UNMANNED AERIAL VEHICLES FLYING IN THE NEW FRONTIER

EMERGING ACQUISITION, SECURITY, PRIVACY, AND TECHNOLOGY ISSUES

BY DAVID Z. BODENHEIMER AND KATE GROWLEY

This technology has been hailed by many names: drones, remotely piloted vehicles, unmanned aerial vehicles (UAVs), and more. This UAV technology is not new, as the US military tested the unmanned Kettering aerial torpedo with preset flight controls during 1917.[1] But game-changing advances in aviation technology, guidance systems and controls, and payloads have revolutionized UAV systems, as nearly everyone acknowledges.

- *Senator Thune:* Unmanned aviation is undoubtedly the next significant frontier in the aviation sector.[2]
- *Electronic Privacy Information Center (EPIC):* So the [drone] technology is increasing at an exponentially rapid rate, and as we move forward, we are just going to see the capabilities of these devices increase.[3]
- *The Brookings Institution:* Many scientists parallel unmanned systems today to where we were with "horseless carriages" back in 1909–1910, at the start of something so big we can only wrap our minds around what it is not. That is, automobiles and the resulting mechanization didn't just . . . change industry and warfare, it also . . . led to the requirement of new laws, "traffic laws."

* * *

The point here is that every so often in history, the emergence of a new technology changes our world.[4]

With transformative technologies come cutting-edge issues. This maxim is particularly true for UAV technology. The UAV issues range from cybersecurity and privacy to safety and commercialization—many of which have generated vigorous hearings and many bills in the US Congress and state legislatures. Given the breadth of these issues, this analysis focuses more narrowly upon how three specific issues may affect federal acquisitions in the coming years.

1. *Commercialization.* Although military uses dominated the early history of UAV usage, exploding international demand and dramatic cost efficiencies are pushing commercial uses (e.g., agriculture, mapping, communications, and transportation) with

accelerating speed. For federal agencies and contractors, these commercialization trends will drive an increasing number of federal procurement into the commercial item arena, resulting in major shifts in how UAV systems are bought and sold in the federal marketplace.

2. *Security.* As reports mount on the potential for hackers to spoof control links and hijack UAV aircraft, the need will grow for UAV manufacturers, operators, and buyers to develop secure control systems to protect UAV aircraft from spoofing and jamming risks. Establishing acquisition requirements for UAV security and antispoofing safeguards will be an essential component of federal procurements.
3. *Cyberespionage.* Every country and company wants the latest UAV technology—and some are willing to steal it via cyberespionage and other methods. Companies with high-value UAV intellectual property and trade secrets face intensifying legal obligations to safeguard such technology and report losses resulting from cyber breaches.

David Z. Bodenheimer, a partner in Crowell & Moring LLP's Government Contracts Group, heads the Homeland Security practice and currently serves as the ABA Public Contract Law (PCL) Section's representative to the Cybersecurity Legal Task Force, PCL Committee Co-Chair (Cybersecurity, Privacy, and Data Protection), and Science & Technology Law (SciTech) Section Division Co-Chair (Security, Privacy, and Information Law). Kate M. Growley, an associate at Crowell & Moring LLP, practices in the Privacy & Cybersecurity and Government Contracts Groups, handles a wide range of cybersecurity and UAS issues, and serves as the ABA SciTech Homeland Security Committee Vice-Chair.

The exponential growth of the unmanned aerial systems (UAS) market and technological complexities will propel corresponding complexities in the already difficult issues of commercialization, privacy, and security. As UAS technology gains expanding market share in the private and public markets, both federal agencies and contractors will confront the familiar conundrum of technology outpacing existing law, thus creating further stresses in the federal procurement process.

Emerging Issues in the Use and Acquisition of UAV Systems

In the past few years, UAS aircraft have been in the vortex of a host of knotty legal issues—including inter alia weaponized UAS platforms, safety in domestic airspace, and export controls. From this long list, the discussion below selects three of the many issues likely to confront federal agencies and contractors in the acquisition process: commercialization, security, and cyberespionage.

Commercialization and UAV Technology Acquisitions

In the beginning, UAV aircraft performed military functions. Even today, the military represents a major user and deployer of UAV technology.[5] However, the list of commercial uses continues to grow—and economics will drive rapid expansion of the commercial UAV marketplace. In turn, expanding UAV commerciality will change how federal agencies buy UAV systems.

Commercial Drivers for UAV Technologies

Some of the world's largest commercial enterprises have made headlines and captured attention within Congress for their roles in UAV aviation and the payloads they carry.

- *Google's Solar-Powered UAVs:* "Google is getting into the emerging market for solar-powered drones, competing with rival Facebook, as the two Internet companies look for new ways to get more of the world's population online."[6]
- *Amazon's Delivery Plans:* "According to Amazon CEO Jeff Bezos, the company is fixing to deliver packages to its customers via drones. It is called 'Amazon Prime Air.'"[7]
- *Walmart's UAV Cameras:* "Both systems [Draganflyer X6 and Falcon] are used to carry cameras, which are commercially available. In fact, you can buy the very same camera that we put on the Draganflyer X6 at Walmart."[8]

As the Congressional Research Service (CRS) noted, UAS have many nonmilitary applications.[9] (See Table 1.)

Similarly, the Government Accountability Office (GAO) described commercial uses as including "pipeline, utility, and farm-fence inspections; vehicular traffic monitoring; real-estate and construction-site photography; relaying telecommunication signals; film industry production; and fishery protection and monitoring."[10]

Internationally, UAV aircraft and systems have a proven track record of commercial uses. In Japan, UAV aircraft have delivered fertilizer and dusted crops for 20 years.[11] As Dr. Mary Cummings testified before the Senate, other countries have an established legacy of UAV commercial uses:

> For example, in Japan drones make up more than 90 percent of crop dusting, which is a very dangerous job for human pilots. In the U.K. you can use drones for commercial photography, you can use them for crop monitoring, they can deliver food to your table at a restaurant, and they can deliver pizza to your home. And while I do appreciate Amazon's big announcement about drone

TABLE 1

NONMILITARY UAS APPLICATIONS

BORDER SURVEILLANCE
SUSPECT TRACKING
TRAFFIC MONITORING
DISASTER RESPONSE/RELIEF
DAMAGE ASSESSMENT
ATMOSPHERIC/WEATHER RESEARCH
CRITICAL INFRASTRUCTURE MONITORING
DAMAGE SURVEYING
AERIAL PHOTOGRAPHY
WILDLIFE MONITORING
PIPE/POWERLINE SURVEILLANCE
AGRICULTURAL APPLICATIONS
COMMUNICATIONS/BROADCAST
MOVIE PRODUCTION
AERIAL NEWS COVERAGE
MAIL/FREIGHT TRANSPORT
FLOOD MAPPING
REAL ESTATE MAPPING
MINING
SPORTING EVENTS COVERAGE

Source: Association for Unmanned Vehicle Systems International (AUVSI), *Unmanned Aircraft System Integration into the United States National Airspace System: An Assessment of the Impact on Job Creation in the U.S. Aerospace Industry* 8 (2010)

> package delivery, unfortunately, there are companies in China and Australia that beat them to the punch.[12]

Just as international demand will power the commercial UAV markets, so will economics. Already, small UAV aircraft "can be purchased online for under $100" and can be flown "with an iPhone app."[13] Compared with manned aircraft or other alternatives, UAV applications can often deliver performance for pennies on the dollar for certain applications.

> Each year, Mesa County spends nearly $10,000 on a manned aerial survey of our landfill to determine the increase in waste over the previous year. My team and I completed that very same survey for a mere $200.
>
> * * *
>
> I estimate unmanned aircraft can complete 30 percent of the missions of manned aviation for 2 percent of the cost. The Mesa County Sheriff's Office projects direct cost of unmanned flight at just $25 an hour as compared to the cost of manned aviation that can range from $250 to thousands of dollars an hour.[14]

In summary, the combination of global commercial demand and huge cost savings will spread UAV applications throughout the private sector, as competitive forces will lead more companies to embrace the technology to do more with less. In turn, these market forces will create more UAV options and innovation, tilting the UAV market toward commercial uses.

Commercial Item Acquisition Rules for Federal Agencies

Commercial UAV applications will have profound effects upon federal acquisitions in two ways.

First, both the governing statutes and regulations require federal agencies to procure commercial items to the maximum extent practicable. The legislative history of the Federal Acquisition Streamlining Act of 1994 recognized the need for federal agencies to have access to technologies widely available in the commercial marketplace.[15] To expand the federal government's access to commercial technology, Congress directed federal agencies to acquire commercial items "to the maximum extent practicable."[16] The statutes governing federal acquisitions codify this mandate:

> The head of an agency *shall* ensure that procurement officials in that agency, *to the maximum extent practicable—*
>
> (1) acquire commercial items or nondevelopmental items other than commercial items to meet the needs of the agency;
> (2) require prime contractors and subcontractors at all levels under the agency contracts to incorporate commercial items or nondevelopmental items other than commercial items as components of items supplied to the agency[.][17]

The implementing acquisition regulations reinforce this statutory requirement for commercial items.[18]

Second, when a federal agency buys commercial items, both the statute and regulations restrict the contractual terms and conditions applicable to commercial item procurements. In the Federal Acquisition Streamlining Act of 1994, Congress imposed specific prohibitions on what conditions or burdens that agencies could lawfully impose on commercial acquisitions:

> (b) CONTRACT CLAUSES—
> (1) The regulations prescribed under subsection (a) shall contain a list of contract clauses to be included in contracts for the acquisition of commercial end items. Such list shall, to the maximum extent practicable, include *only those contract clauses—*
> (A) that are required to implement provisions of law or executive orders applicable to acquisitions of commercial items or commercial components, as the case may be; or
> (B) that are determined to

be consistent with standard commercial practice.[19]

In Part 12, the Federal Acquisition Regulation (FAR) implements this requirement, expressly limiting commercial item terms to those specifically mandated by law or executive order or those "[d]etermined to be consistent with customary commercial practice."[20] Furthermore, these terms governing commercial items trump other parts of the FAR.[21]

In summary, the market forces and economics driving UAV technology will also force federal agencies to rethink UAV acquisitions, as commercial UAV applications fill an expanding array of needs at ever more affordable prices. With these commercial developments, federal contracting officers will shoulder the responsibility for conducting market research and acquiring commercial UAV items as they become available.[22]

Security Risks for UAV Aircraft

With aircraft flown by pilots in the cockpit, hijackers generally had to take physical control in order to take over the aircraft. In contrast, UAV aircraft may pose the risk of a cyber-jamming or hijacking (spoofing), resulting in loss of control of the aircraft. Both types of threats may jeopardize the security and safety of UAV aircraft.

Jamming Issues for UAV Aircraft

Jamming effectively severs the link between the UAV aircraft and its ground control system:

> The jamming of the GPS signal being transmitted to the UAS could also interrupt the command and control of UAS operations. In a GPS jamming scenario, the UAS could potentially lose its ability to determine its location, altitude, and the direction in which it is traveling. Low cost devices that jam GPS signals are prevalent. According to one industry expert, GPS jamming would become a larger problem if GPS is the only method for navigating a UAS.[23]

To mitigate the jamming risk, the UAV manufacturer or operator may employ a second or redundant navigation system onboard the UAV aircraft, as the Department of Defense (DoD) and Department of Homeland Security (DHS) have typically done with larger UAV systems.[24] Presumably, the FAA test site operators will also address these jamming issues as part of the overall safety and security evaluation of UAV operation in the domestic airspace. In turn, the test site experience and FAA actions will inform federal agencies in the acquisition of UAV aircraft and systems.

Spoofing Issues for UAV Aircraft

In additional to jamming, UAV aircraft may be exposed to a spoofing attack allowing a cyberhijacker to seize control of the aircraft:

> Additionally, unmanned aircraft command and control links could potentially be intentionally jammed or hacked resulting in a loss or hostile takeover of control. For example, Todd Humphreys, an assistant professor at the University of Texas at Austin, demonstrated a remote hijacking of an unmanned aircraft by GPS guidance signals. In congressional testimony, he warned that advances in software-defined radio and the availability of GPS signal simulators may provide average hackers with the capability to interfere with unmanned aircraft operations.[25]

During his congressional testimony, FAA Administrator Michael Huerta confirmed that he was "very concerned about the cyber issue" of hackers taking control of UAV aircraft.[26]

Currently, military GPS signals are encrypted to prevent spoofing attacks. However, no easy solutions are readily available for civil UAS aircraft. Currently, nonmilitary GPS signals are not encrypted, thus creating a potential spoofing risk.[27] One recommendation would be for larger nonrecreational civilian UAV aircraft to "be required to have spoof-resistant navigation systems" that, while not guaranteeing protection, would "'make successful spoofing much harder.'"[28] According to Administrator Huerta, the FAA is working "to establish what is an appropriate technological standard to ensure that we have cyber protections in place so that we can ensure the safe operation of these aircraft."[29]

Cyberespionage and UAV Technology

Given the enormous economic and military value of UAV technology, cyberspies have targeted both the public and private sectors to steal UAV intellectual property (IP), trade secrets, and technology. For companies in the UAV business, such cyber thefts may not only damage corporate IP and trade secret portfolios, but also trigger regulatory scrutiny and enforcement risks.

Cyberthreats to UAV Technology

Five years ago, a trend analysis of the defense industry warned of the "risk of intensive foreign-originated efforts to acquire UAV-related technologies or information."[30] Two years later, the National Counterintelligence Executive report stated that, of aerospace and aeronautics technology, "[t]he greatest interest may be in UAVs because of their recent successful use for both intelligence gathering and kinetic operations in Afghanistan, Iraq, and elsewhere."[31] In 2015, cyberespionage remains a continuing threat to UAV technology:

> Military analysts say China has long tried to replicate foreign drone designs. Some Chinese drones appearing at recent air

shows have closely resembled foreign ones. Ian M. Easton, a military analyst at the Project 2049 Institute in Virginia, said cyberespionage was one tool in an extensive effort over years to purchase or develop drones domestically using all available technology, foreign and domestic.[32]

In summary, both public-sector agencies and private-sector contractors must presume that cyberspies are ever lurking to steal UAV technology. For individual companies, the economic impact of cyber thefts can result in $1 billion technology losses, double-digit stock losses, and reduced international competitiveness.[33]

Regulatory Risks of Cyberespionage

For a company losing its UAV technology to cyberspies, the economic damage may be only the first injury flowing from the theft. After the breach, the company may then face a gauntlet of regulatory notifications and scrutiny, depending upon the nature of the data and the status of the company.

Cleared Defense Contractors

For cleared defense contractors, a "successful penetration" may trigger a duty for "rapid reporting" to DoD. Such reports must include the "technique or method used," a "sample of the malicious software," and a summary of DoD information on the system.[34]

Controlled Technical Information

For UAV technology, defense contractors may possess "controlled technical information"—for which "technical information" is broadly defined to include research and engineering data, engineering drawings, specifications, standards, process sheets, and other similar data.[35] Such data would be an inviting target for UAV technology thieves. In the event of loss of covered technical data, the defense contractor generally has 72 hours to report the incident and to include "as much of the following information as can be obtained" relating to 13 categories of information.[36]

Publicly Held Corporations

For publicly held corporations, the Securities and Exchange Commission (SEC) issued guidance for such companies to report material risks relating to cybersecurity.[37] In the event of a data breach in which a UAV manufacturer or operator lost substantial UAV technology, this guidance may require the corporation to describe what was stolen and its impact, if material to the company's financial condition.

In summary, cyberespionage may victimize a UAV company twice—once through the loss of valuable IP and trade secrets for cutting-edge UAV technology, and again through the scrutiny of federal regulators after the cyber theft. In such cases, UAV companies have a strong business case for robust cyberdefenses to protect their UAV technology.

Conclusion

With cutting-edge UAV technology comes cutting-edge legal issues for federal agencies and contractors. Although commercialization, security, and cyberespionage do not represent the full list, both the public and private sectors will inevitably face them in the acquisition process. For some UAV issues, technology advances and innovations may provide solutions (e.g., antispoofing technology), while other technology

IN THE PAST FEW YEARS, UAS AIRCRAFT HAVE BEEN IN THE VORTEX OF A HOST OF KNOTTY LEGAL ISSUES.

may turn up the heat of debates over UAV applications (e.g., surveillance and privacy). But in any case, international market forces and economic efficiencies will power a kaleidoscope of UAV uses in the commercial sector—and the spillover will, in turn, change how federal agencies and contractors buy and sell UAV technology. ◆

Endnotes

1. Aerospace Industries Association (AIA), *Unmanned Aircraft Systems: Perceptions and Potential*, p. 3 (Sept. 9, 2011) (http://www.aia-aerospace.org/assets/AIA_UAS_Report_small.pdf).

2. *The Future of Unmanned Aviation in the U.S. Economy: Safety and Privacy Considerations: Hearings before the Sen. Commerce, Science, and Technology Comm.,* 113th Cong. (Jan. 15, 2014), CQ Transcripts, p. 9 (statement of Sen. Thune) (hereinafter 2014 Senate Commerce Hearings on Future of Unmanned Aviation).

3. *The Future of Drones in America: Law Enforcement and Privacy Considerations: Hearings before the Sen. Judiciary Comm.,* 113th Cong. (Mar. 20, 2013), CQ Transcripts, p. 40 (statement of Ms. Amie Stepanovich) (hereinafter 2013 Senate Judiciary Hearings on Future of Drones).

4. *Rise of the Drones: Unmanned Systems and the Future of War: Hearings Before the House Subcomm. on National Security and Foreign Affairs of the Comm. on Oversight and Government Reform,* 111th Cong. (Mar. 23, 2010) (statement of Dr. Peter Singer) (http://oversight.house.gov/wp-content/uploads/2012/01/20100323Singer.pdf).

5. *See, e.g.,* GAO, *Defense Acquisitions: Assessment of Selected Weapon Programs,* (Mar. 2014) (GAO-14-340SP) (listing and summarizing major UAV defense programs).

6. Alistair Barr, "Google Agrees to Buy Drone Maker Titan Aerospace," *Digits: Tech News & Analysis From WSJ* (Apr. 14, 2014).

7. 159 *Cong. Rec.*, p. H7399 (Dec.3, 2013) (statement of Rep. Poe).

8. 2013 Senate Judiciary Hearings on Future of Drones, p. 6 (statement of Mr. Miller).

9. CRS, *Unmanned Aircraft Systems (UAS): Manufacturing Trends,* p. 5 (Jan. 30, 2013).

10. GAO, *Unmanned Aircraft Systems: Continued Coordination, Operational Data, and Performance Standards Needed to Guide Research and Development,* p. 2 (Feb. 15, 2013) (GAO-13-346T).

11. 2014 Senate Commerce Hearings on Future of Unmanned Aviation, pp. 5, 8 (statement of Sen. Rockefeller).

12. 2014 Senate Commerce Hearings on Future of Unmanned Aviation, p. 14 (statement of Dr. Cummings, Duke University).

13. 2014 Senate Commerce Hearings on Future of Unmanned Aviation, p. 38 (statement of Sen. Markey).

14. 2013 Senate Judiciary Hearings on Future of Drones, pp. 6–7 (statement of Mr. Miller).

15. S. Rep. No. 103-258 (1978), *as reprinted in* 1994 U.S.C.C.A.N. 2561, 2563–66.

16. Pub. L. No. 103-355, § 8104(b), *as reprinted in* 1994 U.S.C.C.A.N. 3243, 3391.

17. *See, e.g.,* 10 U.S.C. § 2377(b) (emphasis added).

18. *See, e.g.,* FAR §§ 1.102(b)(1)(i) ("Maximizing the use of commercial products and services"), 1.102-2(a)(4) (same), 12.101 ("Acquire commercial items . . . when they are available").

19. Federal Acquisition Streamlining Act of 1994, Pub. L. No. 103-355, § 8002 *reprinted at* 1994 U.S.C.C.A.N 3386 (emphasis added).

20. FAR § 12.301(a) (same).

21. FAR § 12.102(c) ("When a policy in another part of the FAR is inconsistent with a policy in this part, this part 12 shall take precedence for the acquisition of commercial items").

22. FAR § 12.101(a), (b).

23. GAO, *Unmanned Aircraft Systems: Continued Coordination, Operational Data, and Performance Standards Needed to Guide Research and Development,* p. 15 (Feb. 15, 2013) (GAO-13-346T).

24. *Id.*

25. CRS, *Pilotless Drones: Background and Considerations for Congress Regarding Unmanned Aircraft Operations in the National Airspace System,* p. 12 (Sept. 10, 2012) (R42718).

26. 2014 Senate Commerce Hearings on Unmanned Aviation, p. 51 (statement of Administrator Huerta).

27. GAO, *Unmanned Aircraft Systems: Continued Coordination, Operational Data, and Performance Standards Needed to Guide Research and Development,* p. 15 (Feb. 15, 2013) (GAO-13-346T).

28. CRS, *Pilotless Drones: Background and Considerations for Congress Regarding Unmanned Aircraft Operations in the National Airspace System,* p. 12 (Sept. 10, 2012) (R42718).

29. 2014 Senate Commerce Hearings on Unmanned Aviation, p. 52 (statement of Administrator Huerta).

30. Defense Security Service, *Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry*, p. 8 (2009).

31. Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace,* p. 8 (Oct. 2011).

32. CRS, *China Naval Modernization: Implications for U.S. Navy Capabilities—Background and Issues for Congress,* p. 33 (Feb. 28, 2014) (RL33153).

33. Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace,* pp. 3–6 (Oct. 2011); CRS, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, pp. 2–3 (Mar. 1, 2013) *quoting* Executive Assistant Director Shawn Henry, Responding to the Cyber Threat, FBI, Baltimore, MD, 2011; *Economic Espionage: A Foreign Intelligence Threat to American Jobs and Homeland Security: Hearings before House Homeland Security Comm.,* 112th Cong. (June 28, 2012) (statement of Mr. Wortzel).

34. 2013 National Defense Authorization Act, Pub. L. No. 112-239, Div. A, Title IX, Subtitle D, § 941, 126 Stat. 1889. Although this requirement applies to "cleared defense contractors," it remains unresolved whether the notification requirement applies to both cleared and uncleared networks—or only classified networks.

35. DFARS § 252.204-7012(a).

36. DFARS § 252.204-7012(d).

37. SEC, *Cybersecurity: CF Disclosure Guidance: Topic No. 2* (Oct. 13, 2011).