PRIORITY Criminal Justice NEEDS INITIATIVE

A project of the RAND Corporation, the Police Executive Research Forum, RTI International, and the University of Denver

Countering the Emerging Drone Threat to Correctional Security

Joe Russo, Dulani Woods, Michael J. D. Vermeer, Brian A. Jackson

EXECUTIVE SUMMARY

Incarcerated individuals are conspiring to deliver dangerous contraband into correctional institutions using drones. In some cases, this contraband includes drugs and cell phones; in other cases, more-serious contraband, such as weapons and tools to facilitate escape, has been introduced via drone (Dix et al., 2022; Kravets, 2017). Correctional administrators routinely face evolving security threats; defending an institution's airspace and interdicting drone incursions represent relatively new and complex challenges that must be addressed.

The University of Denver and RAND, on behalf of the National Institute of Justice, hosted a workshop to explore the challenges and opportunities associated with preventing, detecting, and responding to drone incidents. The workshop, which was part of the Priority Criminal Justice Needs Initiative, a research effort intended to support innovation within the criminal justice enterprise, brought together a group of prison and jail administrators and other policy experts to identify and prioritize the key needs that, if addressed, would have the greatest impact on countering the threats posed by drones. (*Need* is a term we use to describe a specific requirement tied to either solving a problem or taking advantage of an opportunity to better address a challenge.)

Drone incursions are an emerging threat, one that many institutions have yet to address to any significant degree. As a result, there are many knowledge gaps that must be filled to better understand the threat and implement effective measures to counter it. One of the broad themes that emerged from the workshop is the need for a standard definition of the term *drone incident* to improve analysis of the nature and scope of the problem. Correctional staff might not be experts in drone technology and drone detection technology, fields that are rapidly evolving. Staff require support and guidance to assess their needs; understand the available options and their applicability to correctional use; and evaluate, select, and implement the appropriate solutions. Guidance is also needed to effectively incorporate technology solutions into core correctional security practices, as part of a multilayered approach to addressing the

SELECTED HIGH-PRIORITY NEEDS

RESULTS

Determining the scope of the problem

- Develop standard terminology and best practices for more-granular reporting of drone incidents.

Assessing risk and needs

- Develop corrections-specific vulnerability assessment tools for drone incidents based on relevant factors.
- Develop guidebooks to help agencies identify their needs, and articulate operational requirements and specific objectives for each facility.

Selecting, acquiring, and implementing solutions

- Develop resources and support (e.g., templates, guides) to help those agencies that do not have grant-writing expertise prepare quality proposals.

Testing and evaluating solutions

- Develop minimum performance standards for drone detection solutions (e.g., detection rates, false-alarm rates, detection range, tracking capabilities, identification capabilities, alert notification system capabilities, regulatory compliance).
- Conduct operational evaluations of configurations of layered approaches (e.g., radio frequency, acoustic sensors, radar, cameras, intrusion detection, netting, correctional practices) to determine the most-effective methods of deterring drone activity and/or detecting drones in a timely manner to allow staff to intercept contraband.

Policy and practice

- Develop best practices for using intelligence sources to interdict and/or investigate drone incidents.
- Develop (or expand an existing) national data-sharing system to report and track drone incidents.

threat. Finally, several needs were related to the legal and regulatory landscape pertaining to drones; these included

- better education about the gravity of threats posed to both institutional security and broader public safety
- better awareness of the legality of certain detection solutions
- the need for more-effective deterrents (e.g., stiffer penalties for drone incursions and more-aggressive prosecution)
- support for the development of solutions to safely and cost-effectively neutralize drones and, if solutions are successfully developed, removal of barriers to their deployment.

WHAT WE FOUND

Workshop participants identified and prioritized 29 needs. Thirteen needs were ranked as high-priority, and the following themes emerged:

- Standard terminology defining a drone incident and national data collection and reporting are required to better quantify the extent of the drone problem.
- Guidance is needed for agencies to assess an institution's vulnerability to drone incursion, articulate the associated operational requirements and objectives, select the appropriate solutions, and effectively implement those solutions to achieve the objectives.
- Drone technology, solutions to detect drones, and the associated legal and regulatory landscape are rapidly evolving. Administrators need access to independent and objective sources of current and accurate information so that they can make better technology selection decisions.
- Testing and evaluating drone detection solutions can be challenging. Minimum performance standards are needed, as well as operational evaluations of solutions in varying configurations (e.g., radio-frequency detection with radar) to assess the effectiveness of these solutions in a correctional environment.
- Because drones represent a relatively new threat, administrators would benefit from best practices to better leverage core correctional practices, including intelligence, investigations, and forensics, as part of a multilayered approach to addressing the threat. Furthermore, detailed reporting of incidents (e.g., drone used, flight data, payload, packaging characteristics) to a secure, shared national database would support the investigative process.
- Drone detection technology can be expensive, and acquisition can be difficult to justify. Agencies need (1) guidance on how to quantify the return on investment for these technologies and (2) templates and guides to help prepare grant proposals.

Drone incursions are an emerging threat, one that many institutions have yet to experience to any significant degree. As a result, there are many knowledge gaps that must be filled to better understand the threat and implement effective measures to counter it.

INTRODUCTION

Correctional institutions face an array of security threats. Some threats, such as violence and escape, have existed since early civilizations first conceptualized incarceration to remove individuals from society. While these threats remain, societal shifts and technological advancements continually present new and complex challenges. For example, in recent years, contraband cell phones and the advent of synthetic drugs have posed new threats, which, in turn, require innovative responses and countermeasures (Russo et al., 2019). Today, correctional administrators face yet another challenge: securing their institution's airspace. Across the United States—and, indeed, the world—unmanned aircraft systems, or *drones*, are emerging as one of the latest threats to correctional security (Crumley, 2023). Incarcerated individuals are coordinating with conspirators in the community to deploy drones to infiltrate these institutions. While most of this activity involves the delivery of contraband, such as drugs and cell phones, there have also been reports of incursions intended to facilitate escape attempts, surveil institutions, and/or attack institutions (Dix et al., 2022).

To explore the challenges and opportunities associated with preventing, detecting, and responding to the threats posed by drones to correctional security, project staff assembled a group of prison and jail administrators and other policy experts and held a workshop, titled "Drones: Countering an Emerging Threat to Correctional Security." This workshop was part of the Priority Criminal Justice Needs Initiative (PCJNI), a research effort intended to support innovation within the criminal justice enterprise. This report details the methodology of the workshop and key findings and recommendations that emerged. Throughout the report, comments from experts who participated in the workshop are presented in gray quote bubbles. The workshop participants and their affiliations are shown in the box at right.

PARTICIPANTS

Joel Anderson
South Carolina Department of Corrections

Todd Craig
Federal Bureau of Prisons (retired)

Dustin Flanery
Tennessee Department of Correction

Brandeshawn Harris
North Carolina Department of Adult Correction

Wes Kirkland
Florida Department of Corrections

Vinko Kucinic
Ohio Department of Rehabilitation and Correction

Shawn Laughlin
Broomfield Police Department Detention and Training Center (Colorado)

Ben Mendoza
California Department of Corrections and Rehabilitation

Elizabeth Quillen
Virginia Department of Corrections

Ghislain Sauvé
Correctional Service Canada

Brent Travelbee
Michigan Department of Corrections

Mark Wasylyshyn
Wood County Sheriff's Office (Ohio)

Paul Wilder
Texas Department of Criminal Justice

Quantifying the Scope of the Problem

There are no publicly available national statistics regarding the frequency of drone incursions into correctional institutions; however, there is some evidence to suggest that, in some jurisdictions, the problem is significant and growing rapidly.

> "[Correctional institutions] get assaulted almost daily."

Drones were first sighted over institutions as early as 2013 (Teale, 2023), and what began as a rare occurrence is now a daily challenge for some agencies. For example, between 2013 and 2016, the Georgia Department of Corrections reported a total of three drone sightings (Travis, 2018), but in 2018 alone, approximately 300 sightings were reported (Bruce, 2021). Similarly, the South Carolina Department of Corrections reported 262 drone incidents in 2022, up from 69 in 2019 (Ashworth, 2023). At the national level, the Federal Bureau of Prisons has described drones as a major security threat (Office of the Inspector General, 2020). The agency reported that

drone incidents have steadily increased since it began collecting data in 2015, and, in 2019, the number increased by more than 50 percent over the previous year (Office of the Inspector General, 2020). Finally, according to a 2020 survey of prisons conducted by the National Gang Crime Research Center, more than one-third of respondents reported that drones had been used to smuggle contraband into their institutions (Knox and Gilbertson, 2020).

"It's an epidemic at this point. It's a daily occurrence, and I'm sure there's many more that go undetected."

These limited data represent a partial picture because, for a variety of reasons, drone incidents are likely significantly underreported (Dix et al., 2022). For example, the corrections sector lacks standard terminology for what constitutes a *drone incident*; furthermore, data collection and reporting within agencies may be unreliable (Office of the Inspector General, 2020). Definitional issues aside, it can be very challenging to detect a drone (Michel, 2019). As discussed in more detail below, human observation is an imperfect method, and emerging drone detection systems have gaps and limitations. That said, in the relatively few institutions in which drone detection technology is used, the number of reported sightings has increased substantially since the deployment of this technology (Dix et al., 2022). Ultimately, untold numbers of drone incidents go undetected and unreported, making the frequency of drone incursions almost impossible to quantify.

"We've only had four documented incidents, but we don't know what we don't know."

Drivers of Drone Incidents

Historically, drones were developed and used for military purposes; however, in the past decade, "the consumer drone market has experienced unprecedented growth" (Kitanovic, 2022; Vyas, 2023). Over the period from 2012 to 2023, the number of drone manufacturers has increased, and competition has driven down consumer prices. Today, small drones are relatively inexpensive and accessible to most people. Furthermore, such features as autonomous flying and obstacle avoidance sensors have made drones much easier to operate right out of the box (Dix et al., 2022). As of 2022, more than 1 million recreational drones were registered with the Federal Aviation Administration (FAA); however, countless others were unregistered (Jordan, 2023).

"[The criminal use of drones is] a low-risk, high-reward proposition."

Increased accessibility of drones has been a boon to hobbyists and commercial industries; however, criminal elements are also taking advantage. Incarcerated individuals and their conspirators have recognized that the use of drones to deliver contraband, which can be resold inside the institution, can be highly lucrative. Compared with more-traditional methods of contraband introduction (e.g., mail, visitors, corrupt staff, throw-overs [i.e., contraband thrown over the prison wall]), drones can move much larger quantities in a single flight. Drops containing upward of 32 cell phones and 8 pounds of marijuana have been reported (Marnin, 2022; Ormseth, 2023; Wallace, 2020). Conspirators operating drones can make up to $4,000 per flight, and each payload can be worth $90,000 or more based on "prison value"[1] (Knox and Gilbertson, 2020). The drones themselves are relatively inexpensive and somewhat expendable (Atherton, 2020). While some drone incidents are one-offs, organized criminal groups have coordinated multiple incursions to the same institution. In some cases, these groups have operated fleets of drones to deliver contraband to several institutions in a state (Bischoff, 2023; Chavez, 2023; Ormseth, 2023). These groups likely also engage in interstate operations, though such operations have not been officially documented.

"There's big money to be made. An iPhone can go for $4,000 or more."

"It's very hard to respond in time to catch the drone operator in the act."

Finally, although several major federal and state investigations have resulted in arrests and successful prosecutions (Bischoff, 2023; Dix et al., 2022; Villarreal, 2023), it appears that, for a variety of reasons, the risk of apprehension remains relatively low (Wolfe, 2019). For example, conspirators can control a drone from great distances—miles, in some cases—from the target institution (Jay, 2022), well outside the purview of correctional staff. Furthermore, the drone can be operated autonomously, beyond the conspirators' line of sight, to deliver contraband to a designated point that has been coordinated with an incarcerated individual. In many cases, the conspirators can quickly launch the drone, deliver the payload, and return it undetected, minimizing the risk of apprehension.

"There is not much teeth in legislation . . . . Unless [the conspirators] are caught with the contraband, it's hard to prosecute."

A patchwork of overlapping laws and regulations (e.g., FAA regulations and federal, state, and local laws) apply to the operation of drones in general, flight over correctional institutions in particular, and the introduction of contraband. For example, several states have enacted legislation characterizing correctional facilities as critical infrastructure and have criminalized the act of flying a drone over or near these facilities (National Conference of State Legislatures, 2023). In some states, laws explicitly prohibit the introduction of contraband to a correctional facility via drone. Depending on the state and the case circumstances, violations can be treated as misdemeanors or felonies. Criminal penalties are also attached to violation of FAA rules. For example, the Bureau of Prisons has secured temporary flight restrictions that prohibit drone flights over the majority of its facilities, and violators face up to a year in prison (Sheehan, 2019; Office of the Inspector General, 2020). Furthermore, operation of an unregistered drone anywhere in the United States is punishable by up to three years of imprisonment (Sheehan, 2019). That said, cases can be challenging to prosecute (Link, 2022). Given the potential for high rewards,

"FAA violations are not enforced."

the consequences of conviction might not be a sufficient deterrent for determined conspirators and incarcerated individuals with little to lose (Office of the Inspector General, 2020).

Specific Threats

Drones pose a variety of threats to correctional institutions. For example, incarcerated people, often affiliated with criminal groups operating both inside and outside of institutions, are arranging the delivery of a variety of dangerous contraband, including drugs, cell phones, cell phone chargers, and SIM cards (Knox and Gilbertson, 2020). In the words of U.S. Attorney Chad Meacham, "Contraband drone deliveries are quickly becoming the bane of prison officials' existence. Illicit goods pose a threat to guards and inmates alike—and when it comes to cell phones, the threat often extends outside prison walls" (Pavlo, 2022).

"If we didn't have a contraband cell phone problem, we wouldn't have a drone problem."

Cell phones are one of the most dangerous forms of contraband in an institution. They have been used to plan the murders of witnesses in the community, facilitate escapes, arrange attacks on correctional staff, and coordinate disturbances (Hynes and Jordan, 2019). Cell phones have also been used to terrorize victims and operate ongoing criminal enterprises ranging from drug trafficking to elaborate wire fraud and money laundering schemes. Furthermore, cell phones are often used to covertly plan drone deliveries of even more cell phones, as well as other contraband (Chavez, 2023; Ormseth, 2023; Walsh, 2022). A phone's native location services can be exploited to guide a drone directly to an incarcerated person's cell window (Ormseth, 2023; Travis, 2018).

"When inmates get high, it can lead to assaults on staff."

Drug trafficking organizations have used drones to deliver large quantities of dangerous drugs, such as cocaine, heroin, methamphetamine, and synthetics (Bruce, 2021; Powell, 2022). The impact of drugs on the safety and security of an institution is well understood. For example, violence may increase as rivals

fight for control of the black market inside the institution. In Ohio, a fight broke out among several incarcerated individuals as they tried to recover an errant delivery of drugs ("Drone Drops Drugs in Ohio Prison Yard, Spurring Inmate Fight," 2015). Individuals under the influence of drugs may be more prone to violence when interacting with staff and their peers (Esack, 2018), and individuals who are unable to pay their drug debts are vulnerable to physical harm. In addition, the risk of overdose is elevated. For example, a package of drugs tainted with fentanyl was dropped into a Canadian prison, resulting in the death of one incarcerated individual and medical intervention for 48 others (Braich, 2023).

> "A major concern is that a drone can easily drop a loaded weapon that can be used against our staff. That keeps me up at night."

Although much less frequent, there have been reports of more-serious contraband deliveries, such as guns, ammunition, and ceramic knives, which pose immediate threat of harm to staff and incarcerated individuals (Braich, 2023; Ling, 2015; Link, 2022). For example, in Italy, an incarcerated individual fired shots using a handgun that Italian authorities believed was delivered by drone ("Italian Prisoner Shoots at Rivals with Gun 'Smuggled in by Drone,'" 2021). Anticipating worst-case scenarios, correctional administrators have expressed the concern that "individuals [could use] a drone offensively by arming it with firearms or explosives and targeting persons on the ground" (Office of the Inspector General, 2020, p. 2). Reports indicate that a drug cartel deployed three drones to drop explosives over a prison in Ecuador in an attempt to kill leaders of a rival cartel (Hambling, 2021).

> "If staff don't feel safe, it's hard to keep them."

Drones have directly and indirectly facilitated escape attempts. Escape tools, such as cell phones, wire cutters, and hacksaw blades, have been dropped into institutions (Ellison, 2022; Harvey, 2018; Williams, 2015). In South Carolina, an escape was facilitated by a cell phone and wire cutters that investigators believed had been delivered by drone (Levenson and Jones, 2017). Drones have also been used to surveil institutions to aid in escape planning. For example, drones were used to conduct reconnaissance in preparation for a mission to helicopter a notorious gangster out of a French prison (Andrews and Bradpiece, 2018). As technology advances and costs come down, it could become feasible for a consumer drone to bear the weight of an incarcerated person, and drones could be used instead of helicopters to facilitate escape via air (Office of the Inspector General, 2020).

Addressing the Drone Threat

Some correctional administrators have argued that actively mitigating or defeating drones is the best way to eliminate the threat (Ashworth, 2023). Mitigation capabilities generally fall into two categories: nonkinetic and kinetic. Nonkinetic mitigation approaches include the use of signal jamming, hacking, spoofing, and nondestructive directed-energy weapons to disrupt or disable drones (U.S. Department of Justice [DOJ], U.S. Department of Transportation [DOT], Federal Communications Commission [FCC], and U.S. Department of Homeland Security [DHS], 2020; Thompson, 2022). Kinetic solutions employ physical measures, such as projectiles and net launchers, to shoot down or capture drones (Rupprecht, undated). Technology developers offer a variety of mitigation solutions, some of which are being tested under the auspices of the FAA; however, federal law prohibits state and local correctional institutions from deploying these solutions (Dix et al., 2022). Legal limitations notwithstanding, there are significant questions about the practicality, safety, and effectiveness of these approaches, suggesting that further development is required before they may be considered viable (Michel, 2019).

> "The technology is out there, but we know we can't shoot [the drones] down or interfere with them. . . . We need mitigation options when a drone is over our facility."

Therefore, correctional institutions must assume a detect-and-respond posture. That is, they must be able to identify, locate, and track a drone; alert staff; and quickly execute a response plan designed to search for and safely recover the drone and/or the payload before it reaches the intended recipient and circulates within the institution. Most institutions rely on human observation for detection, but this is problematic for several reasons. For example, many agencies are experiencing

significant staff shortages (Duncan, 2023; Pavlo, 2022; Thrush, 2023), and perimeter patrols and tower posts might not operate at full capacity, particularly during overnight hours, when most drone activity is likely to occur (Girten, 2022). Furthermore, at a distance, drones can be virtually invisible to the naked eye or mistaken for a bird or another object (Dix et al., 2022; Michel, 2019), and the sound of a drone can be easily misinterpreted.

Drone Detection Systems

To help overcome the limitations associated with human observation, technology developers are increasingly marketing drone detection systems to the corrections sector, and several of these systems have been piloted and deployed in the United States (Ashworth, 2023; Coppola, 2017; Travis, 2018). These systems may leverage a variety of techniques; see Table 1.

Remote electronic identification technology is another method that is deployed. This approach enables the detection and tracking of drones from a specific manufacturer (e.g., DJI), and it can provide key information, such as model type, altitude, speed, direction, and serial number (Michel, 2019; Park et al., 2021).

As Dix et al. (2022) and Michel (2019) point out, no detection system is close to perfect; all have weaknesses. For example, radar systems may struggle to detect small drones and may misidentify other objects, such as birds. Camera systems are challenged by weather and low-visibility conditions. Radio-frequency (RF) systems detect only frequency bands in a preset library, and sensors may be affected by electromagnetic interference common in urban environments. Acoustic sensors rely on a library of sounds emitted by known drones; however, as new drone models emerge, the library will never be fully up to date. To help compensate for these limitations, technology providers often integrate two or more sensor types to improve probability of detection. That said, both drone technology and drone detection technology are evolving rapidly, which is a complicating factor. Experts have expressed concerns about the effectiveness of detection systems in an operational environment, noting that their performance is often not as advertised (Michel, 2019).

> "Systemwide, we are spending over $1 million on drone detection technology."

As opposed to mitigation technology, the use of drone detection systems is generally permissible by state and local agencies; however, there are nuances, and agencies should seek legal counsel before acquiring and deploying such systems. For example, some systems may be subject to FAA and FCC laws and regulations, and RF-based systems that detect and track drones by monitoring the communications between the controller and the drone may be subject to federal surveillance law, such as the statute on pen registers and trap and trace devices (18 U.S.C. Chapter 206) and the Wiretap Act (18 U.S.C. Chapter 119; DOJ, DOT, FCC, and DHS, 2020).

Table 1. Terms Related to Drone Detection

Term	Definition
Radar	Detects the presence of small unmanned aircraft by their radar signature, which is generated when the aircraft encounters radio frequency pulses emitted by the detection element. These systems often employ algorithms to distinguish between drones and other small, low-flying objects, such as birds.
Radio-frequency (RF)	Detects, locates, and in some cases identifies nearby drones by scanning for the frequencies on which most drones are known to operate.
Electro-optical (EO)	Identifies and tracks drones based on their visual signature.
Infrared (IR)	Identifies and tracks drones based on their heat signature.
Acoustic	Detects drones by recognizing the unique sounds produced by their motors. Acoustic systems rely on a library of sounds produced by known drones, which are then matched to sounds detected in the operating environment.
Combined sensors	Many systems integrate a variety of different sensor types in order to provide a more robust detection, tracking, and identification capability.

SOURCE: Reproduced from Michel, 2019, p. 3.

Conspirator Countermeasures

Regardless of whether an institution uses drone detection technology, the ability to effectively detect and respond to an incident is often challenged by the actions of conspirators. For example, some drone manufacturers use geofencing to prevent their devices from flying over sensitive locations, such as correctional institutions (Park et al., 2021). However, conspirators can circumvent geofencing in a variety of ways, including by building their own drones without this functionality, hacking into the operating system to shut off the native functionality, or using GPS spoofing to trick the geofencing software into believing that the drone is in an innocuous location (Bubna, 2022). Conspirators can also turn off the RF signals for the drone and the controller and instead use GPS waypoints for autonomous navigation along a preplanned flight path; the drone becomes "dark" in the sense that it is invisible to RF-based detection systems (Dix et al., 2022). Drones may be built, or modified, with designs and materials that increase stealth, making detection more difficult for radar-based systems (Michel, 2019). Other common measures include flying unregistered drones, flying at very high altitudes before and after a drop, and making nighttime incursions with tape covering the drone's lights (Chavez, 2023; Dix et al., 2022; Kotowski, 2021; Thompson, 2022; Villarreal, 2023). Electronic identification systems can be compromised by overriding a drone's ability to broadcast information, thereby defeating detection; by masking the drone's registration information to obscure the operator's identity; or by using a less popular drone that is unattached to an identification system (Skove, 2022). Conspirators have also been known to use multiple drones, or *swarms*, to surveil institutions to see where staff are deployed, or they may use one drone to attract staff to a location while another drone delivers contraband to an unguarded part of the institution (Ashworth, 2023; DOJ, DOT, FCC, and DHS, 2020).

"They jailbreak the drones all the time. [The drones] fly at 1,000 feet."

"Criminals know that we are good at detecting DJI drones, so they go to Parrot or SwellPro—[drones] that are harder to detect."

Response

When a drone is detected, through a detection system, human observation, or other means, the operational response becomes critically important. Institutions must have processes in place that address such issues as identifying and assessing the threat; determining the direction of flight; ascertaining whether a payload has been dropped and, if so, deploying staff to secure the incarcerated population; searching for and recovering the contraband; safely recovering the drone while preserving evidence; and, if possible, coordinating a law enforcement response to the drone operator's location (Dix et al., 2022).

Correctional institutions may also take measures to prevent a drone incident or to gather evidence to support investigation and prosecution. For example, core correctional practices, such as monitoring communications, conducting frequent searches, leveraging informants, and hardening vulnerable points, can help interdiction efforts. Trail camera surveillance at the perimeter can capture images of a drone operator (Marnin, 2022), while institutional closed-circuit television (CCTV) can capture a drone drop and the individual or individuals who retrieve it (Johnson, 2019). Fingerprints and forensics on recovered drones, payloads, and confiscated contraband cell phones can help identify conspirators and link them to incarcerated individuals and specific incidents. Furthermore, institutions often partner with law enforcement to share information about plots, surveil areas outside the perimeter, and support investigations.

As drone technology continues to advance and become more affordable, incursions into correctional institutions likely will continue to pose a security threat. At this point, there is no easy solution, and institutions must apply a layered security approach that includes technology solutions, vigilant application of core correctional practices, well-trained staff, and law enforcement partnerships to address the threat (Dix et al., 2022).

METHODOLOGY

For the workshop (mentioned above), a pool of candidate participants was identified in consultation with the National Institute of Justice (NIJ). Candidates were identified via existing networks, focused searches for organizations and individuals with relevant experience, and referrals. Ultimately, a group of 13 correctional security experts was convened. Each participant was well versed in the threats posed by drones. Several of

the agencies represented had experienced significant numbers of incursions and had subsequently implemented measures to counter the threats.

The workshop was conducted in two stages. During the initial stage (in early April 2023), project staff conducted interviews with each participant via a web-conferencing app. The length of these interviews ranged between 45 and 60 minutes. The purpose of the interviews was to gather participant insights on the challenges posed by drone incursions, the scope of the problem, and what agencies need to better address these challenges. Project staff provided an outline of discussion points in advance of the interviews; however, participants were encouraged to speak about the issues most germane to them according to their roles and experiences. Discussion points were as follows:

- Describe the extent of drone incursions in your facilities and their impact on security and operations.
- Are there challenges and needs related to quantifying the extent of the problem? For example, are there clear definitions for what constitutes a *drone incident*? Are data collected in a systemic manner?
- What countermeasures are being taken? What has been most successful or least successful?
- What are the challenges and needs related to technology approaches to deter, detect, and track drones? For example, are the approaches effective, reliable, accurate, and affordable? Where are the gaps or limitations? Are there needs related to evaluating the options?
- What are the challenges and needs related to lower-tech approaches (e.g., cameras, netting, hardened windows, clearing perimeters)?
- What are the challenges and needs related to policy and procedure, staffing, and training to deter or respond to drone incursions? Are best practices needed in particular areas?
- What are the challenges and needs related to optimizing intelligence (e.g., leveraging inmate communication systems, informants, and forensic capacity to interrogate recovered drones) to interdict drone activity?
- What are the challenges and needs related to partnerships with local law enforcement and prosecutors to address drone activity?
- What legislative changes are needed, if any?
- Are there any research- or evaluation-related needs (for example, studies to determine best practices for mitigating threats or disseminating effective strategies among peers, guidebooks on effective layered security models for various operational environments, independent test and evaluation of technology approaches)?
- What are the considerations for planning of future institutions (e.g., design, sighting)?
- What are other major challenges and needs?

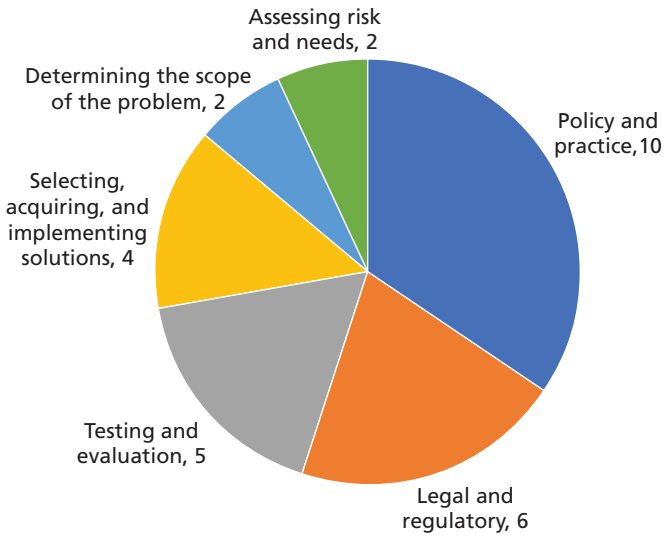
Project staff captured participants' input and synthetized it into an initial list of 19 problems with 29 associated *needs*, a term we use to describe a specific requirement tied to either solving a problem or taking advantage of an opportunity to better address a challenge.[2] The list of problems and needs was provided to the participants so that they could review it in preparation for the second stage of the workshop. In this stage, project staff convened the participants for in-person meetings in Washington, D.C., on April 26 and 27, 2023. During these meetings, the participants fine-tuned the wording of the problems and needs and identified additional problems and needs that had not been previously raised. The participants were then led through an exercise to prioritize the revised needs on the basis of two dimensions: the importance of the need (*importance*) and the probability that the need would be successfully addressed (*probability of success*). During this process, facilitators drew on participant input to add new needs and consolidate some needs that were closely related. Ultimately, a final set of 29 needs emerged; these were then clustered into three groups: high-, medium-, and low-priority (also referred to as Tier 1, Tier 2, and Tier 3) needs. More details on the methods used to structure the workshop and identify and prioritize the needs are provided in the technical appendix. The following section describes the results of the prioritization exercise.

RESULTS

The 29 needs identified by the participants were organized into six major categories: *determining the scope of the problem*; *assessing risk and needs*; *selecting, acquiring, and implementing solutions*; *testing and evaluating solutions*; *policy and practice*; and *legal and regulatory issues.* See Figure 1 for the distribution of needs across the six categories. (The full list of needs is provided in Table A.2, in the technical appendix).

The prioritization exercise, which we describe in greater detail in the technical appendix, elicited participant rankings of the importance and probability of success of the identified

Figure 1. Total Number of Needs, by Category (*n* = 29)



needs. These rankings were used to sort the needs into the three tiers mentioned above. Ultimately, 13 of the needs fell into Tier 1 and were categorized as high-priority needs; these are shown in Table 2. Figure 2 shows a breakdown of the high-priority needs by category. We discuss the high-priority needs in greater detail in the next section. As a result of the prioritization exercise, none of the needs in the legal and regulatory issues category fell into Tier 1, so this category is omitted from Table 2, Figure 2, and the discussion.

DISCUSSION

Determining the Scope of the Problem

Quantifying the prevalence of drone incidents is important for several reasons. Such data can help agencies determine the resources required and help support funding requests for solutions to address the issue. Furthermore, data can provide a baseline that can be used to measure the impacts of solutions on drone incidents. That said, quantifying drone incidents can be challenging, according to the workshop participants.

> "Leadership asks, 'How big is the problem?' But we just don't know what we don't know."

As we discussed earlier, drones are difficult to detect, and an unknown percentage of incursions simply go without notice.

Human observation of a drone is very challenging, particularly at night, and can be subjective. Participants noted cases in which staff reported a drone incident on the basis of visual or auditory observation; however, the incident was unsubstantiated and likely the result of staff misidentifying what they saw or heard. On the other hand, participants described other situations in which a contraband package was recovered and staff could intuit that it was delivered by drone, even if the vehicle was not observed and confirmed. For example, packages found on the roof or with fishing line attached are almost certainly the result of a drone delivery, as opposed to a throw-over, according to participants.

> "We often hear that staff think they see or hear a drone, but it can be hard to validate."

Like any technology, drone detection systems are not perfect. They can produce false positives by misidentifying a drone or false negatives by not detecting one. An additional layer of nuance is presented by some drone detection systems, which assign a threat level to the incident based on such factors as range to the perimeter, speed, and direction, so that not all sightings are equal in terms of the actual threat but all could be characterized as *incidents*. Ultimately, *incidents* could include such variations as a suspected sighting, a confirmed sighting, a suspected drop, a confirmed drop, a recovered drone, and the apprehension of a conspirator in possession of a drone. To better quantify the scope of the problem and allow consistent comparisons across institutions, the participants recommended the development of standard terminology to describe the various types of drone incidents in the correctional environment, as well as best practices to guide more-granular data collection and reporting and coding of incidents in institutional data systems.

> "Documenting these incidents has been pretty loose. There are a ton of variables, and we don't have a real good definition."

Table 2. The 13 High-Priority Needs, by Category

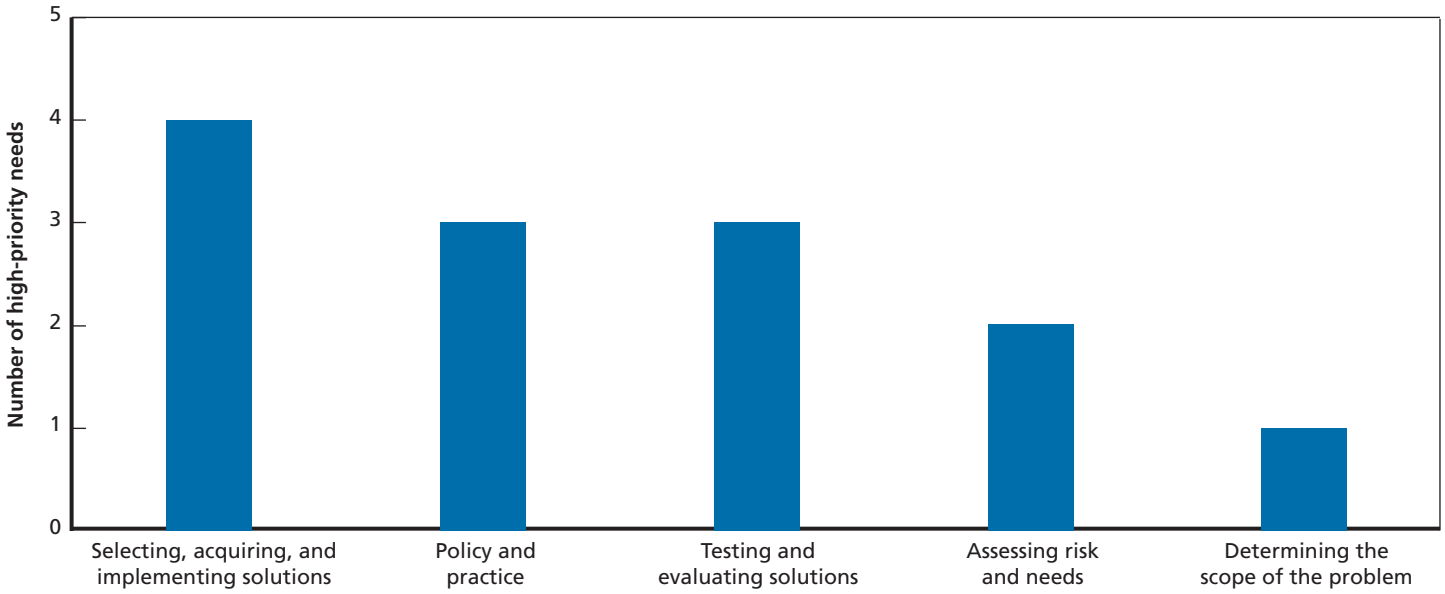
Problem or Opportunity[a]	Potential Solution	Tier
Determining the scope of the problem		
There is no standard definition of what constitutes a *drone incident* (e.g., suspected or confirmed sighting, suspected or confirmed drop, drone recovery), which makes it challenging to quantify the scope of the problem and make comparisons across facilities or systems.	• Develop standard terminology and best practices for more-granular reporting of drone incidents.	1
Assessing risk and needs		
Drones represent a relatively new challenge for the corrections sector, and guidance is needed to help determine and implement the best approach to address the challenge.	• Develop corrections-specific vulnerability assessment tools for drone incidents based on relevant factors (e.g., physical infrastructure, facility footprint, urban or rural setting, vicinity to critical infrastructure, operational procedures, existing perimeter security systems, inmate population makeup, staffing levels and patterns). • Develop guidebooks to help agencies identify their needs, and articulate operational requirements and specific objectives for each facility (e.g., is the goal to quantify the frequency of drone incidents or to alert staff so that they can quickly intercept contraband, or is finding and tracking the drone and controller the priority?).	1
Selecting, acquiring, and implementing solutions		
Drone technologies and drone detection technologies are rapidly evolving, and it can be challenging to obtain useful and objective information.	• Develop and maintain a clearinghouse or directory of commercially available detection solutions that includes such data as the technology used, spectrum of detection capabilities (e.g., range, sensitivity), limitations, costs, legal and regulatory compliance, and correctional facility deployments and points of contact.	1
As drone technology and threats evolve, current detection solutions may be rendered less effective, which can deter agencies from investing in them.	• Develop guidance and educational materials to help agencies assess the projected future landscape of drone technology and drone detection technology and to help them understand and manage risks associated with obsolescence and technology lock-in.[b]	
Drones represent a relatively new challenge for the corrections sector, and guidance is needed to help determine and implement the best approach to address the challenge.	• Develop selection and application guides to help agencies effectively implement and operationalize solutions. Potential issues to include in these guides are acquisition models (purchase versus lease or subscription), optimal sensor placement, information technology considerations, National Institute of Standards and Technology compliance, alert notification and response protocols, notification to law enforcement, management of staff access to detection systems prioritizing alerts, data analysis and reporting capabilities, legal compliance, and staffing implications.	

Table 2—Continued

Problem or Opportunity[a]	Potential Solution	Tier
Drone detection technologies can be cost-prohibitive; many agencies lack dedicated grant writers, which can deter them from applying for funding.	• Develop resources and support (e.g., templates, guides) to help those agencies that do not have grant-writing expertise prepare quality proposals.	
Testing and evaluating solutions		
Existing drone detection technologies have gaps and are not 100 percent effective.	• Develop minimum performance standards for drone detection solutions (e.g., detection rates, false-alarm rates, detection range, tracking capabilities, identification capabilities, alert notification system capabilities, regulatory compliance). • Conduct operational evaluations of configurations of layered approaches (e.g., RF, acoustic sensors, radar, cameras, intrusion detection, netting, correctional practices) to determine the most-effective methods of deterring drone activity and/or detecting drones in a timely manner to allow staff to intercept contraband. • Develop models for determining the return on investment of both individual solutions and solutions used in combination as part of a multilayered approach.	1
Policy and practice		
Drone incidents are often highly coordinated by criminal organizations, which can make interdiction challenging.	• Develop best practices for using intelligence sources to interdict and/or investigate drone incidents. Intelligence sources that could be of use include security threat group intelligence, information-sharing with law enforcement, informants, inmate communication systems, social media analyses, drone detection system analyses (e.g., delivery methods, payloads, launch points, type of drone), forensic analyses of recovered drones, and cell phones. • Develop a national data-sharing system (or expand an existing one) to report and track drone incidents.	1
Basic correctional strategies and practices and human capital can be a critical part of a multilayered approach to combat drone incidents and contraband delivery.	• Develop best practices and case studies documenting effective approaches (e.g., clear sight lines, area searches before inmate movement, perimeter patrols, hardened windows and screens, staffing towers, netting, outward-facing lighting and cameras, trail cameras to detect launch areas or operators, community outreach to encourage reporting of suspicious drone activity).	

[a] A *need* is the combination of a problem or opportunity and a potential solution. Some of the problems or opportunities are repeated in the table because they are combined with more than one potential solution.
[b] *Technology lock-in* refers to the idea that agencies are stuck with a particular technology and cannot easily switch to a different one.

Figure 2. Breakdown of the High-Priority Needs (*n* = 13)



"We collect data, but when you dig into some incident reports coded as a drone, it turns out it was an anonymous tip that an inmate was planning a delivery but never confirmed."

Assessing Risk and Needs

The challenges associated with identifying a drone incident notwithstanding, every correctional institution will have a different set of vulnerabilities, as well as a different set of needs and objectives to address the threat. The workshop participants identified two high-priority needs to address key challenges in this category.

Vulnerability Assessment

Many correctional agencies employ vulnerability assessments to evaluate the effectiveness of their security systems and processes (Turner, 2003). With the advent of drones, the traditional threat profile has changed, and, according to the participants, there is a need to update these tools, or create stand-alone tools, to account for this new reality. The main principles of vulnerability assessment (e.g., characterizing the institution, operations, and population; defining the threat; identifying targets; determining security-system objectives; evaluating the effectiveness of existing physical-protection system elements; and identifying deficiencies) remain applicable (Spencer and Morrison, 1998), but the focus might require refinement based on the unique nature of the drone threat. For example, institutions that are located in rural areas or that occupy vast perimeters (e.g., farming or agricultural operations) might be more vulnerable to drone activity because of the remoteness of the setting and because of the large areas and airspace that must be protected. On the other hand, the proximity of a correctional institution to an airport or other critical infrastructure might be a protective factor if the airport has drone detection systems in place that also cover the institution's airspace. Although the participants recommended the development of corrections-specific vulnerability assessment tools, existing resources could be leveraged as a foundation. For example, the Cybersecurity and Infrastructure Security Agency recently published guidance for federal agencies on best practices for assessing and protecting against the threat of drones (Interagency Security Committee, 2020).

"A self-assessment tool would be very valuable, especially for institutions that have not yet experienced drone incursions."

"We have institutions that are up to 20,000 acres. It's a lot of airspace to protect and area to search for dropped contraband."

Articulation of Needs and Objectives

Better quantification of incidents and a drone-specific vulnerability assessment can provide valuable information about the potential scope of the problem, but the participants noted that institutions would benefit from additional guidance. They recommended the development of a corrections-focused guidebook that outlines a process to help institutions understand and articulate their objectives and operational requirements with respect to addressing the drone threat. Such a guidebook would, in turn, assist in the identification of potential solutions that best fit an institution's needs. For example, institutions should be able to identify the primary threat scenario and their primary goals. In some cases, they might simply be trying to quantify the frequency of drone incursions more accurately, so the ability to identify the presence of a drone might be more important than the capacity to determine the speed and direction of the drone. Agencies with multiple institutions might value the flexibility of mobile deployments of drone detection technologies, rather than fixed (i.e., stationary) deployments, so that operators can move the detection equipment to different locations as needed. Others agencies might seek solutions that give staff the most time to respond to incursions before contraband can be recovered by incarcerated individuals, or the priority might be the ability to gather identifying information about the drone and track the direction and location of the drone and its controller to facilitate apprehension and criminal charges.

Selecting, Acquiring, and Implementing Solutions

Most correctional staff are not experts in drone technology and drone detection technology; they require support and guidance to understand the available options and their legality and applicability to correctional use and to select and implement the appropriate solutions. The workshop participants identified four high-priority needs to address key challenges in this category.

Access to Objective Information

According to the participants, it can be challenging to gather useful and objective information about available drone detection solutions. Part of the challenge is the sheer volume of options. For example, in 2019, it was estimated that at least 537 counter-drone (i.e., detect, defeat) products were either on the market or in development around the world (Michel, 2019). While not every product is suitable for deployment by state or local correctional institutions in the United States, 323 products are designed to detect (as opposed to defeat) drones; products designed to detect drones generally present fewer legal obstacles than products designed to defeat them. Given rapid market growth, the number of options will likely continue to increase. To help agencies identify potential viable solutions, the participants recommended the development and maintenance of a directory by an independent and trusted organization. The directory should include such data as the product manufacturer, product name, technologies used, general capabilities and limitations, cost range, U.S. legal and regulatory compliance, and points of contact for correctional institution deployments. Although now defunct, the Center for the Study of the Drone at Bard College developed a similar database that could be used as a model for a future corrections-specific tool (Michel, 2019).

> "Knowing what technology options are available, as well as other agencies' experience with them, would be very valuable."

> "There is an information void that is filled by vendors; they focus on sales and promise the world."

Selection Considerations

The participants recommended the development of educational materials and a selection and application guidebook for drone detection technology. With respect to selection and procurement, the participants noted that specific guidance is needed to help agencies understand the legal implications associated with some solutions. For example, some RF drone detection solutions can extract data from the communications signals between the controller and the drone, and the extraction of these data could violate federal surveillance laws. Therefore, agencies need to understand exactly how the technology works, as well as any legal implications it might have, before procuring it. Guidance is also needed regarding the advantages and disadvantages of purchasing the solution versus using a subscription services model, and guidance is needed on how to contractually account for necessary technology refreshes and general maintenance. Furthermore, agencies should understand the implications associated with localized versus cloud-based solutions; how the solutions may interface with or affect existing informa-

tion technology infrastructure; and how to evaluate whether the solutions comply with relevant information technology standards (e.g., National Institute of Standards and Technology Special Publication 800-53, 2020).

"If you get any data that constitutes [personally identifiable information], you've got to have a warrant."

"Vendors don't always give accurate information about what types of data their tools collect."

"Corrections tends to do a really good job at buying and deploying technology, but we don't have the resources to support it."

The participants also expressed significant concern about the speed at which drone technology is advancing. For example, drones are being designed to carry larger payloads, enabling conspirators to deliver more contraband per flight. Next-generation batteries will enable longer flights, and solar-powered systems could charge drones while they are in flight, offering the potential for unlimited range under optimal conditions (Crawford, 2023). Lighter components, including composite materials, are enabling drones to fly faster and more stealthily. For example, drones made primarily from cardboard have been used in support of Ukraine's war efforts because the material is difficult to detect with radar systems (Peck, 2023). Finally, as noted earlier, drones are increasingly capable of autonomous flight and do not rely on an RF link with the operator, negating the effectiveness of some detection systems.

"I'm concerned with how quickly drone technology changes. We may have something in place today that detects 90 percent of drones, but next month it may be completely ineffective."

Drone detection technology is also rapidly evolving and will continue to do so as the threat profile changes. This fluidity, according to the participants, can make it challenging for institutions to confidently make investments in solutions. The participants recommended the development of educational materials to keep the sector informed about the current and projected landscape so that agencies can better understand and manage the risks associated with obsolescence and technology lock-in.

"I can't recommend investing millions of dollars if I don't know the long-term viability of the solution."

Operationalization and Implementation of Solutions

The participants recommended the development of guidebooks to help institutions effectively operationalize and implement solutions. Alert notification, threat assessment, and response can be critically important to operationalization, according to the participants, regardless of whether an institution has deployed a drone detection system. For example, policies and protocols for how alerts are generated, which staff (e.g., the warden or administrator, the institution's central control room, the agencywide incident command center) receive notification and how (e.g., app, call, text, email), how alerts are prioritized relative to other simultaneous events (e.g., officer down), how notifications are sent to local law enforcement (e.g., a police department, the sheriff, the state police), which immediate response actions should be taken, and what the implications are for staffing should all be addressed. Furthermore, participants discussed the importance of evaluating which staff or roles should have access to the drone detection system, as well as what levels of access (e.g., view-only versus administrative functions) they should have, to protect system security.

Beyond policies and protocols, participants called for the development of model training modules for correctional staff on drone recognition, awareness of the threats that drones pose, and incident response.

"We can have the greatest technology, but the key is how to operationalize it."

"Our staff need better guidance in terms of what to do when they observe a drone; what are the appropriate response protocols."

"We need to distinguish the true threats. [Is the drone over the prison or on the outskirts?] We can't send the cavalry out every time there is an incident."

Obtaining Funding

Operating correctional institutions is expensive, and funding has not always kept pace with rising costs. The advent of drones and the corresponding need for countermeasures represent yet another demand on agencies that were already resource constrained. The participants noted that some measures to detect drones can be cost-prohibitive. For example, detection systems can cost more than $200,000 per facility, not including annual support and maintenance (Cook, 2017; Dix et al., 2022; Sabol, 2022). Federal agencies, such as NIJ and the Bureau of Justice Assistance, can be sources of grant funding; however, according to the participants, correctional agencies may be deterred from pursuing opportunities because they lack dedicated grant writers on staff. To help overcome this barrier, participants recommended the development of resources, such as guides and templates, that agencies can use to more easily prepare effective grant proposals to acquire solutions.

"We don't have a dedicated grant writer. If I want a piece of technology, I have to write the grant."

"Our agency has identified solutions that we like, but we are in a budget crunch and can't move forward."

Testing and Evaluating Solutions

According to the participants, many correctional institutions lack the expertise to effectively test and evaluate the growing number of commercially available detection solutions. Furthermore, some products have yet to mature and might not perform as advertised (Michel, 2019); the participants expressed varying degrees of satisfaction with the drone detection systems they had piloted or acquired. The participants identified three high-priority needs in this category.

Need for Standards

The participants recommended the development of minimum performance standards for drone detection technology. Standards would provide such benefits as common terminology to measure and evaluate performance and a mechanism to build trust that products meeting the established standards have a degree of validity. While operational evaluations in the correctional setting would still be recommended, a first cut in evaluating products might be conformity with established standards. Elements of the standards would likely vary depending on the technology deployed but could include detection rates, false alert rates, detection ranges, directional and tracking capabilities, alert notification system features, and compliance with relevant laws and regulations.

"Vendors are eager to get your business, and the presentations look good, but when you put the system in use it doesn't work very well."

Operational Evaluations

Although the participants expressed the belief that minimum performance standards for drone detection solutions would be useful, the value of these standards would be somewhat limited because of the nature of conformity assessment programs. For example, depending on the structure of these programs, they typically rely on independent laboratories to test and certify products as conforming to the established standards, or they allow product manufacturers to self-attest that their products conform (Carnahan and Phelps, 2018). Furthermore, because it is generally acknowledged that a layered security approach is more effective than a single solution (Dix et al., 2022), it is important to evaluate various configurations of solutions working in tandem (e.g., electronic identification, RF detection, and radar).

The participants recommended the facilitation of independent operational evaluations of various technology configurations in real-world conditions (i.e., the correctional environment). These evaluations would yield important data on the most effective combination of solutions to detect drones, while

"We need real experts to help us evaluate these tools. Our staff are good and interested, but it takes time to get up to speed, and they have so many other duties."

"We're willing to make an investment. . . . We've talked to vendors and hosted pilots, but, so far, we haven't found a system that we are impressed with."

accounting for such conditions as environmental and RF interference, weather, terrain, geographic location, line of sight, and time of day. Furthermore, the practical application of solutions (e.g., the alert notification system, realistic staff response time relative to the alert) could be evaluated. Relatedly, participants called for the development of information-sharing networks and other mechanisms for agencies to safely and securely share relevant data, including evaluation results. National organizations, such as the American Correctional Association and the Correctional Leaders Association, could serve as hosts for these networks.

"It would be great if there could be a counter-drone center of excellence."

Return on Investment

The participants noted that it can be challenging to justify investment in drone detection technology given such concerns as expense and variability of system performance. To help agencies determine how to best allocate their scarce resources, the participants recommended the development of cost-benefit analysis models to help quantify the return on investment of both individual solutions and solutions used in combination as part of a multilayered approach.

"There are many 'unknowns' with respect to drones. For me, the biggest unknown is what is the best solution for the money."

Although such analyses are important, the participants acknowledged several challenges associated with them. For example, it might be difficult to isolate the relative impacts of individual solutions in a multilayered configuration. Furthermore, the effectiveness of some solutions might be highly dependent on such factors as staffing issues and alert response protocols, which can introduce significant variables. For example, a solution might be effective in detecting a drone, but its value is diminished if staff are unable to respond in a timely manner to intercept the contraband. Successful detection can have life and safety implications (e.g., deterring or intercepting a payload of fentanyl-laced drugs or escape tools) that can be challenging to analyze in cost-benefit terms. Similarly, detection systems may improve staff perceptions of their personal safety, which can affect morale and retention, according to the participants.

"In our world, the absence of chaos is a positive metric."

"It's hard to put a price on that, because one life is worth every bit of money."

Policy and Practice

Although drone detection systems certainly play an important role in countering the drone threat, the participants also recognized the value of core correctional practices and lower-cost solutions as key elements in a multilayered approach to the problem. Three high-priority needs fell into this category.

"We tend to emphasize technology solutions, but sometimes our greatest resource is under our noses: our staff."

Core Correctional Security Practices

The participants discussed several measures that institutions have implemented to address the drone threat. For example, some rural institutions have deployed trail cameras at strategic locations (i.e., likely launch points) outside the perimeter to

detect and identify drone operators. Several participants noted that incarcerated individuals have been able to compromise their cell windows and/or screens, allowing them to simply reach out and gather packages hanging from drones. One participant called this practice "DroneDash," likening it to a food delivery service. In response, institutions are hardening or replacing cell windows and mesh screening. Institutions generally position their CCTV cameras to focus on the grounds; however, because of the threat of drones, they are adding or repositioning cameras to face outward and upward. Participants also discussed the value of community outreach. For example, informing the neighbors living around an institution about the drone issue and asking them to notify the institution of suspicious activity can be helpful. Taking steps to make the institutional schedule (e.g., recreation period, count times) less predictable may be beneficial because it can make coordination between incarcerated individuals and conspirators more difficult.

> "We used to see high-altitude drops to avoid detection . . . now we have drones flying right to the cell window."

> "We have seen drone drops during our count times [because the conspirators] know that staff are occupied."

Other practices mentioned include clearing trees around the perimeter of the institution to improve sight lines, adjusting tower staffing, modifying the landscape to make it easier to discern and detect packages that have been dropped, and bolstering perimeter patrols and area searches before mass movement so that staff can intercept contraband before it reaches the incarcerated population.

> "Not all towers are staffed at all times. . . . We're reconsidering that due to drones."

As institutions adapt to the drone threat, it is unclear which measures, if any, are producing the desired impact. Therefore, the participants recommended the development of best practices and case studies highlighting the most-effective strategies.

> "[The conspirators] wrap the packages with turf or other material to blend in with the grounds so that it's harder for staff to find."

Intelligence and Investigations

Given that it can be challenging to detect drone incursions, the participants recognized the importance of investigations to hold conspirators accountable for their actions and serve as general deterrence to future bad actors. The participants also recommended the development of best practices for gathering intelligence and conducting investigations specific to drone activity.

> "Usually we are reactive, but sometimes we get the intel in advance, so we can interdict a delivery before it occurs."

> "Getting intel on every incident is critical."

Traditional intelligence-gathering methods, such as monitoring security threat groups, leveraging informants, reviewing camera footage, coordinating with law enforcement sources, and screening incarcerated individuals' communications, remain relevant; however, other methods are playing a growing role. For example, drone incursions require planning and coordination between incarcerated individuals and conspirators, who themselves are sometimes formerly incarcerated individuals. Conspirators need to know where and when to drop the contraband to increase the probability that the intended recipient recovers it. Contraband cell phones are often used by incarcerated people to plan incursions, so forensic analyses of confiscated devices can be a particularly effective tool in establishing relationships between conspirators and uncovering plots. Forensic analyses of recovered drones and payloads can

be a treasure trove for investigators. Fingerprints and/or DNA may be left on the drone, linking it and/or the package to the operator. The participants also discussed the value of payload analyses as an investigative tool. For example, capturing information about such details as how the recovered contraband package was prepared (e.g., the color and type of tape), how the package was camouflaged (e.g., it was wrapped in grass turf), and whether fishing line was used to tether the payload could reveal patterns that identify operators. Furthermore, the drone's circuit board (or boards), onboard cameras, sensors, chips, operating system log, and removable media contain data that might have investigative value. Personal information, such as username or credit card details, could link the drone to its owner (McSweeney, 2018). Drone identification data; videos taken by the drone; and/or data on patterns, such as flight dates and times, launch points, speed, height, and path, could link operators to previous incidents. Furthermore, drone video may have inadvertently captured images of the operator, the person's home, or the license plate of the drone operator's vehicle.

"Gangs like the Crips and the Mexican Mafia are conducting drops at multiple institutions."

"Anytime a drone crashes, we want it. Forensic analysis is critical, and we've had a lot of success in our investigations."

Relatedly, the participants recognized that conspirators do not necessarily limit their incursions to a particular correctional system. For example, the same individuals or groups can conduct incursions across different jurisdictions in the same geographic area (e.g., facilities that are located near each other but in different states and/or federal, state, and local institutions in the same state). To better identify and counter these incursions, correctional agencies need to share incident reports and investigative data at the national level. This recommendation could be accomplished via a specialized platform or existing information-sharing systems, such as the Federal Bureau of Investigation's National Data Exchange.[3]

"[Security threat groups] control contraband . . . so they are probably responsible for the majority of drone activity."

CONCLUSION

As discussed throughout this report, drones represent a serious and emerging threat to the safety and security of correctional institutions. Drones have been used to deliver large quantities of dangerous contraband, including tools to facilitate escape attempts, and could be weaponized to attack institutions. They are quickly deployed and often undetected, which makes it difficult to respond in time to recover payloads and/or facilitate apprehension of the operators. In a workshop convened to explore the challenges and opportunities associated with preventing, detecting, and responding to drone incidents, prison and jail administrators and other policy experts identified key needs that, if addressed, would significantly help meet these challenges.

Several broad themes emerged from the workshop. Foundationally, it is challenging to accurately quantify the scope and impact of the drone problem. Contributing factors include the lack of a standard definition for the term *drone incident*; limited effectiveness in detecting drones, through either human observation or technological solutions; difficulty tracing contraband in the institution to a drone incident; and the relatively low probability of apprehending drone operators. Correctional staff are often not experts in drone technology and drone detection technology, and these fields are evolving rapidly. Technology providers are often the only source of information, and solutions offer varying degrees of effectiveness. Staff require independent sources of support, guidance, and best practices to assess their needs; understand the available options and their legality and applicability to correctional use; and evaluate, select, and implement the appropriate and most cost-effective approaches, which might include various types of sensors. Core correctional security practices (e.g., well-trained staff, immediate responses to incidents, perimeter security, landscape modifications, searches, intelligence, forensics, and law enforcement partnerships) complement technology solutions as part of a multilayered approach to addressing the threat. Several needs that participants identified pertain to the legal and regulatory landscape; the sector needs ongoing education about the legality of certain detection solutions. Furthermore, stakeholders

need to understand the potentially grave impact of drone incursions and support more-effective deterrents through enhanced criminal penalties and more-aggressive prosecution.

While incursions remain lucrative for conspirators and drone technology continues to advance and become even more affordable, these criminal activities will likely persist. Ultimately, unless and until drone mitigation (i.e., defeat) technology becomes a safe, cost-effective, and legally available option, the sector must maintain a detect-and-respond posture. For the foreseeable future, it appears that a combination of proven, cost-effective drone detection systems; vigilant application of core correctional security and investigative practices; partnerships with law enforcement; and greater accountability for conspirators will have the greatest impact on addressing the threat of drones to correctional security.

TECHNICAL APPENDIX

This appendix presents additional details on the workshop and our process for identifying and prioritizing research and technology needs and turning them into the research agenda that is presented in the main report. The descriptions in this appendix are drawn and adapted from previous PCJNI publications and reflect adjustments to the needs identification and prioritization process implemented at this workshop.

Workshop Scope and Participant Selection

The topics for PCJNI workshops are selected by reaching a consensus among the action officers and subject-matter experts at NIJ and research staff at the organizations that will be facilitating the workshop. Multiple topic areas, accompanied by brief scoping descriptions, are typically suggested months before the workshop by one or more of the parties involved, and staff engage in group deliberations with NIJ to reach consensus on the topic. We then engage in further scoping of the workshop to craft a discussion agenda through literature review or informal discussions with other practitioners and subject-matter experts, or both. Once the topic and scope have been determined, we recruit participants by identifying knowledgeable individuals through existing professional and social networks (e.g., LinkedIn) and by reviewing literature published on the topic. We then extend an invitation to those individuals and provide a brief description of the workshop's focus areas.

The process of expert elicitation described here was designed to gather unbiased, representative results from experts and practitioners in the field. However, several limitations could affect the findings. The process typically elicits opinions from a relatively small group of experts. To limit the effect of group size on the representativeness of the results, we strive to make the group as representative as possible of different disciplines, perspectives, and geographic regions. However, the final output of the workshop likely is significantly influenced by the specific group of experts invited to participate. It is possible that the workshop's findings would be different if a different group of experts were selected. Moreover, although the discussion moderators make every effort to act as neutral parties when eliciting opinions from the collected experts, the backgrounds and experiences of the moderators have the potential to influence which questions they pose to the group and how they phrase those questions. This could also introduce bias that could influence the findings.

Identification and Prioritization of Needs

To develop and prioritize a list of technology and policy issues that are likely to benefit from research and investment, we followed a process similar to processes we used in previous PCJNI workshops (see, for example, Jackson et al., 2015; Jackson et al., 2016, and references therein). Participants discussed and refined problem statements and identified potential solutions (or *needs*) that could address each problem. In addition, needs could be framed in response to opportunities to improve performance by adopting or adapting a new approach or practice (e.g., applying a new technology or tool in the sector that had not been used before). After identifying and refining the needs, we used a voting process based on the Delphi method, a technique developed at RAND, to elicit prioritization information from the group about the identified needs (RAND Corporation, undated).

Interviews

Prior to the workshop, we conducted remote interviews with the participants to discuss challenges they saw that were related to the topic of the workshop. We asked the participants to identify areas in which additional investment in research and development could help alleviate those challenges. During these discussions, participants suggested additional areas that were potentially worthy of research or investment. We consolidated and integrated the problems, opportunities, and potential solutions described by the participants in the separate interviews into a single summarized list. In advance of the in-person workshop, we emailed the summarized list of issues and needs to the participants.

In-Person Workshop

For the workshop, participants traveled to the Office of Justice Programs offices in Washington, D.C. During the workshop, we started by asking the participants to collectively review, discuss, and correct the wording of the consolidated list of problems from the interviews. Each identified problem was placed on a Microsoft PowerPoint slide and displayed at the front of the room for discussion. Once the participants agreed on the wording of the problems, they were asked to vote on the importance of each problem on a scale from 1 (lowest) to 9 (highest). Participant votes on each problem were recorded anonymously using a handheld device (specifically, the ResponseCard RF LCD from Turning Technologies).

After the participants provided their individual ratings using the handheld devices, we displayed a histogram-style summary of participant responses within the polling system's interface. If there was significant disagreement among the participants, then they were asked to verbally discuss or explain their votes at one end of the spectrum or the other. (The degree of disagreement was determined by our visual inspection of the histogram.) If a second round of discussion occurred, participants were given an opportunity to adjust their ratings on the same question. With the data from the voting, we prioritized the list of problems by calculating the median vote for each problem.

We used the prioritized list of problems as an agenda for the remaining workshop time. If time ran short, then only the more highly rated problems were examined for potential solutions or opportunities. For each problem, participants were asked to identify potential opportunities and potential solutions. Again, we used Microsoft PowerPoint slides that were displayed at the front of the room and edited in real time to incorporate participants' revisions and comments. In some cases, the facilitators provided solutions that were previously identified during the interviews.

Once the participants reached consensus on a group of needs, we conducted a real-time voting prioritization exercise using Delphi techniques. We asked the participants to anonymously vote using a handheld device (again, the ResponseCard RF LCD from Turning Technologies). Each participant was asked to score each need and associated strategies to address those needs using a 1–9 scale for two dimensions: *importance* and *probability of success*.

For the *importance* dimension, participants were instructed that 1 was a low score and 9 was a high score. Participants were told to score a need's importance with a 1 if the need would have little or no impact on the problem and with a 9 if it would reduce the impact of the problem by 20 percent or more. Anchoring the scale with percentage improvements in the need's performance is intended to help make rating values comparable from participant to participant.

For the *probability of success* dimension, participants were instructed to treat the 1–9 scale as a percentage chance that the need could be met and broadly implemented successfully. That is, they could assign the need's chance of success between 10 percent (i.e., a rating of 1) and 90 percent (i.e., a rating of 9). This dimension was intended to include not only technical concerns (i.e., whether the need would be hard to meet) but also the effect of factors that might cause practitioners to not adopt the new technology, policy, or practice even if it were developed. Such factors could include, for example, cost, effect on practitioner workloads, other staffing concerns, and societal concerns.

After the participants provided their individual ratings using the handheld devices (i.e., for importance or probability of success), we displayed a histogram-style summary of participant responses within the polling system's interface. If there was significant disagreement among the participants, then they were asked to verbally discuss or explain their votes at one end of the spectrum or the other. (The degree of disagreement was determined by our visual inspection of the histogram.) If a second round of discussion occurred, participants were given an opportunity to adjust their ratings on the same question. This process was repeated for each question and dimension at the end of each topic area.

Post-Session Prioritization

Once the participants had completed this rating process for all of the topic areas, we put the needs into a single prioritized list. We ordered the list by calculating an expected value using the method outlined in Jackson et al. (2016). For each need, we averaged the median problem importance with the median potential-solution importance (from the second round of voting, if necessary). This formed the overall importance score for each need. This score was then multiplied with the median probability of success for each need to produce an expected value. We then calculated the median of that product across all of the respondents and used that as the group's collective expected value score for the need.

Next, we clustered the resulting expected value scores into three tiers using a hierarchical clustering algorithm. (We used the "ward.D" spherical algorithm from the "stats" library in the

R statistical package, version 4.1.3). We chose this algorithm to minimize within-cluster variance when determining the breaks between tiers. We chose to use three tiers in part to keep the methodology consistent across the set of needs-prioritization workshops we have conducted for NIJ. Also, the choice of three tiers provides a manageable system for policymakers. Specifically, the Tier 1 needs are the priorities that should be the primary policymaking focus, the Tier 2 needs should be examined closely, and the Tier 3 needs are probably not worth much attention in the short term (unless, for example, they can be addressed with existing technology or approaches that can be readily and cheaply adapted to the identified need).

Because the participants initially rated the needs one topic area at a time, we gave them an opportunity at the end of the workshop to review and weigh in on the tiered list of all identified needs. The intention of this step was to let participants see the needs in the context of the other tiered needs and allow them to consider whether there were some that appeared too high or low relative to the others. Participants were able to see all of the ranked needs collected across all of the sessions; this provided a top-level view that was complementary to the rankings provided session by session. To collect the participants' assessments, we emailed the entire tiered list to them in a Microsoft Word document. The participants were then asked to examine where each of the needs landed on the overall tiered list and whether this ordering was appropriate or needed fine-tuning. Participants had the option to indicate whether each problem-and-need pairing should be voted up or down on the list. Table A.1 provides an example of this form.

We then tallied the participants' responses and applied those votes to produce a final list of prioritized and tiered needs. To adjust the expected values using the up and down votes from the third round of prioritization, we implemented a method equivalent to the one we used in previous work (Hollywood et al., 2016). Specifically, if every participant voted "up" for a need that was at the bottom of the list, then the collective effect of those votes should be to move the need to the top. (The opposite would happen if every participant voted "down" for a need that was at the top of the list.) To determine the point value of a single vote, we divided the full range of expected values by the number of participants voting.

To prevent the (somewhat rare) situation in which small numbers of votes have an unintended outsized impact—for example, when some or all of the needs in one tier have the same or very similar expected values—we also set a threshold that at least 25 percent of the workshop participants must have voted on that need (and then rounded to the nearest full participant). For this workshop, there were 13 participants, so, for any votes to have an effect on changing a need's tier, at least three participants would have had to vote to move the need up or down.

After applying the up and down vote points to the second-round expected values, we compared the modified scores with the boundary values for the tiers to see whether the change was enough to move any needs up or down in the prioritization. (Note that there were gaps between these boundaries, so some of the modified expected values could fall in between tiers. See Figure A.1.) As with prior work, we set a higher bar for a need to move up or down two tiers (from Tier 1 to Tier 3, or vice versa) than for a need to move to the tier immediately above or below. Specifically, a need could *increase by one tier* if its modified expected value was higher than the highest expected value score in its initial tier. And a need could *decrease by one tier* if its modified expected value was lower than the lowest expected value in its initial tier. However, to *increase or decrease by two tiers* (which was possible only for needs that started in Tier 1 or Tier 3), the score had to increase or decrease by an amount that fully placed the need into the range two tiers away. For example, for a Tier 3 need to jump to Tier 1, its expected value score had to fall within the boundaries of Tier 1, not just within the gap between Tier 1 and Tier 2. Figure A.1 illustrates the greater score change required for a need to move two tiers (one need on the far right of the figure) compared with one tier (all other examples shown).

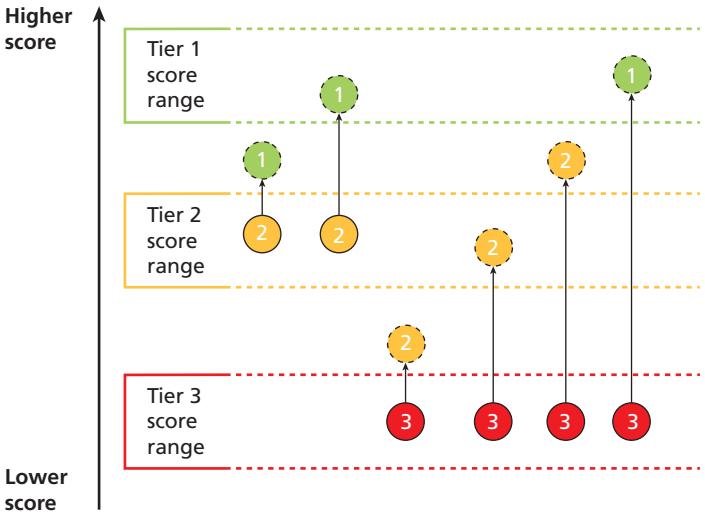
Applying these decision rules to integrate the participants' third-round inputs into the final tiering of needs resulted in numerical separations between tiers that were less clear than the separations that resulted when we used the clustering algorithm in the initial tiering. This can occur because, for example, when the final expected value score for a need that was originally in Tier 3 falls just below the boundary value for Tier 1, that need's final score could be higher than that of some other needs in the item's new tier (Tier 2). See Figure A.2, which shows the distribution of the needs by expected value score after the second-round rating process and then after the third-round voting process.

For the third round of voting, we received votes from several participants. However, no needs changed position during the third round. The output from this process became the final ranking of the participants' prioritized results.

Table A.1. Example of the Delphi Third-Round Voting Form

Question	Tier	Vote Up	Vote Down
Tier 1			
Issue: There is no standard definition of what constitutes a drone incident (e.g., suspected or confirmed sighting, suspected or confirmed drop, drone recovery), which makes it challenging to quantify the scope of the problem and make comparisons across facilities or systems. **Need:** Develop standard terminology and best practices for more-granular reporting of drone incidents.	1	[redacted]	
Issue: Existing drone detection technologies have gaps and are not 100 percent effective. **Need:** Develop minimum performance standards for drone detection solutions (e.g., detection rates, false-alarm rates, detection range, tracking capabilities, identification capabilities, alert notification system capabilities, regulatory compliance).	1	[redacted]	
Tier 2			
Issue: Agencies might not be fully leveraging the power of forensics to investigate and interdict drone activity. **Need:** Develop best practices, case studies, and implementation guides for conducting forensic analyses on recovered drones (as well as on contraband cell phones, which may be connected to drone activity) to support investigations. Consider the implications and pros and cons of building internal capacity versus relying on law enforcement partnerships.	2		
Issue: Justice-system stakeholders (e.g., correctional agencies, law enforcement, and prosecutors), state and local legislators, and the public might not fully appreciate the threats that drones pose to safety and security. **Need:** Develop educational campaigns, targeted to specific audiences, to increase awareness of the dangers that drones pose to correctional staff and inmates, as well as to the public (e.g., drone-facilitated escapes, delivery of contraband cell phones used to orchestrate crimes in the community).	2		
Tier 3			
Issue: Current legal and regulatory restrictions force correctional agencies into a detect-and-respond posture. Solutions are needed to proactively and safely mitigate threats. **Need:** Educate, and engage in discussions with, legislators on why and under what circumstances restrictions against interfering with drones should be relaxed.	3		[redacted]
Issue: It can be challenging to understand and keep up with the legal and regulatory issues associated with drone detection and mitigation solutions. **Need:** Facilitate ongoing communication and collaboration among relevant federal agencies (e.g., DOJ, FAA, FCC), state and local correctional agencies, and professional organizations on issues related to drones and drone detection and mitigation.	3		[redacted]

Figure A.1. How a Need's Increase in Expected Value Might Result in Its Movement Across Tier Boundaries



NOTE: Each example need's original tier is shown by a circle with a solid border (the two needs starting in Tier 2 and the four needs starting in Tier 3). Each need's new tier after the third-round score adjustment is shown by the connected circle with a dotted border.

Figure A.2. Final Distribution of the Tiered Needs

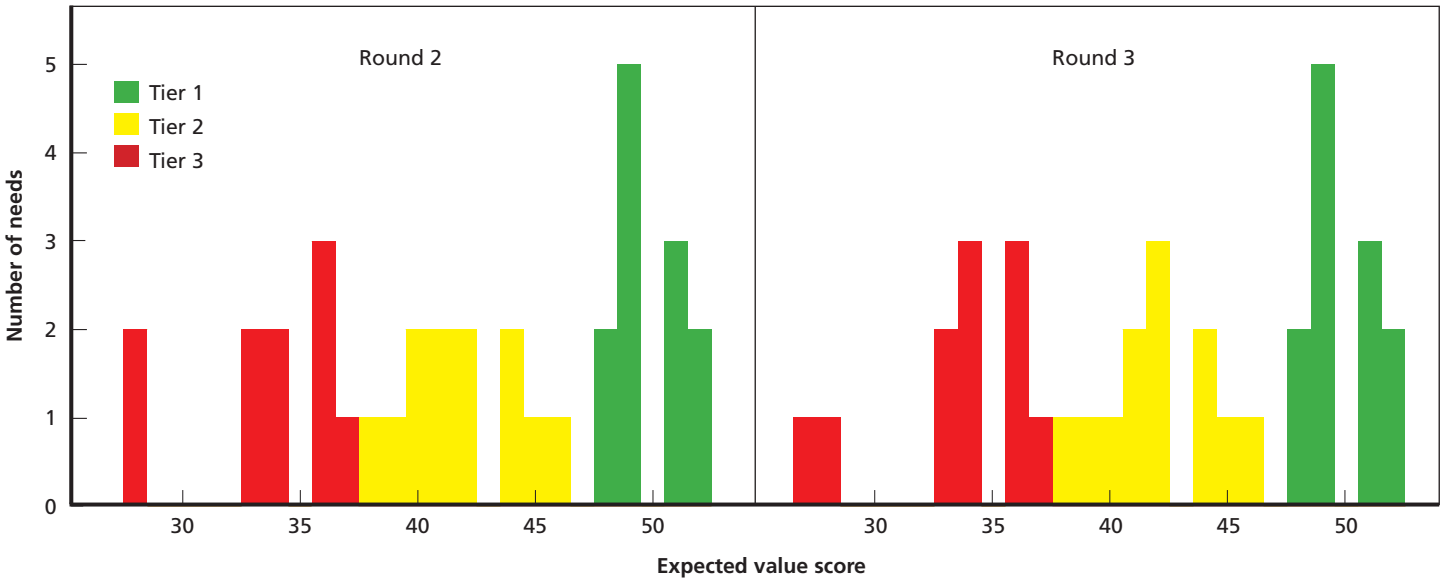


Table A.2. Complete List of Needs, by Tier and Category

Problem or Opportunity[a]	Potential Solution	Tier
Determining the scope of the problem		
There is no standard definition of what constitutes a *drone incident* (e.g., suspected or confirmed sighting, suspected or confirmed drop, drone recovery), which makes it challenging to quantify the scope of the problem and make comparisons across facilities or systems.	• Develop standard terminology and best practices for more-granular reporting of drone incidents.	1
Assessing risk and needs		
Drones represent a relatively new challenge for the corrections sector, and guidance is needed to help determine and implement the best approach to address the challenge.	• Develop corrections-specific vulnerability assessment tools for drone incidents based on relevant factors (e.g., physical infrastructure, facility footprint, urban or rural setting, vicinity to critical infrastructure, operational procedures, existing perimeter security systems, inmate population makeup, staffing levels and patterns). • Develop guidebooks to help agencies identify their needs, and articulate operational requirements and specific objectives for each facility (e.g., is the goal to quantify the frequency of drone incidents or to alert staff so that they can quickly intercept contraband, or is finding and tracking the drone and controller the priority?).	1
Selecting, acquiring, and implementing solutions		
Drone technologies and drone detection technologies are rapidly evolving, and it can be challenging to obtain useful and objective information.	• Develop and maintain a clearinghouse or directory of commercially available detection solutions that includes such data as the technology used, spectrum of detection capabilities (e.g., range, sensitivity), limitations, costs, legal and regulatory compliance, correctional facility deployments and points of contact.	1
As drone technology and threats evolve, current detection solutions may be rendered less effective, which can deter agencies from investing in them.	• Develop guidance and educational materials to help agencies assess the projected future landscape of drone technology and drone detection technology and to help them understand and manage risks associated with obsolescence and technology lock-in.	
Drones represent a relatively new challenge for the corrections sector, and guidance is needed to help determine and implement the best approach to address the challenge.	• Develop selection and application guides to help agencies effectively implement and operationalize solutions. Potential issues to include in these guides are acquisition models (purchase versus lease or subscription), optimal sensor placement, information technology considerations, National Institute of Standards and Technology compliance, alert notification and response protocols, notification to law enforcement, management staff access to detection systems prioritizing alerts, data analysis and reporting capabilities, legal compliance, and staffing implications.	
Drone detection technologies can be cost-prohibitive; many agencies lack dedicated grant writers, which can deter them from applying for funding.	• Develop resources and support (e.g., templates, guides) to help those agencies that do not have grant-writing expertise prepare quality proposals.	

Table A.2—Continued

Problem or Opportunity[a]	Potential Solution	Tier
Testing and evaluating solutions		
Existing drone detection technologies have gaps and are not 100 percent effective.	• Develop minimum performance standards for drone detection solutions (e.g., detection rates, false-alarm rates, detection range, tracking capabilities, identification capabilities, alert notification system capabilities, regulatory compliance). • Conduct operational evaluations of configurations of layered approaches (e.g., RF, acoustic sensors, radar, cameras, intrusion detection, netting, correctional practices) to determine the most-effective methods of deterring drone activity and/or detecting drones in a timely manner to allow staff to intercept contraband. • Develop models for determining the return on investment of both individual solutions and solutions used in combination as part of a multilayered approach.	1
Policy and practice		
Drone incidents are often highly coordinated by criminal organizations, which can make interdiction challenging.	• Develop best practices for using intelligence sources to interdict and/or investigate drone incidents. Intelligence sources that could be of use include security threat group intelligence, information-sharing with law enforcement, informants, inmate communication systems, social media analyses, drone detection system analyses (e.g., delivery methods, payloads, launch points, type of drone), forensic analyses of recovered drones, and cell phones. • Develop a national data-sharing system (or expand an existing one) to report and track drone incidents.	1
Basic correctional strategies and practices and human capital can be a critical part of a multilayered approach to combat drone incidents and contraband delivery.	• Develop best practices and case studies documenting effective approaches (e.g., clear sight lines, area searches before inmate movement, perimeter patrols, hardened windows and screens, staffing towers, netting, outward-facing lighting and cameras, trail cameras to detect launch areas or operators, community outreach to encourage reporting of suspicious drone activity).	
Determining the scope of the problem		
Quantifying the scope of the problem can be challenging because drone incidents may go undetected and/or recovered contraband may be mistaken as a throw-over incident.	• Evaluate the utility and cost-effectiveness of various approaches (e.g., different technologies and methods, rotating mobile and fixed detection equipment) to help determine the extent of the problem.	2
Testing and evaluating solutions		
Agencies might not have the internal capacity and expertise to evaluate the effectiveness of drone detection solutions.	• Create or better leverage existing research centers to conduct independent, objective testing of both individual detection solutions and multilayered approaches. • Develop tools (e.g., best practices, model testing protocols, performance measures, evaluation criteria) to assist agencies in conducting testing, evaluations, and pilot programs in their operational environments.	2

Table A.2—Continued

Problem or Opportunity[a]	Potential Solution	Tier
Policy and practice		
Drone technologies and drone detection technologies are rapidly evolving, and it can be challenging to obtain useful and objective information.	• Facilitate information-sharing networks and other mechanisms for agencies to safely and securely share information, such as policies, best practices, lessons learned, test and evaluation results, drone operator tactics and trends, and circumvention techniques.	2
Correctional staff require better situational awareness regarding the risks posed by drones.	• Develop model training modules that cover basic issues, such as what a drone is, what it looks and sounds like, its capabilities (e.g., payload capacity, speed, range), the skill level required to operate it, its specific threats and risks, how to identify characteristics of packages likely delivered via drone, and laws and regulations governing drone activity in general and drone activity over correctional facilities in particular.	
Correctional staff require better guidance on how to respond to a drone incident.	• Develop best practices and model policies and procedures to address such issues as assessing and communicating the threat, carrying out specific response protocols (e.g., inmate management, area or roof search), securing contraband, rendering the drone safe, recovering the drone while preserving evidence, and reporting and documenting the incident.	
Correctional agencies must often rely on outside law enforcement agencies because drones are launched from the community and are largely beyond the control of the facility.	• Develop model memorandums of understanding and best practices to develop effective partnerships with law enforcement agencies to share drone-related intelligence; plan coordinated responses to drone incidents or alerts (e.g., attempt to apprehend drone operators); coordinate the preservation, sharing, and processing of evidence; and/or assist with ongoing investigations.	
Agencies might not be fully leveraging the power of forensics to investigate and interdict drone activity.	• Develop best practices, case studies, and implementation guides for conducting forensic analyses on recovered drones (as well as on contraband cell phones, which may be connected to drone activity) to support investigations. Consider the implications and pros and cons of building internal capacity versus relying on law enforcement partnerships.	
There are opportunities for agencies to leverage their own drones to combat contraband introduction (e.g., scan perimeters to deter or detect operators, search rooftops, test detection solutions and operational response).	• Develop best practices and implementation guides for developing internal drone capacity. (Specific topics to cover include policies and procedures, initial and ongoing costs, staffing implications, pilot licensing, drone selection, and camera integration.)	
Justice-system stakeholders (e.g., correctional agencies, law enforcement, and prosecutors), state and local legislators, and the public might not fully appreciate the threats that drones pose to safety and security.	• Develop educational campaigns, targeted to specific audiences, to increase awareness of the dangers that drones pose to correctional staff and inmates, as well as to the public (e.g., drone-facilitated escapes, delivery of contraband cell phones used to orchestrate crimes in the community).	

Table A.2—Continued

Problem or Opportunity[a]	Potential Solution	Tier
Legal and regulatory issues		
It can be challenging to understand and keep up with the legal and regulatory issues associated with drone detection and mitigation solutions.	• Develop educational campaigns (e.g., bulletins, conference presentations) to keep stakeholders informed of the current legal and regulatory landscape and changes as they occur.	2
Existing enforcement mechanisms and penalties for using drones to introduce contraband into correctional facilities might not be an effective deterrent to prevent incidents.	• Conduct research to assess the deterrent impact of specific laws (e.g., prohibitions on flying a drone over a correctional facility or using a drone to deliver or attempt to deliver contraband) and general federal regulations on reducing drone incidents.	
Current legal and regulatory restrictions force correctional agencies into a detect-and-respond posture. Solutions are needed to proactively and safely mitigate threats.	• Research and develop solutions that can safely and cost-effectively mitigate unauthorized drones.	
Legal and regulatory issues		
Existing enforcement mechanisms and penalties for using drones to introduce contraband into correctional facilities might not be an effective deterrent to prevent incidents.	• Develop best practices and guidance for leaders of correctional agencies to engage with state prosecutors and other stakeholders to educate them on the severity of the problem and the importance of even and aggressive enforcement across jurisdictions (i.e., not left to the discretion of individual local prosecutors).	3
Current legal and regulatory restrictions force correctional agencies into a detect-and-respond posture. Solutions are needed to proactively and safely mitigate threats.	• Educate, and engage in discussions with, legislators on why and under what circumstances restrictions against interfering with drones should be relaxed.	
It can be challenging to understand and keep up with the legal and regulatory issues associated with drone detection and mitigation solutions.	• Facilitate ongoing communication and collaboration among relevant federal agencies (e.g., DOJ, FAA, FCC), state and local correctional agencies, and professional organizations on issues related to drones and drone detection and mitigation.	

[a] A *need* is the combination of a problem or opportunity and a potential solution. Several of the problems or opportunities are repeated throughout the table because they are combined with a variety of potential solutions.

ENDNOTES

[1] *Prison value* refers to estimated value within the correctional setting, inflated because of scarcity and difficulty smuggling prohibited goods into correctional institutions.

[2] Some problems had multiple needs attached to them, representing different ways to address the same problem.

[3] The National Data Exchange "is a no fee unclassified national information sharing system that enables criminal justice agencies to search, link, analyze, and share local, state, tribal, and federal records" (Federal Bureau of Investigation, undated).

REFERENCES

Andrews, Frank, and Sam Bradpiece, "Redoine Faid: French Convict Helped to Freedom by Drones," CNN, July 3, 2018.

Ashworth, Caitlin, "Drones Fuel Contraband Trade at SC Prisons; Federal Government Called to Act," *Post and Courier*, February 5, 2023.

Atherton, Kelsey, "Anti-Drone Tech's Tangled Regulatory Landscape," Brookings, October 2, 2020.

Bischoff, Laura A., "3 Men Accused of Using Drones to Drop Drugs at Ohio Prisons Face 116 Criminal Counts," *Columbus Dispatch*, May 9, 2023.

Braich, Baneet, "Drug-Smuggling Drones Rampant in Canadian Prisons, Says Correctional Officers' Union," CBC, last updated May 14, 2023.

Bruce, Matt, "Powder Springs Convict, Brother Sentenced for Using Drone in Georgia Prison Smuggling Scheme," *Atlanta Journal-Constitution*, July 12, 2021.

Bubna, Gaurav, "A Primer on Geofencing for Drones and the Contentious Debate over It," *Directions Magazine*, September 20, 2022.

Carnahan, Lisa, and Amy Phelps, *Conformity Assessment Considerations for Federal Agencies*, National Institute of Standards and Technology, NIST Special Publication 2000-02, September 2018.

Chavez, Marcela, "DOJ: 4 Indicted After Drugs Delivered by Drone into Fresno County Prison," YourCentralValley.com, April 13, 2023.

Cook, Rhonda, "At Georgia Prisons, Inmates Use Drones, Apps to Skirt Security," *Atlanta Journal-Constitution*, March 21, 2017.

Coppola, Michele, "New York Prison Using UAS Detection Technology," *TechBeat*, June 2017.

Crawford, Mark, "Five Ways Drone Technology Is Improving," American Society of Mechanical Engineers, May 18, 2023.

Crumley, Bruce, "Illicit Drone Delivery of Contraband to Global Prisons Soared in 2022," DroneDJ, January 3, 2023.

Dix, M. O., M. Mecray, J. Man, E. Vetter, M. Tucker, N. Parsons, T. Craig, and Criminal Justice Testing and Evaluation Consortium, *Contraband and Drones in Correctional Facilities: An Overview of Technologies and Issues Associated with Detection and Response*, National Institute of Justice, Office of Justice Programs, U.S. Department of Justice, October 2022.

DOJ—*See* U.S. Department of Justice.

DOJ, DOT, FCC, and DHS—*See* U.S. Department of Justice, U.S. Department of Transportation, Federal Communications Commission, and U.S. Department of Homeland Security.

"Drone Drops Drugs in Ohio Prison Yard, Spurring Inmate Fight," Associated Press, August 4, 2015.

Duncan, Charles, "Shortage of Prison Guards Forces North Carolina to Shut Down Some Units," Spectrum News 1, April 26, 2023.

Ellison, Heath, "SC Man Arrested for Dropping 550 Grams of Pot, Four Hacksaw Blades into Jail with Drone," ABC 15 News, March 1, 2022.

Esack, Steve, "Smuggled K2 Drug Turning Pa. Inmates Violent," Corrections1, August 23, 2018.

Federal Bureau of Investigation, "National Data Exchange (N-DEx)," webpage, undated. As of January 25, 2024: https://ndex.fbi.gov/error/AUTHENTICATE_FOR_USE.html?entityID=https%3A%2F%2Fndex.fbi.gov%2Fmellon%2Fmetadata&return=https%3A%2F%2Fndex.fbi.gov%2Fmellon%2Flogin%3FReturnTo%3Dhttps%253A%252F%252Fndex.fbi.gov%252F&returnIDParam=IdP

Girten, Nicole, "Montana Department of Corrections Researching Drones as Possible Solution to Staffing Shortage," *Great Falls Tribune*, November 16, 2022.

Hambling, David, "Drug Cartels Carry Out Drone Bombings, Evade Jammers," *Forbes*, October 1, 2021.

Harvey, Kyle, "Hair Dye Kits, Heroin and Hacksaw Blades Among Items Delivered to Prisons via Drones," KBAK, April 20, 2018.

Hollywood, John S., Dulani Woods, Andrew Lauland, Sean E. Goodison, Thomas J. Wilson, and Brian A. Jackson, *Using Future Broadband Communications Technologies to Strengthen Law Enforcement*, RAND Corporation, RR-1462-NIJ, 2016. As of July 27, 2023: https://www.rand.org/pubs/research_reports/RR1462.html

Hynes, Mike, and Nick Jordan, "How to Cure Prisons' Contraband Mobile Phone Epidemic," *Security*, July 16, 2019.

Interagency Security Committee, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, *Protecting Against the Threat of Unmanned Aircraft Systems (UAS)*, November 2020.

"Italian Prisoner Shoots at Rivals with Gun 'Smuggled in by Drone,'" *The Guardian*, September 20, 2021.

Jackson, Brian A., Duren Banks, John S. Hollywood, Dulani Woods, Amanda Royal, Patrick W. Woodson, and Nicole J. Johnson, *Fostering Innovation in the U.S. Court System: Identifying High-Priority Technology and Other Needs for Improving Court Operations and Outcomes*, RAND Corporation, RR-1255-NIJ, 2016. As of July 27, 2023: https://www.rand.org/pubs/research_reports/RR1255.html

Jackson, Brian A., Joe Russo, John S. Hollywood, Dulani Woods, Richard Silberglitt, George B. Drake, John S. Shaffer, Mikhail Zaydman, and Brian G. Chow, *Fostering Innovation in Community and Institutional Corrections: Identifying High-Priority Technology and Other Needs for the U.S. Corrections Sector*, RAND Corporation, RR-820-NIJ, 2015. As of July 27, 2023: https://www.rand.org/pubs/research_reports/RR820.html

Jay, Suranga, "How Far Can a Drone Fly and Factors That Decide Drone Range," Trailoka, December 2, 2022.

Johnson, Lauren M., "A Drone Was Caught On Camera Delivering Contraband to an Ohio Prison Yard," CBS 58, September 27, 2019.

Jordan, Grant, "Drone Problems Are Increasing. What Can Event Owners Do?" *Sports Destination Management*, February 3, 2023.

Kitanovic, Bojan, "Drone Industry in the US: An Overview of a Game-Changer," The Drones World, January 26, 2022.

Knox, George, and D. Lee Gilbertson, "The Use of Drones by Gangs to Smuggle Contraband into Correctional Institutions," study guide for the 2021 National Gang Crime Research Center Video Training Program, National Gang Crime Research Center, last updated December 5, 2020.

Kotowski, Jason, "Drone Carrying Cellphones Crashed in Kern Valley State Prison Yard: Report," KGET.com, December 17, 2021.

Kravets, David, "Drone Dropped 'Tools' Enabling Inmate to Escape, Prison Officials Say," Ars Technica, July 7, 2017.

Levenson, Eric, and Sheena Jones, "South Carolina Inmate Used Drone, Makeshift Dummy to Escape Prison," CNN, July 7, 2017.

Ling, Justin, "Someone Used a Drone to Deliver a Handgun into a Notorious Canadian Prison," Vice, December 14, 2015.

Link, Jeff, "Drone Contraband Deliveries Are Rampant at US Prisons," Wired, July 29, 2022.

Marnin, Julia, "Men Hid in Woods to Fly Drones over New Jersey Prison to Drop Items, Feds Say," *Miami Herald*, February 4, 2022.

McSweeney, Kelly, "How Drone Forensics Can Reveal Pilot Identity," ZDNET, December 28, 2018.

Michel, Arthur Holland, *Counter-Drone Systems*, 2nd ed., Center for the Study of the Drone at Bard College, December 2019.

National Conference of State Legislatures, "Current Unmanned Aircraft State Law Landscape," March 27, 2023.

National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, 5th rev., National Institute of Standards and Technology, U.S. Department of Commerce, September 2020.

Office of the Inspector General, U.S. Department of Justice, *Audit of the Department of Justice's Efforts to Protect Federal Bureau of Prisons Facilities Against Threats Posed by Unmanned Aircraft Systems*, September 2020.

Ormseth, Matthew, "Special Delivery: Drones Are Smuggling Contraband into California Prisons, Feds Say," *Los Angeles Times*, April 9, 2023.

Park, Seongjoon, Hyeong Tae Kim, Sangmin Lee, Hyeontae Joo, and Hwangnam Kim, "Survey on Anti-Drone Systems: Components, Designs, and Challenges," *IEEE Access*, Vol. 9, 2021.

Pavlo, Walter, "The Drone Is Quickly Becoming a Federal Prison Contraband Nightmare," *Forbes*, December 27, 2022.

Peck, Michael, "Ukraine's Humble Cardboard Drones Are a Master Class in Stealth," *Popular Mechanics*, March 28, 2023.

Powell, Tori B., "20 People Arrested for Using Drones to Deliver over 100 Pounds of Contraband to South Carolina Prison," CBS News, February 4, 2022.

RAND Corporation, "Delphi Method," webpage, undated. As of July 27, 2023:
https://www.rand.org/topics/delphi-method.html

Rupprecht, Jonathan, "Big Problems with Counter Drone Technology (Anti Drone Guns, Drone Jammers, Etc.)," Rupprecht Law P.A., undated.

Russo, Joe, Michael J. D. Vermeer, Dulani Woods, and Brian A. Jackson, *Community Supervision in a Digital World: Challenges and Opportunities*, RAND Corporation, RR-A108-10, 2021. As of January 25, 2024:
https://www.rand.org/pubs/research_reports/RRA108-10.html

Russo, Joe, Dulani Woods, John S. Shaffer, and Brian A. Jackson, *Countering Threats to Correctional Institution Security: Identifying Innovation Needs to Address Current and Emerging Concerns*, RAND Corporation, RR-2933-NIJ, 2019. As of July 5, 2023:
https://www.rand.org/pubs/research_reports/RR2933.html

Sabol, Blair, "'This Is a War': Drone-Delivered Contraband On the Rise in South Carolina Prisons," WCSC, April 28, 2022.

Sheehan, Mark, "Penalties for Flying a Commercial Drone Without a License," *Lidar News*, March 6, 2019.

Skove, Sam, "How Ukraine Learned to Cloak Its Drones from Russian Surveillance," C4ISRNET, October 17, 2022.

Spencer, Debra S., and G. Steve Morrison, "Assessing the Security Vulnerabilities of Correctional Facilities," Sandia National Laboratories, 1998.

Teale, Chris, "Prisons 'Under Attack' from Drones Delivering Contraband," GCN, May 26, 2023.

Thompson, Loren, "Defeating Drones: The Most Promising Weapons Are All Non-Kinetic," *Forbes*, November 1, 2022.

Thrush, Glenn, "Short on Staff, Prisons Enlist Teachers and Case Managers as Guards," *New York Times*, May 1, 2023.

Travis, Randy, "Fox 5 I-Team Tests Prison Drone Warning System," Fox 5 Atlanta, May 23, 2018.

Turner, Allan, "Developing a Vulnerability-Assessment Process for Corrections," *Corrections Today*, Vol. 65, No. 4, July 2003.

U.S. Code, Title 18, Crimes and Criminal Procedure; Part I, Crimes; Chapter 119, Wire and Electronic Communications Interception and Interception of Oral Communications.

U.S. Code, Title 18, Crimes and Criminal Procedure; Part II, Criminal Procedure; Chapter 206, Pen Registers and Trap and Trace Devices.

U.S. Department of Justice, U.S. Department of Transportation, Federal Communications Commission, and U.S. Department of Homeland Security, "Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems," guidance document, August 2020.

Villarreal, Lupita, "Houston Man Sentenced to 8 Months in Federal Prison for Trying to Use Drone to Drop Contraband in Beaumont Prison," 12 News, March 15, 2023.

Vyas, Kashyap, "A Brief History of Drones: From Pilotless Balloons to Roaming Killers," Interesting Engineering, April 18, 2023.

Wallace, Jim, "2 Arrested After Drone Caught Delivering Contraband to Calhoun State Prison," WALB, December 23, 2020.

Walsh, Jim, "Former Inmate Returning to Prison Due to FCI Fort Dix Smuggling Scheme," *Burlington County Times*, February 11, 2022.

Williams, Martyn, "Drone Carrying Drugs, Hacksaw Blades Crashes into Oklahoma Prison," *Computerworld*, October 27, 2015.

Wolfe, Wes, "After Illicit Prison Deliveries, Georgia Eyes Anti-Drone Law," *Government Technology*, February 13, 2019.

Acknowledgments

We acknowledge the assistance of the experts who participated in the "Drones: Countering an Emerging Threat to Correctional Security" workshop, who are listed in the body of the report. This effort would not have been possible without their willingness to participate. We also acknowledge the contributions of Steve Schuetz of NIJ. Finally, we acknowledge the valuable contributions of the peer reviewers of the report: Todd Craig of the Federal Bureau of Prisons, Ian Mitch of RAND, and the anonymous reviewers from DOJ.

Justice Policy Program

RAND Social and Economic Well-Being is a division of the RAND Corporation that seeks to actively improve the health and social and economic well-being of populations and communities throughout the world. This research was conducted in the Justice Policy Program within RAND Social and Economic Well-Being. The program focuses on such topics as access to justice, policing, corrections, drug policy, and court system reform, as well as other policy concerns pertaining to public safety and criminal and civil justice. For more information, email justicepolicy@rand.org.

About the Authors

Joe Russo is a researcher with the University of Denver, where he has supported a variety of programs funded by NIJ. His research focuses on institutional and community corrections technologies and on identifying the high-priority technology needs of agencies across the nation. He has served in the New York City Department of Correction and the New York City Department of Probation. He has an M.S. in criminal justice.

Dulani Woods is a data science practitioner at RAND. He is adept at data acquisition, transformation, visualization, and analysis, and his research typically focuses on justice and homeland security policy. Woods specializes in maintaining and operating simulation models and has developed or maintained models designed to estimate potential policy impacts on justice outcomes and defense logistics. He holds an M.S. in agricultural economics.

Michael J. D. Vermeer is a senior physical scientist and technologist at RAND, where he researches science and technology policy in criminal justice, homeland security, the intelligence community, and the armed forces. He specializes in assessing opportunities and security risks associated with emerging technologies. He coleads the PCJNI and holds a Ph.D. in inorganic chemistry.

Brian A. Jackson is a senior physical scientist at RAND. His research focuses on criminal justice, homeland security, and terrorism preparedness. His areas of examination have included safety management in large-scale emergency response operations, the equipment and technology needs of criminal justice agencies and emergency responders, and the design of preparedness exercises. He coleads the PCJNI and has a Ph.D. in bioinorganic chemistry.

About This Report

On behalf of the U.S. Department of Justice, National Institute of Justice (NIJ), RAND—in partnership with the Police Executive Research Forum, RTI International, and the University of Denver—is carrying out a research effort to assess and prioritize technology and related needs across the criminal justice community. This research effort, called the Priority Criminal Justice Needs Initiative (PCJNI), is a component of the Criminal Justice Requirements and Resources Consortium (RRC) and is intended to support innovation within the criminal justice enterprise. For more information about the RRC and the PCJNI, please see www.rand.org/well-being/justice-policy/projects/priority-criminal-justice-needs.

This report is one product of the PCJNI. In April 2023, researchers from RAND and the University of Denver conducted a workshop, "Drones: Countering an Emerging Threat to Correctional Security." This report presents the workshop proceedings, discussing the topics considered and overarching themes that emerged from the workshop discussions. The results it presents should be of interest to a wide audience, including justice-system stakeholders, correctional practitioners, technology developers, and researchers. Other RAND research reports from the PCJNI that might be of interest are

- Joe Russo, Michael J. D. Vermeer, Dulani Woods, and Brian A. Jackson, *Community Supervision in a Digital World: Challenges and Opportunities*, RAND Corporation, RR-A108-10, 2021.
- Joe Russo, Dulani Woods, John S. Shaffer, and Brian A. Jackson, *Countering Threats to Correctional Institution Security: Identifying Innovation Needs to Address Current and Emerging Concerns*, RAND Corporation, RR-2933-NIJ, 2019.

Mentions of products or companies do not represent endorsement by NIJ or RAND.

NIJ | National Institute of Justice
STRENGTHEN SCIENCE. ADVANCE JUSTICE.

This publication was made possible by Award Number 2018-75-CX-K006, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice, the RAND Corporation, or the organizations represented by any of the workshop participants.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

www.rand.org

RAND

RAND is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.

RR-A108-21