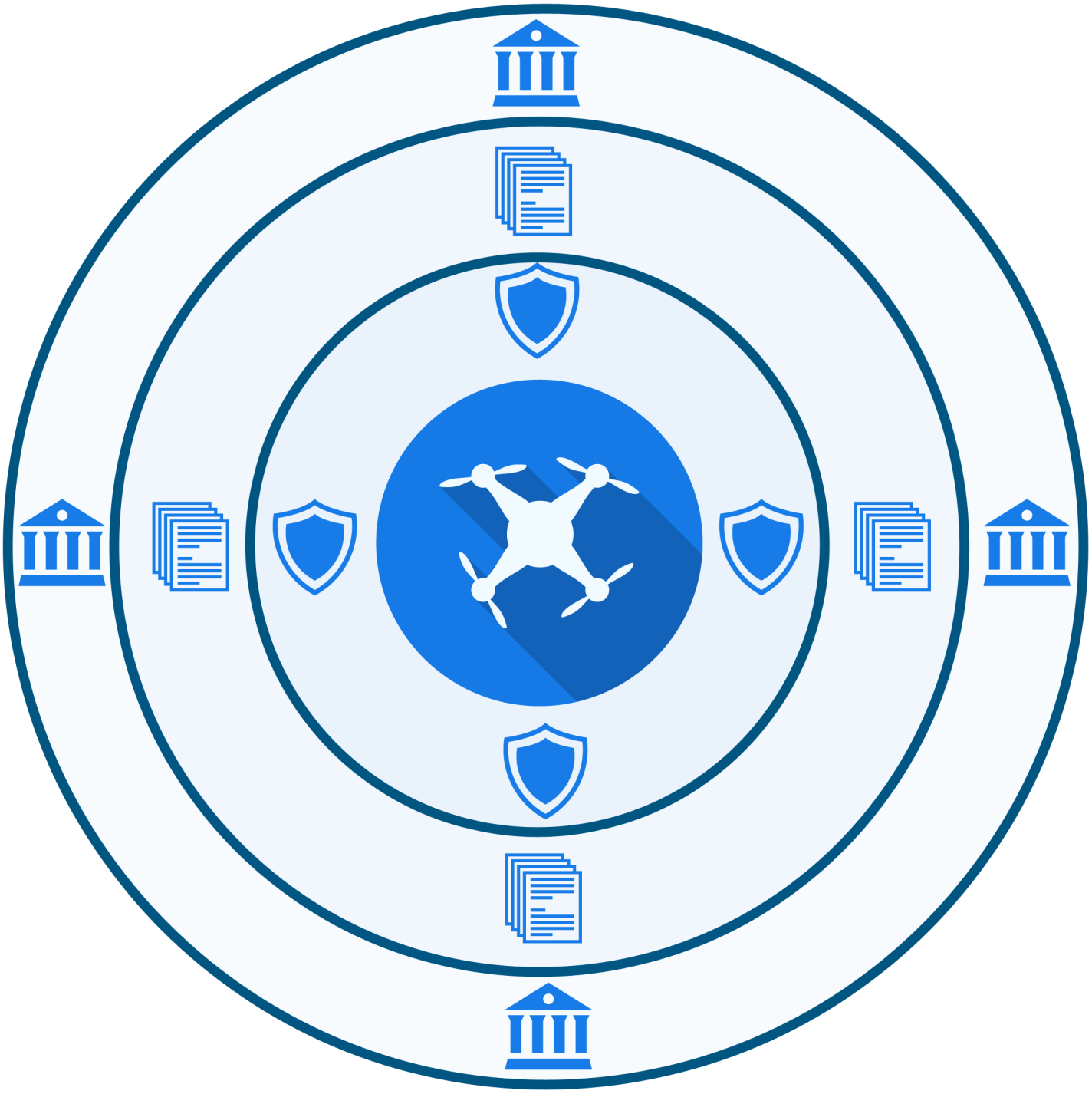
NASCIO
Representing Chief Information Officers of the States

Unmanned Aerial Systems, Governance and State CIOs: On the Radar



NASCIO Staff Contact:
Amy Hille Glasscock | Senior Policy Analyst

201 East Main Street, Suite 1405 Lexington, KY 40507 Phone: (859) 514-9153

Unmanned Aerial Systems, Governance and State CIOs: On the Radar

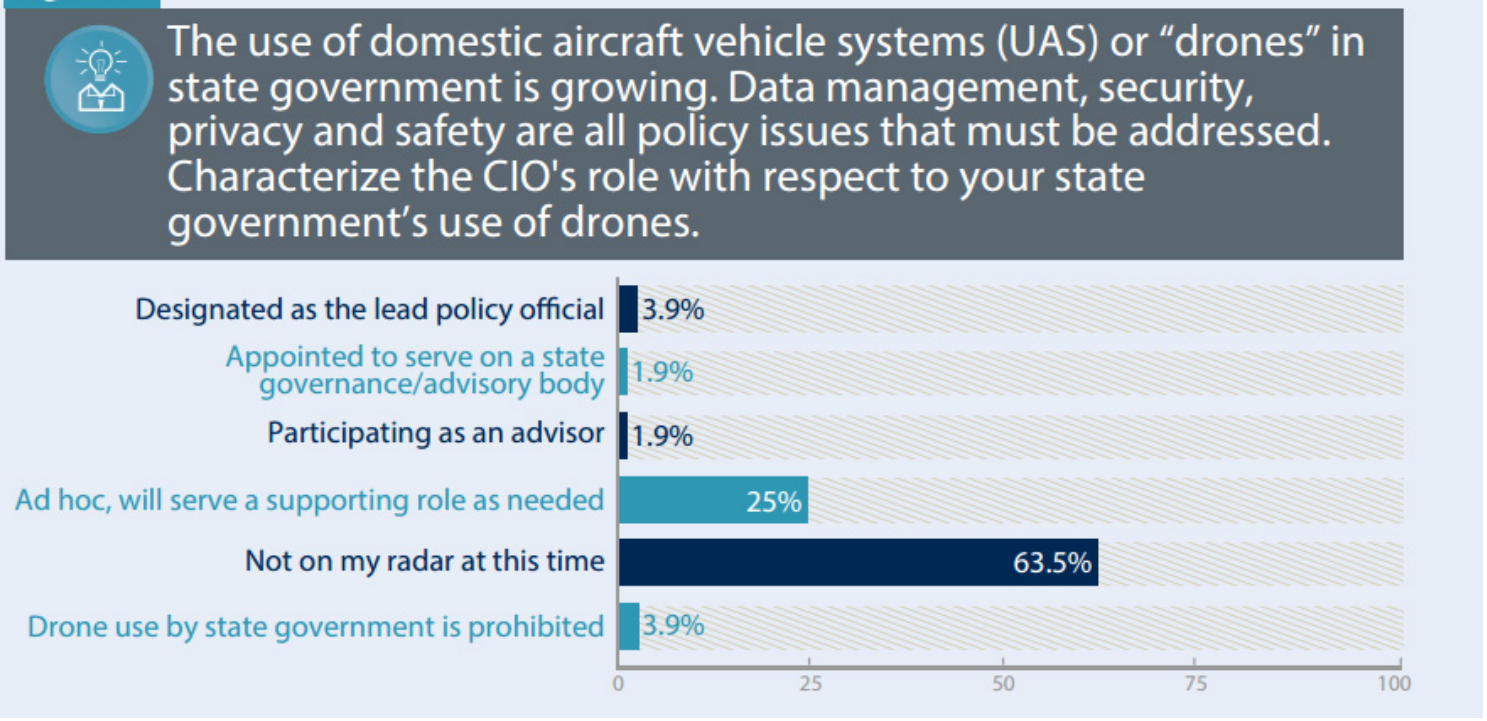
They're used to monitor crops, evaluate environmental concerns, provide disaster relief, monitor borders or for fun by amateur photographers. We call them unmanned aerial vehicles (UAV), unmanned aircraft systems (UAS), or simply drones, and they are becoming a more common sight in our skies.

The sale and manufacturing of UAS is on the upswing. In its 2014 UAS Market Profile, the Teal Group predicted the UAS market will total $91 billion in the next ten years. The group believes that 65% of worldwide research, development, test and evaluation (RDT&E) will come from the United States as well as about 41% of procurement.[1]

While the idea of operating a UAS certainly isn't a new concept—they have been used by militaries in some form since the early 1900s—UAS are gaining in popularity and usage among civilians. The Federal Aviation Administration (FAA) even put out a video in December of 2014 explaining how to stay off the naughty list and safely fly the unmanned aircraft that was received as a Christmas gift. The FAA and UAS industry advocates also created the knowbeforeyoufly.org website to provide guidance for safe operations of UAS by public entities and recreational and business users.

Much like in the commercial sector, demand for UAS use in state government is growing, as is legislative debate on the merits and associated issues. States must consider data management, security, privacy, and safety policy issues related to the use of UAS. Despite these important considerations, in NASCIO's 2014 State CIO Survey, 63.5% of respondents said that UAS were "not on my radar at this time" when asked about their role with respect to their state government's use of UAS.

Figure 38



1 Teal Group Predicts Worldwide UAV Market Will Total $91 Billion in Its 2014 UAV Market Profile and Forecast. http://www.tealgroup.com/index.php/about-teal-group-corporation/press-releases/118-2014-uav-press-release

So what does all of this mean for states, and state CIOs? UAS are here and they should be on your radar.

Legislative and Regulatory Landscape

Several states have been working on legislation to address UAS. According to the National Conference of State Legislatures, in 2013, 103 bills were introduced in 43 states. At the end of that year 16 new laws were enacted in 13 states, and 16 resolutions were adopted in 11 states. In 2014, 35 states considered bills or resolutions and 10 of those states enacted new laws. States that have enacted legislation include Virginia, North Carolina, Florida, Tennessee, Indiana, Illinois, Wisconsin, Texas, Montana, Idaho, Utah and Oregon.
States have a limited role in regulating UAS operations because the national airspace is controlled by the Federal Aviation Administration (FAA). States could, for example, enact laws about takeoff and landing from public property such as parks. The FAA has established regulations related to maximum altitude, not flying near airports or over crowds, and keeping UAS within the operators' line of sight. States do not have the authority to enforce laws that contradict the FAA's standards for use of the national airspace. Currently the FAA requires any state government agencies to get approval to fly UAS through a Certificate of Authorization (COA). From the FAA website[2]:

> *COA is an authorization issued by the Air Traffic Organization to a public operator for a specific UA activity. After a complete application is submitted, FAA conducts a comprehensive operational and technical review. If necessary, provisions or limitations may be imposed as part of the approval to ensure the UA can operate safely with other airspace users. In most cases, FAA will provide a formal response within 60 days from the time a completed application is submitted.*

In March 2015, the FAA released proposed rules laying out regulations for usage of small commercial UAS. The COA requirements still apply for government usage.

States Use UAS

State governments will find that the use of UAS is more useful, economical and often safer than using manned aircraft. State agencies use UAS in some of the following ways:

- Law Enforcement/Emergency Management
  - Search and rescue
  - Pre and post-disaster photos
  - Communications augmentation
- Homeland Security
  - Terrorism
- Agriculture
  - Drought conditions
  - Disease in crops

2 Certificates of Waiver or Authorization (COA) https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/coa/

  - Insect infestations
  - Livestock monitoring
- Geographic Information Systems (GIS)
  - Precise surveying and mapping
- Infrastructure Inspection
  - Bridges
  - Equipment parked on pipelines
  - Buildings and homes impacted by severe weather
- Public Buildings, Facilities and Asset Management
- Fish and Wildlife
  - Migration
  - Endangered species
- Environment and natural resources
  - Monitor air quality
  - Erosion
- Cultural
  - Historic sites
- Public Affairs
  - Video and photos of state events or parks
  - Promotion
- Traffic Monitoring
  - Accidents
  - Traffic conditions
- Local Emergency Management
  - Firefighting and fire spotting
  - Public safety
  - 911

The most common state agencies to use UAS are the departments of transportation, emergency management, environment/natural resources, public safety, commerce, and agriculture. State colleges and universities may also conduct research on UAS or want to utilize them for other purposes.

New Challenges

The main challenges states face in the increasing use of UAS has less to do with flight technology, and everything to do with the vast amount of data that will be created as a result. The increasing use of UAS means "big data" sensors are airborne, versatile, and inexpensive, and states are generating incredible amounts of data in the form of digital video, photos, GPS coordinates, and sound. Today a drone, using a standard camera to capture video and photos, can produce half a terabyte of data an hour.[3] On the extreme end, the Defense Advanced Research Projects Agency (DARPA) has developed ARGUS-IS, a 1.8 gigapixel video surveillance platform that can produce 6,000 terabytes of data a day.[4] As states take in such expansive and unstructured amounts of data there will be challenges.

Public Policy Considerations

Despite all the great benefits and uses of UAS technology, it is imperative that state CIOs consider several important issues before their states move forward.

Data Standardization

Most UAS applications on the state level involve data gathering in the form of photography, video or other recorded data. If UAS-gathered data is obtained by six different state agencies, it is likely treated six different ways. States should define a process for data collection, labeling, storage, retention, usage, sharing and deletion. States should also consider working with other states to streamline the process for cross-state information sharing, much like interstate highways and road signs are standardized nation-wide.

States will find that much of the collected data is public record, and they must deal with categorizing the data appropriately and should expect Freedom of Information Act requests and associated legal issues, especially when data is collected that could be used as evidence.

Privacy

While it can be argued that the data collected from UAS is no different from that collected from manned aircraft, privacy advocates have some concerns. For one, UAS are smaller and quieter than manned aircraft, so it may not always be obvious to a person that they are being monitored. In addition, it is less expensive to gather data using UAS instead of manned aircraft, and much more data will be gathered as a result. Video or photos of illegal activity may be captured unintentionally. Evidence gathered by *manned* aircraft is not considered to be the product of a "search," and therefore does not require a warrant. According to the Supreme Court, under the Fourth Amendment, an operation is considered a search, and therefore requires a warrant if a person has a reasonable expectation of privacy and the expectation is one that society would consider reasonable.[5] The International Association of Chiefs of Police (IACP) Aviation Committee recommends that UAS be painted a high visibility color, and that warrants be obtained if it is believed the UAS will collect evidence of wrongdoing and will intrude upon reasonable expectation of privacy.[6] States will need to have thoughtful consideration of Fourth Amendment issues and develop a comprehensive framework for separating data that does and does not require a warrant.

3 The Drone Economy Prepares for Takeoff. http://iq.intel.com/drone-economy-prepares-takeoff/
4 DARPA Shows Off 1.8-Gigapixel Surveillance Drone, Can Spot a Terrorist From 20,000 Feet. http://www.extremetech.com/extreme/146909-darpa-shows-off-1-8-gigapixel-surveillance-drone-can-spot-a-terrorist-from-20000-feet
5 Legal Information Institute: Fourth Amendment. https://www.law.cornell.edu/wex/fourth_amendment
6 Recommended Guidelines for the use of Unmanned Aircraft. http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf

Safety

The FAA has proposed rules for small commercial UAS for a reason—they can cause more harm than good if care is not taken. UAS must avoid crossing paths with manned aircraft, crashing into power lines, crashing into people, and causing traffic accidents. States should put in place regulations for the safety of UAS such as height limits for flying, restricted areas and required training for operators. IACP recommends that all operators be trained and certified and if possible alert people in the vicinity of a UAS operation. They also strongly discourage equipping UAS with any kind of weapon.[6]

Broadband Spectrum and Communications Infrastructure Concerns

As some state agencies move toward more effective use of UAS and instantaneous sharing of data, the state may need to address expanding broadband and communications infrastructure, particularly in rural areas. Additionally, if the FAA were to allow UAS control via manned relay or non-line-of-sight via tower or satellite relay, there are frequency deconfliction issues to be considered.

Security and Risk Management

Just as with other important information, states will need to consider the serious consequences if UAS devices and the data they collect are not secure. They should consider if a UAS can be hacked, and how to most securely store the collected data and protect the flight control frequencies. From a risk management perspective, there are many security dimensions to be considered, including issues of both cybersecurity and information security.

IT Asset Management

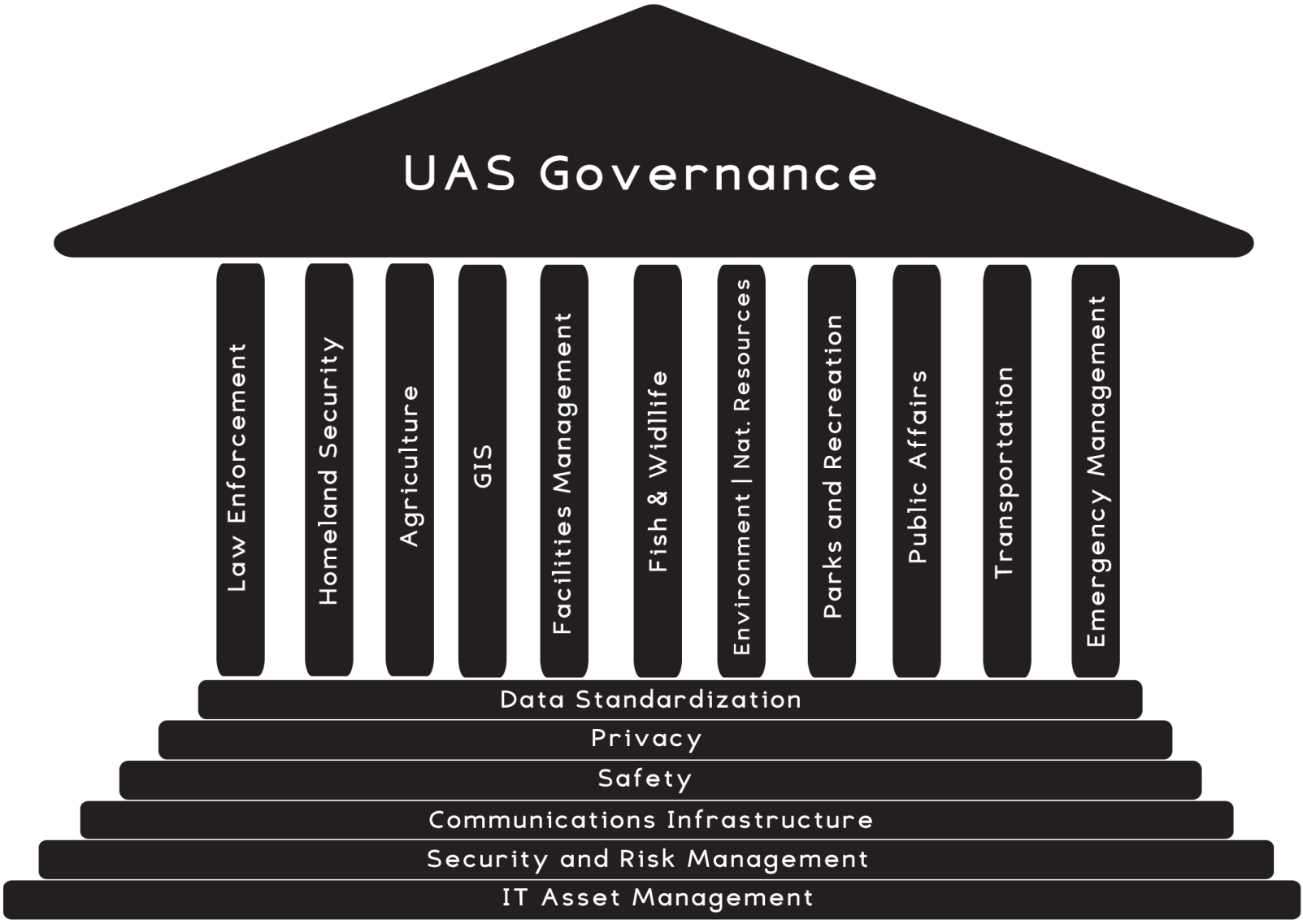
State CIO offices generally have enterprise policies requiring a current and accurate inventory of IT assets, both hardware and software. These policies support an important business practice to validate hardware deployment, software licensing information, disposal and security of hardware and software assets utilized by state agencies. As with any new information technology used in an enterprise as complex and diverse as state government, maintaining an inventory of agency UAS ownership, applications and ultimate disposition is recommended.

Governance

A few states have developed a governance structure such as a working group or advisory group for dealing with UAS. Groups like these can provide input to legislatures and agencies, or even be the body to approve UAS usage in the state. With a proper governance structure in place, the state will be better able to implement regulations on standardization, privacy, safety, infrastructure and security.

The sooner a governance structure for UAS is put in place the better. An overarching organizational framework is needed to fully integrate existing efforts of state agencies, identify policy concerns, formalize internal controls and anticipate issues that may arise. State agencies are already using UAS and gathering data without a cohesive structure in place. The more time that elapses between when UAS are deployed, data is gathered and when state guidance is put in place, the more work must be done to go back and re-organize stored data, deal with privacy challenges, address lawsuits due to safety issues, catch up with infrastructure needs, and manage the consequences of security incidents. Because of the visibility and public debate on the use of UAS, state CIOs should expect state auditors to add these devices to the list of technologies that fall under review of both security and performance audits.

Governance around UAS should be collaborative within the state and with other states if possible. It should also fall in line with the enterprise architecture of the state for the best results and outcomes.



The State CIO Role

With their enterprise view of technology acquisition, deployment and oversight, state CIOs are in a unique position to lead the governance of UAS. CIOs serve as the head of an office that regularly deals with all of these issues around the policy framework for new technology, communications infrastructure, data and cybersecurity. CIOs must determine whether they will play an advisory role or an authoritative role, keeping in mind that agencies have no requirement to follow advisory recommendations. It is likely that even if the CIO doesn't play a role in the governance of UAS, they will end up having to deal with the consequences of the lack of data governance, asset tracking or security controls. State CIOs should anticipate surprises; therefore governance over UAS should be done by design, not by default.

Contributors

Chris Estes
CIO, State of North Carolina

David Hinton
Special Advisor for Unmanned Systems at Office of the Secretary of Technology, Commonwealth of Virginia

Doug Robinson
Executive Director, NASCIO

Emily Lane
Programs and Brand Coordinator, NASCIO

FOLLOW NASCIO