAA, DHS, DOJ, Federal Communications Commission, or another entity on deconflicting UAS operations (with manned aircraft and with other UAS) by both civil and public users, the risk of accidents is increasing.²⁶⁴ These limitations inform the need to avoid populated areas and/or to maintain LOS between the operator and aircraft at all times.

However, the danger of UAS should not be overstated. sUAS, for example, are lightweight and carry little or, in the case of battery-operated sUAS, no fuel. In recognition of that fact, the National Transportation Safety Board (NTSB) only requires reporting of UAS crashes in which "[a]ny person suffers death or serious injury" or "[t]he aircraft has a maximum gross takeoff weight of 300 pounds or greater and sustains substantial damage."²⁶⁵

Current-generation UAS appear to have a worse present-day safety record than manned aircraft, though safety is rapidly improving.²⁶⁶ Unmanned aviators often state that “we’re in 1925”—a reference to the era when manned flight ceased to be the exclusive domain of the armed forces and a handful of aviation pioneers. As with manned flight in the 1920s, UAS accidents are relatively frequent due to the nascent nature of the technology and still-emerging safety regime. In an investigative report examining the crashes of U.S. military UAS globally from 2001 to 2013, the *Washington Post* suggested that the primary causes for UAS crashes included “limited ability to detect and avoid trouble ... pilot error ... persistent mechanical defects ... basic electrical malfunctions ... bad weather ... [and] unreliable communications links.”²⁶⁷ In the HSE, CBP/OAM has crashed two of its original fleet of 10 General Atomics Predator B UAS.²⁶⁸

Ongoing research into aircraft safety by the FAA, DoD, NASA, and others aims to improve the safety of operations, particularly through test sites announced in 2013, which will study flight safety under varying geographic and climatic conditions.²⁶⁹ To that end, the Senate report on the 2015 DHS Appropriations Bill “encourages the Department to use the FAA’s six test sites to meet its goal of enabling and enhancing small UAS access to the NAS and to ensure that new technologies developed through the Department’s air based technology research meet the operational and safety standards the FAA will develop at the test sites.”²⁷⁰

Additionally, current-generation unmanned systems are vulnerable to spoofing, hacking, and jamming. Researchers at the University of Texas have demonstrated that “a destructive GPS spoofing attack against a rotorcraft UAV is both technically and operationally feasible.”²⁷¹ In addition, wireless connections can be jammed or denied and offer a point of entry for would-be hackers. Hobbyists have demonstrated multiple software and hardware approaches to “hijacking” wireless connections to sUAS, including a UAS that functions autonomously and seeks out other UAS to bring under its control.²⁷²

Since 2012, when Congress directed the FAA to safely integrate UAS into the NAS by late 2015 (see below, section IV.B.3.2, “Federal Statutes, Regulations, and Orders”), the agency has been working to formulate rules that enable such integration. But progress reportedly has been slow,²⁷³ and in the absence of a regulatory framework, the law surrounding UAS use is confusing and occasionally contradictory.

Safe integration will have to take place within the already codified airspace categories: controlled airspace, uncontrolled airspace, and special-use airspace. Controlled airspace must have traffic control service and is divided into Class A, B, C, D, and E airspaces.²⁷⁴ The distinctions between controlled and uncontrolled airspace affect how aircraft operate, including what flight rules are permitted and whether air traffic control is mandated. For example, systems operating beyond operator LOS in Class G airspace require some form of sensor to maintain separation from both cooperative and non-cooperative aircraft.²⁷⁵ This will create additional financial costs and may impose platform limitations on any UAS designed to operate in these airspaces.

1. THE U.S. CONSTITUTION AND THE SUPREME COURT

The Constitution is understandably silent regarding air safety. As noted above, however, the Supremacy Clause gives federal laws precedence over state laws that conflict with them; federal laws governing air safety are discussed below.

2. FEDERAL STATUTES, REGULATIONS, AND ORDERS

The Federal Aviation Act,²⁷⁶ passed in 1958, created the FAA. Like other administrative agencies, the FAA makes regulations to implement and interpret laws passed by Congress.²⁷⁷ The Federal Aviation Act mandated that the FAA administrator “shall prescribe air traffic regulations ... for (A) navigating, protecting, and identifying aircraft; (B) protecting individuals and property on the ground; (C) using the navigable airspace efficiently; and (D) preventing collision between aircraft, between aircraft and land or water vehicles, and between aircraft and airborne objects.”²⁷⁸

The act defined aircraft as any airborne contrivance “now known or hereafter invented, used or designed for navigation of or flight in the air.”²⁷⁹ The FAA has long interpreted this definition to include UAS. Many UAS users and advocacy groups have disputed this, but a ruling by the NTSB in November 2014 upheld the FAA’s inclusive interpretation: “An aircraft is ‘any’ ‘device’ that is ‘used for flight.’ We acknowledge that the definitions are as broad as they are clear, but they are clear nonetheless.”²⁸⁰

In 2007, the FAA issued a Notice of Policy stating that “no person may operate a UAS in the National Airspace System without specific authority.”²⁸¹ To be granted such authority, civil UAS users must seek one kind of authorization²⁸² and public UAS users another.²⁸³

Public entities are required to obtain a COA.²⁸⁴ A COA allows an operator to fly a UAS within a defined block of airspace for a limited time; some COAs are valid for up to two years. After an operator applies for a COA, which can now be done online, the FAA performs “a comprehensive operational and technical review” of the application and may apply special provisions or limitations on a case-by-case basis. For example, a COA might only allow flying under visual flight rules, limit flying to daylight hours, require coordination with air traffic controllers, or require the UAS to carry a transponder.²⁸⁵ COAs also require that UAS operations be conducted by both a “pilot-in-command,” who must meet certain minimum qualifications, and an observer, whose role is to “observe the activity of the unmanned aircraft and surrounding airspace, either through line-of-sight on the ground or in the air by means of a chase aircraft.”²⁸⁶

The FAA reports that public entities are currently following this process to employ UAS for law enforcement, firefighting, border patrol, disaster relief, SAR, military training, and other operations.²⁸⁷ Several DHS components—including CBP, USCG, and S&T—are operating UAS under the COA process.²⁸⁸ These components report having very good relations with the FAA and have found the process in recent years to be straightforward; they also noted that the process ensures they meet mission requirements.²⁸⁹

Private users of UAS, as noted above, currently must receive a SAC-EC from the FAA. Such certificates are granted to applicants who can show that their UAS “can operate safely within an assigned flight test area and cause no harm to the public.” The FAA provided rules for model aircraft in 1981 that allow hobbyists to operate sUAS in the NAS.²⁹⁰ The rules require stipulate model aircraft to fly below 400 feet from ground level and not to venture within three miles of an airport.²⁹¹

UAS use by private parties enters the realm of homeland security in at least two ways. First, as UAS use by private parties becomes more popular and thus more frequent, it complicates aviation operations by DHS and other groups in the HSE, especially in the immediate aftermath of any incident. First responders have reported being

surprised by encounters with UAS being operated (in some cases illegally) by members of the media, private citizens, and even other first responders.²⁹² Such encounters underscore the potential for accidents involving civil and public UAS. Second, some HSE operations—notably monitoring of critical infrastructure—could be performed by unmanned systems owned and operated by private companies. Until the FAA releases rules that allow some commercial UAS, HSE entities will not be able to turn to the private sector.

In 2012, the Congressional Research Service reported that the FAA “continues to address requests to operate unmanned aircraft on a case-by-case basis. This approach is becoming increasingly untenable as growing numbers of public and commercial entities seek authorization to operate unmanned aircraft in domestic airspace.”²⁹³

That same year, responding to growing interest in UAS and their commercial potential, Congress passed the FAA Modernization and Reform Act (FMRA) of 2012. Among other provisions, the act directed the Secretary of Transportation, whose department includes the FAA, to “develop a comprehensive plan to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system.”²⁹⁴ Safe integration had to be completed “as soon as is practicable, but not later than September 30, 2015.”²⁹⁵

The FMRA set deadlines for tasks that the FAA was to complete before full UAS integration, including creation of an integration road map and designation of six UAS test sites. Of the 17 interim tasks, the FAA had completed nine as of mid-2014. However, the FAA met only one deadline and missed 11; five deadlines have yet to pass.²⁹⁶ One of the most closely watched deadlines was for the release of a rule governing certification and operation of sUAS. When the August 2014 deadline passed, the FAA had not issued a rule on sUAS, nor had it issued a Notice of Proposed Rulemaking, which is required in advance of a final rule.²⁹⁷

A wide range of interested individuals and groups have expressed doubt that the FAA will meet its deadline of 30 September 2015 for UAS integration. In June 2014, the Transportation Department’s Office of Inspector General reported that “FAA officials told us that by 2015 they expect to issue their rule for small UAS, approve a ground-based detect and avoid system, and have operational test ranges. However, these actions do not represent full, safe integration.”²⁹⁸

Safe integration of UAS into this system will depend on incorporation of SAA technologies to allow UAS to maintain separation from other aircraft. SAA refers to a host of systems that enable manned or unmanned systems to detect and avoid objects and other vehicles without human input. SAA “capability must provide for self-separation and ultimately for collision avoidance protection between UAS and other aircraft analogous to the ‘see and avoid’ operation of manned aircraft that meets an acceptable level of safety.”²⁹⁹ SAA technologies will allow UAS to maintain separation minima when operating in uncontrolled airspace.³⁰⁰

Certain types of SAA may also permit more autonomous operations for all classes of unmanned aircraft. They can be classified as ground-based, air-based autonomous cooperative, and air-based autonomous non-cooperative.

Ground-based SAA (GBSAA) relies on the use of a ground-based sensor, normally a 3D air-search radar, to detect other aircraft operating in the vicinity of a UAS. This information is then used by the UAS’s remote operator to maintain separation. As currently envisioned, GBSAA technology relies on a human pilot to interpret sensor data

and take appropriate action.³⁰¹ The advantage of GBSAA is that it interfaces well with current UAS, would not require additional payload requirements, and can more readily be put into operation. This is particularly relevant for sUAS, which have significant payload and other operational constraints that could make SAA integration difficult, if not impossible. GBSAA may also be the most economical solution for operators with large numbers of UAS, as one GBSAA system can work for numerous platforms. However, costs related to procurement and operations will likely relegate this solution to large organizations or would need to be borne by government.

Cooperative airborne SAA (ABSAA) relies on aircraft to broadcast their location information to other aircraft and to air traffic control. At present, aircraft transponders only transmit when queried by secondary surveillance radars, and they only broadcast altitude and assigned identification code. But cooperative ABSAA—including the FAA's next-generation replacement system, Automatic Dependent Surveillance-Broadcast (ADS-B)—goes a step further by routinely transmitting GPS-based location and heading to both air traffic control and other aircraft.³⁰² ADS-B offers significant improvement in situational awareness for pilots. ADS-B information may be integrated into an ABSAA approach where a UAS is able to cooperatively self-separate from other air traffic, with or without direct human intervention.³⁰³

Because certain airspace contains many non-cooperative aircraft³⁰⁴ that may not be equipped with ADS-B systems, a challenging technical problem is developing a non-cooperative ABSAA system to autonomously maintain separation from non-cooperative aircraft. This requires active sensors—most likely onboard radar—to build situational awareness, and advanced algorithms to dynamically reroute the aircraft.³⁰⁵ These systems place great payload and other technical burdens on any UAS. In addition, the miniaturized radar systems required for non-cooperative ABSAA are very expensive and are still in development.³⁰⁶

Safety considerations are further complicated by vast differences in the size and performance of modern UAS. The FAA has divided UAS into two categories. The first is simply referred to as UAS and includes everything that does not fall into the second category, sUAS, which is any UAS under 55 pounds.³⁰⁷ This taxonomy based solely on aircraft weights may have limited utility for the varying capabilities of some systems that fit the sUAS description. For example, the Scan Eagle is capable of flying over 19,000 feet, while the Iris+ has a ceiling of approximately 1,000 feet; both weigh less than 55 pounds.

3. STATE AND LOCAL MEASURES

The Federal Aviation Act says that the federal government “is declared to possess and exercise complete and exclusive national sovereignty in the airspace of the United States.”³⁰⁸ Accordingly, any state or local measures that deal specifically with the national airspace would almost certainly be preempted by federal law and regulations. Indeed, a federal appeals court in 2007 held that the Federal Aviation Act “and regulations promulgated pursuant to it establish complete and thorough safety standards for air travel, which are not subject to supplementation by, or variation among, state laws.”³⁰⁹

4. VOLUNTARY GUIDELINES

Just as various groups have adopted and published voluntary codes and recommendations regarding privacy (see above), voluntary safety guidelines are also in circulation. The Academy of Model Aeronautics, which

describes itself as the world's largest model aviation association with 170,000 members, has an extensive list of guidelines in its *Model Aircraft Safety Code*.³¹⁰ In addition, UAS operators who adopt AUVSI's voluntary code of conduct agree to follow three safety and five professionalism guidelines.³¹¹

D. Cost

While advocates of unmanned systems asserted that they offer considerable cost savings over the use of manned systems in every domain, documenting such savings can be difficult. In particular, there is not a broadly accepted standard that allows “apples to apples” comparison of cost per flight hour (CPFH) for manned versus unmanned aircraft.³¹² While considerable study of CPFH has occurred inside DHS, those data have not been publicly released and were not made available to the research team.

A significant obstacle to CPFH analysis of any aircraft conducting ISR missions (i.e., aircraft with data-collecting sensors) is understanding the fully burdened costs of both the platform and sensor package from preflight through intelligence dissemination, including repair/replacement. Further complicating the costing is the broad CPFH guidance provided by the Office of Management and Budget (OMB), which does not require that CPFH accounting systems be “uniform in their design or operation” but merely that they capture a prescribed set of fixed costs and “other costs.”³¹³ OMB has provided no additional clarification to account for particularities of ISR aircraft or unmanned systems. In addition, OMB is focused on justification of government operation but not necessarily on encouraging comparison between platforms.

Despite these issues, research suggests that UAS CPFH could be significantly less than that of their manned counterparts. Publicly available USAF CPFH data are consistent with these conclusions.³¹⁴ In addition, these differences are even more pronounced when comparing traditional manned platforms with sUAS.³¹⁵ Some sUAS users, for example, say that their CPFH are only the cost of the operator, the recharging of a lithium-ion battery, and limited maintenance.³¹⁶

In interviews and in working groups organized by the research team, a wide variety of participants offered an almost equally wide variety of assessments of whether UAS offered significant savings. For example, while one participant said that five-figure hourly costs associated with flying large UAS probably made them unaffordable for most HSE tasks, another said that he was already using small UAS for HSE-like operations at an hourly cost under three figures. As another example, while some local officials noted that expense had curtailed their use of UAS that they had already purchased, other officials contended that it was more cost effective to keep UAS in the air than to let them sit idle. Perhaps the only thing that can be said with certainty regarding cost is that the subject needs to be studied further, with depth and precision.

E. Other

Other constraints identified in the team's research included interoperability and liability. On the former, a participant in one of the research team's working groups noted that manufacturers of unmanned systems currently are designing and marketing proprietary control systems. Until open architecture becomes the norm, another participant said, operators with different kinds of systems will not be able to work together.³¹⁷ Another

described the problem as “heterogeneous systems working for heterogeneous groups.”³¹⁸ On liability, accidents involving unmanned systems appear unlikely to present legal issues that differ from those presented by accidents involving manned systems. As with manned systems, the potential for accidents caused by uninsured operators have been cited as a concern. In particular, some operators who are operating UAS for commercial purposes before such operations are allowed by the FAA may be unable to buy insurance. On the other hand, one operator who acknowledged using a UAS in his work as a professional photographer said that he had been able to obtain insurance.³¹⁹



VII. Implications

Unmanned systems present a variety of growing implications—positive and potentially negative—for the HSE. This section presents those implications, and certain recommendations, by considering the report’s most important findings in a broad context and highlighting their importance to DHS and the HSE going forward.

Overall, unmanned systems appear to hold promise for the HSE. They comprise a rapidly developing and maturing technology that appears to offer effective and efficient capabilities. They are becoming more affordable and easier to use, and they provide unique capabilities to meet existing HSE requirements.

Technologies that can be applied to homeland security are increasingly emanating from the commercial sector, and not from DoD. DHS should effectively adapt to this opportunity to meet its requirements. Efforts such as DHS S&T’s RAPS project illustrate how DHS has led in understanding commercially available technology and its applicability for a range of homeland missions. At the same time, however, (perhaps understandable) bureaucratic resistance in components across DHS is threatening its ability to effectively acquire and operate unmanned systems, not least sUAS. For example, discussions with CBP OAM and the USCG suggest they are waiting on the outcome of the FAA rulemaking process for sUAS, while at the same time claiming that the temporary FAA COA process necessary for large UAS operation meets their needs. The adoption of sUAS may be disruptive to existing views on aviation within these organizations. Indeed, DHS could make significant use of commercial-off-the-shelf sUAS, which will outpace other unmanned systems in domestic quantity and use over the next decade. Although large UAS will grow in number and use, and developments are expected in UGS autonomy and in UMS, these shifts will be more incremental and less significant in comparison to sUAS. sUAS may not offer radically different capabilities than are already available in manned aircraft, but they can offer those capabilities in a more affordable way, and potentially can be fielded and operated in far greater numbers.

Advances in unmanned systems technology and use present both an opportunity and a threat for the HSE. They may increase the congestion of airspace, roads, and waterways and the likelihood of accidents, as well as misuse by bad actors.

The constraints surrounding government and civilian use of unmanned systems are significant; public perception and safety will continue to be the biggest obstacles. Fairly or not, unmanned systems in general and UAS specifically play a central part in the public discussion of mass surveillance programs by the government. Concerns about the stealth and persistence that unmanned systems offer have spurred public fears that they will be used to infringe on Americans' privacy rights. As a result, users across the HSE must meet a high standard in demonstrating responsible use of unmanned systems, yet statutes and case law offer no clear indication of where that standard will be set. In addition, significant safety concerns regarding UAS must be overcome through rigorous testing and evaluation, leveraging the FAA UAS test sites.

The rapid increase in the use of unmanned systems by a range of users will add complexity to many homeland security missions, including the potential that such systems, especially sUAS, may be used to do harm. The number of sUAS operating at any given time over the average American city or town will likely transform in the near future from only a few, mostly in the hands of hobbyists, to scores performing a range of commercial and public safety missions. This will present HSE entities with a range of complex problems, such as how to respond to sUAS flying over a major public event and how to identify their operators. The potential for bad actors to use unmanned systems to do harm is also an undeniable consideration. For example, the New York Police Department made public in November 2014 that it has been investigating the threat posed by sUAS, including as firearm-armed or explosives delivery platforms. Its concern is based in part on web videos showing paintball gun-equipped sUAS and a real-world encounter in city airspace between a police helicopter and an sUAS taking threatening, aggressive actions.³²⁰

On balance, the HSE is not yet well poised to capitalize on, or respond to widespread commercial and consumer use of, unmanned systems. While work is underway in DHS, for example, it appears to be largely reactive, siloed, focused primarily (though not exclusively) on the air domain, and limited to DHS vice the larger HSE. This is not sufficient for what is likely to be a disruptive technology.

Beyond DHS and its HSE partners, the broader U.S. government lacks overarching policy and strategy on the domestic use of unmanned systems, which creates public safety, public affairs, and economic risks. Put simply, domestic use of unmanned systems is complicated, and it must be understood in all its complexity and broader context. That means cultivating an awareness and understanding of the capabilities of a technology that is evolving each day; dealing with (and tracking) legal ambiguities in a shifting statutory landscape; and understanding overarching threats and opportunities for homeland security, economic prosperity, and implications for civil rights and civil liberties. The potential for unmanned systems to do harm or good, and the keen public interest in the issue reflected in media coverage, point to the need for a more coherent internal, if not external, policy process regarding the crosscutting considerations and implications related to unmanned systems.

Guided by the research, the research team makes several recommendations. First, the Deputy Secretary of Homeland Security should convene a 12-month internal working group to assess how DHS should best organize and posture to respond to the existing and emerging opportunities and threats presented by unmanned systems. The Deputy Secretary would be optimally positioned to undertake such a task because the issues associated cut across the full scope of missions and functions in DHS: requirements, resource prioritization, and

program execution in components and headquarters elements. The Deputy Secretary would present findings to the Secretary of Homeland Security, who may wish to initiate an interagency conversation. The scope of the working group would be to:

- assess current DHS use of unmanned systems;
- identify potential additional uses of unmanned systems to meet high-priority requirements;
- understand the threat of use of unmanned systems by terrorists or criminals and how to mitigate this threat;
- discuss the national role DHS should play in regards to unmanned systems, including questions of greater cooperation with the Department of Transportation (FAA), DOJ, DoD, and others; and
- consider options for public-private dialog on privacy concerns relating to the use of unmanned systems.

Additionally, and to support the proposed working group, DHS should seek to incorporate unmanned systems into virtually all of its exercises. By getting systems into the hands of operators, it can examine their full potential across a range of missions, including critical infrastructure security and resilience and emergency preparedness and response.

Informed by expertise resident within DHS S&T from its RAPS project, CBP and USCG should begin testing operational use of sUAS in the border security mission.

NIJ and DHS should collaborate closely going forward—working with relevant non-governmental organizations such as the International Association of Chiefs of Police—in helping to set standards for state and local operators of unmanned systems, particularly sUAS.

And DHS operators and DHS S&T technologists should continue to liaise with federal partners, such as the U.S. Navy; U.S. Army; the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics; and DARPA on R&D in UGS and UMS.



VIII. Conclusions and Thoughts for Future Research

Drawing from a deep review of the literature, semi-structured interviews and working groups with a large number of relevant experts, and HSSAI-CSIS staff analysis, this paper has presented information on unmanned systems in the homeland security context. Overall, the research suggests that unmanned systems hold promise for the HSE. They are becoming more affordable and easier to use, and they provide unique capabilities to meet existing HSE requirements. However, the constraints surrounding government and civilian use of unmanned systems are significant. Public perception and safety pose the biggest obstacles, and the rapid increase in the use of unmanned systems by a range of users raises the possibility that they may be used to do harm. As it happens, the HSE does not yet appear to be well poised to capitalize on or fully deal with unmanned systems; and beyond DHS and its HSE partners, the broader U.S. government appears to lack overarching policy and strategy on the domestic use of unmanned systems, which creates public safety, public affairs, and economic risks. The paper presented certain recommendations to address identified issues.

Lastly, avenues for future research exist. For example:

- Development of a standardized apples-to-apples cost comparison framework could enable methodologically sound comparisons between manned and unmanned systems. This study could improve acquisition decisions throughout the HSE by supporting formal, comparable cost analyses (a lack of which was highlighted numerous times as hindering decision making at all levels of the HSE).
- An international comparison could highlight the different approaches being undertaken by foreign jurisdictions on the use of unmanned systems generally and for homeland security applications more specifically. Such a study could examine the emerging regulatory and policy frameworks and any lessons learned therein, including interactions between industry and governments, as well as novel homeland security use cases. Focus on UGS and UMS would be particularly helpful, as these have received lesser treatment in the literature.
- A deeper analysis of the commercial use of unmanned systems, not least sUAS, could facilitate better future understanding of a very dynamic environment and growing global market. This study could serve as a

complement to the numerous studies that examine unmanned systems in national security and the present paper that examines unmanned systems in homeland security.

- A holistic analysis of the manner in which entities in the HSE could and should counter threats posed by malicious use of unmanned systems in all domains could guide R&D and clarify HSE roles and responsibilities. Such research could add to any work already underway; it would be sensitive and likely classified.



Appendix I. State Laws on the Use of Unmanned Systems

Table 4. Passed Legislation

STATE	BILL(S)	PROVISIONS
Alaska	HB 255 (2014)	HB 255 sets guidelines for law enforcement agencies seeking to develop a UAS program; creates parameters for law enforcement use; and sets retention limits on images/video captured by a UAS used by law enforcement. It also allows the University of Alaska to establish a UAS training program.
California	AB 2306, AB 1327 (2014)	AB 2306 bans the use of UAS by paparazzi and other individuals for any activity that would be considered an invasion of privacy. The law does not mention UAS specifically but rather bans “any device” that could be used to violate existing privacy laws. AB 1327 defines the term UAS and requires that law enforcement agencies seeking to operate UAS obtain a warrant unless they are using the aircraft to evaluate traffic accidents, inspect state parks for illegal fires and vegetation, respond to emergency situations where an individual’s life is in immediate danger, and/or to natural or man-made disasters. Public agencies that are not law enforcement agencies may use UAS “to achieve the core mission of the agency” provided their use does not involve any activities related to law enforcement. The law also establishes data retention and use requirements for public agencies and bars the deployment of weapons onboard UAS unless explicitly authorized by federal law.
Colorado	Ban by Colorado Parks and Wildlife Commission (2014)	The Colorado Parks and Wildlife Commission banned the use of UAS for scouting, hunting, and the taking of wildlife.
Florida	SB 92/HB 119 (2013)	SB 92/HB 119 defines the term “drone”; permits law enforcement use of UAS to counter a terrorist attack if intelligence is deemed credible by DHS; requires a search warrant for any UAS use; permits use in cases of missing persons or to prevent danger to life or damage to property; and creates provisions for civil action against violators.
Hawaii	SB 1221 (2013)	SB 1221 appropriated funds for two staff positions for aviation education through the University of Hawaii.

Table 4. Passed Legislation

STATE	BILL(S)	PROVISIONS
Idaho	SB 1134 (2013)	SB1134 amends Idaho Code, adding a new section (Section 21-213) relating to UAS. It defines a UAS; requires warrants for use by law enforcement except for emergency response, SAR, or controlled substance investigations; bans individuals, entities, and state agencies from using UAS to photograph or record activities for the purpose of publishing without consent; and creates provisions for civil action against violators.
Illinois	HB 1652, SB 1587 (2013)	HB 1652 is an amendment to Illinois state wildlife code and prohibits the use of a drone, which is defined as "any aerial vehicle that does not carry a human operator," to interfere with hunters or fishermen. SB 1587 defines a drone; permits use of UAS by law enforcement to counter a terrorist attack if intelligence is deemed credible by DHS; requires a search warrant; permits use in cases of missing persons, imminent harm to life or to forestall imminent escape of a suspect; limits UAS use to 48 hours; sets standards for destruction of data gathered by law enforcement within 30 days, with some exceptions; deems evidence gathered in violation to be inadmissible; and requires the Illinois Criminal Justice Information Authority to report which law enforcement agencies have UAS and how many.
Indiana	HB 1009, SR 27 (2014)	HB 1009 defines the term UAV; creates warrant requirements and exceptions for police use of unmanned aircraft and real-time geo-location tracking devices; requires warrants for passwords for electronic devices; and creates the new crime of "Unlawful Photography and Surveillance on Private Property." SR 27 urges the legislative council to establish "the interim study committee on the use of aircraft to study the use of unmanned aerial vehicles." The committee, if established, shall have 11 members.
Iowa	HF 2289 (2014)	HF 2289 bans the use of UAS for traffic law enforcement; requires a warrant for use of information gathered by a UAS in a criminal or civil proceeding; and requires the Department of Public Safety to develop guidelines for UAS use and report findings by the end of 2014.
Louisiana	HB 1029 (2014)	HB 1029 defines a UAS; bans use of UAS to collect information about a facility without written consent; and establishes penalties for breaking the law, which include a small fine and up to a year in jail time.
Maryland	HB 100 (2013)	HB 100 appropriated \$500,000 for the state's UAS test site.
Montana	SB 196 (2013)	SB 196 defines the term UAV and limits use of information gathered by UAV as evidence in prosecution or proceeding, unless information is obtained pursuant to a warrant or through recognized exception.
Nevada	AB 507 (2013)	AB 507 appropriated \$4 million to the UAV program to be used only if Nevada is selected as an FAA test site.
North Carolina	SB 402, SB 744 (2013)	SB 402 defines the term UAS and bans use of UAS by state and local personnel until July 2015 unless use is approved by the CIO for the Department of Transportation. If the CIO determines that UAS can assist state and local agencies, he or she is authorized to assist and oversee planning regarding the development, implementation, and operation of UAS. SB 744 amends SB 402 and bans the use of UAS by state and local personnel until December 2015 unless the use is approved by the CIO for the Department of Transportation. The law also establishes "crimes committed by the use of unmanned aircraft systems," which include interfering with manned aircraft, using them to hunt/fish (or harass someone hunting and fishing), and publishing photographs/videos taken with thermal imaging/infrared cameras. The law also establishes licensing protocols for UAS use.
North Dakota	SB 2018 (2013)	SB 2018 grants \$1 million to pursue designation as the FAA test site and subsequent \$4 million if selected.

Table 4. Passed Legislation

STATE	BILL(S)	PROVISIONS
Ohio	HB 292 (2014)	HB 292 establishes the Aerospace and Aviation Technology Committee. Among other things, its job is to research and develop aviation technology, including unmanned aerial vehicles.
Oregon	HB 2710 (2013)	HB 2710 defines the term drone; allows law enforcement to operate UAS with a warrant (exceptions apply) and for training purposes; requires that law enforcement use must not exceed five days; makes information obtained in violation of the law inadmissible; requires UAS operated by public body be registered with the Oregon Department of Aviation; creates crimes and penalties for arming UAS; and, in certain cases, allows landowners to bring action against someone flying a UAS less than 400 feet above their property.
Tennessee	SB 796, HB 591 (2013); SB 1777, SB 1892 (2014)	SB 796/HB 591 defines the term drone; permits law enforcement use to counter a terrorist attack if intelligence is deemed credible by DHS; and a warrant is obtained; to prevent imminent danger to life or if “swift” action is needed. States that evidence in violation of this is not admissible in court; and creates provisions for civil action against violators. SB 1777 establishes a Class C misdemeanor for a private entity to use a UAS for video surveillance of individuals hunting or fishing. SB 1892 names many lawful uses of UAS, including for professional or scholarly research in airspace designated as an FAA test site, as part of a U.S. military mission; establishes a Class C misdemeanor for an individual using a UAS to conduct surveillance of a person or property, for an individual possessing such images (Class C), or distributing or using them (Class B).
Texas	HB 912 (2013)	HB 912 names 19 lawful uses of unmanned aircraft, which include for research purposes by an academic institution; in designated FAA test sites; for U.S. military missions, operations, and training; for utility work; with the consent of the individual whose property is being photographed, if photographs were taken from a height no more than eight feet above ground level in a public place, if the image was captured without using any electronic, mechanical, or other means to amplify the image beyond normal human perception; if a warrant has been obtained or an individual’s life is in danger (for public agencies only); for responding to a natural disaster or conducting crime scene investigation (for public agencies only); and for supporting port-authority security. The law also creates two new crimes: illegal use of UAS to capture images (defined as using a UAS to “capture an image of an individual or privately owned real property in this state with the intent to conduct surveillance on the individual or property captured in the image”) and possession or distribution of such images (both Class C crimes). Accidental collection of images in violation of the law is a defense to prosecution, provided the images were not shared or disseminated. Law enforcement and other first responders are allowed to use UAS if they have obtained a warrant, someone’s life is in danger, and to support investigative activities (such as filming a crime scene). Images obtained in violation of this law may not be used in court or subpoenaed. The law also requires that all law enforcement agencies and municipalities that used UAS in the past 24 months submit a report to the governor and lieutenant governor every odd-numbered year between 1 January and 15 January that lists the number of UAS used (as well as when, where, and why), “the number of criminal investigations aided by the use of an unmanned aircraft and a description of how the unmanned aircraft aided each investigation,” the number of times a UAS was used for non-criminal investigative purposes and a justification as to why, “the type of information collected on an individual, residence, property, or area that was not the subject of a law enforcement operation and the frequency of the collection of this information,” and “the total cost of acquiring, maintaining, repairing, and operating or otherwise using each unmanned aircraft for the preceding 24 months.”

Table 4. Passed Legislation

STATE	BILL(S)	PROVISIONS
Utah	SB 167 (2014)	SB 167 defines the term UAV; permits law enforcement use with a warrant or in the case of emergency; requires data gathered with a UAV be destroyed “as soon as reasonably possible”; and adds reporting requirements for any UAV activity.
Virginia	HB 2012/SB 1331 (2013)	HB 2012/SB 1331 prevent UAS use by any state agencies “having jurisdiction over criminal law enforcement or regulatory violations” or units of local law enforcement until 1 July 2015; includes many exceptions like Amber Alerts, Blue Alerts, use by the National Guard, higher education institutions, search and rescue, etc.; requires Virginia Department of Criminal Justice Services and other agencies to research and develop protocols for drone use by law enforcement in the state. Findings to be reported by 1 November 2013.
Wisconsin	SB 196 (2014)	SB 196 defines the term drone; requires a warrant for law enforcement use except in cases of emergency, aid in SAR, or to prevent imminent harm; makes evidence obtained in violation inadmissible; creates a Class H felony for possession or use of a weaponized UAS; creates a Class A misdemeanor preventing a person, except law enforcement with a warrant, from using a UAS to conduct surveillance where an individual has a reasonable expectation of privacy.

Sources: National Conference of State Legislatures, Institute for National Security and Counterterrorism, American Civil Liberties Union, Drone-Laws, LegiScan, and individual state legislature websites.

Table 5. Pending Legislation

STATE	BILLS/STATUS
Alabama	SB 240
Connecticut	HB 5217
Georgia	SB 200, HB 848, HB 846, HB 560
Hawaii	SB 783, SB 2068
Idaho	SB 1067
Indiana	SB 20
Iowa	HF 410
Kentucky	BR 11, HB 342
Massachusetts	S1664, HB 1357
Michigan	HB 4455, HB 4456, SB 926
Minnesota	HF 1994, HB 2553, HF 1620, SF 485, HF 612, HF 990, HF 1076
Missouri	HB 46, HB 1204
Nebraska	LB 412 (indefinitely postponed in April 2014)
New Jersey	A3157, A1039, A2147, SB 2310
New York	S4537/A06370, A6244, A6541, A9697, A7639
North Carolina	HB 1099
Ohio	SB 189, HB 207, HB 364
Oklahoma	SB 2043
Oregon	SB 524, SB 71, SB 853
Pennsylvania	HB 452, SB 875, HB 961, SB 1332, HB 2158
Rhode Island	SB 411
South Carolina	HB 3415, SB 395
Vermont	SB 169, HB 540
Washington	SB 5782, HB 1771
West Virginia	HB 2732, HB 2948, HB 2997

Sources: National Conference of State Legislatures, Institute for National Security and Counterterrorism, American Civil Liberties Union, Drone-Laws, LegiScan, and individual state legislature websites. Note: Delaware, Mississippi, and South Dakota have no legislation passed or currently pending. Arizona, Arkansas, Kansas, Maine, New Hampshire, and Wyoming have attempted but failed to pass legislation in 2013 or 2014.

A U.S. Navy helicopter, likely a Sikorsky HO4S, is shown in flight over a vast, calm ocean under a clear blue sky. The helicopter's main rotor blades are blurred due to motion, and its landing gear is extended. The image has a blue tint.

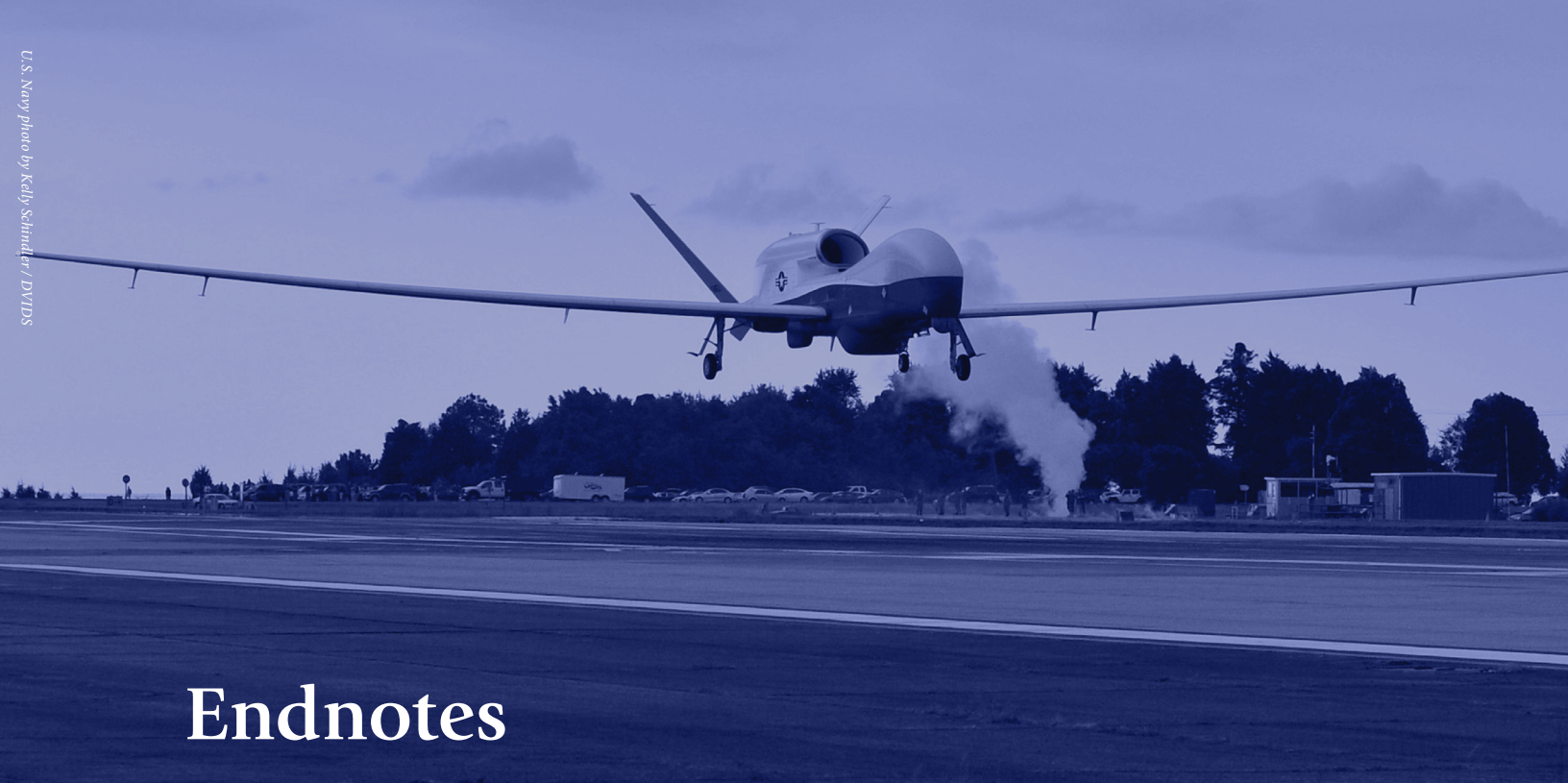
Appendix II. Working Group Participants and Interviewees

More than 100 individuals very generously participated in working groups and semi-structured interviews during the course of this research. The authors are most grateful for their input. Save for individuals who requested anonymity, participants and interviewees included the following (note, however, that inclusion here does not indicate endorsement of the report):

- Paul C. Balutis, senior program manager, Technology Organization, iRobot
- Parag Batavia, PhD, president, Neya Systems, LLC
- Jim Bueermann, president, Police Foundation
- Christopher Calabrese, legislative counsel, American Civil Liberties Union
- Dallas E. Cormier, P.E., senior project manager, San Diego Gas & Electric Company
- Dave Duggins, program manager, Near Earth Autonomy, Inc.
- Lothar Eckardt, executive director, National Air Security Operations, U.S. Customs and Border Protection
- Bill English, senior air safety investigator, Office of Aviation Safety, Major Investigations, National Transportation Safety Board
- Philip Finnegan, director of corporate analysis, Teal Group Corp.
- Helen Greiner, founder and CEO, CyPhy Works; co-founder, iRobot Corporation
- Stephen J. Guerra, PhD, senior political scientist, RAND Corporation
- Doug Hardison, strategic development, Navy and Marine Corps Programs, General Atomics Aeronautical Systems
- James E. Harris, mission systems engineer, unmanned systems, Raytheon
- Glenn Ignazio, global maritime security director, unmanned systems subject matter expert, Liquid Robotics Inc.
- Robert Johns, branch chief, Aviation Architecture and Plans Directorate, Domestic Nuclear Detection Office, Department of Homeland Security

- Col. Soren Jones, USAF, deputy director, Intelligence, Surveillance, and Reconnaissance Operations Directorate, Office of Under Secretary of Defense for Intelligence, Department of Defense
- Douglas J. Koupash, executive director, mission support, Office of Air and Marine, Customs and Border Protection
- Andrew Lacher, unmanned and autonomous systems research lead, The MITRE Corporation
- Duncan McBranch, chief technology officer, Los Alamos National Laboratory
- Michael McNerney, associate director, Homeland Security and Defense Center, RAND Corporation
- Michael K. O'Shea, senior law enforcement program manager, Office of Justice Programs, U.S. Department of Justice
- Michael Perry, company spokesperson, DJI
- Jorgen Pedersen, president and CEO, RE2, Inc.
- Capt. Matt Pregmon, U.S. Navy, assistant professor, Eisenhower School for National Security and Resource Strategy, National Defense University
- John R. Reid, USAF strategic development, General Atomics Aeronautical Systems, Inc.
- Patti Rote, robotics business consultant and co-founder, Girls of Steel Robotics, Carnegie Mellon University
- Paul Scharre, director of the 20YY Warfare Initiative, Center for a New American Security
- Joseph Scott, program manager, Homeland Security Advanced Research Projects Agency, Science and Technology Directorate, U.S. Department of Homeland Security,
- Chief Donald L. Shinnamon, Sr., ret., Shinnamon & Assoc., LLC
- Rita Siemion, policy counsel, The Constitution Project
- Sanjiv Singh, CEO, Near Earth Autonomy
- Sarjoun Skaff, PhD, founder and CTO, Bossa Nova Robotics
- Jeff Sloan, project lead and UAS operator, National Unmanned Aircraft System Project Office, U.S. Geological Survey
- Thomas Snitch, PhD, distinguished senior professor, Institute for Advanced Computer Studies, University of Maryland
- Lt. Gen. Keith Stalder, U.S. Marine Corps (ret.), CEO, Keith Stalder and Associates
- Jay Stanley, senior policy analyst and editor, Free Future blog, Speech, Privacy, and Technology Project, American Civil Liberties Union
- Amie Stepanovich, senior policy counsel, Access
- Jeffrey D. Stern, PhD, state coordinator, Virginia Department of Emergency Management
- Rachel Stohl, senior associate, Managing Across Boundaries, The Stimson Center
- Col. Bill Tart, U.S. Air Force (ret.), senior director, unmanned systems and robotics, ASRC Federal
- Adam Thiel, deputy secretary of public safety and homeland security, Commonwealth of Virginia
- John Villasenor, professor of electrical engineering and public policy, UCLA; nonresident senior fellow, The Brookings Institution; National Fellow, The Hoover Institution, Stanford University

- Christopher Vo, PhD, chief scientist, Sentien Robotics; president, DC Area Drone User Group
- Capt. Robert P. Wagner, U.S. Coast Guard, Eisenhower School for National Security and Resource Strategy, National Defense University
- Steven Weiss, PhD, distinguished analyst, Homeland Security Studies and Analysis Institute
- Robert Zitz, senior vice president and chief architect, Leidos



Endnotes

- 1 General Atomics Aeronautical Systems, Inc., "Predator/Gray Eagle Series Surpasses Three Million Flight Hours," news release, October 14, 2014, http://www.ga-asi.com/news_events/index.php?read=1&id=442.
- 2 See, for example, DoD, *Unmanned Systems Integrated Roadmap: FY2013-2038*, 14-S-0553, <http://www.defense.gov/pubs/DOD-USRM-2013.pdf>; and USAF, *United States Air Force RPA Vector: Vision and Enabling Concepts 2013-2038*, (2013), http://www.defenseinnovationmarketplace.mil/resources/USAF-RPA_VectorVisionEnablingConcepts2013-2038_ForPublicRelease.pdf.
- 3 See, for example, Samuel J. Brannen, Ethan Griffin, and Rhys McCormick, *Sustaining the U.S. Lead in Unmanned Systems: Military and Homeland Considerations through 2025* (Washington, DC: Center for Strategic and International Studies, February 2014), <http://csis.org/publication/sustaining-us-lead-unmanned-systems>; Paul Scharre, *Robotics on the Battlefield Part I: Range, Persistence and Daring* (Washington, DC: Center for a New American Security, May 2014), <http://www.cnas.org/range-persistence-daring#.VBHKEfldVyw>; Robert O. Work and Shawn Brimley, *20YY: Preparing for War in the Robotic Age* (Washington, DC: Center for a New American Security, January 2014), http://www.cnas.org/sites/default/files/publications-pdf/CNAS_20YY_WorkBrimley.pdf; Scott Savitz, et al., *U.S. Navy Employment Options for Unmanned Surface Vehicles* (Santa Monica, CA: RAND Corporation, 2013), http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR384/RAND_RR384.pdf; and Peter Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin, 2009).
- 4 Human Rights Watch, *A Wedding That Became a Funeral* (Washington, DC: Human Rights Watch, February 20, 2014), <http://www.hrw.org/reports/2014/02/19/wedding-became-funeral-0>; Amnesty International, *Will I Be Next? U.S. Drone Strikes in Pakistan* (London: Amnesty International, 2013), <https://www.amnestyusa.org/sites/default/files/asa330132013en.pdf>; Micah Zenko, *Reforming U.S. Drone Strike Policies* (New York: Council on Foreign Relations, January 2013), <http://www.cfr.org/wars-and-warfare/reforming-us-drone-strike-policies/p29736>; and John P. Abizaid and Rosa Brooks, *Recommendations and Report of the Task Force on US Drone Policy* (Washington, DC: Stimson Center, June 2014), http://www.stimson.org/images/uploads/task_force_report_final_web_062414.pdf.
- 5 See, for example, United Nations Office at Geneva, "CCW Meeting of Experts on Lethal Autonomous Weapon Systems (LAWS)," 13-16 May 2014 meeting, <http://www.unog.ch/80256EE600585943/%28httpPages%29/6CE049BE22EC75A2C1257C8D00513E26?OpenDocument>.
- 6 See, for example, Cristina Costantini, "U.S. Border Patrol Increases Use Of Unmanned Drones For Surveillance," Huffington Post, May 1, 2012, http://www.huffingtonpost.com/2012/05/01/us-border-patrol-increase_n_1467196.html; Somini Sengupta, "U.S. Border Agency Allows Others to Use Its Drones," *New York Times*, July 3, 2013, <http://www.nytimes.com/2013/07/04/business/us-border-agency-is-a-frequent-lender-of-its-drones.html?pagewanted=all&r=0>.
- 7 *How to Improve the Efficiency, Safety and Security of Maritime Transportation: Better Use and Integration of Maritime Domain Awareness Data*, Before the House Transportation and Infrastructure Subcommittee on Coast Guard and Marine Transportation, 113th Cong. (2013) (statement of William Vass, CEO of Liquid Robotics); *Testimony of Director, Northern Region Office of Air and Marine, John S. Beutlich*, Before the House Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications, 112th Cong. (2011) (statement of John S. Beutlich, Director of the Northern Region Office of Air and Marine); *The Future of Unmanned Aviation in the U.S. Economy: Safety and Privacy Considerations*, Before the U.S. Senate Committee on Commerce, Science, and Transportation, 113th Cong. (2014) (statement of Mary Cummings, Director of the Humans and Autonomy Laboratory, Duke University).
- 8 Tom Barry, *Drones Over the Homeland: How Politics, Money and Lack of Oversight Have Sparked Drone Proliferation, and What We Can Do*

- (Washington, DC: Center for International Policy, April 2013), http://www.ciponline.org/images/uploads/publications/IPR_Drones_over_Homeland_Final.pdf.
- 9 Science and Technology Directorate, *Privacy Impact Assessment for the Robotic Aircraft for Public Safety (RAPS) Project*, DHS/S&T/PIA-026 (Department of Homeland Security, 2012); U.S. Customs and Border Protection, *Privacy Impact Assessment for the Aircraft Systems*, DHS/CBP/PIA-018 (Washington, DC: DHS, 2013).
 - 10 Government Accountability Office, *Unmanned Aircraft Systems: Use in the National Airspace System and the Role of the Department of Homeland Security*, Statement of Gerald L. Dillingham, GAO-12-889T (Washington, DC: Government Accountability Office, 2012); GAO, *Unmanned Aircraft Systems: Continued Coordination, Operational Data, and Performance Standards Needed to Guide Research and Development*. Statement of Gerald L. Dillingham, GAO-13-346T (Washington, DC: Government Accountability Office, 2013).
 - 11 Office of the Inspector General, *A Review of Remote Surveillance Technology Along U.S. Land Borders*, OIG-06-15 (Washington, DC: DHS, 2005); Office of the Inspector General, *U.S. Coast Guard's Acquisition of the Vertical-Takeoff-and-Landing Unmanned Aerial Vehicle*, OIG-09-82 (Washington, DC: DHS, 2009).
 - 12 Office of the Inspector General, *Interim Report on the Department of Justice's Use and Support of Unmanned Aircraft Systems*, Report 13-37 (Washington, DC: Department of Justice, 2013).
 - 13 Bart Elias, *Pilotless Drones: Background and Considerations for Congress Regarding Unmanned Aircraft Operations in the National Airspace System* (Washington, DC: Congressional Research Service, September 10, 2012).
 - 14 Formally, per the first Quadrennial Homeland Security Review (QHSR, published in 2010), the HSE is defined as “the federal, state, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of America and the American population.” DHS, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*, (Washington, DC: DHS, 2010), iii, <http://www.dhs.gov/sites/default/files/publications/2010-qhsr-report.pdf>. The present research does not examine use of unmanned systems by “individuals, families, and communities.” The HSE is often referred to now as the “whole community”; see, for example, DHS, *2014 Quadrennial Homeland Security Review* (Washington, DC: DHS, 2014), 74, <http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf>. Note also that in general, DHS maintains no command authority over non-DHS entities in the HSE. Rather, DHS is a persuasive but nonbinding body, save for select circumstances in which DHS serves as a regulator (as with certain critical infrastructure sectors) or incident response coordinator. Lastly, for information on roles and responsibilities of entities in the HSE, see the 2014 QHSR, 83-93.
 - 15 The HSE executes numerous missions. These are enumerated in the QHSR, the most recent of which was published in June 2014. Per the 2014 QHSR, the HSE serves to prevent terrorism and enhance security; secure and manage U.S. borders; enforce and administer U.S. immigration laws; safeguard and secure cyberspace; and strengthen national preparedness and resilience. DHS, *2014 Quadrennial Homeland Security Review*.
 - 16 Written definition of the term *unmanned system* is relatively rare in the literature, or, when offered, is contradictory or unsatisfying. Even DoD has not formally defined the term in its seminal publication, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*. (see Department of Defense, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, JP 1-02 (Washington, DC: DoD, 2014)), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.) That said, *Joint Publication 1-02* does define “unmanned aircraft” as “an aircraft that does not carry a human operator and is capable of flight with or without human remote control”; it also defines “unmanned aircraft system” as “that system whose components include the necessary equipment, network, and personnel to control an unmanned aircraft” (it does not, however, define “aircraft”). For completeness, note that both Congress and the FAA have also defined “unmanned aircraft systems.” With respect to lexicon, this paper—and much of the recent literature—employs *unmanned system* and the domain-specific derivatives *unmanned aerial system* or *unmanned aircraft system* (UAS); *unmanned ground system* (UGS); and *unmanned maritime system* (UMS). Different terminology is occasionally used, however. For example, the engineering community often refers to unmanned systems as *robots* (and *robotics* for the field as a whole). And the USAF prefers the term *remotely piloted aircraft* (RPA) for UAS to emphasize that a human pilot remains necessary for successful operation (though not in the aircraft itself). Of course, the term *drone* is sometimes used to refer to UAS or RPA. “Drone is one of the oldest official designations for remotely controlled aircraft in the American military lexicon,” notes aviation historian Steve Zaloga in a letter to *Defense News*; the term dates to 1935, when it was used by the American military to refer to remotely controlled aircraft employed for anti-aircraft gunnery practice in honor of the British DH 82B Queen Bee, a similar aircraft (see Aaron Mehta, “History Tuesday: The Origin of the Term Drone,” *Defense News*, May 14, 2014, <http://intercepts.defensenews.com/2013/05/the-origin-of-drone-and-why-it-should-be-ok-to-use/>). Drone carries with it a negative connotation, though, rooted in a depiction of the underlying technology as autonomous and aggressive, informed in part by dystopian science fiction. The use of the term drone (and *drone wars* and *drone strikes*) has also become synonymous with the United States’ use of armed UAS against terrorist combatants in the Middle East, North Africa, and South Asia. Experts in and operators of unmanned systems often suggest that use of the term drone displays a lack of technical understanding, or believe those who use the term to be biased and inherently adversarial; use of the term is also thought to discount the significant human input necessary for effective use of current generation UAS. Additionally, note that UAS, UGS, and UMS are sometimes referred to as *vehicles*, using the terms *unmanned aerial vehicle* (UAV); *unmanned ground vehicle* (UGV); and, in the maritime domain, *unmanned surface vehicle* (USV) and *unmanned underwater vehicle* (UUV). Technically, however, the vehicle is a part of the larger system (as noted above, the vehicle comprises the platform and mission payload, not the unmanned system in its entirety). Lastly, note also that by the definition set forth

- in the present paper, immobile platforms, such as tethered aerostats, are excluded from consideration. Also outside the scope of the research are unmanned space-based systems.
- 17 The body of literature on various specific aspects of unmanned systems is large and derives from diverse fields, including engineering, robotics, computer science, acquisition, security, policy, and the like. For more on unmanned systems and their associated elements, see, for example, Suraj G. Gupta, et al., "Review of Unmanned Aircraft System," *International Journal of Advanced Research in Computer Engineering & Technology* 2, no. 4 (2013), <http://ijarcet.org/wp-content/uploads/IJARCET-VOL-2-ISSUE-4-1646-1658.pdf>; Scott Savitz, et al., *U.S. Navy Employment Options for Unmanned Surface Vehicles (USVs)*, (Santa Monica, CA: RAND Corporation, 2013), PDF e-book, http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR384/RAND_RR384.pdf; DoD, *Unmanned Systems Integrated Roadmap: FY2013-2038*; U.S. Air Force, *United States Air Force RPA Vector: Vision and Enabling Concepts 2013-2038* (Washington, DC: USAF, 2013), http://www.defenseinnovationmarketplace.mil/resources/USAF-RPA_VectorVisionEnablingConcepts2013-2038_ForPublicRelease.pdf.
 - 18 For a discussion of the technology and tactical advantages of remote split operations, see USAF, *United States Air Force RPA Vector*.
 - 19 Wireless connectivity has traditionally been viewed as more elegant than tethered operation. But recent innovations in the vendor community suggest the potential benefits of hardwired connectivity, including higher bandwidth, more reliable connectivity, and greater information assurance. Interview by Sam Brannen with Helen Greiner, President and CEO, CyPhy Works, October 17, 2014; see also "Our Technology," CyPhy Works, <http://cyphyworks.com/technology/>.
 - 20 "Lost link" functionality returns an unmanned vehicle to a predetermined point for safe recovery or instructs the vehicle to operate in a predetermined manner until the communications link is restored. SAA technology seeks to allow the unmanned vehicle to autonomously avoid collisions with other mobile objects (such as manned aircraft, when thinking of UAS). For more on lost-link and SAA technology, see, for example, Andrew Lacher, Andrew Zeitlin, Chris Jella, Charlotte Laqui, and Kelly Markin, *Analysis of Key Airspace Integration Challenges and Alternatives for Unmanned Aircraft Systems*, F046-L10-021-001 (MITRE Corporation, July 2010).
 - 21 Notably, *automation* is different than *autonomy*. Automation implies an unmanned system executing a limited, set routine. Autonomy implies an unmanned system fully in control and able to adapt to changes in the environment. Automation is currently widely available, including in commercial aircraft and increasingly in automobiles. Formally, per the National Institute of Standards and Technology (NIST), autonomy refers to "the condition or quality of being self-governing" and "an [unmanned system's] own ability of sensing, perceiving, analyzing, communicating, planning, decision-making, and acting, to achieve its goals as assigned by its human operator(s) through designed HRI [human-robot interface]. Autonomy is characterized into levels by factors including mission complexity, environmental difficulty, and level of HRI to accomplish the missions." See NIST, *Autonomy Levels for Unmanned Systems (ALFUS) Framework*, ed. Hui-Min Huang (Gaithersburg, MD, NIST, September 2004, http://www.nist.gov/el/isd/ks/upload/NISTSP_1011_ver_1-1.pdf). Also, though of little relevance to entities in the HSE, who appear unlikely to employ armed unmanned systems, the topic of lethal autonomy is receiving considerable attention in the research community (see, for example, the Ethical Autonomy Project of the Center for a New American Security, <http://www.cnas.org/ethicalautonomy>). Note, of course, that unmanned systems capable of autonomous function must carry more complex control sensors and more powerful onboard processors. For instance, the Google self-driving car relies upon a light detection and ranging (LIDAR) sensor that "sees" surrounding obstacles and augments position, navigation, and timing information provided by GPS and IMUs (see Erico Guizzo, "How Google's Self-Driving Car Works," *IEEE Spectrum*, October 18, 2011, <http://spectrum.ieee.org/automaton/robotics/artificial-intelligence/how-google-self-driving-car-works>).
 - 22 For an overview of the challenge and opportunity areas for advancement, see Daniel Gonzales and Sarah Harting, *Designing Unmanned Systems with Greater Autonomy*, (Santa Monica, CA: RAND Corporation, 2014), http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR626/RAND_RR626.pdf. Artificial intelligence, which enables machine autonomy, is currently limited. Increasingly, artificial intelligence allows the performance of specific, narrowly defined tasks absent human input. However, this is far different from an artificial intelligence that could broadly substitute for human cognition, which experts consider to be several decades away. Current artificial intelligence is data-driven, requires significant processing power, and focuses on discrete challenges or problems. For a discussion of the current limits of artificial intelligence, see Peter Bock, Paul Cohen, and Andrew McAfee, "The Future of Artificial Intelligence: Robots and Beyond," interview by Amy Alving, Council on Foreign Relations, typed transcript (October 2, 2014), <http://www.cfr.org/technology-and-foreign-policy/future-artificial-intelligence-robots-beyond/p33579>.
 - 23 A number of sources in the literature present similar lists, to differing levels of specificity and often mixing apples and oranges. For a fairly exhaustive list, see Gupta, et al., "Review of Unmanned Aircraft System." Note that *all* unmanned systems sense—some act.
 - 24 The current capabilities—and remaining technological shortcomings—of unmanned systems equipped to perform real-world tasks have been on display in Japan's response to the 2011 Fukushima Daiichi nuclear disaster response and ongoing decommissioning. See Eliza Strickland, "Dismantling Fukushima: The World's Toughest Demolition Project," *IEEE Spectrum*, February 28, 2014, <http://spectrum.ieee.org/energy/nuclear/dismantling-fukushima-the-worlds-toughest-demolition-project>.
 - 25 The "dirty, dull, dangerous, and difficult" mantra is widely used (and hews to common sense) but receives little analytical attention in the literature.
 - 26 Discussions held during the course of this research suggest that aerial crime scene photography might be an example of such beneficial use. In this case, COTS quadcopters, some available for \$500, can substitute for manned helicopters, which are considerably

- more expensive to purchase and operate (though the latter are used for multiple missions, of course).
- 27 Other potentially disruptive technologies include the Internet of Things and 3D printing.
- 28 Clayton Christensen, *The Innovator's Dilemma* (Harper Business: New York, 2011), xviii.
- 29 For more information, see "Urban Challenge Overview," DARPA, <http://archive.darpa.mil/grandchallenge/overview.html>; and "DARPA Robotics Challenge Overview," DARPA, <http://www.theboticschallenge.org/overview>.
- 30 This insight was raised at each of the four working groups held as part of this study at CSIS in Washington, DC, on 16 June, 17 July, and 10 and 17 September 2014.
- 31 An unmanned system may be created from an existing vehicle designed for manned operation by retrofit with an "appliqué kit" that enables unmanned operation. For example, the Office of Naval Research has sponsored the Autonomous Aerial Cargo/Utility System (AACUS), a control package (with associated sensors) that can be added to an existing utility helicopter to allow for teleoperated or autonomous function. See "Autonomous Aerial Cargo/Utility System Program," Office of Naval Research, <http://www.onr.navy.mil/en/Science-Technology/Departments/Code-35/All-Programs/aerospace-research-351/Autonomous-Aerial-Cargo-Utility-AACUS.aspx>. The U.S. Army recently demonstrated similar appliqué kits for ground vehicles, enabling fully autonomous operation. See U.S. Army, "Second Autonomous Convoy Demonstration Completed by U.S. Army TARDEC, Lockheed Martin," news release, June 23, 2014, http://www.army.mil/article/128643/Second_Autonomous_Convoy_Demonstration_Completed_by_U_S_Army_TARDEC_Lockheed_Martin/. The well-known Google self-driving car is also an appliqué kit unmanned system.
- 32 For a description of the unique attributes of unmanned systems in a military context, see Scharre, *Robotics on the Battlefield Part I*, 10-12.
- 33 Charles Q. Choi, "Indestructible Starfish Robots Could Save Your Life One Day," *Popular Mechanics*, September 9, 2014, <http://www.popularmechanics.com/technology/engineering/robots/indestructible-starfish-robots-could-save-your-life-one-day-17190305>.
- 34 Carnegie Mellon University, "Press Release: Carnegie Mellon Snake Robot Winds Its Way Through Pipes, Vessels of Nuclear Power Plant," July 9, 2013, http://www.cmu.edu/news/stories/archives/2013/july/july9_snakerobot.html.
- 35 See Michael Van Cassell, "Hardy Throwbot helps SWAT team avoid danger in buildings," *Wyoming Tribune Eagle*, March 24, 2010; "Throwbot XT with Audio Capabilities," Recon Robotics, http://www.recon-scout.com/products/Throwbot_XT_audio.cfm; "Recon Scout Throw-bot LE," Recon Robotics, http://www.recon-scout.com/products/recon-scout_throwbot_LE.cfm; "Recon Scout XL," Recon Robotics, http://www.recon-scout.com/products/Recon_Scout_XL.cfm; "Micro Unmanned Ground Vehicle helps soldiers, first responders," Homeland Security Newswire, August 22, 2011, <http://www.homelandsecuritynewswire.com/micro-unmanned-ground-vehicle-helps-soldiers-first-responders>; "Pointman Tactical Robot: Maximum Mobility," Applied Research Associates, Inc., <http://forcepro.ara.com/products/force-protection/pointman-tactical-robot-maximum-mobility>, Applied Research Associates; "Pointman Selected as Border Patrol Tunnel Robot," press release, January 15, 2014, <http://forcepro.ara.com/pointman-selected-border-patrol-tunnel-robot>; "iRobot 110 FirstLook" (iRobot Corporation), 1-4, <http://www.irobot.com/~media/Files/Robots/Defense/FirstLook/iRobot-110-FirstLook-Specs.pdf>; Leon Engelbrecht, "QinetiQ's Dragon Runner robots sent to Afghanistan," *defenceweb*, November 20, 2009, http://www.defenceweb.co.za/index.php?option=com_content&task=view&id=5435&Itemid=105; and "Dragon Runner™ 20: Small Unmanned Ground Vehicle" (Reston, VA: QinetiQ North America), 1-2, https://www.qinetiq-na.com/wp-content/uploads/data-sheet_dr-20.pdf; QinetiQ North America, 1-2, and "Dragon Runner Unmanned Robotic Systems" (Reston, VA: QinetiQ North America), 1-2, https://www.qinetiq-na.com/wp-content/uploads/brochure_dr-10-20.pdf; "iRobot 310 SUGV," iRobot, <http://www.irobot.com/For-Defense-and-Security/Robots/310-SUGV.aspx#PublicSafety>; "iRobot 310 SUGV" (Bedford, MA: iRobot, 2012), 1-2, <http://www.irobot.com/~media/Files/Robots/Defense/SUGV/iRobot-310-SUGV-Specs.pdf>; "Police robot seeks out the bad guys," Homeland Security Newswire, August 31, 2010, <http://www.homelandsecuritynewswire.com/police-robot-seeks-out-bad-guys>; "PackBot Tactical Robot," Defense Update, 2007, <http://defense-update.com/products/p/pacbot.htm>; "iRobot 510 Packbot" (iRobot Corporation), 1-5, <http://www.irobot.com/~media/Files/Robots/Defense/PackBot/iRobot-510-PackBot-Specs.pdf>; "iRobot 510 Packbot CBRNe" (iRobot Corporation), 1-4, http://www.irobot.com/~media/Files/Robots/Defense/PackBot/iRobot_510_PackBot_HazMat_CBRNe.pdf; "Cameleon Lab – Develop your own application," ECA Robotics, [http://www.eca-robotics.com/en/robotic-vehicle/robot-ics-terrestrial-robots-et-vehicules-terrestres-\(ugv\)-cameleon-lab-develop-your-own-application/511.htm](http://www.eca-robotics.com/en/robotic-vehicle/robot-ics-terrestrial-robots-et-vehicules-terrestres-(ugv)-cameleon-lab-develop-your-own-application/511.htm); "Cameleon: Light Weight Modular UGV" (Toulon, France: ECA Robotics, 2011), 1-2, http://www.eca-robotics.com/ftp/ecatalogue/511/CAMELEON_GB.pdf; "Talon," QinetiQ North America, <https://www.qinetiq-na.com/products/unmanned-systems/talon/>; "Talon: The Warfighter's Choice" (Reston, VA: QinetiQ North America), https://www.qinetiq-na.com/wp-content/uploads/brochure_talon.pdf; "Caliber T5," ICOR Technology, <http://icortechology.com/caliber-t5/>; "The Chaos Robotics Platform," Autonomous Solutions Inc., <http://www.asirobots.com/products/chaos/>; David Hambling, "Are Robot Warriors Finally Coming to the Battlefield?" *Popular Mechanics*, July 24, 2013, <http://www.popularmechanics.com/technology/military/robots/are-robot-warriors-finally-coming-to-the-battlefield-15729762>; "iRobot 710 Kobra," iRobot Corporation, <http://www.irobot.com/us/learn/defense/kobra.aspx>; and "iRobot 710 Kobra" (Bedford: iRobot Corporation), 1-2, http://www.irobot.com/~media/Files/Robots/Defense/710/710_Specs.pdf; "MAARS: Modular Advanced Armed Robotic System," QinetiQ North America, <https://www.qinetiq-na.com/products/unmanned-systems/maars/>; Modular Advanced Armed Robotic System (MAARS) (Reston, VA: QinetiQ North America), 1-2, https://www.qinetiq-na.com/wp-content/uploads/data-sheet_maars.pdf; Jean Dubiel, "Robots can stand in for Soldiers during risky missions," U.S. Army, August 11, 2008, <http://www.army.mil/article/11592/robots-can-stand-in-for-soldiers-during-risky-missions/>; C.J. Lin, "Smart gun on wheels, robotic mule latest steps in automated warriors," *Stars and Stripes*, October 12, 2012, <http://www.stripes.com/news/smart-gun-on-wheels-robotic-mule-latest-steps-in-automated-warriors-1.192943>; "Black-I

- Robotics Landshark UGV," Black-I Robotics, http://blackirobotics.com/LandShark_UGV_UCOM.html; John Reed, "Semi-autonomous killer drones from around the globe," *Foreign Policy*, April 29, 2013; "Guardium Mark 2 UGV" (G-NIUS Unmanned Ground Systems), 1-2, <http://g-nius.co.il/pdf/brochures/GuardiumLS.pdf>; "Guardium-Mk II," G-NIUS Unmanned Ground Systems, 2008, <http://g-nius.co.il/unmanned-ground-systems/guardium-2.html>; "Guardium: A New Dimension in Controlled Area Defense" (Israeli Aircraft Industries Ltd.), 1-6, http://www.iai.co.il/Sip_Storage/FILES/0/33810.pdf; "Guardium UGV: Driven by Innovation" (G-NIUS Unmanned Ground Systems), 1-2, <http://g-nius.co.il/pdf/brochures/GuardiumUGV.pdf>; "Upgrades and Autonomy Improvements Lead UGV Technology Advances," *COTS Journal*, April 2013, <http://www.cotsjournalonline.com/articles/view/103307>; "Minotaur," QinetiQ North America, <https://www.qinetiq-na.com/products/unmanned-systems/minotaur/>, and "U.S. Army REF Minotaur" (Reston: QinetiQ North America), 1-2, https://www.qinetiq-na.com/wp-content/uploads/data-sheet_minotaur.pdf; "Unmanned Ground Vehicle," Oshkosh Defense, <http://oshkoshdefense.com/technology-1/unmanned-ground-vehicle/>; "Taxibot to Enter Service in 2014," TLD Group, April 2, 2014, <http://www.tld-group.com/news/taxibot-enter-service-2014/>; "Taxibot: Pilot Controlled Taxiing System Without Engines Running" (Israeli Aerospace Industries and TLD), 1-2, http://media.wix.com/ugd/865bf2_95beaa98ba904712aecbc956f1297c16.pdf. Images: iRobot 310 SUGV, <http://www.aviationnews.eu/blog/wp-content/uploads/2011/01/SUGV.jpg>; QinetiQ Talon, <https://www.qinetiq.com/media/Image%20Library/talon-robot-large.jpg>; Oshkosh TerraMax, http://www.unmannedsystemstechnology.com/wp-content/uploads/2012/08/Terramax_cargo_UGV_Unmanned_Ground_Vehicle_Oshkosh_Defense_United_States_defence_industry_002.jpg.
- 36 See "ATLAS SeaFox Mk II ROV for Identification and Mine Disposal" (Bremen, Germany: ATLAS Elektronik), 1-6, https://www.atlas-elektronik.com/fileadmin/user_upload/documents/products/Unmanned_Vehicles/005_SeaFox_11_2013.pdf; "REMUS 100," Woods Hole Oceanographic Institute, <http://www.whoi.edu/main/remus100>; "GNOM: Underwater Remotely Operated Vehicle," Indel Partner Ltd., <http://www.gnomrov.com/>; Bluefin Robotics, "HAUV Hovering Autonomous Underwater Vehicle," Factsheet, July 2, 2011, 1-2, <http://www.bluefinrobotics.com/assets/Downloads/Bluefin-HAUV-Product-Sheet.pdf>; "ATLAS SeaCat" (Bremen, Germany: ATLAS Elektronik), https://www.atlas-elektronik.com/fileadmin/user_upload/documents/products/Unmanned_Vehicles/241_SeaCat.pdf; "ATLAS Mardian SeaOtter Autonomous Underwater Vehicle (AUV)" (Denmark: ATLAS Mardian, 2012), 1-5, http://auvac.org/uploads/configuration_spec_sheets/Atlas%20sea%20otter.pdf; "REMUS 600," Woods Hole Oceanographic Institute, <http://www.whoi.edu/main/remus600>; "Talisman M configuration," Autonomous Undersea Vehicle Applications Center, <http://auvac.org/configurations/view/4>; "Talisman M Unmanned Underwater Vehicle" (Surrey, United Kingdom: BAE Systems, 2011), 1-2, http://auvac.org/uploads/configuration_spec_sheets/Talisman%20M%20data%20sheet.pdf; "QX Ultra," i-Tech 7, <http://www.interventionstechnology.com/en/services.php?id=31>; "QX Ultra: Work Class ROV" (i-Tech 7, 2013), 1-2, http://www.interventionstechnology.com/en/cms/user_files/File/ROVs/QX%20Ultra.pdf; "AUV System Spec Sheet: Proteus configuration," Autonomous Undersea Vehicle Applications Center, <http://auvac.org/configurations/view/239>; "AUV System Spec Sheet: Echo Ranger configuration," Autonomous Undersea Vehicle Applications Center, <http://auvac.org/configurations/view/13>; Randy Jackson, "Deep diver: Echo Ranger makes big splash for unmanned submersibles," *Boeing*, August 17, 2011; James Ferguson, Allan Pope, Bruce Butler, and Ronald I. Verall, "Theseus AUV—Two Record Breaking Missions: Designed to Lay Fiber-Optic Cable from a Site Near the Shore of Ellesmere Island to a Scientific Acoustic Array in the Arctic Ocean," *Sea Technology*, February 1999, 65-70, <http://cradpdf.drdc-rddc.gc.ca/PDFS/zbd89/p515380.pdf>; James McFarlane and Raymond F. Murphy, "AUVs Survey The Canadian Arctic," *Sea Technology*, http://www.sea-technology.com/features/2013/0513/6_AUVs.php; and Department of the Navy, "The Navy Unmanned Undersea Vehicle (UUV) Master Plan," (Washington, DC: DoD, 2004), xxii-xxiv and 67-72, <http://www.navy.mil/navydata/technology/uuvmp.pdf>. Images: Remus, <http://auvac.org/uploads/configuration/REMUS100Water.jpg>; SeaCat, https://www.atlas-elektronik.com/fileadmin/user_upload/images/products/Unmanned_Vehicles/SeaCat_afloat.png; Echo Ranger, <http://auvac.org/uploads/configuration/Echo%20Ranger%205.jpg>.
- 37 See "Kingfisher," Clearpath Robotics Inc., <http://www.clearpathrobotics.com/kingfisher/>; "Kingfisher – Tech Specs," Clearpath Robotics, <http://www.clearpathrobotics.com/kingfisher/tech-specs/>; Clearpath Robotics, "Kingfisher Unmanned Surface Vehicle Technical Specifications," Factsheet, http://www.clearpathrobotics.com/wp-content/uploads/2013/08/KINGFISHER_DATA_SHEETv4.pdf; "Kingfisher – Overview," Clearpath Robotics, <http://www.clearpathrobotics.com/kingfisher/>; "Designed to go everywhere," Liquid Robotics, <http://liquidr.com/technology/waveglider/sv3.html>; Liquid Robotics, "Wave Glider SV3 Base Platform Specifications," Factsheet; "METOC Wave Glider," Liquid Robotics, <http://liquidr.com/prodserv/wg/metoc.html>; "Security Wave Glider," Liquid Robotics, <http://liquidr.com/prodserv/wg/security.html>; "GATEWAY Wave Glider," Liquid Robotics, <http://liquidr.com/prodserv/wg/gateway.html>; "ENVIRONMENTAL Wave Glider," Liquid Robotics, <http://liquidr.com/prodserv/wg/environmental.html>; GEOPHYSICAL Wave Glider," Liquid Robotics, <http://liquidr.com/prodserv/wg/geophysical.html>; "Remotely Piloted Boats," NjordWorks Inc.; "Pioneer Unmanned Boat," NjordWorks Inc.; "Pioneer Tech Specs," NjordWorks Inc.; "Applications for Pioneer," NjordWorks Inc.; NjordWorks Inc., "Small, Affordable, and Capable: Pioneer," Factsheet; "SeaRobotics Corporation offers a wide variety of small, COTS marine robots," SeaRobotics Corporation, <http://www.searobotics.com/products.html>; "C-Stat Mobile Buoy Systems," Autonomous Surface Vehicles Ltd., <http://www.asvglobal.com/military-and-security/c-stat>, Autonomous Surface Vehicles Ltd.; "C-Stat Station Keeping Buoy," Factsheet, 1-2, <http://www.asvglobal.com/files/datasheets/c-stat-datasheet.pdf>; "C-Target 3 Naval Target Drone," Autonomous Surface Vehicles Ltd., <http://www.asvglobal.com/marine-targets/c-target-3>; Autonomous Surface Vehicles Ltd., "C-Hunter Semi-Submersible," Factsheet, 2014, <http://www.asvglobal.com/files/datasheets/c-hunter-datasheet.pdf>; "Piraya USV Group Control of Unmanned Surface Vehicles," Saab Automobile, <http://www.saabgroup.com/en/Naval/Kockums-Naval-Solutions/Naval-Surface-Ships/Piraya-USV/>; "C-Sweep Multi-role MCM USV," Autonomous Surface Vehicles Ltd., <http://www.asvglobal.com/military-and-security/c-sweep>; Autonomous Surface Vehicles Ltd., "C-Sweep," Factsheet, 2014, <http://www.asvglobal.com/files/datasheets/c-sweep-datasheet.pdf>; "C-Target 13 Naval Target Drone," Autonomous Surface Vehicles Ltd., <http://www.asvglobal.com/marine-targets/c-target-13>; Mike Hanlon, "Nanotube-reinforced carbon fiber Piranha USV," *Gizmag*, February 24, 2010, <http://www.gizmag.com/nanotube-reinforced-carbon-fiber-piranha-usv/14321/>; James Holloway, "Unmanned nanomaterial Piranha threatens to redefine naval warfare," *Gizmag*, April 10, 2012, <http://www.gizmag.com>.

- com/zyvex-piranha-usv/22078/; and "Naval Systems – Unmanned Surface Vehicle," Elbit Systems, 2014, <https://www.elbitsystems.com/elbitmain/area-in2.asp?parent=10&num=92&num2=92>. Images: Kingfisher, http://clearpath.wpengine.netdna-cdn.com/wp-content/uploads/2012/12/Gallery_Kingfisher_Pool_Side.jpg; Piraya; Piranha, <http://compositesmanufacturingmagazine.com/wp-content/uploads/2014/06/Piranha-unmanned-vessel-Zyvex-Technologies-carbon-nanotube-CNT-reinforced-carbon-fiber-boat.jpg>.
- 38 See "Compare Phantom 2 Series," DJI, <http://www.dji.com/products/compare-phantom/>; "Phantom," DJI, <http://www.dji.com/product/phantom/feature/>; "Phantom 2," DJI, <http://www.dji.com/product/phantom-2/spec/>; "Iris," 3DRobotics Inc., <http://3drobotics.com/iris/>; "Features," Yamaha Motor Australia, <http://rmax.yamaha-motor.com.au/features/>; "Frequently Asked Questions: What is the maximum height, distance, speed & duration that the RMAX can fly at?" Yamaha Motor Australia, <http://rmax.yamaha-motor.com.au/faq#n128>; "Specifications," Yamaha Motor Australia, <http://rmax.yamaha-motor.com.au/specifications/>; Bill Swindell, "Drones could become familiar sight over Wine Country vineyards (w/video)," *Press Democrat* (Santa Rosa, CA), October 15, 2014, <http://www.pressdemocrat.com/business/2980362-181/drones-could-become-familiar-sight#page=2>; "Fire-X VUAS," (Northrop Grumman Corporation, 2011), http://www.northropgrumman.com/Capabilities/FireX/Documents/Fire-X_Brochure.pdf; "Fire-X Medium-Range Vertical Unmanned Aerial System, United States of America," Army-Technology, <http://www.army-technology.com/projects/firexmediumrangevert/>. Images: RMAX, <http://www.turfmate.com.au/uploads/articles/1145/image/1145.png>; Fire Scout, http://aviationintel.com/wp-content/uploads/2014/01/northrop_grumman_mq-8c_fire_scout-920x613.jpg.
- 39 See Gary Mortimer, "Mesa County Police purchase Falcon fixed wing sUAS," sUAS News, January 16, 2012, <http://www.suasnews.com/2012/01/11259/ mesa-county-police-purchase-fixed-wing-suas/>; "Raven: Overview" (AeroVironment, Inc.), http://www.avinc.com/downloads/Raven_Gimbal.pdf; National Guard Bureau, 2014 *National Guard Bureau Posture Statement: Sustaining an Operational Force* (Washington, DC: DoD 2014), 18; "RQ-11 Raven Unmanned Aerial Vehicle, United States of America," Army-Technology, <http://www.army-technology.com/projects/rq11-raven/>; "ScanEagle System," Insitu Inc., <http://www.insitu.com/systems/scaneagle/>; "ScanEagle Imagers," Insitu Inc., <http://www.insitu.com/systems/scaneagle/imagers/>; U.S. Coast Guard, "ScanEagle UAS Takes Flight from Coast Guard Cutter Stratton," news release, August 30, 2012, <http://www.uscg.mil/acquisition/newsroom/features/uas083012.asp>; Insitu Inc., "ScanEagle Options and Capabilities," Factsheet, http://www.insitu.com/images/uploads/product-cards/Scaneagle_OptionsAndCapabilities.pdf; Jason Paur, "Boeing's Best-Selling Aircraft Fits on Your Shoulder," *Wired*, August 14, 2009, <http://www.wired.com/2009/08/boeing-uav/>; "AAI RQ-7 Shadow 200," sUAS News, <http://www.suasnews.com/aai-rq-7-shadow-200/>; CBP, "Unmanned Aircraft System MQ-9 Predator B," Factsheet, February 6, 2014, http://www.cbp.gov/sites/default/files/documents/FS_2013_UAS_new.pdf; Michael C. Kostelnik, "UAS on Leading Edge in Homeland Security," PowerPoint presented at National Defense Industrial Association, October 4, 2012, <http://www.dtic.mil/ndia/2012/targets/TKostelnik.pdf>; General Atomics, "MQ-9 Reaper/Predator B," Factsheet, 2012, http://www.ga-asi.com/products/aircraft/pdf/Predator_B.pdf; Office of the Inspector General, *CBP's Use of Unmanned Aircraft Systems in the Nation's Border Security*, OIG-12-85 (Washington, DC: DHS, 2012), 1-3; CBP, *Concept of Operations for CBP's Predator B Unmanned Aircraft System* (Washington, DC: DHS, 2010), 17-20; National Aeronautics and Space Administration, "NASA Armstrong Fact Sheet: Global Hawk High-altitude, long-endurance science aircraft," Factsheet, February 28, 2014, http://www.nasa.gov/centers/armstrong/news/FactSheets/FS-098-DFRC.html#VE_IR_nF9yw; Department of Transportation, Office of the Inspector General, *Office of Inspector General Audit Report: FAA Faces Significant Barriers to Safely Integrate Unmanned Aircraft Systems into the National Airspace System*, AV-2014-061 (Washington, DC: Department of Transportation 2014), 1-24, <https://www.oig.dot.gov/sites/default/files/FAA%20Oversight%20of%20Unmanned%20Aircraft%20Systems%5E6-26-14.pdf>; DoD, *Unmanned Systems Integrated Roadmap FY2011-2036*, 20-22. Images: Scan Eagle, <http://www.uscg.mil/acquisition/uas/images/2012/UAS3.jpg>; Guardian, http://upload.wikimedia.org/wikipedia/commons/f/f5/MQ-9_Reaper_CBP.jpg.
- 40 USAF, *RPA Vector: Vision and Enabling Concepts 2013-2038*, 30.
- 41 See, for example, the iRobot-designed "uPoint" platform, iRobot Corporation, "iRobot Unveils Its First Multi-Robot Tablet Controller for First Responders, Defense Forces and Industrial Customers," news release, October 9, 2014, <http://media.irobot.com/2014-10-09-iRobot-Unveils-Its-First-Multi-Robot-Tablet-Controller-for-First-Responders-Defense-Forces-and-Industrial-Customers>.
- 42 One such example is 3D Robotics' "Follow Me" technology that works with the company's existing UAS to follow a user (ostensibly for the purposes of aerial filming of outdoor events/sports). See 3D Robotics, "3DR Announces Follow-Me Mode: Free for DroidPlanner 2.0," news release, June 2014, <http://3drobotics.com/2014/06/follow-me-mode/>.
- 43 See, for example, Vijay Kumar, "Robots that fly ... and cooperate," YouTube video, 16:46, from a TED Talk aired in March 2012, posted by TED Talks, https://www.youtube.com/watch?v=4ErEBkj_3PY. See also a discussion of this technology in a military context in Scharre's *Robotics on the Battlefield Part I*.
- 44 Significant experimentation in manned-unmanned teaming is ongoing across DoD. For example, the USAF is exploring integrating greater autonomy into the concept to develop what it has called a "loyal wingman" unmanned aircraft that would team with a manned platform. The U.S. Army has already begun to implement the teaming of UAS with its Apache helicopters. See David Vergun, "Apache-UAV Teaming Combines 'Best Capabilities of Man, Machine,'" U.S. Army News Service, May 8, 2014, <http://www.army.mil/article/125676/>; and USAF, *RPA Vector*, 40, <http://www.af.mil/Portals/1/documents/news/USAFRPAVectorVisionandEnablingConcepts2013-2038.pdf>.
- 45 Use of unmanned systems in the homeland security context is discussed in sections on current use and future requirements (later in the present paper).
- 46 "Amazon Announces Futuristic Plan: Delivery by Drone" CBS News, December 1, 2013, <http://www.cbsnews.com/news/amazon-unveils->

[futuristic-plan-delivery-by-drone/](#).

- 47 See, for example, commentary by Jason Lomborg, "Amazon's drone-delivery service is a pipe dream (for now)" *Electronic Component News*, December 6, 2013, <http://www.ecnmag.com/blogs/2013/12/amazon%E2%80%99s-drone-delivery-service-pipe-dream-now>.
- 48 Alexis Madrigal, "Inside Google's Secret Drone Delivery Program" *The Atlantic*, August 28, 2014, <http://www.theatlantic.com/technology/archive/2014/08/inside-googles-secret-drone-delivery-program/379306/>.
- 49 These are exemptions granted permitted under Section 333 of the FAA Modernization and Reform Act of 2012 (the Reform Act) and the procedures contained in 14 C.F.R. 11. These include exemptions granted to Astraeus Aerial, Aerial MOB, LLC, HeliVideo Productions, LLC, Pictorvision Inc, RC Pro Productions Consulting, LLC dba Vortex Aerial, and Snaproll Media, LLC. See FAA, "Press Release – U.S. Transportation Secretary Foxx Announces FAA Exemptions for Commercial UAS Movie and TV Production," news release, September 25, 2014, http://www.faa.gov/news/press_releases/news_story.cfm?newsId=17194&cid=TW251. That said, recent media reporting suggests that upcoming FAA rules may hinder or preclude delivery drone activity (Jack Nikas and Alistair Barr, "Those Amazon Delivery Drones? Not So Fast," *Wall Street Journal*, 25 November 2014, <http://online.wsj.com/articles/faas-planned-drone-rules-would-pose-commercial-concerns-1416951084>).
- 50 For instance, the world's largest model aircraft association, the Academy of Model Aircraft, dates to 1936. See "Academy of Model Aeronautics (AMA) History," Academy of Model Aeronautics, http://www.modelaircraft.org/museum/ama_history.aspx.
- 51 Despite significant overlap between the communities, there is active discussion between "drone users" and model aircraft users about their similarities and differences. Organizations with a specific focus on "drones," such as the DC Area Drone User Group, exist alongside more traditional model aviation hobbyist groups (see <http://www.meetup.com/DC-Area-Drone-User-Group/>).
- 52 Parrot has sold more than 700,000 of its AR.Drones. See Parrot, "New Progress in Civil and Commercial Drones," news release, February 27, 2014, <http://www.parrotcorp.com/en/pressrelease/newprogressincommercialandcivildrones>. In an interview, a DJI representative noted that his company has grown from 50 employees in 2009 to 2,500 today. Michael Perry (Public Relations Manager, DJI), interview by Sam Brannen, Matthew Fleming, and Richard Say, October 22, 2014.
- 53 See, for instance, Alexander Stoklosa, "We Go for a Ride in Audi's 'Piloted Driving' Autonomous A6 Avant Prototype," *Car and Driver* (blog), January 10, 2013, <http://blog.caranddriver.com/we-go-for-a-ride-in-audis-piloted-driving-autonomous-a6-avant-prototype-2013-ces/>.
- 54 Future autonomous vehicles may rely on V2V networking to communicate amongst themselves, warning nearby vehicles of potential hazards as well as impending course changes (in the same way that human operators use turn signals). V2V networking may be augmented by onboard cellular data links permitting autonomous vehicles to draw on cloud data sources for real-time updates. Such technologies currently exist and are being implemented into high-end consumer vehicles such as the Audi A8 and Tesla Model S. See Jonathan M. Gitlin, "Prepare for the part-time self-driving car: the only thing it won't do is transform into an autobot," *ArsTechnica*, October 29, 2014, <http://arstechnica.com/cars/2014/10/prepare-for-the-part-time-self-driving-car/>.
- 55 "Tesla's Elon Musk: Autonomous Driving Is Five Years Away," Bloomberg Television, 3:36, October 10, 2013, <http://www.bloomberg.com/video/elon-musk-on-tesla-s-auto-pilot-and-legal-liability-BubZcwLORpyq84SkK1lp5A.html>.
- 56 This is based on an estimate from data provided in DoD, *Unmanned Systems Integrated Roadmap FY2013-2038*, 5.
- 57 Teal Group Corporation, "Executive Overview: World Unmanned Aerial Vehicle Systems" (2014), 19.
- 58 Association for Unmanned Vehicle Systems International, *Economic Impact of Unmanned Systems Aircraft Integration in the United States* (March 2013), 2, https://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedImages/New_Economic%20Report%202013%20Full.pdf.
- 59 Teal Group reports that growth would be strongest on the civil government side; AUVSI reports that growth would be strongest in precision agriculture. See Teal Group Corporation, 11 and 16-18; AUVSI, *Economic Impact of Unmanned Systems Aircraft Integration in the United States*, 2 and 6.
- 60 "Unmanned Ground Vehicle Market by Application (Commercial, Defense, & Homeland Security), Technology (Tethered, Tele-operated, Semi-autonomous, Fully-autonomous), Payload (Fixed, Role Specific), Type (Locomotion, Size, Weapons, Energy Source) & by Geography (North America, Europe, Asia-Pacific, the Middle East, Latin America, Africa) – Forecasts & Analysis 2014–2020," MarketsandMarkets, September 2014, <http://www.marketsandmarkets.com/Market-Reports/unmanned-ground-vehicles-market-72041795.html?gclid=CKq6t-Pk6MACFU9k7AodXBEAfg>.
- 61 "Unmanned Underwater Vehicles Market worth \$4.84 Billion by 2019," press release, MarketsandMarkets, July 31, 2014, <http://www.marketsandmarkets.com/PressReleases/unmanned-underwater-vehicles.asp>.
- 62 Isaac Arnsdorf, "Rolls-Royce Drone Ships Challenge \$375 Billion Industry: Freight," Bloomberg News, February 25, 2014, <http://www.bloomberg.com/news/2014-02-25/rolls-royce-drone-ships-challenge-375-billion-industry-freight.html>.
- 63 These countries are widely discussed as leaders in the unmanned systems/robotics literature, and were raised in interviews with the

research team.

- 64 Many in U.S. industry believe that the FAA's approach to UAS testing and use—allowing only limited numbers of test sites and requiring Certificates of Authorization (COAs) for use—has disadvantaged U.S. UAS industry at a critical time, particularly in the sUAS market. This point was raised repeatedly in discussions with a range of U.S.-based manufacturers who felt that U.S. economic competitiveness in the industry may be at stake.
- 65 See, for example, DIY Drones, <http://diydrones.com/>.
- 66 No single document captures the use of unmanned systems in the HSE. Accordingly, this section draws on a large body of academic and policy literature; working group discussions and semi-structured interviews; and reviews of the DHS budget, strategies related to homeland security, grant programs, and FAA COAs, among other sources.
- 67 Office of Inspector General, *A Review of Remote Surveillance Technology Along U.S. Land Borders* (Washington, DC: DHS, December 2005), 13, http://www.oig.dhs.gov/assets/Mgmt/OIG_06-15_Dec05.pdf.
- 68 Note that use of UAS in the NAS requires an FAA COA. A list of COAs granted to users—DHS and otherwise—is available via the FAA: http://www.faa.gov/uas/public_operations/foia_responses/.
- 69 Office of Inspector General, *A Review of Remote Surveillance Technology Along U.S. Land Borders*, 13.
- 70 *Ibid.*, 14.
- 71 *On OAM Operations and Investments, Before the House Appropriations Committee, Subcommittee on Homeland Security*, 111th Cong. (2010) (statement of Michael Kostelnik, Assistant Commissioner, OAM, CBP).
- 72 CBP, "CBP Launches New Maritime Unmanned Aircraft System," news release, December 9, 2009, <http://www.cbp.gov/newsroom/local-media-release/2009-12-09-050000/cbp-launches-new-maritime-unmanned-aircraft-system>.
- 73 *Ibid.*
- 74 CBP, *Concept of Operations for CBP's Predator B Unmanned Aircraft System*, 6 (note: redacted version, declassified and released under FOIA).
- 75 *Ibid.*, 51-52.
- 76 CBP, "Unmanned Aircraft System MQ-9 Predator B," fact sheet, February 6, 2014, http://www.cbp.gov/sites/default/files/documents/FS_2013_UAS_new.pdf.
- 77 DHS OIG, *CBP's Use of Unmanned Aircraft Systems in the Nation's Border Security*, 16.
- 78 *Ibid.*
- 79 GAO, *Unmanned Aerial Systems: Department of Homeland Security's Review of U.S. Customs and Border Protection's Use and Compliance with Privacy and Civil Liberty Laws and Standards*, GAO14-849R (Washington, DC: GAO, September 30, 2011), 11, <http://www.gao.gov/assets/670/666282.pdf>.
- 80 *Ibid.*, 6.
- 81 See Craig Whitlock and Craig Timberg, "Border-Patrol Drones Being Borrowed by Other Agencies More Often Than Previously Known," *Washington Post*, January 14, 2014, http://www.washingtonpost.com/world/national-security/border-patrol-drones-being-borrowed-by-other-agencies-more-often-than-previously-known/2014/01/14/5f987af0-7d49-11e3-9556-4a4bf7bcbd84_story.html.
- 82 GAO, *Unmanned Aerial Systems: Department of Homeland Security's Review of U.S. Customs and Border Protection's Use and Compliance with Privacy and Civil Liberty Laws and Standards*, 11.
- 83 CBP, *Concept of Operations for CBP's Predator B Unmanned Aircraft System*, 5.
- 84 "UAS on Leading Edge in Homeland Security," presentation by Michael Kostelnik, Assistant Commissioner, CBP OAM, to National Defense Industrial Association, October 4, 2012, 17, <http://www.dtic.mil/ndia/2012targets/TKostelnik.pdf>.
- 85 Associated Press, "US Government Patrolling Nearly Half Of Mexican Border By Drones Alone," CBS Houston, November 13, 2014, <http://houston.cbslocal.com/2014/11/13/us-government-patrolling-nearly-half-of-mexican-border-by-drones-alone/>.
- 86 *Ibid.*; discussion at Second Working Group, 17 July 2014.
- 87 Sandia National Laboratories, "Sandia airborne pod seeks to trace nuclear bomb's origins," press release, January 9, 2013, https://share.sandia.gov/news/resources/news_releases/airborne_pods/#VGC7k_nF_zg.
- 88 *Ibid.*, 7.
- 89 *Ibid.*, 6.

- ⁹⁰ GAO, *Unmanned Aerial Systems: Department of Homeland Security's Review of U.S. Customs and Border Protection's Use and Compliance with Privacy and Civil Liberty Laws and Standards*; "MTS-B Multi-Spectral Targeting System," Raytheon, http://www.raytheon.com/capabilities/products/mts_b/; "Lynx Multi-mode Radar," General Atomics, http://www.ga-asi.com/products/sensor_systems/lynxsar.php; William Matthews, "Man Hunting Radar," *Defense News*, April 26, 2010, <http://www.defensenews.com/article/20100426/DEFENET01/4260311/Man-hunting-Radar>; "Sea View Overland and Maritime Surveillance Radar," Raytheon, <http://www.raytheon.com/capabilities/products/seavue/>. Images: MTS-B, <http://nhia.la9.jp/10JBLM/03-33123-2.jpg>; Lynx Radar, <http://generalatomics.files.wordpress.com/2013/04/radar-system.png?w=946>; VADER, http://media.npr.org/assets/img/2013/06/11/163356026_wide-9fabf4b3d0d3f9f59166590a9a8165297e8f430f.jpg; SeaVue, <https://4gwar.files.wordpress.com/2009/12/guardian-2.jpg>.
- ⁹¹ HSSAI-CSIS interview with a DHS official, 24 October 2014.
- ⁹² Ibid.
- ⁹³ Jeff Vajda, "Coast Guard UAS Program," PowerPoint presentation, 7 August 2014.
- ⁹⁴ Ibid., and HSSAI-CSIS interview with a DHS official, 14 October 2014.
- ⁹⁵ Ibid.
- ⁹⁶ DHS, "The Robotic Aircraft for Public Safety Project Will Evaluate SUAS for First Responder and Border Security Applications," public announcement, July 17, 2012.
- ⁹⁷ RAPS was cited repeatedly during working groups and research interviews as an important DHS-led initiative designed to understand the potential of sUAS for homeland security missions and to inform acquisition decisions for a range of potential applications. It is important to note that these reports and subsequent results are protected and are shared only with federal, state, and local government entities.
- ⁹⁸ Office of the Inspector General, *CBP's Strategy to Address Illicit Cross Border Tunnels*, OIG-12-132 (Washington, DC: DHS, 2012), 7, http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-132_Sep12.pdf.
- ⁹⁹ *Illegal Tunnels on the Southwest Border, Before the Senate Caucus on International Narcotics Control*, 112th Cong. (2011) (statement of James A. Dinkins, Executive Associate Director of U.S. Immigration and Customs Enforcement), <http://www.dhs.gov/news/2011/06/15/testimony-executive-associate-director-james-dinkins-immigration-and-customs>.
- ¹⁰⁰ *Border Security Threats to the Homeland: DHS' Response to Innovative Tactics and Techniques, Before the House Committee on Homeland Security, Subcommittee on Border and Maritime Security*, 112th Cong. (2012) (written statement of Donna Bucella, Assistant Commissioner of U.S. Customs and Border Protection, Office of Intelligence and Investigative Liaison), <http://www.dhs.gov/news/2012/06/15/written-testimony-us-customs-border-protection-house-homeland-security-subcommittee>.
- ¹⁰¹ *Testimony of Chief Michael Fisher, U.S. Border Patrol, and Acting Assistant Commissioner Kevin Mcaleenan, Office of Field Operations, Before the House Committee on Homeland Security, Subcommittee on Border and Maritime Security*, 112th Cong. (2012) (statement of Michael J. Fisher, Chief, U.S. Border Patrol, and Kevin Mcaleenan, Acting Assistant Commissioner, Office of Field Operations, U.S. Customs and Border Protection, Department of Homeland Security), <http://docs.house.gov/meetings/HM/HM11/20130226/100300/HHRG-113-HM11-Wstate-FisherM-20130226.pdf>. See also Dan Verton, "DHS: Effective Counter-Tunnel Technology Remains Elusive, CBP Says," *Homeland Security Today*, March 13, 2013, <http://www.hstoday.us/channels/dhs/single-article-page/effective-counter-tunnel-technology-remains-elusive-cbp-says/467ee7f79618b1ffc95c308b916a3f69.html>.
- ¹⁰² "Versatrax 150," Inuktun US LLC, <http://www.inuktun.com/crawler-vehicles/versatrax-150.html>; Fernana Santos, "Border's New Sentinels Are Robots, Penetrating Deepest Drug Routes," *New York Times*, February 22, 2014, http://www.nytimes.com/2014/02/23/us/borders-new-sentinels-are-robots-penetrating-deepest-drug-routes.html?_r=0; and "Pointman Tactical Robot: Maximum Mobility," Applied Research Associates, Inc., <http://forcepro.ara.com/products/force-protection/pointman-tactical-robot-maximum-mobility>.
- ¹⁰³ Brian Skoloff and Jacques Billeaud, "Drug-tunnel robots are latest border security gizmo," *USA Today*, January 14, 2014, <http://www.usatoday.com/story/news/world/2014/01/14/drug-tunnels-us-mexico-border/4478073/>.
- ¹⁰⁴ For manned tunnel detection technology efforts, see the Rapid Reaction Tunnel Detection (R2TD), a joint effort with DoD/NORTHCOM and the Tunnel Detection Project, a joint partnership with Lockheed Martin Advanced Technology Laboratories.
- ¹⁰⁵ "Counter Tunnel Testing," U.S. Navy, http://www.public.navy.mil/spawar/Pacific/Robotics/Pages/CT_Testing.aspx.
- ¹⁰⁶ "Dismantling a Pipe Bomb – and Preserving the Evidence," DHS S&T, 2012, <http://www.dhs.gov/st-snapshot-sapber>.
- ¹⁰⁷ DHS S&T, *Standards Office—Robot Response Standards Program* (Washington, DC: DHS, 2013), <http://www.dhs.gov/sites/default/files/publications/Standards%20Office%20-%20Robot%20Response%20Standards%20Program-508.pdf>.
- ¹⁰⁸ "Protecting our Harbors and Ships with the BIOSwimmer," DHS S&T, 2012, <http://www.dhs.gov/st-snapshot-bioswimmer>.
- ¹⁰⁹ Designers are beginning to explore unique platform designs, such as Liquid Robotics' Wave Glider. Using the energy of the oceans' waves to propel itself, it is capable of extremely long-duration deployment and autonomous function (including staying in one

geolocated position, like a buoy), and it is essentially silent, making it an ideal platform for the collection of acoustic data.

- 110 UAS are subject to a different level of scrutiny in the DoD process as compared to manned aircraft per a September 28, 2006, document from the Deputy Secretary of Defense on "Interim Guidance for the Domestic Use of Unmanned Aircraft Systems."
- 111 National Guard Bureau, *2013 National Guard Bureau Posture Statement: Security America Can Afford*, (Washington, DC: DoD), 13, <http://www.nationalguard.mil/portals/31/Documents/PostureStatements/2013%20National%20Guard%20Bureau%20Posture%20Statement.pdf>.
- 112 National Guard Bureau, *2015 National Guard Bureau Posture Statement: Trusted at Home, Proven Abroad*, (Washington, DC: DoD), 26, <http://www.nationalguard.mil/portals/31/Documents/PostureStatements/2015%20National%20Guard%20Bureau%20Posture%20Statement.pdf>.
- 113 See "After Action Review and Lessons Learned in the Use of a Remotely Piloted Aircraft (RPA) MQ-1 on the Rim Fire," Wildland Fire Lessons Learned Center, <http://www.wildfirelessons.net/communities/resources/viewdocument/?DocumentKey=74e7834b-634b-4c5f-8744-e65ae6ffa669>; and "Emerging Uses of UAV Technology," Stimson Center, <http://www.stimson.org/events/emerging-uses-of-uav-technology/>.
- 114 National Guard Bureau, *2014 National Guard Bureau Posture Statement: Sustaining an Operational Force*, (Washington, DC: DoD), 18.
- 115 National Guard Bureau, *2015 National Guard Bureau Posture Statement*, 26.
- 116 Title 32 of the *U.S. Code* relates to the National Guard.
- 117 For more on the 1033 Program, see "1033 Program FAQ," Defense Logistics Agency, Disposition Services, <http://www.dispositionservices.dla.mil/leso/pages/1033programfaqs.aspx>.
- 118 Certain other federal entities outside of the HSE currently operate UAS for a wide variety of purposes unrelated to law enforcement. For example, the National Oceanic and Atmospheric Administration (NOAA) operates several different types of sUAS for gathering meteorological data, training personnel, and testing new equipment (Robbie Hood, Director of NOAA's Unmanned Aircraft Systems Program, NOAA, interview by Richard Say, 4 November 2014). The National Aeronautic and Space Administration (NASA), which operates two RQ-4 Global Hawks and one MQ-9 Predator B along with several types of sUAS, uses these systems to conduct research, collect atmospheric data, and support the ongoing integration of UAS into the NAS ("NASA Armstrong Fact Sheet: Ikhana/Predator B Unmanned Science and Research Aircraft System," Factsheet, February 28, 2014, http://www.nasa.gov/centers/armstrong/news/FactSheets/FS-097-DFRC.html#VGUjW_nF9yx; NASA, "NASA Armstrong Fact Sheet: Global Hawk High-altitude, long-endurance science aircraft," Factsheet, February 28, 2014, <http://www.nasa.gov/centers/armstrong/news/FactSheets/FS-098-DFRC.html#VGUjWvnF9yx>; and NASA, "Small UAS (sUAS)," Factsheet, September 9, 2014. While these programs vary in size and scope, the use of UAS by federal entities for non-HSE missions is generally limited.
- 119 Office of the Inspector General Audit Division, *Interim Report on the Department of Justice's Use and Support of Unmanned Aircraft Systems*, Report 13-37 (Washington, DC: DOJ, 2013) <http://www.justice.gov/oig/reports/2013/a1337.pdf>.
- 120 Non-attribution interview with government official.
- 121 "Holder: ATF 'In Process' of Planning, Using Domestic Drones," CBS DC News, April 9, 2014, <http://washington.cbslocal.com/2014/04/09/holder-atf-in-process-of-planning-using-domestic-drones/>.
- 122 Office of the Inspector General, Audit Division, *Interim Report on the Department of Justice's Use and Support of Unmanned Aircraft Systems*, i. The report notes: "As of May 2013, four DOJ law enforcement components had either tested for evaluation or used UAS to support their operations. Although the Federal Bureau of Investigation (FBI) is the only DOJ component to have used UAS to support its mission, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) reported to us that it plans to deploy UAS to support future operations. The Drug Enforcement Administration (DEA) and the United States Marshals Service (USMS) have acquired UAS for testing, but told us that they have no plans to deploy them operationally. Specifically, the DEA stated that it plans to transfer its UAS to another federal agency, while the USMS stated that it plans to destroy its UAS because its UAS are obsolete and no longer operable. From 2004 to May 2013, DOJ law enforcement components reported spending in total approximately \$3.7 million on UAS, with the FBI accounting for over 80 percent of this amount."
- 123 Memorandum of Understanding between the FAA Unmanned Aircraft Systems Integration Office and the U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, Concerning Operation of Unmanned Aircraft Systems by Law Enforcement Agencies (no further document identifying information available.)
- 124 "Counter-IED Operations," FBI, <http://www.fbi.gov/about-us/cirg/hazardous-devices>.
- 125 Specific grant information is difficult to find and no comprehensive assessment is available. For examples, see: Barry, *Drones Over the Homeland*, 14-15.
- 126 The majority of insights regarding state and local use were captured during the Third Working Group – Emergency Response, Public Safety, and Infrastructure Protection, CSIS, Washington DC, September 10, 2014.

- ¹²⁷ Melissa Pamer and Mark Mester, "LAPD's 2 Drones Will Remain Grounded During Policy Review, Police Commission Says Amid Protest," KTLA5, September 15, 2014, <http://ktla.com/2014/09/15/anti-spying-group-drone-free-lapd-to-protest-state-bill-that-would-allow-police-drones/>.
- ¹²⁸ Steve Gorman, "Los Angeles Police Try to Reassure Public on Newly Acquired Drones," Reuters, September 16, 2014, <http://news.yahoo.com/los-angeles-police-try-reassure-public-newly-acquired-222310538.html>.
- ¹²⁹ The Mesa County Sheriff's Office in particular is identified as a leader in experimentation and integration of sUAS. The office has operated rotary sUAS since 2009 and in 2012 added fixed wing sUAS. From experimentation, the office observes, "It appears, at this time, that this new technology will work with law enforcement similar to a K-9 unit in that we are training current staff to operate these systems and allow them to carry the equipment in the back of their patrol car, not requiring the addition of new staff. Each pilot then shares the patrol car, UAV included." See "Mesa County Sheriff's Office Law Operations Division: Unmanned Aerial System Team," Mesa County Sheriff's Office, <http://sheriff.mesacounty.us/uav/>; "UAS Operations Most Frequently Asked Questions," Mesa County Sheriff's Office, <http://sheriff.mesacounty.us/WorkArea/DownloadAsset.aspx?id=11383>.
- ¹³⁰ Dan Gettinger, "How American Police Receive Robots from the U.S. Military" Center for the Study of the Drone at Bard College, August 25, 2014, <http://dronecenter.bard.edu/how-american-police-receive-robots-from-the-u-s-military/>; and Andrew Metcalf, "Threats Led to Bomb Squad Search in Bethesda," *Bethesda Magazine*, September 3, 2014, <http://www.bethesdamagazine.com/Bethesda-Beat/2014/Bomb-Squad-Robot-Searches-Vehicle-on-Woodmont-Avenue-Tuesday-Night/>. See also "FY 2014 Homeland Security Grant Program (HSGP)," FEMA, July 25, 2014, <http://www.fema.gov/fy-2014-homeland-security-grant-program-hsgp>. As an example of a smaller municipality purchasing such systems, see Carbondale, Illinois, which has a population of 26,000, and used funds from DHS to purchase an Andros-6 UGS in 2009 (Andrea Hahn, "Bomb-disposal robot, X-ray machine will aid police," Southern Illinois University, February 26, 2009, <http://news.siu.edu/2009/02/022609amh90035.html>).
- ¹³¹ San Diego Gas & Electric, "FAA Approves Experimental Airspace for SDG&E to Test Unmanned Aircraft System," news release, July 11, 2014, <http://www.sdge.com/newsroom/press-releases/2014-07-11/faa-approves-experimental-airspace-sdge-test-unmanned-aircraft>.
- ¹³² "Federal Aviation Administration, "Press release – FAA Approves First Commercial UAS Flights Over Land," news release, http://www.faa.gov/news/press_releases/news_story.cfm?newsId=16354.
- ¹³³ Patrick Tucker, "How the Fukushima Disaster Is Changing the Future of Robotics" *Defense One*, 2014, <http://www.defenseone.com/technology/2014/06/how-fukushima-disaster-changing-future-robotics/87454/>; Erico Guizzo, "Fukushima Robot Operator Writes Tell-All Blog," *IEEE Spectrum*, 2011, <http://spectrum.ieee.org/automaton/robotics/industrial-robots/fukushima-robot-operator-diaries>; Marina Koren, "3 Robots That Braved Fukushima," *Popular Mechanics*, <http://www.popularmechanics.com/technology/engineering/robots/3-robots-that-braved-fukushima-7223185#slide-1>.
- ¹³⁴ See, for example, "Robotic Tool Makes Direct Assessment A Reality," *Underground Construction*, 2013, <http://undergroundconstructionmagazine.com/robotic-tool-makes-direct-assessment-reality>; and Patrick Marshall, "Robots stand guard on bridges and ports," *Government Computer News*, 2014, <http://gcn.com/articles/2014/06/02/robotic-bridge-repair.aspx?m=1>.
- ¹³⁵ See, for example, the Mobile Detection Assessment and Response System from General Dynamics (General Dynamics, *Mobile Detection Assessment and Response System*, 2014, <http://www.gdrs.com/robotics/capabilities/sentry.asp>.)
- ¹³⁶ This section addresses requirements from a forward-looking, theoretical standpoint (a normative view). Of course, consideration of current and past use of unmanned systems in the HSE can illustrate current and past requirements (a positive view). This is especially true for documentation, such as MNS and ORDs, that may have been produced to drive past acquisition decisions. In the event, representatives from entities within the HSE noted that existing requirements-related documents were likely to be of little use in answering the team's research question, as they were some combination of: cursory, incomplete, or dated (and sometimes in the midst of significant revision).
- ¹³⁷ Defense Acquisition University, *Glossary: Defense Acquisition Acronyms and Terms*, 5th ed. (2012), B192 (requirement) and B156 (operational requirement), http://www.dau.mil/publications/publicationsDocs/Glossary_15th_ed.pdf.
- ¹³⁸ DHS, *Developing Operational Requirements: A Guide to the Cost-Effective and Efficient Communication of Needs*, version 2.0 (2008), 8, http://www.dhs.gov/xlibrary/assets/Developing_Operational_Requirements_Guides.pdf.
- ¹³⁹ This paper does not examine the requirements-setting (or larger acquisition) process in DHS or the HSE. In DHS, the requirements process—indeed, the acquisition process—is in a period of transition, driven by Secretary Johnson's "unity of effort" initiative and the reinvigoration of the Joint Requirements Council. For context, see Secretary Jeh Johnson, "Strengthening Departmental Unity of Effort," 22 April 2014, <http://www.hlswatch.com/wp-content/uploads/2014/04/DHSUnityOfEffort.pdf>; DHS, *Directive 102-01: Acquisition Management Directive* (Washington, DC: DHS, 20 January 2010), https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_102-01_acquisition_management_directive.pdf; DHS, *DHS Instruction Manual 102-01-001: Acquisition Management Instruction/Guidebook* (Washington, DC: DHS, 1 October 2011); and DHS, *Management Directive 1405: Charter of DHS Joint Requirements Council* (Washington, DC: DHS, 17 September 2003), https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_1405_charter_dhs_joint_requirements_council.pdf.

- ¹⁴⁰ HSE missions/sub-missions also include ensuring the efficient free flow of goods and people (i.e., facilitating “customs and exchange”), as part of managing U.S. borders; benefits administration; cybersecurity; and VIP protection. All are important, and have a connection to unmanned systems, but are largely outside the scope of the present paper. Note that critical infrastructure security could be more accurately categorized as a subset of emergency preparedness, and critical infrastructure resilience a subset of emergency response. Also, this list seeks to begin to isolate the kinds of operations employed to prosecute each mission. Of course, critical infrastructure security is thought to have a counter-threat element to it; this is clearly the case, but is captured under the “counter dangerous or illegal people and goods” bullets.
- ¹⁴¹ DHS, *2014 Quadrennial Homeland Security Review*, 32.
- ¹⁴² International Organization for Standardization (ISO), *ISO31000: Risk management* (2009), 3.
- ¹⁴³ Per DHS, *risk* is defined (in its extended definition) as “potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence”; *threat* is a “natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property”; *vulnerability* is a “physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard”; and *consequence* refers to “effect[s] of an event, incident, or occurrence” (DHS, *DHS Risk Lexicon*, 2010 ed., [Washington, DC: DHS, 2010], 27, 36, 38, 10, <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>).
- ¹⁴⁴ The phases presented in boxes 1-3 represent a more granular version of “identify, assess, and treat.” A reasonable question might be: Why does this paper not consider requirements by examining the missions, goals, objectives, and priority areas specified in the 2014 QHSR? Unfortunately, these missions, goals, objectives, and priority areas provide useful context, but they are not sufficiently granular—sufficiently operational—to allow for an understanding of mission needs (and the ability of unmanned systems to fill those needs). For example, per the 2014 QHSR, the “secure and manage our [U.S.] borders” mission includes the following goal and objectives (though not formally called objectives): “Goal 2.1: Secure U.S. air, land, and sea borders and approaches: prevent illegal import and entry [objective]; prevent illegal export and exit [objective].” As written, even the objectives say little about the operational phases required to secure borders. A variety of sources exist that present, in some way, phases of threat, vulnerability, and consequence management. The sources used here were assessed by the research team to provide clear and concise articulation of operational phases. See also DHS, *Functional Capabilities and Activities Catalog, Version 1.0* (Washington, DC: DHS, 2013).
- ¹⁴⁵ Interdiction is commonly focused on people or goods. But phases for managing natural threats, like wildfires, are not drastically different, in that natural threat management requires cueing, detection/monitoring, etc.
- ¹⁴⁶ The training course from which this information is adapted is clearly tailored for the use of individual infrastructure facilities. However, the process that it advocates for (considering options to address vulnerabilities) may be generalizable and, therefore, can likely be applied at other levels.
- ¹⁴⁷ This phase was not included in the source material and was added by the research team.
- ¹⁴⁸ The entire course can be found at <https://www.fema.gov/media-library/assets/documents/4655>.
- ¹⁴⁹ Additional detail on the activities involved in executing each of the capabilities listed here can be found in the *National Response Framework*, the *National Disaster Recovery Framework*, and their associated annexes (see <https://www.fema.gov/national-preparedness-resource-library>).
- ¹⁵⁰ Across the HSE, unmanned systems are owned and operated by the user (referred to as “government owned, government operated” or GOGO). In addition to GOGO, DHS and others could also pursue services contracts with private companies that would allow for government-owned unmanned systems operated by a private contractor (“GOCO”), or company-owned and company-operated (“COCO”) unmanned systems. COCO offers the potential advantage that government can simply set requirements for the sensor data desired without having to acquire, maintain, or operate systems. This is a relevant consideration for a technology as fast-evolving as unmanned systems, and also could allow broader experimentation and demonstration in the integration of unmanned systems into various missions without major upfront capital investment. Of course, COCO can sometimes be more expensive when requirements are enduring.
- ¹⁵¹ The answer to this is “yes, in certain missions.” The apprehension phase of interdiction, for example, requires specific personnel; disruption may also require the use of lethal force, which is a manned activity. Interviews conducted during the course of this research suggest that the need for and availability of personnel for disruption/endgame/apprehension phases might be a limiting factor in the need for unmanned systems (in that more unmanned systems may not lead to more successful interdictions, given limits on personnel).
- ¹⁵² A requirement might exist—but the desire to fill it might be hindered by constraints including legal authorities (and uncertainty in the legal environment), public perceptions, social mores, and so on. In certain cases, constraints may be temporary (e.g., interviewees from certain DHS operational components suggested that they’re interested in sUAS, but not until the FAA has provided clear guidance on their use in the NAS). The existence of such constraints might also affect technical specifications, as technical workarounds may be employed to compensate for constraints. Note that constraints are discussed in a subsequent section of the present paper.

- ¹⁵³ This idea is captured in a 2006 memorandum on the use of UAS in HD and DSCA missions from Deputy Secretary of Defense Gordon England, in which he noted “under certain circumstances, use of UAS in lieu of manned aircraft may be appropriate. Such circumstances may be when: manned aircraft would be at risk; long, sustained endurance efforts are required; unmanned aircraft provide superior capability; or physical infrastructure limitations do not allow use of rotary or fixed-wing manned aircraft.” Deputy Secretary of Defense, “Memorandum: Interim Guidance for the Domestic Use of Unmanned Aircraft Systems,” 28 September 2006.
- ¹⁵⁴ There does not yet appear to be an accepted, apples-to-apples, full-life-cycle-cost approach to estimating unit costs for manned and unmanned systems, one that facilitates comparison between them. This is discussed further in “Constraints,” below. Note that a “Life-Cycle Cost Estimate (LCCE) provides an exhaustive and structured accounting of all past (or sunk), present, and future resources and associated cost elements required to develop, produce, deploy, sustain and dispose of a particular system (program) regardless of funding sources” (DHS, *DHS Instruction Manual 102-01-001*, 35).
- ¹⁵⁵ This appears to have been the approach taken with the existing CBP/USCG Predator/Guardian UAS fleet.
- ¹⁵⁶ Several reports by research groups and articles in legal journals discuss the issue from a wide variety of viewpoints. See, for example, Wells C. Bennett, *Civilian Drones, Privacy, and the Federal-State Balance* (Washington, DC: Brookings Institution, 2014); Alissa M. Dolan and Richard M. Thompson II, *Integration of Drones into Domestic Airspace: Selected Legal Issues* (Washington, DC: Congressional Research Service, January 30, 2013); Hillary B. Farber, “Eyes in the Sky: Constitutional and Regulatory Approaches to Domestic Drone Deployment,” *Syracuse Law Review* 64 (2014); Margot E. Kaminski, “Drone Federalism: Civilian Drones and the Things They Carry,” *California Law Review Circuit* 4 (2013); Orin S. Kerr, “The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution,” *Michigan Law Review* 102 (2004); Jay Stanley and Catherine Crump, *Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft* (New York: American Civil Liberties Union, 2011); Richard M. Thompson II, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses* (Washington, DC: CRS, April 3, 2013); John Villasenor, “Observations from Above: Unmanned Aircraft Systems and Privacy,” *Harvard Journal of Law and Public Policy* 36 (2013).
- ¹⁵⁷ Discussion in Working Group 1, 16 June 2014; Working Group 2, 17 July 2014; Working Group 3, 10 September 2014; and Working Group 4, 17 September 2014 (see appendix II for a list of attendees). The vast majority of scholarship and opinion about privacy on unmanned systems focuses on UAS; very little has been written about privacy and UGS or UMS.
- ¹⁵⁸ *The Future of Drones in America, Testimony before the U.S. Senate Judiciary Committee* (2013) (statement of Amie Stepanovich, Director, Domestic Surveillance Project, Electronic Privacy Information Center).
- ¹⁵⁹ Jennifer Lynch, “Are Drones Watching You?” Electronic Frontier Foundation, *Deeplinks* (blog), January 10, 2012, <https://www.eff.org/deeplinks/2012/01/drones-are-watching-you>.
- ¹⁶⁰ Memorandum from Tamara J. Kessler, Acting Officer, Office of Civil Rights and Civil Liberties, Department of Homeland Security, and Jonathan R. Cantor, Acting Chief Privacy Officer, Department of Homeland Security, “Working Group to Safeguard Privacy, Civil Rights, and Civil Liberties in the Department’s Use and Support of Unmanned Aerial Systems (UAS)” (September 14, 2012).
- ¹⁶¹ CBP has also allowed its UAS to be used by other HSE agencies more than 700 times, for a variety of tasks. See “Customs & Border Protection Drone Flight List,” Electronic Frontier Foundation, <https://www.eff.org/document/customs-border-protection-drone-flight-list>. The CBP Office of Air and Marine “has authority under its fiscal year 2014 appropriation to support federal, state, and local agencies in enforcing homeland security laws, and the Secretary of Homeland Security has the discretion to authorize OAM to assist law enforcement and emergency humanitarian efforts.” GAO, *Unmanned Aerial Systems: DHS’s Review of U.S. Customs and Border Protection’s Use and Compliance with Privacy and Civil Liberty Laws and Standards*, 28.
- ¹⁶² Discussion in Working Group 3, September 10, 2014; HSSAI-CSIS interview with local law enforcement official, September 16, 2014.
- ¹⁶³ HSSAI-CSIS interview with local law enforcement official, September 16, 2014.
- ¹⁶⁴ OAM, CBP, *Privacy Impact Assessment for the Aircraft Systems*.
- ¹⁶⁵ HSSAI-CSIS interview with federal law enforcement official, September 26, 2014.
- ¹⁶⁶ GAO, *Unmanned Aerial Systems: DHS’s Review of U.S. Customs and Border Protection’s Use and Compliance with Privacy and Civil Liberty Laws and Standards*, 13.
- ¹⁶⁷ Discussion in Working Group 3, September 10, 2014.
- ¹⁶⁸ See, for example, *The Future of Drones in America* (Stepanovich statement), 8; Stanley and Crump, *Protecting Privacy from Aerial Surveillance*, 16; Discussion in Working Group 4, September 25, 2014.
- ¹⁶⁹ *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965).
- ¹⁷⁰ U.S. Const. amend. IV.
- ¹⁷¹ Dolan and Thompson II, *Integration of Drones into Domestic Airspace*, 11. See also *Entick v. Carrington*, 95 Eng. Rep. 807 (K.B. 1765); *Boyd v. United States*, 116 U.S. 616 (1886).

- ¹⁷² *Olmstead v. United States*, 277 U.S. 438, 466 (1928). In a dissenting opinion, Justice Louis D. Brandeis warned: “Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.” *Ibid.* at 473.
- ¹⁷³ See, for example, *Goldman v. United States*, 316 U.S. 129 (1942); *Silverman v. United States*, 365 U.S. 505 (1961).
- ¹⁷⁴ *Katz v. United States*, 389 U.S. 347, 351 (1967). The Court made clear “that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.” 389 U.S. at 353. Any place in which a person had a reasonable expectation of privacy was as protected as the “persons, houses, papers, and effects” specified in the amendment. Over the next 40-plus years, however, the Supreme Court would apply *Katz* fairly narrowly. Some legal scholars suggest that the reasonable-expectation test had not supplanted the traditional reliance on property law principles, but had only augmented it. This ambiguity lies at the heart of debate over how the Supreme Court might rule on privacy cases involving unmanned systems.
- ¹⁷⁵ *Ibid.* at 361 (Harlan, J, concurring).
- ¹⁷⁶ 476 U.S. 207 (1986).
- ¹⁷⁷ 476 U.S. 227 (1986).
- ¹⁷⁸ *Ibid.* at 238.
- ¹⁷⁹ *Ibid.*
- ¹⁸⁰ 488 U.S. 445 (1989).
- ¹⁸¹ *Ibid.* at 451.
- ¹⁸² *Ibid.* at 452. Justice O’Connor added: “[P]ublic use of altitudes lower than [400 feet]—particularly public observations from helicopters circling over the curtilage of a home—may be sufficiently rare that police surveillance from such altitudes would violate reasonable expectations of privacy, despite compliance with FAA air safety regulations.” *Ibid.* at 455. *Curtilage* is “the land or yard adjoining a house, usu. within an enclosure.” *Black’s Law Dictionary*, 3rd pocket edition, Bryan A. Garner, ed. (St. Paul, MN: Thomson/West, 2006), 171.
- ¹⁸³ 533 U.S. 27 (2001).
- ¹⁸⁴ *Ibid.* at 34.
- ¹⁸⁵ *Ibid.* at 47 (Stevens, J, dissenting). “The record describes a device ... that is ‘readily available to the public’ for commercial, personal, or law enforcement purposes, and is just an 800–number away from being rented from ‘half a dozen national companies’ by anyone who wants one.” *Ibid.*, fn. 5.
- ¹⁸⁶ 132 S.Ct. 945 (2012).
- ¹⁸⁷ See Sean M. Kilbane, “Note: Drones and *Jones*: Rethinking Curtilage Flyover in Light of the Revived Fourth Amendment Trespass Doctrine,” *Capital University Law Review* 42 (2014).
- ¹⁸⁸ “Awareness that the Government may be watching chills associational and expressive freedoms. And the Government’s unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. ... I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.” 132 S.Ct. at 956 (Sotomayor, J, concurring).
- ¹⁸⁹ “In circumstances involving dramatic technological change, the best solution to privacy concerns may legislative. ... A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.” *Ibid.* at 964 (Alito, J, concurring).
- ¹⁹⁰ Kaminski, “Drone Federalism,” 65.
- ¹⁹¹ H.R. 972, Preserving Freedom from Unwanted Surveillance Act of 2013, would require any federal entity to obtain a warrant before conducting UAS surveillance in a criminal investigation. Exceptions to the warrant requirement would be granted to prevent or deter illegal persons or illegal drugs from entering the United States, when “swift action” is required “to prevent imminent danger to life or serious damage to property” or to keep suspects from fleeing or destroying evidence, or when the DHS Secretary “determines credible intelligence indicates a high risk of a terrorist attack by a specific individual or organization.” H.R. 637, Preserving American Privacy Act of 2013, would prohibit the use of UAS to collect “information that is reasonably likely to enable identification of an individual” or “information about an individual’s property that is not in plain view.” It would also prohibit disclosure of such information. Exceptions would be granted when there was a warrant, court order, a border search, or an emergency, or if the targeted individual granted consent. H.R. 1262, Drone Aircraft Privacy and Transparency Act of 2013, would require the Secretary of Transportation to study potential threats to privacy posed by the introduction of UAS in the national airspace. The FAA would be prohibited from issuing a UAS license to a government entity unless it filed a data collection statement. Any law enforcement agency that operated UAS would have

- to file a data minimization statement with the FAA. See Thompson, *Drones in Domestic Surveillance Operations*, 18.
- ¹⁹² Title 5 U.S.C. § 552a.
- ¹⁹³ *Privacy: Federal Law Should Be Updated to Address Changing Technology Landscape, Testimony Before the Senate Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs* (2012) (statement of Gregory C. Wilshusen, director, Information Security Issues, Government Accountability Office), 2.
- ¹⁹⁴ *Ibid.*
- ¹⁹⁵ GAO, *Unmanned Aerial Systems: DHS's Review of U.S. Customs and Border Protection's Use and Compliance with Privacy and Civil Liberty Laws and Standards*, 14.
- ¹⁹⁶ OAM, CBP, *Privacy Impact Assessment for the Aircraft Systems*, 12.
- ¹⁹⁷ *Ibid.*
- ¹⁹⁸ *Ibid.*, 19; GAO, *Unmanned Aerial Systems: DHS's Review of U.S. Customs and Border Protection's Use and Compliance with Privacy and Civil Liberty Laws and Standards*, 16.
- ¹⁹⁹ *The Future of Unmanned Aviation in the U.S. Economy: Safety and Privacy Considerations: Hearing before the U.S. Senate Committee on Commerce, Science, and Transportation* (2014) (statement of Christopher R. Calabrese, Legislative Counsel, American Civil Liberties Union), 14-15.
- ²⁰⁰ *The Future of Drones in America* (Stepanovich statement), 7. Some existing federal privacy laws could be relevant to the issue, particularly so-called peeping tom laws. Federal law provides a one-year criminal penalty for capturing an image of a "private area of an individual" without the individual's consent in a circumstance where the individual has a reasonable expectation of privacy. This law only applies on federal property. *The Future of Unmanned Aviation in the U.S. Economy* (Calabrese statement), 13.
- ²⁰¹ Unmanned Aircraft System Test Site Program, 78 Fed. Reg. 68,360, 68,384 (November 14, 2013) (to be codified at 14 C.F.R. Part 91).
- ²⁰² "The Site Operator must: (i) Have privacy policies governing all activities conducted under the OTA, including the operation and relevant activities of the UAS authorized by the Site Operator; (ii) Make its privacy policies publicly available; (iii) Have a mechanism to receive and consider comments from the public on its privacy policies; (iv) Conduct an annual review of test site operations to verify compliance with stated privacy policy and practices and share those outcomes annually in a public forum with an opportunity for public feedback; (v) Update its privacy policies as necessary to remain operationally current and effective; and (vi) Ensure the requirements of its privacy policies are applied to all operations conducted under the OTA." *Ibid.* at 68,364.
- ²⁰³ Bennett, *Civilian Drones, Privacy, and the Federal-State Balance*, 2.
- ²⁰⁴ *Ibid.*, 11.
- ²⁰⁵ Explanatory Statement, Consolidated Appropriations Act of 2014, H.R. 3547, 113th Cong., Division L at 6 (Jan. 14, 2014).
- ²⁰⁶ Also, "DHS has established a UAS Working Group that is charged with establishing a forum to discuss privacy, civil rights, and civil liberties issues; ensuring Privacy Office and CRCL guidance and policies are reflected in the concept of operations for UAS uses; identifying potential privacy, civil rights, and civil liberties concerns with current or planned UAS uses; and promoting best practices for safeguarding privacy, civil rights, and civil liberties by DHS partners and grant recipients." GAO, *Unmanned Aerial Systems: DHS's Review of U.S. Customs and Border Protection's Use and Compliance with Privacy and Civil Liberty Laws and Standards*, 17.
- ²⁰⁷ In July 2014, *Politico* reported that President Obama planned "to issue an executive order to develop privacy guidelines for commercial drones operating in U.S. airspace. ... The order would put the National Telecommunications and Information Administration, an arm of the Commerce Department, in charge of developing the guidelines." Erin Mershon and Kevin Robillard, "President Barack Obama to issue executive order on drone privacy," *Politico*, July 23, 2014, <http://www.politico.com/story/2014/07/executive-order-drone-privacy-barack-obama-109303.html#ixzz3J4s5mZul>.
- ²⁰⁸ U.S. Const. art. VI., cl. 2.
- ²⁰⁹ Erwin Chemerinsky, *Constitutional Law: Principles and Policies*, 3rd edition (New York: Aspen Publishers, 2006), 392.
- ²¹⁰ "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people." U.S. Const. amend. X.
- ²¹¹ Those states are Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington. McAdam and Webb, "Privacy," 56.
- ²¹² Delaware and South Dakota appear to be the only two states that have not officially debated some form of UAS legislation. Officials in both states are expected to do so in the coming months.

- 213 The four states with laws on driverless cars are California, Florida, Michigan, and Nevada. Riya Bhattacharjee, "Audi Gets First Permit to Test Driverless Cars in California," NBC Bay Area, September 17, 2014, <http://www.nbcbayarea.com/news/local/Audi-Gets-First-Permit-to-Test-Driverless-Cars-in-California-275534551.html>. For an analysis of the privacy issues raised by UGS, see Dorothy J. Glancy, "Privacy in Autonomous Vehicles," *Santa Clara Law Review* 52 (2012): 1171.
- 214 Allie Bohm, "Status of 2014 Domestic Drone Legislation in the States," American Civil Liberties Union, June 30, 2014, <https://www.aclu.org/blog/technology-and-liberty/status-2014-domestic-drone-legislation-states>.
- 215 Dawn M.K. Zoldi, "Drones at Home: Domestic Drone Legislation – A Survey, Analysis, and Framework," *University of Miami National Security and Armed Conflict Law Review* 4 (2013), 3.
- 216 Those states are Alabama, Arizona, California, Connecticut, Georgia, Hawaii, Kansas, Kentucky, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Nebraska, New Hampshire, New Jersey, New York, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, Vermont, Virginia, Washington, West Virginia, and Wyoming.
- 217 Allie Bohm, "The First State Laws on Drones," American Civil Liberties Union, April 15, 2013, <https://www.aclu.org/blog/technology-and-liberty-national-security/first-state-laws-drones>. The measure says that "[n]o state or local government department, agency, or instrumentality having jurisdiction over criminal law enforcement and regulatory violations ... and no department of law enforcement ... of any county, city, or town shall utilize an unmanned aircraft system before July 1, 2015."
- 218 Use of UAS for "specified humanitarian purposes" is exempted from the moratorium. 2013 Va. Acts ch. 755.
- 219 Florida, Idaho, Illinois, Indiana, Montana, Tennessee, Texas, Utah, and Wisconsin.
- 220 Florida, Illinois, Montana, Tennessee, Texas, Utah, and Wisconsin.
- 221 Alabama, Hawaii, Illinois, Tennessee, and Utah.
- 222 See, for example, Kaminski, "Drone Federalism"; Paul Rosenzweig, Steven P. Bucci, Charles D. Stimson, and James Jay Carafano, *Drones in U.S. Airspace: Principles for Governance*, Backgrounder No. 2732 (Washington, DC: Heritage Foundation, 2012); Stanley and Crump, *Protecting Privacy from Aerial Surveillance; Using Unmanned Aerial Systems within the Homeland: Security Game Changer? Hearing before the Testimony before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, U.S. House of Representatives* (July 19, 2012) (Statement of Amie Stepanovich, Associate Litigation Counsel, Electronic Privacy Information Center).
- 223 Kaminski, "Drone Federalism," 65.
- 224 Although local measures governing UAS generally tend to be aimed at addressing privacy issues, some also contain provisions addressing public safety.
- 225 American Civil Liberties Union, "Governor Proposes Limited Amendments to Two-Year Moratorium on Drones," news release, March 26, 2013, <https://www.aclu.org/technology-and-liberty/virginia-set-become-first-state-pass-statewide-limitation-drone-use>.
- 226 "City passes sweeping anti-surveillance law," KCCI News 8, June 19, 2013, <http://www.kcci.com/news/central-iowa/city-passes-sweeping-antisurveillance-law/20628142#19pUqt>.
- 227 Bob Roberts, "Evanston Approves 2-Year Ban on Drones," CBS Chicago, May 30, 2013, <http://chicago.cbslocal.com/2013/05/30/evanston-approves-2-year-ban-on-drones/>.
- 228 Tom Meersman, "St. Bonifacius says no to drones," *Minneapolis Star Tribune*, April 6, 2013, <http://www.startribune.com/local/west/201723501.html>.
- 229 Nicholas Bergin, "Mayor to police: No drones," *Lincoln Journal Star*, January 8, 2014, http://journalstar.com/news/local/mayor-to-police-no-drones/article_99f3a916-d92a-5df8-9816-d417442bd80d.html.
- 230 Tim Knauss, "Syracuse bans police drones until privacy regulations in place," *Syracuse.com*, December 16, 2013, http://www.syracuse.com/news/index.ssf/2013/12/syracuse_bans_police_drones_until_privacy_regulations_in_place.html.
- 231 Aviation Committee, International Association of Chiefs of Police, "Recommended Guidelines for the Use of Unmanned Aircraft" (2012), http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf.
- 232 Discussion in Working Group 3, September 10, 2014.
- 233 Aerospace States Association, *UAS Privacy Considerations* (2013), <http://aerostates.org/events/uas-state-privacy-considerations>.
- 234 AUVSI, *Unmanned Aircraft System Operations Industry "Code of Conduct"* (2012), reprinted in Bart Elias, *Pilotless Drones: Background and Considerations for Congress Regarding Unmanned Aircraft Operations in the National Airspace System* (Washington, DC: CRS, September 10, 2012), 16.
- 235 George Orwell, *Nineteen Eighty-Four* (London: Secker and Warburg, 1949), 2.

- 236 Farber, "Eyes in the Sky," 34, 38.
- 237 Kaminski, "Drone Federalism," 60.
- 238 Dolan and Thompson, *Integration of Drones into Domestic Airspace*, 15.
- 239 See *Branzburg v. Hayes*, 408 U.S. 665 (1972).
- 240 *Kleindienst v. Mandel*, 408 U.S. 753, 762-63 (1972).
- 241 Brief of News Media *Amici* in Support of Respondent Raphael Pirker at 6, *Huerta v. Pirker*, Docket CP-217 (National Transportation Safety Board, May 6, 2014).
- 242 408 U.S. 665 (1972).
- 243 *Ibid.* at 707.
- 244 *Ibid.* at 681.
- 245 *Ibid.* at 684. However, a concurring opinion by Justice Lewis Powell, the deciding vote in the 5-4 decision, recognized a qualified privilege for reporters. "The Reporter's Privilege Compendium: An Introduction," Reporters Committee for Freedom of the Press, accessed November 14, 2014, <http://www.rcfp.org/browse-media-law-resources/guides/reporters-privilege/introduction>.
- 246 *Cohen v. Cowles Media Co.*, 501 US 663, 669 (1991).
- 247 Jack Gillum and Joan Lowy, "AP Exclusive: Ferguson no-fly zone aimed at media," Associated Press, November 2, 2014, <http://bigstory.ap.org/article/674886091e344ffa95e92eb482e02be1/ap-exclusive-ferguson-no-fly-zone-aimed-media>.
- 248 No agencies have been granted specific responsibility for governing unmanned ground or maritime systems.
- 249 Dolan and Thompson, *Integration of Drones into Domestic Airspace*, 6.
- 250 FAA Modernization and Reform Act §333 (a), Pub. L. 112-95 (2012).
- 251 *Ibid.*, § 333 (b) (1). Significantly, the FAA has ruled that Section 333 allows the Secretary to waive existing statutory restrictions imposed on aircraft under 49 U.S.C. § 44704 but not from those under 49 U.S.C. § 44711. This means that the need for an SEC or a COA can be waived, but not the requirement that the aircraft be operated by a licensed pilot. See Exemption No. 11138: In the Matter of the Petition of Douglas Trudeau, Docket No. FAA-2014-0481, Department of Transportation (2014).
- 252 FAA, "FAA Approves First Commercial UAS Flights over Land," press release, June 10, 2014, http://www.faa.gov/news/press_releases/news_story.cfm?newsid=16354.
- 253 FAA, "U.S. Transportation Secretary Foxx Announces FAA Exemptions for Commercial UAS Movie and TV Production," press release, September 25, 2014, http://www.faa.gov/news/press_releases/news_story.cfm?newsid=17194.
- 254 FAA, "FAA Grants Five More Commercial UAS Exemptions," press release, December 10, 2014, http://www.faa.gov/news/press_releases/news_story.cfm?newsid=17934.
- 255 Hilda Munoz, "Drone Use by WFSB Employee at Fatal Crash under Investigation," *Hartford Courant*, February 7, 2014, http://articles.courant.com/2014-02-07/community/hc-hartford-wfsb-drone-0208-20140207_1_drone-use-drone-video-drone-incident.
- 256 "The Reporter's Privilege Compendium: An Introduction," Reporters Committee for Freedom of the Press, accessed November 14, 2014, <http://www.rcfp.org/browse-media-law-resources/guides/reporters-privilege/introduction>.
- 257 Preserving Freedom from Unwarranted Surveillance Act, Missouri House of Representatives, HB 46 (2013). The bill passed the House but died in the state Senate.
- 258 A number of programs, both military and civilian, have sought to advance use of UGS; see, for example, National Robotics Engineering Center, "Crusher," <http://www.nrec.ri.cmu.edu/projects/crusher/>; and Google's driverless car.
- 259 On the other hand, the land domain may be the most complex of all for safe operation, given its varied terrain, fixed and mobile obstacles, and the fact that the potential for system-to-human contact is perhaps greatest (especially in congested urban areas). In the maritime domain, especially subsurface, communications are difficult, so systems depend on autonomy.
- 260 "About FAA," FAA, accessed November 17, 2014, <http://www.faa.gov/about/>.
- 261 GAO, *Unmanned Aircraft Systems: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System*, GAO-12-981 (Washington, DC: GAO, September 2012). <http://www.gao.gov/products/GAO-12-981>.
- 262 "There are currently about 300 active public-use authorizations, 18 experimental special airworthiness certificates, and 2 restricted category airworthiness certificates for over 100 aircraft types." Office of Inspector General, *Audit Report: FAA Faces Significant Barriers to Safely Integrate Unmanned Aircraft Systems into the National Airspace System*.

- ²⁶³ Discussion in Working Group 3, September 10, 2014. Spectrum-related issues have been raised in numerous documents on the subject of UAS NAS integration, including FAA, *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap*, 1st edition (Washington: DOT, 2013), 56-64.
- ²⁶⁴ Goal 5 of the 2013 FAA integration road map is to develop a common strategy for DOJ and other stakeholders (including DHS) in the law enforcement, fire, and first responder communities. As of November 2014, this work remains ongoing. See *ibid.*, 63-64.
- ²⁶⁵ 49 830.2 CFR Revised as of October 1, 2013, <http://www.gpo.gov/fdsys/pkg/CFR-2013-title49-vol7/pdf/CFR-2013-title49-vol7-sec830-2.pdf>.
- ²⁶⁶ There are insufficient data to make comparable determinations in the ground and maritime domains. The most comprehensive large UAS data set is available through the U.S. Air Force Safety Center. See "Aircraft Statistics," <http://www.afsec.afmil/organizations/aviation/aircraftstatistics/index.asp>.
- ²⁶⁷ Craig Whitlock, "When Drones Fall from the Sky," *Washington Post*, June 20, 2014, <http://www.washingtonpost.com/sf/investigative/2014/06/20/when-drones-fall-from-the-sky/>.
- ²⁶⁸ One was replaced; there are nine UAS in the fleet at present.
- ²⁶⁹ FAA, "Press Release – FAA Selects Unmanned Aircraft Systems Research and Test Sites," news release, December 30, 2013, https://www.faa.gov/news/press_releases/news_story.cfm?newsid=15576.
- ²⁷⁰ Committee on Appropriations, Department of Homeland Security Appropriations Bill 2015, S. Report, No. 113-198, pt. 4 (2014).
- ²⁷¹ A.J. Kerns, D.P. Shepard, J.A. Bhatti, and T.E. Humphreys, "Unmanned Aircraft Capture and Control via GPS Spoofing," *Journal of Field Robotics*, 31:4, (2014), 633, <http://radionavlab.ae.utexas.edu/images/stories/files/papers/unmannedCapture.pdf>.
- ²⁷² See, for example, Samy Kamkar, "SkyJack," December 2, 2013, <http://samy.pl/skyjack/>.
- ²⁷³ Office of Inspector General, *FAA Faces Significant Barriers*, 5.
- ²⁷⁴ Airspace classes are extremely important for civil aviation operations because they govern the complex airspaces surrounding high-volume airports. Class A airspace is airspace from 18,000 feet above mean sea level (MSL) up to 60,000 feet MSL. All flights in Class A airspace must fly under instrument flight rules unless otherwise authorized. Class B, C, and D airspaces are all related to airport operations; the differences depend on the capabilities and business of the airport in question. These airspaces range from ground level to either 10,000 feet MSL, 4,000 feet MSL, or 2,500 feet MSL, respectively. Class E airspace is a catchall category for controlled airspace not included in classes A through D. Class E extends upward from either 700 feet MSL, 1,200 feet MSL, or 14,500 feet MSL to the beginning of Class A airspace. These lower altitudes are used to transition flights from/to takeoff and landing procedures to/from cruising altitudes. Any airspace not meeting these requirements is Class G uncontrolled airspace, which extends upward to either 700 feet MSL, 1,200 feet MSL, or 14,500 feet MSL, depending on the location. Class G uncontrolled airspace may be most permissive for UAS operations, as pilots do not have to establish contact with air traffic control and are permitted to follow visual flight rules. In a national emergency, airspace may be closed, which may allow for greater use of UAS by HSE actors. However, such a use case is not relevant for the vast majority of day-to-day use cases. For more information, see FAA, *Pilot's Handbook of Aeronautical Knowledge*, FAA-H-8083-25A (FAA, 2008), http://www.faa.gov/regulations_policies/handbooks_manuals/aviation/pilot_handbook/media/FAA-H-8083-25A.pdf, 14-1 – 14-3.
- ²⁷⁵ In the context of manned operations in Class G airspace, the pilot-in-command must maintain vigilance to "see and avoid" other aircraft. While operating under instrument flight rules in controlled airspace, air traffic control will maintain separation. However, it is ultimately the responsibility of the pilot-in-command to avoid collision. See 14 C.F.R. 91.113 and Lacher, et al., *Analysis of Key Airspace Integration Challenges and Alternatives for Unmanned Aircraft Systems*, 4.
- ²⁷⁶ Federal Aviation Act of 1958, Pub. L. No. 85-726, 72 Stat. 731 (1958).
- ²⁷⁷ Regulations are formulated through a rulemaking process that includes internal drafting and review, publication of a draft rule in the *Federal Register*, a period of public comment, revisions based on the comments, and publication of a final rule. Villasenor, "Observations from Above," 469.
- ²⁷⁸ 49 U.S.C. § 40103(b)(2). Among the most fundamental and far-reaching of the FAA's regulations is Sec. 91.13(a) of the Federal Aviation Regulations, which states that "(n)o person may operate an aircraft in a careless or reckless manner so as to endanger the life or property of another."
- ²⁷⁹ Federal Aviation Act § 101(5).
- ²⁸⁰ Opinion and Order, *Huerta v. Pirker*, Docket CP-217 (National Transportation Safety Board, November 17, 2014), 6.
- ²⁸¹ FAA, "Unmanned Aircraft Operations in the National Airspace System," 72 Fed. Reg. 6,689. In interviews, officials pointed out that the FAA's jurisdiction over public entities' aviation operations—manned or unmanned—is limited to matters of safety. The FAA's basic legal mandate extends over civil aircraft, not public aircraft, which federal law defines as aircraft that are only used for government purposes,

are leased or owned by the government, and are limited to operations that do not include commercial activity or transportation of individuals who are not crew members.

282 Nevertheless, the FAA's mandate to ensure air safety can only be effective if it applies to all aircraft, private and public. As such, public users are responsible for certifying the airworthiness of any UAS they operate. In addition, public users who acquire consumer-grade platforms are accepting risk and may endanger the general public. See FAA, *Public Aircraft Operations*, Advisory Circular 00-1.1A (Washington, DC: DOT, 2014), http://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_00-1.1A.pdf; Tim Adelman and Leonard Ligon, *The Law and Operating Unmanned Aircraft in the U.S. National Airspace System*, white paper (n.d.), available at <http://www.suasnews.com/2012/03/13397/the-law-and-operating-unmanned-aircraft-in-the-u-s-national-airspace-system/>.

283 Interviews and written materials make clear that many private UAS owners do not consider the FAA's regulation of UAS to have the force of law. They point out that FAA dictates have been issued in the form of policy statements, advisories, and interpretations, but not as formal rules. The FAA maintains that its dictates are binding.

284 The COA process was actually instituted two years before the FAA's 2007 Notice of Policy. See FAA, "Unmanned Aircraft Systems Operation in the U.S. National Airspace System," UAS Policy 05-01 (2005).

285 "Public Operations (Governmental)," FAA, accessed November 17, 2014, http://www.faa.gov/uas/public_operations/.

286 FAA, "Unmanned Aircraft Operations in the National Airspace System," 6,689.

287 "Public Operations (Governmental)," FAA.

288 Interviews with government officials; USCG Office of Aviation Forces, "Coast Guard UAS Program: UAS Program Overview," PowerPoint presentation (August 7, 2014).

289 During several interviews with government officials familiar with the COA process, it was learned that there is a good relationship between various HSE-related organizations and the FAA. It is understood that these relations were the product of continued and sustained interactions. Relations between the FAA and public UAS operators were developed over many years, and the user community is very small.

290 In November 2014, the NTSB ruled that the model aircraft carve-out does not exempt unmanned or model aircraft from the Federal Aviation Regulation banning reckless operation of an aircraft. Opinion and Order, *Huerta v. Pirker*, Docket CP-217 (NTSB, November 17, 2014), 7. However, the FMRA's Section 336 lays out rules for model aircraft, raising the carve-out to federal statutory level. The FMRA provision has not been tested.

291 FAA, *Model Aircraft Operating Standards*.

292 Discussion in Working Group 3, 10 September 2014.

293 Elias, *Pilotless Drones*, 5.

294 FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, Sec. 332(a)(1) (2012).

295 *Ibid.*, Sec. 332 (a)(3). The FMRA set several deadlines for tasks that the FAA was instructed to meet before full UAS integration, including creation of an integration road map and designation of six UAS test sites. Of 17 interim deadlines, the FAA met one and missed 11; five deadlines have yet to pass. Office of Inspector General, *FAA Faces Significant Barriers*, 23-24.

296 Office of Inspector General, *FAA Faces Significant Barriers*, 23-24.

297 *Ibid.*, 15. But see Yasmin Tadjdeh, "FAA Official: Small Drone Rule To Be Released by End of Year," *National Defense*, November 7, 2014, <http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=1663>.

298 Office of Inspector General, *FAA Faces Significant Barriers*, 15.

299 FAA, *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap*, 56-64.

300 *Separation minima* refer to the safe distances pilots should maintain between aircraft. These distances can vary based on flight rules. Generally speaking, horizontal separation ranges between three and five miles with vertical separation ranging between 500 and 2,000 feet.

301 Lacher, et al., *Analysis of Key Airspace Integration Challenges and Alternatives for Unmanned Aircraft Systems*, 5-6.

302 ADS-B is a major component of the Next Generation Air Transportation System (NextGen). This is a multi-year program begun in 2003 that aims to radically overhaul and improve the NAS. The end goals are to improve fuel efficiency, reduce delays, decrease noise, and increase throughput. See *Next Generation Air Transportation System: FAA Has Made Some Progress in Implementation, but Delays Threaten to Impact Costs and Benefits*, Before the House Committee on Transportation and Infrastructure, Subcommittee on Aviation, 112th Cong. (2011) (statement of Gerald L. Dillingham, Director, Physical Infrastructure Issues, Government Accountability Office).

303 Lacher, et al., *Analysis of Key Airspace Integration Challenges and Alternatives for Unmanned Aircraft Systems*, 8-10, 15.

- 304 Aircraft with an active transponder are considered cooperative, and aircraft without a transponder (or without a broadcasting transponder) are considered non-cooperative. For more information see *ibid.*, 4; and 14 CFR 91.113.
- 305 Lacher, et al., *Analysis of Key Airspace Integration Challenges and Alternatives for Unmanned Aircraft Systems.*, 10-11, 15.
- 306 The U.S. Navy has attempted to field non-cooperative ABSAA on its MQ-4C Triton UAS but has scaled back the program after cost overruns and delays. See Dave Majumdar, "AUVSI: US Navy pauses development of MQ-4C Triton 'sense and avoid' radar," Flightglobal, August 15, 2013, <http://www.flightglobal.com/news/articles/auvsi-us-navy-pauses-development-of-mq-4c-triton-39sense-and-avoid39-389504/>; and Stephen Trimble, "US Navy re-starts sense and avoid radar for MQ-4C," Flightglobal, November 4, 2014, <http://www.flightglobal.com/news/articles/us-navy-re-starts-sense-and-avoid-radar-for-mq-4c-405625/>.
- 307 See FAA, *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap*.
- 308 49 U.S.C. § 1508 (a).
- 309 *Montalvo v. Spirit Airlines*, 508 F.3d 464, 468 (9th Cir. 2007).
- 310 Academy of Model Aeronautics, *Model Aircraft Safety Code* (2014), available at <https://www.modelaircraft.org/files/105.PDF>.
- 311 AUVSI, *Unmanned Aircraft System Operations Industry "Code of Conduct"* (2012), reprinted in Elias, *Pilotless Drones*, 16.
- 312 There has been some work on CPFH for unmanned systems, notably a 2011 GAO report and a 2013 piece written by Chris Mailey of AUVSI. However, this work is either limited solely to UAS in the case of the GAO report or specific cases and platforms in the case of Mailey's article. It should be noted that Mailey's piece discusses the issues with CPFH comparisons and presents some case studies albeit with estimated figures. See: Government Accountability Office, *DOD's Role in Helping to Secure the Southwest Border*, Statement of D'Agostino, Davi M., GAO-11-856R; and Chris Mailey, "Are UAS More Cost Effective than Manned Flights?," AUVSI, October 24, 2013, <http://www.auvsi.org/HamptonRoads/blogs/chris-mailey/2013/10/24/are-uas-more-cost-effective-than-manned-flights>.
- 313 See Office of Management and Budget, *Circular No. A-126 Revised: Improving the Management and Use of Government Aircraft*, Washington, DC: Office of Management and Budget, May 22, 1992, http://www.whitehouse.gov/omb/circulars_a126.
- 314 For example, an MQ-9 Reaper had a CPFH of \$3,612 in 2012 while a TH-1H helicopter had a CPFH of \$4,906. The TH-1H used as a point of comparison is an UH-1 Huey remanufactured with largely commercial parts and is the USAF platform that most closely resembles the type of rotary-wing asset that would be used in the HSE. The Air Force data includes the HH-60G helicopter which, while similar to CBP Black Hawks, is much more complex owing to its specialized mission packages and has a correspondingly high cost per flight hour of \$24,149. For the complete data set, see Mark Thompson, "Costly Flight Hours," *Time Battleland*, April 2, 2013, <http://nation.time.com/2013/04/02/costly-flight-hours/>.
- 315 For more information, see Mailey, "Are UAS More Cost Effective than Manned Flights?" AUVSI.
- 316 Certain HSE missions, like migrant or narcotics interdiction, require humans in the endgame and apprehension phases, so while unmanned systems may offer cost savings for particular mission phases, these savings may fail to contribute meaningfully to broader full-mission cost savings.
- 317 Discussion at First Working Group, June 16, 2014.
- 318 Discussion at Second Working Group, July 17, 2014.
- 319 Press conference, National Press Club, Washington, D.C., June 18, 2014.
- 320 Jeff Pegues, "NYPD scanning the sky for new terrorism threat," CBS News video, 4:44, October 29, 2014, <http://www.cbsnews.com/news/drone-terrorism-threat-is-serious-concern-for-nypd/>. The global picture also speaks to reason for U.S. domestic concern. In October and November 2014, multiple sUAS were spotted operating over French nuclear plants, and French authorities were unclear as to who operated the UAS and for what purpose (Tara Patel, "France Probes Mystery Drones Flying Over Nuclear Reactors," Bloomberg News, October 30, 2014, <http://www.bloomberg.com/news/2014-10-29/edf-confirms-probe-into-mystery-drones-flying-over-nuclear-sites.html>). The Chinese government takes so seriously the threat of sUAS that it has developed and deployed a laser weapon system with a 1.2 mile range that it will deploy during major public events ("China unveils laser drone defence system" *Agence France-Presse*, November 3, 2014, <http://www.theguardian.com/world/2014/nov/03/china-unveils-laser-drone-defence-system>). A recent report by the United Kingdom-based Birmingham Policy Commission including former senior government officials warned that in the hands of bad actors, "RPA could become a dangerous and destabilizing (sic) delivery system," including as a chemical or biological weapons dispersal platform (Birmingham Policy Commission, *The Security Impact of Drones: Challenges and Opportunities for the UK* (2014), 12 and 75-76, <http://www.birmingham.ac.uk/Documents/research/policycommission/remote-warfare/final-report-october-2014.pdf>).

