DRONERESPONDERS

An Introduction to *The Five C's: Principles on the Responsible Use of Drones by Public Safety Agencies*

Drone technology is transforming public safety for the better. Fire, emergency management, and law enforcement agencies use drones every day to provide situational awareness during emergency situations when every moment matters. Obtaining real-time awareness in dangerous scenarios results in better outcomes, greater accountability, and increased leadership involvement in events as they unfold. Drones also provide a means of de-escalation--providing a perspective that allows for safe and thoughtful problem solving. Like body worn cameras, drones provide an account of what occurred, but they also provide a pre-emptive capability to prevent tragedy and protect the community. When used appropriately, drones are a tool for good.

With 2,000 members in almost 30 countries, DRONERESPONDERS is the leading organization dedicated to advancing the use of drones by first responders. Our members have pioneered the use of drones to protect the public and those sworn to protect them. We believe every public safety agency needs access to this transformative technology. In order to realize the benefits of drones, agencies must use drones in a responsible manner that acknowledges the importance of community engagement and the protection of privacy and civil liberties.

To advance that objective, DRONERESPONDERS is proud to issue a set of foundational principles to guide the development and deployment of drones by first responders: *The Five C's: Principles on the Responsible Use of Drones by Public Safety Agencies*. Over the past decade, there has been no shortage of materials released on the development of public safety drone programs; the Police Executive Research Forum (PERF), the U.S. Department of Justice (DOJ), the National Institute of Justice (NIJ), and the International Association of Chiefs of Police (IACP) have all issued guidance in some form or another.[i] But sorting through this maze of reports can be a struggle. Agencies need clear guidance that is *easy to apply in practice*.

The Five C's solve that issue. Now, agencies can begin by consulting a single set of principles that every agency should follow. We believe these principles represent a significant step forward for public safety drone programs around the world. The principles center on five critical pillars:

I. **Community Engagement and Transparency**
II. **Civil Liberties and Privacy Protection**
III. **Common Operating Procedures**
IV. **Clear Oversight and Accountability**
V. **Cybersecurity**

We invite stakeholders across the community--public safety agencies, industry associations, manufacturers, and civil society organizations--to review and endorse the principles. The release of the principles marks the beginning of a broader effort to promote awareness and adoption. To endorse or express a view on the principles, contact DRONERESPONDERS at principles@droneresponders.org.

DRONERESPONDERS developed these principles with the support and assistance of Skydio, the largest U.S. drone manufacturer. Based in Redwood City, California, Skydio leverages breakthrough Artificial Intelligence to build the world's most advanced autonomous drones. Public safety agencies across the country rely on Skydio drones, which are designed, assembled, and supported in the United States. Demonstrating its commitment to public safety, Skydio recently launched the Skydio Emergency Response Program to donate 100+ drones to public safety programs nationwide. Skydio is committed to building drone technology--and supporting the development of standards and best practices--that advance the responsible use of drones by public safety agencies.

DRONERESPONDERS

The Five C's:
Principles on the Responsible Use of Drones by Public Safety Agencies
(August 10, 2020, Rev. 1)

I. Community Engagement and Transparency

Public service is a public trust. When developing and operating a drone program, it is critical to engage in an ongoing conversation with the community you serve. Effective community engagements consists of two parts: public participation and transparency.

Public Participation: First, public safety drone programs require close and continuing coordination with the local community. Before establishing a drone program, we recommend:

> "undertaking a methodical process of explaining [proposed] plans publicly; holding public meetings and other forums in which community members can express their concerns; and working with the community to reach acceptable compromises or consensus approaches to issues such as defining the purposes of police drones, managing the use and possible storage of video or other data obtained by drones, and addressing the public's legitimate concerns and questions."[ii]

This process takes time. But slow is smooth. Take it from Captain Vern Sallee, who oversees CVPD's public safety drone program. Captain Sallee followed a "crawl, walk, run strategy" for obtaining and maintaining public trust and "found that slowly developing plans for a drone program was helpful to fostering the public's trust."[iii] In general, community engagement should occur before an agency even begins to purchase drones.[iv]

Agencies should also engage with a range of civil society organizations, such as the American Civil Liberties Union (ACLU). Along those lines, DRONERESPONDERS believes it is critical to engage with "community organizations that are likely to have reservations about drone use, such as civil liberties groups, *prior* to program implementation."[v]

CVPD's approach to community engagement paid dividends, forming a strong foundation of public support that has enabled the program to conduct thousands of successful missions.[vi] Agencies that take a similar approach are likely to experience similar results, provided they treat community engagement as a continuous conversation, rather than a one-time requirement.

Transparency: Second, community engagement requires transparency. The public deserves to know that promises made in the development of a drone program are kept in its operation. Transparency is a crucial ingredient in building public trust. The policies and procedures that govern a drone program should be easily accessible by the public.[vii] We recommend creating a website with up-to-date information on the use of drones, along with relevant policies.[viii] Agencies should continue to hold media briefings and conduct community outreach on an ongoing basis.[ix]

Drones made by a variety of manufacturers, including Skydio, generate telemetry and other analytics that create an objective digital record of their use. DRONERESPONDERS encourages public safety agencies to share information of that nature, as appropriate, in order to foster transparency and build public trust. For excellent examples of departments sharing information with the community, we recommend reviewing the drone programs in Lakewood, Washington and Fairfax County, Virginia, among others.[x]

II. Civil Liberties and Privacy Protections

Above all else, public safety drone programs should be designed to promote and protect privacy and civil liberties.

Civil liberties: Drone programs must be consistent with the bedrock obligation to uphold civil liberties, especially--but not exclusively--the liberties expressed in the First and Fourth Amendments. The First Amendment protects, among other things, the freedom of speech, the freedom of the press, and the right to peaceably assemble and petition for change. Public safety agencies should use drones in a manner that protects these fundamental freedoms and avoids chilling free expression and assembly.

In particular, it is critically important to respect the rights of journalists and news organizations to conduct their operations without interference. Many news organizations use drones to obtain compelling perspectives on current events. Newsgathering is an activity protected by the Constitution. Public safety agencies should take steps to ensure that officers will not unduly interfere with the ability of journalists to use drones lawfully in carrying out their work.

The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Agencies should work closely with legal counsel, local government bodies, and community stakeholders to strike the right balance between privacy rights and public safety. When required by law, agencies must obtain a search warrant before using a drone. More broadly, drones must be used in a manner that comports with reasonable expectations of privacy. In particular, drones must *never* be used to conduct random or mass surveillance.[xi]

Privacy: Privacy is often the foremost concern surrounding the use of drones. Agencies should address that concern head on, developing safeguards and training procedures that ensure the protection of privacy at every level of a drone program.

In particular, agencies must have policies in place that protect privacy across the full operational lifecycle: acquisition, use, dissemination, and retention. The third principle on common operating procedures discusses measures designed to limit the acquisition of potentially private information, which must be directly related to an authorized mission.

The use and dissemination of information gathered by drone should generally be limited to the extent necessary to facilitate a civil proceeding, criminal investigation or prosecution, or other authorized reason (such as facilitating community engagement by showing the operation of the program, including illustrative examples of success and challenges).

It is also important to place limits on retention. First, to the extent feasible, only information directly related to the authorized purpose of the mission should be retained. Second, data obtained from drones should be retained only as long as necessary. DOJ limits the retention of information collected by drones to 180 days, unless retention "is determined to be necessary for an authorized purpose," such as to facilitate a civil action or criminal investigation or prosecution.[xii] For many agencies, a shorter period of time may be appropriate, with extensions authorized for information necessary to facilitate criminal investigations or civil proceedings.

The ACLU recommends that images taken by a drone "should be retained only when there is reasonable suspicion that they contain evidence of a crime or are relevant to an ongoing investigation or trial."[xiii] That is generally sound advice for law enforcement agencies, although it may be prudent to permit the retention, for a limited period, of information related to training missions or other authorized missions outside of the criminal investigative context, such as a bridge inspection performed as authorized assistance to another government agency.

Annual privacy assessments: We recommend that agencies complete (1) a privacy impact assessment before establishing a drone program and conduct (2) annual assessments during the operation of the program.[xiv] A privacy assessment aims to "ensure compliance with existing laws, regulations, and policies relating to privacy and civil liberties and, where appropriate, make recommendations to [leadership] consistent with applicable privacy and civil liberty protections."[xv] Annual assessments offer an opportunity to step back and consider how a program could improve upon the core task of protecting privacy and civil liberties. Agencies that regularly assess privacy impacts--and implement the results of those assessments--will be better prepared to address any examples of misuse, provided they have a history of taking seriously any recommendations made during the assessment process.

Ultimately, drone programs predicated on the protection of privacy and civil liberty are likely to earn the support of the community in the long run while avoiding potential missteps that could reduce support for this important new tool.

III. Common Operating Procedures

Every program needs a clear policy outlining the responsible, safe, and effective use of drone technology. We strongly recommend that departments develop and adopt common operating procedures consistent with templates and best practices presented in reports issued by PERF, DOJ COPS, NIJ, and IACP.[xvi]

Effective policies will cover a wide range of critical topics, including FAA compliance; safety procedures (before, during, and after flight operations); reporting requirements; training, proficiency and credentialing requirements; cybersecurity; accident and incident reporting procedures; authorized missions; approval processes; video management procedures; and language prohibiting weaponization.

Six topics--FAA compliance, training/proficiency/credentialing requirements, authorized missions, approval processes, video management, and non-weaponization--merit special focus in this section.

- **FAA Compliance:** Compliance with FAA regulations forms the cornerstone of every public safety drone program.
    - Part 107 and Part 91: Agency operating procedures should discuss in detail measures to ensure compliance, including whether the program operates as a public aircraft operator (under Part 91 with a COA) or follows the rules for non-recreational operations (under Part 107), or both. To ensure maximum versatility, we strongly recommend operating under a COA *and* Part 107.
    - Partnering with the FAA: There is no better way to establish a safe and effective drone program than to establish strong relationships with the FAA. The FAA offers a variety of resources to agencies at every stage of creating and operating a drone program. Agencies new to drones should consult the FAA's resource page on starting a drone program,[xvii] which includes a helpful starter guide.[xviii]
- **Training, proficiency, and credentialing:** Based on studies and in-person meetings conducted by DRONERESPONDERS, the number one concern among public safety drone programs has been the need for standardized training and certification. Recently released standards help to resolve that issue.
    - In particular, we recommend that every public safety program review and follow the ASTM standard on Training for Public Safety Remote Pilot of UAS Endorsement (ASTM 33.79) and the Standard Test Methods for Small Unmanned Aircraft Systems prepared by the National Institute for Standards and Technology (NIST). The ASTM standard outlines "the minimum training requirements for public safety remote pilots," and references the test methods developed by NIST.
        - The ASTM and NIST standards provide helpful guidance for training, proficiency and credentialing to ensure safety in the national airspace system. It comes as no surprise that public safety agencies across the nation are integrating these standards into their operations.
- **Authorized missions:** This section should clearly state the missions for which drone use is authorized, such as:[xix]
    - Training flights;
    - Search and rescue;
    - Disaster response;
    - Fire response;
    - Explosive ordnance detection support;
    - Crime and accident scene documentation and reconstruction;
    - Damage assessment;

- Tactical support for emergencies and high-risk situations, such as the execution of search or arrest warrants;
- Authorized assistance to other government agencies, such as:[xx]
    - Wildlife and environmental impact surveys;
    - Promotional purposes (e.g., taking videos of new county buildings for a video posted on the county website);
    - Construction site surveys (e.g., surveying city buildings under construction).
    - Bridge and highway inspections (regular inspections of which are typically required by law); and
- Other authorized reasons (which should be clearly specified in the policy following consultation with government oversight bodies and community organizations).

- **Approval Process**: This section should outline the approval process required to deploy drones in support of authorized missions. "All sUAS missions should be approved by a supervisor," with appropriate exceptions for exigent situations.[xxi]
    - Risk-based review and approval processes: Approval processes should be tailored to address the level of risk and sensitivity associated with particular categories of missions. In this context, risk should be broadly defined to encompass safety, class of airspace, privacy impacts, operator training, and other relevant factors.
        - As a general rule, the higher the risk, the higher the level of review and approval that may be required. Recognizing that first responders live in a world where minutes matter, processes requiring pre-approval should generally contain exceptions for exigent circumstances, enabling operators to alert supervisors of their intention to deploy a drone and file a report as soon as practicable.
    - ACLU Perspective on Authorization:
        - The ACLU recommends that law enforcement agencies deploy drones only:
            - "where there are specific and articulable grounds to believe that the drone will collect evidence relating to a specific instance of criminal wrongdoing or, if the drone will intrude upon reasonable expectations of privacy, where the government has obtained a warrant based on probable cause; or
            - where there is a geographically confined, time-limited emergency situation in which particular individuals' lives are at risk, such as a fire, hostage crisis, or person lost in the wilderness; or
            - for reasonable non-law enforcement purposes by non-law enforcement agencies, where privacy will not be substantially affected, such as geological inspections or environmental surveys, and where the surveillance will not be used for secondary law enforcement purposes."[xxii]
        - We recommend adopting that general approach. Agencies may wish to amend the second category, which appears to require first responders to know that a specific person's life is at risk. As long as the situation represents an emergency, it would be reasonable to permit the use of

drones for the duration of the emergency. Policies that incorporate those principles are likely to engender public support while minimizing potential risks to privacy and civil liberties.

- **Video Management:** When used appropriately, the ability to capture video using a drone saves lives and increases efficiency. That critical capability must not be misused.
    - Recommended restrictions: We strongly advise agencies to *prohibit* the use of drone video to:[xxiii]
        - conduct random surveillance activities;
        - target a person based solely on individual characteristics, such as race, ethnicity, national origin, religion, disability, gender, or sexual orientation;
        - harass, intimidate, or discriminate against any individual or group; and
        - conduct personal business of any type.
- **Non-weaponization:** Congress has prohibited the operation of drones equipped with a "dangerous weapon," unless authorized by the Administrator of the FAA.[xxiv] Violations are subject to a civil penalty up to $25,000.[xxv] That provision applies to public safety agencies. We understand that the FAA intends to issue rulemaking or guidance interpreting that provision.
    - Consistent with that provision, drones used by law enforcement agencies should not be equipped with devices intended to harm human beings. In general, agencies should avoid even the appearance of weaponizing drones for law enforcement use, and should not use attachments that could be misconstrued as intended to harm human beings.

IV. Clear Oversight and Accountability

Policies alone are insufficient to ensure responsible use. Agencies need to establish robust oversight measures designed to ensure compliance and accountability. Agencies should establish clear oversight processes that combine both internal and external measures.

- **External oversight:**[xxvi]
    - **Regular briefings and reports to the City Council:** It is imperative to keep relevant elected officials fully and currently informed about the operation of a drone program. Elected leaders should receive regular briefings and reports on successes, challenges, compliance with department policy and the protection of privacy and civil liberties.
    - **Community advisory panels:** To ensure oversight while fostering community engagement, agencies may wish to follow NIJ's suggestion to "[c]reate a permanent community advisory panel on the implementation of new technologies, such as UAS, drawing from a wide cross-section of the population."[xxvii]
- **Internal oversight:**
    - **Complaint Investigations:** Policies should contain clear standards for reviewing and investigating complaints concerning the inappropriate use of drones, including activities that may violate privacy and civil liberties. Complaints should "be handled in accordance with agency protocols for internal investigations."[xxviii]
    - **Routine compliance audits:** Drone programs should undergo regular audits to verify compliance with department policy and measures to protect privacy and

civil liberties.[xxix] As discussed in the second principle, at a minimum, agencies should complete annual reviews of the program and make those reports available to the public.[xxx]

- **Senior leader oversight**: Senior leaders should ensure that emerging technology programs have strong internal leadership and oversight. In particular, department heads have an important role to play in establishing clear approval and compliance structures that promote the responsible--and accountable--use of drone technology.

V. Cybersecurity

Modern drones are more than simple flying machines. In less than a decade, drones have joined the Internet of Things--a class of devices intended to be connected to networks. Drones typically rely on internet and GPS connectivity to access map data, report their position, and transmit data.

Organizations acquiring IoT devices should take steps to guard against potential cybersecurity vulnerabilities. That is no less true for drones. In April 2020, DOJ warned that public safety agencies "must be attuned to the cybersecurity and supply chain risks associated with" drones, citing the threat of hackers and criminal groups gaining access to government networks.[xxxi]

DOJ also cited a "risk that a foreign entity might gain unauthorized access to law enforcement and public safety agency data from drones,"[xxxii] and suggested that "any responsible assessment of cybersecurity and supply chain risks" by state and local departments "will include a recognition that legislatures and executives at the federal and state level are moving to limit public agencies' purchase and deployment of certain foreign-made UAS, in light of the risks they present."[xxxiii] For context, federal agencies including DHS / FEMA and DOJ have issued cybersecurity restrictions--including country-of-origin considerations--on the use of federal grants to purchase drones.[xxxiv]

This document does not take a position on that topic. Departments should review the issues and reach an informed conclusion. We recommend taking two fundamental steps to ensure cybersecurity:

1. **Ensure your organization implements cybersecurity best practices across every aspect of the agency, including drone operations. In particular, agencies should follow recommended cybersecurity guidelines, such as the Framework for Improving Critical Infrastructure Cybersecurity published by the National Institute of Standards and Technology**.[xxxv]
    a. A DHS survey conducted in 2018 revealed that 36% of agencies had not "instituted cybersecurity best practices, such as risk assessments, continuous monitoring, and identity management"--even though 47% of respondents had experienced cyber incidents that impacted their ability to communicate in the course of emergency response operations.[xxxvi]
    b. We recommend reviewing a DHS guidance document on Cyber Resiliency Resources for Public Safety, released in August 2020.[xxxvii] That document collates resources designed to help agencies "identify and prioritize [cyber] risks, protect

resources, detect threats, and enable coordinated response and recovery efforts."[xxxviii] We also recommend consulting resources by IACP, including a helpful report on managing cybersecurity risk.[xxxix]

c. Agencies should also review the Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems issued by DHS.[xl] According to DHS, those recommendations intend to address "unsecured" drones that cannot be trusted from a cybersecurity perspective.[xli] As a result, the best practices are very restrictive and include the following recommendations, among others:[xlii]
   i. Ensure that the devices used for the download and installation of UAS software and firmware do not access the enterprise network;
   ii. Thoroughly review any license agreements prior to approval. During installation, do not follow "default" install options and disable automatic software updates;
   iii. Use standalone UAS-associated mobile devices with no external connections, or disable all connections between the Internet and the UAS and UAS-associated mobile devices during operations;
   iv. If using Wi-Fi, ensure the data link supports an encryption algorithm for securing Wi-Fi communications;
   v. Use the most secure encryption standards available and complicated encryption keys that are changed regularly;
   vi. Use a standalone computer to connect to the UAS or removable storage device to ensure no access to the Internet or enterprise network; and
   vii. Verify a firewall on the computer or mobile device is enabled to check for potentially malicious inbound and outbound traffic caused from the connection of the UAS or removable storage device.

2. **When developing or expanding a drone program, factor cybersecurity into the acquisition process.** Drones were formerly hardware-centric devices that did not rely on network connectivity. Those days are long gone. In reflection of that reality, cybersecurity should be a consideration in the acquisition of new drone technology. To guard against cybersecurity risks, agencies should ask questions about data storage, data transfer, and other aspects of cybersecurity and supply chain security. In addition to basic due diligence, DOJ recommends "strong consideration of procurement of UAS made domestically or by trusted allies, though each purchase decision will depend on the specific use case, mission requirements, and assessed risks."[xliii] Ultimately, the mission should drive the choice of technology, and every piece of technology should be purchased with cybersecurity in mind.

---

[i] DOJ's Office of Community Oriented Policing Services, PERF, *Drones: A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call about the Threat of Malicious Drone Attacks* (2020), https://cops.usdoj.gov/RIC/Publications/cops-w0894-pub.pdf ("COPS Report"); NIJ, *Considerations and Recommendations for Implementing an Unmanned Aircraft Systems (UAS) Program* (2016), https://www.ncjrs.gov/pdffiles1/nij/250283.pdf ("NIJ Report"); IACP, *Law Enforcement Policy Center, Model Policy on Small Unmanned Aircraft Systems* (2019), pages 2-5, https://tinyurl.com/y9a9slf4 ("IACP Model Policy."). We also highly recommend consulting and following recommendations from civil society stakeholders. For example, this document draws from the American Civil Liberties Union's (ACLU's) recommendations on the use of drones. *See* ACLU, *Domestic Drones*,

https://tinyurl.com/yayyv4ju ("ACLU Recommendations on Domestic Drones"); ACLU, *Protecting Privacy from Aerial Surveillance: Recommendations for Government Use of Drone Aircraft*, December 2011, https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf ("*ACLU Report on Protecting Privacy from Aerial Surveillance*").

[ii] COPS Report, at p. xiii.

[iii] *Id.* at 20.

[iv] *Id.*

[v] *Id.* at 18 (emphasis added).

[vi] Chula Vista Police Department, *UAS Drone Program*, https://www.chulavistaca.gov/departments/police-department/programs/uas-drone-program ("CVPD Website").

[vii] *See* ACLU Report on Protecting Privacy from Aerial Surveillance, at p. 16 ("While it is legitimate for the police to keep the details of particular investigations confidential, policy decisions regarding overall deployment policies—including the privacy tradeoffs they may entail—are a public matter that should be openly discussed.").

[viii] *See, e.g., id*. CVPD's website includes a "Drone-Related Activity Dashboard" that displays up-to-date information on the operation of the program.

[ix] *See, e.g., id.*

[x] *See* Lakewood Police Drone Program, https://cityoflakewood.us/police-homepage/lakewood_police_drone_program/; Fairfax County UAS Program, https://www.fairfaxcounty.gov/uas/unmanned-aircraft-systems.

[xi] *See, e.g.*, ACLU Report on Protecting Privacy from Aerial Surveillance, p. 15 ("To this end, the use of drones should be prohibited for indiscriminate mass surveillance, for example, or for spying based on First Amendment-protected activities.").

[xii] *DOJ Policy on the Use of Unmanned Aircraft Systems*, https://www.justice.gov/jm/9-95000-unmanned-aircraft-systems-uas ("DOJ UAS Policy").

[xiii] ACLU Recommendations on Domestic Drones.

[xiv] For an example of this approach in action, see DOJ's UAS Policy.

[xv] *Id.*

[xvi] *See* footnote 1.

[xvii] FAA, *Operate a Drone, Start a Drone Program*, https://www.faa.gov/UAS/public_safety_gov/drone_program/.

[xviii] FAA, *Drones in Public Safety: a Guide to Starting Operations*, https://www.faa.gov/UAS/public_safety_gov/media/Law_Enforcement_Drone_Programs_Brochure.pdf.

[xix] The COPS Report contains a long and helpful list of sample authorized missions. *See* COPS Report, at p. 43-47.

[xx] We recognize that public safety agencies are sometimes asked to use drones in support of other government agencies to conduct lawful and beneficial activities, such as surveying municipal buildings under construction. This document contains an illustrative, non-exhaustive list of such activities.

[xxi] IACP Model Policy, at p. 3.

[xxii] *See* ACLU Report on Protecting Privacy from Aerial Surveillance, at p. 15.

[xxiii] The foregoing list was directly adapted from page 61 of the COPS report (with added formatting).

[xxiv] FAA Reauthorization Act of 2018, Section 363.

[xxv] *Id.*

[xxvi] For resources on the topic of civilian oversight, consult the National Association for Civilian Oversight of Law Enforcement, https://www.nacole.org/.

[xxvii] NIJ Report, at p. 12.

[xxviii] IACP Model Policy, at p. 2.

[xxix] *See* ACLU Report on Protecting Privacy from Aerial Surveillance, at p. 16 ("[I]ndependent audits should be put in place to track the use of UAVs by government, so that citizens and other watchdogs can

tell generally how and how often they are being used, whether the original rationale for their deployment is holding up, whether they represent a worthwhile public expenditure, and whether they are being used for improper or expanded purposes.").

[xxx] *See id.*

[xxxi] Kevin Jinks, Remarks to the Presidential Commission on Law Enforcement: Reduction of Crime Technology Panel, *Opportunities and Challenges Posed by Unmanned Aircraft Systems to Public Safety and Achieving Law Enforcement and National Security Goals*, p. 366 (p. 4 of Mr. Jink's remarks) (April 21, 2020), https://www.justice.gov/ag/page/file/1277646/download ("Jinks Testimony").

[xxxii] *Id.*

[xxxiii] Jinks Testimony, at p. 366. For awareness, in June 2020, the U.S. Department of Homeland Security (DHS) expressed "concern[] with state and local governments using Chinese manufactured technology to support security and law enforcement operations." Christopher Krebs, Director, Cybersecurity & Infrastructure Security Agency, DHS, Letter to the Honorable Jerrold Nadler, Chairman of the House Judiciary Committee, June 23, 2020, p. 1, https://tinyurl.com/ybpbuo7k ("DHS Letter to House Judiciary Committee"). At the federal level, Congress banned the Defense Department from purchasing drones made in China in 2019. Congress is now considering the American Security Drone Act (S. 2502) (ASDA), which would prohibit all federal agencies from buying "covered UAS," defined to include drones made in China, by Chinese companies, or with certain components of Chinese origin. The ASDA would also apply to federal grants used to purchase drones, but that restriction would not go into effect until two years after enactment.

[xxxiv] DHS Letter to House Judiciary Committee, at p. 2 (FEMA "require[s] state and local governments to review and acknowledge [DHS] guidance before purchasing foreign manufactured UAS with Federal grant funding. Those wishing to continue with the purchase of a foreign manufactured UAS must provide a written justification that is screened against criteria that includes an assessment of the UAS manufacturer's country of origin."); DOJ UAS Policy ("[B]efore authorizing State, Local, Territorial, or Tribal agencies to use Federal grant funding to purchase or use UAS, components must ensure that the grant recipient has in place policies and procedures designed to safeguard privacy and civil liberties and mitigate cybersecurity risks.").

[xxxv] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[xxxvi] DHS, *Cyber Resiliency Resources for Public Safety*, August 2020, https://tinyurl.com/DHSresiliency.

[xxxvii] *Id.*

[xxxviii] *Id.*

[xxxix] IACP, Managing Cybersecurity Risk: A Law Enforcement Guide, April 2017, https://www.iacpcybercenter.org/wp-content/uploads/2015/04/Managing_Cybersecurity_Risk_2017.pdf. We also recommend an article on cybersecurity for law enforcement by Major Christian Quinn of the Fairfax County Police Department. Major Christian Quinn, Fairfax County Police Department, *The Emerging Cyberthreat: Cybersecurity for Law Enforcement*, Police Chief Magazine, December 12, 2018, https://www.policechiefmagazine.org/the-emerging-cyberthreat-cybersecurity/. Major Quinn oversees Fairfax County's highly regarded drone program.

[xl] DHS, CISA, *Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems,* June 2019, https://tinyurl.com/ybkhx4cx ("DHS Best Practices").

[xli] DHS Letter to House Judiciary Committee, at p. 1.

[xlii] DHS Best Practices.

[xliii] Jinks Testimony, at p. 366-67.