PRIORITY
Criminal Justice
NEEDS INITIATIVE
A project of the RAND Corporation, the Police Executive Research Forum, RTI International, and the University of Denver

Countering Threats to Correctional Institution Security

Identifying Innovation Needs to Address Current and Emerging Concerns

Joe Russo, Dulani Woods, John S. Shaffer, Brian A. Jackson

Key Findings

An expert workshop of correctional administrators and researchers identified the following high-priority needs with respect to threats to institutional security:

- Understaffing is a major threat; staffing ratio standards are needed, as are recruitment and retention strategies to meet these standards.
- Supervisors need better training and a manageable span of control in order to properly develop staff.
- Tools are needed to identify staff prone to compromise.
- Better technology and best practices are needed to detect drugs, cell phones, and weapons.
- Fully electronic mail systems should be explored to reduce the influx of drugs and protect staff and inmates from harm.
- Research and testing centers are needed to evaluate emerging technology solutions to threats (e.g., cell phones, drones).
- Administrators need greater awareness of cyber threats and information technology–related risks and need increased capacity to address these risks.
- Best practices are needed to balance inmate access to technology for reentry purposes with security concerns.
- Best practices are needed for security threat group management.
- Technology is needed to automate analysis of inmate communications.
- Best practices are needed for the development of continuity of operations plans.

On behalf of the National Institute of Justice (NIJ), the Priority Criminal Justice Needs Initiative convened an expert workshop to identify current and emerging threats to correctional institution security and the key needs associated with mitigating the risks they pose. The major goal of the workshop was to produce a set of prioritized needs that can help inform NIJ's research agenda and contribute to the national discussion on correctional security issues and options for improvement. Workshop participants included correctional administrators, representatives of relevant federal agencies, and security experts. The recommendations of the participants are presented in this report.

Correctional institutions are responsible for the care, custody, and control of individuals who are detained while awaiting trial or who have been convicted of a crime and sentenced to a term of imprisonment. These institutions are complex organizations with a challenging, sometimes conflicting mission: protecting the public while preparing those under correctional control for successful, law-abiding lives in the community through the reentry process. There are nearly 7,000 correctional institutions in the United States (Wagner and Sawyer, 2018). All institutions, from the largest state prison to the smallest county jail, share similar security threats and vulnerabilities, many of which are related in some way to the characteristics of the population served and the nature of confinement. Although many inmates try to serve their time in a productive manner and are intent on self-improvement, a subset can create serious problems for an institution (DeLisi, 2003). Such inmates can be violent toward staff and each other or could attempt escape. They might seek to acquire contraband in various forms, whether for personal use or for sale or trade (U.S. Department of Justice, 2016).

This group might continue criminal activities in both the institution and the community (DeLisi, 2003). These inmates could leverage authorized and unauthorized communication systems for their own purposes (Grommon, Carter, and Sheer, 2018) or seek to compromise staff for their own benefit. Inmates can exert power over each other through gangs, also referred to as *security threat groups* (STGs; Winterdyk and Ruddell, 2010). In sum, this subset of inmates can create serious safety and management concerns by taking advantage of varied opportunities to manipulate, game, or disrupt the orderly operation of a correctional facility.

Some threats are related to the nature of correctional institutions, which have been described as "small towns surrounded by walls and fences" (Atherton and Phillips, 2007, p. vii). Therefore, correctional administrators must be prepared to manage and mitigate many of the same issues that any community faces. These issues include the development of emergency response plans to deal with natural disasters, the outbreak of disease, and civil unrest. Institutions, much like communities, have critical infrastructure needs, and deferred maintenance can lead to serious consequences over time (Associated Press, 2016).

Furthermore, today's correctional institutions are not the self-contained, closed environments of the past. To keep these small towns operating, visitors, volunteers, medical staff, maintenance staff, and other contractors and vendors must regularly enter and exit facilities. Mail, packages, and large shipments must be processed. The movement of people and things into and out of facilities represents a potential failure point in terms of institutional security, as does the behavior of compromised correctional staff.

Issues and trends in larger society affect the security of correctional institutions as well. For example, the nation's opioid epidemic is spilling over into jails and prisons, and overdose deaths have become increasingly common (Gokavi, 2018; Ovalle, 2018). Street gangs and prison or jail gangs are essentially extensions of each other. The desire for instant and constant communication via text and social media fuels the demand for contraband cell phones among inmates (Wiltz, 2017). Technological advances, such as the popularization of drones, have created security threats as bad actors leverage these innovations to deliver contraband into correctional facilities (Hennigan, 2018). Inmates require increased access to technology and the internet in order to prepare themselves for successful reentry, but this access introduces significant risks that must be managed (Tolbert and Hudson, 2015). Finally, many internal systems, including access controls; heating, ventilation, and air conditioning (HVAC); and communications systems are information technology–based and operate on internet protocols (IPs), creating vulnerability to cyberattack (Newman, Rad, and Strauchs, 2011).

There are a multitude of potential threats to correctional institution security. As the threats evolve, so too must the strategies deployed to mitigate the risks of these threats. A comprehensive security program, therefore, must move beyond physical systems to include information technology and human elements.

As part of its multiyear research effort supporting NIJ, the Priority Criminal Justice Needs Initiative examined correctional institution safety and security concerns. This effort sought to better understand current and emerging security threats and identify the key needs associated with mitigating the risks of these threats.

METHODOLOGY

To explore the complex issues related to threats to correctional institution security, NIJ tasked the RAND Corporation and the University of Denver (DU) to assemble an expert workshop of correctional administrators, representatives of relevant federal agencies, and security professionals. The major task was to produce a set of prioritized needs that can help inform NIJ's research agenda and contribute to the national discussion on correctional security issues and options for improvement.

A pool of candidate participants was identified through a review of published documents and through recommendations from various organizations. We took care to identify potential participants with experience and expertise in jails and prisons because each type of institution faces slightly different challenges. Furthermore, the research team sought representation from different geographic regions as well as types of organization (e.g., federal, state, county). Ultimately, a group of 17 was convened. The list of participants and their organizations is included in the text box.

Prior to convening, participants were asked to complete a pre-workshop questionnaire on 13 security threat categories identified by the research team. Each category was framed as follows:

- **STG activity** includes control of contraband markets, influence on inmates and institutional operations, and radicalization.

- **Inmate attack on infrastructure** includes sabotage of security systems (e.g., programmable logic controllers, cell phone–managed access systems) or infrastructure (e.g., the facility's power grid).
- **Unmonitored communications and unauthorized use of technology** includes use of cell phones or misuse or manipulation of technology to conduct criminal acts, make threats, or coordinate activities.
- **Contraband** includes the possession of drugs, weapons, tools, cash, and other unauthorized items (regardless of the method of entry).
- **Escape** includes escape by force, stealth, or coercion.
- **Violence** includes threats or attacks on staff and/or inmates within or outside a facility, disturbances, and riots.
- **External physical attack** includes blunt force attacks on a facility by outsiders.
- **Chemical, biological, or hazardous material attack** includes attack via mail, water supply, food sources, etc.
- **Cyberattack** includes external hacks that compromise security or information systems.
- **Natural disaster, emergency, or pandemic** includes such major events as earthquakes, fires, floods, and hurricanes.
- **Inability to maintain security systems and infrastructure** includes deteriorating, out of date, or ineffective systems (e.g., fences and perimeter security systems, cameras, cell-locking mechanisms).
- **Insufficient staffing** includes inadequate staffing ratios, unmanned posts, mandatory overtime, fatigue, and the inability to retain experienced staff.
- **Compromised staff** includes manipulated or corrupt staff and gang members or associates.

The first part of the questionnaire was structured to gather input on how the participants prioritized each category in terms of risk. Participants were asked to rank each category on a scale of 1 to 9 where 1 was "low importance" and 9 was "high importance." Figure 1 depicts the prioritization results represented by the percentage of participants who ranked a category in the "high range" (defined as a score of 7, 8, or 9).

The second part of the questionnaire asked participants to identify specific challenges or obstacles faced with respect to each of the major threat categories. Participants also had the opportunity to identify issues that did not necessarily fit the provided framework.

Participants were brought together for a two-day workshop. During the morning of the first day, the research team

Workshop Participants

Kathleen Allison
California Department of Correction and Rehabilitation

Tracy Bailey
Texas Department of Criminal Justice

James Basinger
Indiana Department of Corrections

Quincy Booth
Washington, D.C., Department of Corrections

Terence Clark
Philadelphia, Pennsylvania, Department of Prisons

Darryl Coleman
Harris County, Texas, Sheriff's Office

Todd Craig
Federal Bureau of Prisons

John Daugherty
Montana Department of Corrections

Christopher Glover
U.S. Army Corrections Command

Stephen Hancock
U.S. Department of Homeland Security

Kelly Harrington
Los Angeles, California, Sheriff's Department

Jeff Johnsen
Cook County, Illinois, Sheriff's Office

Daniel Junior
Miami-Dade County, Florida, Corrections and Rehabilitation Department

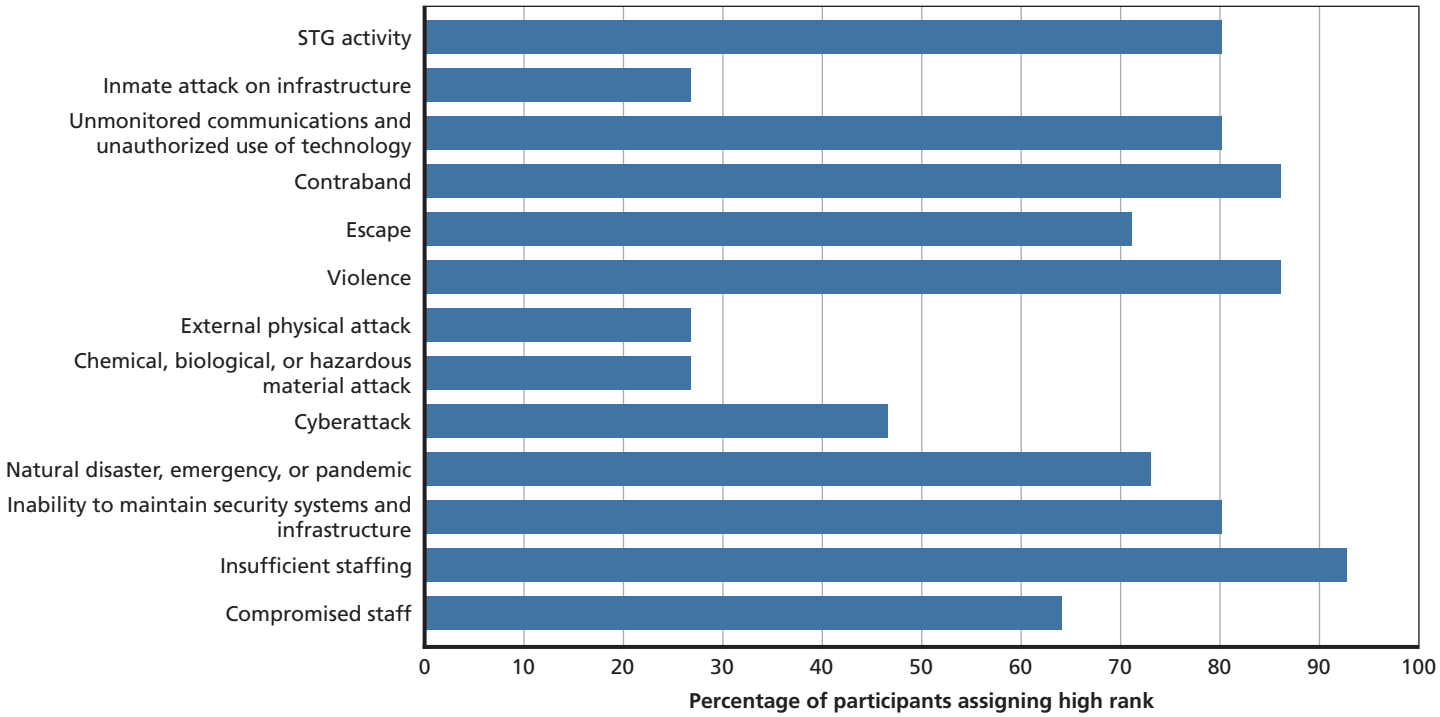
Jay Kirby
Colorado Department of Corrections

Ronald Repasi
Federal Communications Commission

Barry Roska
Maricopa County, Arizona, Sheriff's Office

Brigitta Rubin
The Mitre Corporation

Figure 1. Pre-Meeting Questionnaire Rankings of the Importance of Security Threats



NOTE: *High rank* is defined as a score of 7, 8, or 9. All 17 participants responded to this questionnaire.

outlined the goals of the workshop and presented the results from the pre-workshop questionnaire. These results were used to benchmark perceptions coming into the workshop and guide discussions. Moving forward, the research team used a structured brainstorming approach to develop a set of *needs*—a term used in our work for a specific requirement—tied to either solving a problem or taking advantage of an opportunity to help the corrections sector better address security threats. For expediency, the original 13 threat categories were condensed into the following five categories:

1. staffing issues (insufficient staffing, compromised staff)
2. STGs and violence
3. contraband and technology (contraband, unmonitored communications and unauthorized use of technology)
4. institutional infrastructure and escape (escape, inability to maintain security systems and infrastructure, inmate attack on infrastructure)
5. external threats (cyberattack; chemical, biological, or hazardous material attack; external physical attack; natural disaster, emergency, or pandemic).

The research team made efforts to discuss each of these five categories in distinct blocks of time; however, as expected in complex systems, many facets of a problem are highly interconnected. For example, STGs often control black markets to include contraband cell phones, and facilities that struggle to maintain adequate staffing also may experience higher levels of contraband introduction and violence.

Once the needs were identified in each category, the research team used a variant of the Delphi method (RAND Corporation, undated) and asked the participants to first individually, and then collaboratively, rank each need based on its expected benefit (i.e., how important they thought it would be if the need was met) and the probability of success of actually meeting the need (reflecting both technical and practical constraints that might make it difficult to do so).[1] Needs identified in each module of discussion (e.g., staffing issues) were then rated on a 1–9 scale. Participants voted anonymously using a handheld "clicker" (specifically, the ResponseCard RF LCD from Turning Technologies).

After each rating, the participants saw the aggregate results in real time, displayed as a bar graph of the rankings assigned to the need. Where there was apparent disagreement in the group (e.g., two distinct bands of ratings), the group had the opportunity to discuss the need and the rankings. In some cases, these discussions resolved differences in the interpretation of the need that had led to different rankings. In others, there were simply differences in view in the group about the value or difficulty of meeting a need.

After each discussion, voting on the need was reopened and the participants were given the opportunity to adjust their scores if they desired. These second-round results were not displayed or discussed further.

During a break in the meeting, project staff multiplied these ratings to produce an expected value score, which reflects the value of meeting the need weighted by the likelihood of doing so successfully. These scores were used to cluster the needs into three tiers from the highest scoring (Tier 1) to the lowest scoring (Tier 3). The research team then used a clustering algorithm to identify the best splits among the three groups of needs, where *best* was defined mathematically, minimizing differences between assignments of needs to the groups.

Because the participants ranked each group of needs separately immediately after they were discussed, the participants received a hard copy showing all of the needs and their corresponding tiers at the end of the workshop. This step allowed the workshop attendees to reality-check the results as a whole and flag specific needs if (in the attendee's view) they were in too high or too low a tier relative to the other needs. If an attendee thought that needs were misplaced, they indicated that on the hard copy. Needs that received enough up or down votes (which were converted to numerical adjustments to each need's expected value score) changed ranking tier for the final results. A total of 14 needs were "up-voted" and three needs were "down-voted." A more detailed discussion of the methodology is available in the appendix to this report.

This process yielded a set of 40 needs that were ranked and assigned into priority tiers.[2] The needs were grouped into five distinct themes and are organized by theme and priority in Table 1. It should be noted that many of the needs identified are research-related, reflecting the group consensus that the field is hampered by the lack of empirical evidence necessary to guide policy and practice.

We acknowledge that the needs identified and the priorities assigned to them are—as with all subjective assessments involving a limited number of participants—reflective of the views of the members of the workshop. Although the research team sought to include a broadly representative group of participants, it is likely that a different group would produce somewhat different results. The following sections summarize the workshop discussions and recommendations, organized by five major themes: human resources, contraband, information technology and cyber threats, STGs and criminal activity, and emergency preparedness. Although some of these themes parallel the modules used to organize the workshop (e.g., contraband, STGs), in other cases discussion was more focused and meant that the themes emerging from the workshop were narrower and more specific (e.g., information technology versus infrastructure more broadly).

HUMAN RESOURCES

Although some may think of institutional security in terms of cells, thick stone walls, and other barriers separating inmates from the public, a high-quality staff is arguably one of the most important components of an institution's security apparatus. Indeed, Austin MacCormick, a distinguished penologist, reportedly noted that "an effective prison can be established in an old red barn if it is staffed correctly" (quoted in McShane and Williams, 1996, p. 297). If MacCormick was correct, staff can be an institution's greatest asset or its weakest link. The working group identified several challenges with respect to staffing. Most of these challenges fell under the themes of recruitment and retention of quality staff, the importance of first-line supervisors, and the prevention of staff misconduct. The following sections highlight the group's major recommen-

Table 1. Breakdown of Needs, by Theme and Priority

Theme	Tier 1 Needs	Tier 2 Needs	Tier 3 Needs
Human resources	5	1	3
Contraband	10	1	1
Information technology and cyber threats	3	2	4
STGs and criminal activity	2	2	5
Emergency preparedness	0	1	0
Total	20	7	13

dations with respect to the impact of human resources issues on institutional security. The full list of needs in this area is shown in Table 2.

Quantifying the Need for Staffing

Correctional agencies, like other governmental organizations, have to justify their budget requests on an annual basis. Although every correctional administrator can argue for more staffing, very few, if any, are able to hire the full complement of officers they believe to be necessary to operate institutions in a safe and secure fashion. This is due in large part to budgetary constraints at the state or local level. However, the absence of data relating staffing levels to security and national staffing standards can make it very difficult for administrators to make a compelling case for additional resources to legislative bodies. Although efforts have been made to develop objective staffing ratio formulas that consider a variety of factors (e.g., security level of an institution; number and classification of inmates; physical plant; security capabilities; inmate movement; programming needs; and statutory, contractual, and agency policy requirements), differences among institutions have limited the success of those efforts.

Research is required to develop better models to account for these differences and determine optimal staffing levels that could serve as guidelines for national standards. Moreover, additional research should validate these models by examining the impact of staffing levels on key correctional outcomes. Furthermore, a more compelling case could be made to secure funding if there were better evidence to suggest that these investments might be linked to positive results (e.g., reductions in violence, escapes, contraband, use of force).

Table 2. Needs Identified Related to Human Resources

Tier	Problem or Opportunity	Associated Need
1	Some agencies struggle to recruit staff and attract the current generation of job seekers.	• Conduct research into the potential impacts on recruiting from marketing correctional careers with recruiting and branding strategies (e.g., media, social media).
	Supervisory staff often do not have the time to perform key functions (e.g., mentoring, positive reinforcement, staff recognition).	• Conduct research into the short- and long-term effects of supervisor shortages.
	Some factors may make certain staff more vulnerable to STGs or other negative influences than others, making them more susceptible to compromise.	• Develop a risk assessment (i.e., suitability test) instrument to inform hiring and management decisions.
	The effectiveness of policies to deter staff misconduct and criminal activity is unknown.	• Conduct research to identify the most effective deterrents to undesired staff behavior (e.g., fines, public punishment).
2	Staff are not as committed to correctional careers and supporting their team as they may have historically been (e.g., abuse of the Family and Medical Leave Act [FMLA]).	• Develop training materials for supervisors that consider cultural shifts and attitudes toward work (e.g., "live to work" versus "work to live").
	Training may be inadequate to prepare staff to avoid or manage inmate attempts to manipulate or otherwise compromise their positions.	• Conduct research and assessment to ensure that the educational model and trainers are up to date with the latest approaches (best practices for duration, location, delivery, etc.).
3	Some agencies struggle to recruit staff and attract the current generation of job seekers.	• Conduct research into community perceptions of correctional careers and occupations (with emphasis on such factors as urban/rural, affluent/poor, etc.).
	Officers often are not aware that staff misconduct has been addressed by an effective disciplinary action (e.g., suspension versus demotion).	• Highlight best practices that are intended to keep staff current across organizations (e.g., newsletters, electronic information distribution).
	There is insufficient national-level guidance on staffing ratios, particularly for adult institutions.	• Conduct research to determine optimal staffing ratios and the impacts from having more or less than the optimal levels (to include supervisor's span of control).

Challenges of Understaffing

Correctional officers are the backbone of every institution and represent the first line of defense against security threats. In many parts of the country, however, agencies are experiencing significant challenges in recruiting and retaining officers (Association of State Correctional Administrators, 2017a). In some states, officer vacancy rates can exceed 45 percent (Lyman, 2017). Annual turnover in prisons and jails averages around 20 percent nationwide (Matz et al., 2013); however, some states have reported rates as high as 53 percent (Association of State Correctional Administrators, 2017b). The Federal Bureau of Prisons has had to rely on non-custody civilian staff (e.g., nurses, cooks, teachers, secretaries) to fill posts because of acute correctional officer shortages and overtime limits (Johnson, 2018). The inability to recruit and retain staff leads to understaffed institutions, which are a serious threat to security.

A variety of factors can deter individuals from entering or remaining in the field of corrections. For example, the work is inherently dangerous and stressful, and the fact that most correctional officers are unprepared to interact with the increasing mentally ill inmate population exacerbates this situation. The environment can be physically harsh, and mandatory overtime is common because of insufficient staffing levels. Compensation, in many states, is not competitive with the private sector or other public agencies (Russo et al., 2018). Finally, the sector is challenged by the reality that the public does not consider corrections as a high-status occupation. Current economic, societal, and demographic changes affecting the larger workforce (e.g., low unemployment, decreasing labor force) have exacerbated recruitment and retention difficulties.

The effects of these challenges can be varied and profound. For example, agencies that are understaffed might be compelled to loosen their selection criterion to widen their candidate pool. Similarly, pressure to get new officers on a post may force agencies to abbreviate the length of academy training, in which case the officers are less prepared for their jobs. Ultimately, inadequate staffing impedes an institution's ability to deter, prevent, and respond to security threats (Russo et al., 2018).

The group acknowledged the negative connotations that corrections has for many people and discussed the need to change the way corrections careers are marketed to the public. For example, focused effort is needed to change the image of the correctional officer. A rebranding of sorts is required because many job seekers may not be attracted to a profession they perceive to be custodial in nature. Rather, in addition to the public safety and security aspects, the job should be marketed as an opportunity to serve as a change agent and positive role model to influence offender behavioral change and return better citizens to the community. The group called for research to determine the effect of these strategies on recruitment efforts and the best platforms to implement these approaches (e.g., social media marketing, media programming).

The Importance of Supervisors

The group discussed the importance of first-line supervisors for an institution's organizational culture, which can directly impact security. Participants noted that a dysfunctional culture can manifest as threats in a variety of ways (e.g., staff misconduct, turnover). Supervisors play a key role in establishing a culture because they are responsible for developing and mentoring correctional officers. The dynamics of this relationship are critical. For example, studies have linked inadequate supervisory support and dissatisfaction with supervisors with negative attitudes and turnover intention (Cheeseman et al., 2011). Furthermore, correctional officers who do not feel supported by their supervisors may be more likely to have attitudes that are conducive to institutional deviance, which is directly associated with misconduct (Worley and Worley, 2013). Because supervisors have significant influence on the behavior of officers, any deficiencies in either the quality or quantity of these positions should be addressed.

One deficiency identified by the group was that many supervisors do not receive the training needed to effectively engage with and support new hires. Supervisors should be prepared to employ more mentoring and positive reinforcement techniques and strategies to help correctional officers reach their potential and avoid compromise. This is particularly important with respect to new hires, who are often less mature. Providing greater support to these officers can improve job

Ultimately, inadequate staffing impedes an institution's ability to deter, prevent, and respond to security threats.

satisfaction, engagement, and retention while reducing misconduct and leave abuse. Workshop participants believed that it is particularly important that training include information about shifting generational attitudes toward work so that supervisors can understand and be as responsive as possible to the priorities of younger generations of officers.

Training issues aside, the group noted that supervisors often are unable to perform their important roles because of inadequate staffing. This manifests in two major ways. High vacancy rates among correctional officers can force supervisors to man empty posts. Furthermore, many institutions lack the requisite number of supervisors. This often results in an unmanageable span of control; supervisors who are responsible for too many officers can become overwhelmed and are rendered ineffective. Research is needed to quantify the effects of insufficient supervisor-to-officer ratios, as well as the effects of inadequately trained supervisors on correctional operations across a variety of measures.

Mitigating Threats Related to Staff Misconduct

Although the majority of corrections staff are dedicated professionals and carry out their duties ethically and faithfully, the criminal and unethical behavior of a subset of the sector's membership is an unfortunate reality (Worley and Worley, 2013). The actions of this small subset not only tarnish the reputation of the sector, which can impede recruitment efforts, but also constitute a threat to institutional security. As discussed earlier, supervisors can have a significant impact on institutional culture, including staff misconduct. The group also discussed broader organizational strategies to mitigate threats related to misconduct.

The small subset of staff who become compromised usually do so after they are hired; however, the group also noted that some individuals are recruited and groomed by STGs for the purposes of obtaining employment in a correctional institution. These groups will handpick sympathetic candidates who are associates of or related to members but who have no criminal record so as to avoid red flags in the agency hiring process. Once hired, these staff members are well positioned to help the STG further its criminal enterprises. For example, a sergeant with the Maryland Department of Public Safety and Correctional Services was recently indicted after being accused of being a high-ranking member of the Crips gang and facilitating criminal enterprises in state prisons and in the community on behalf of the gang (Prudente, 2017). To mitigate these types of threats, the group argued for the development of specific screening tools to identify applicants who may be especially vulnerable (or predisposed) to manipulation or compromise. With respect to existing staff, it is understood that circumstances can change over time; therefore, similar tools could be incorporated into regular performance evaluations to determine whether resistance to compromise has waned.

The working group also considered other strategies to prevent staff behaviors that could threaten institutional security. Participants argued that research is needed to better understand the underlying causes of staff misconduct, which perhaps can inform the development of more-effective interventions. One area that was discussed was training. Although all staff typically receive training regarding inmate manipulation techniques and strategies to avoid compromise, the group argued that the adequacy of this training is questionable. Research is needed to determine the most effective training modalities and approaches that can be leveraged to reduce staff misconduct.

Although more-effective training would be helpful, some level of misconduct is inevitable. The way an agency responds to these incidents, therefore, is important, both from an individual and a general deterrence perspective. Depending on the infraction and provisions included in collective bargaining agreements, agency response may include a warning, suspension, loss of pay, demotion, termination, or filing of criminal charges. Furthermore, some agencies maintain a "wall of shame" covered with photographs of disgraced former staff members along with their crimes and consequences. It is not clear which responses, if any, are effective deterrents to future misconduct. Research is needed to identify best practices.

CONTRABAND

The working group identified contraband as a major threat to institutional security. The group identified drugs, cell phones, and weapons as the most serious forms of contraband. Participants also noted that novel delivery systems (e.g., unmanned aerial systems, or drones) pose additional challenges. The following sections highlight the working group's major recommendations with respect to the threats posed by contraband. Given the differences in the needs identified across the distinct contraband categories, each is addressed in turn, and the needs are presented in separate tables. The needs in this category can be found in Tables 3 through 6.

Drugs

More than half of state prisoners and almost two-thirds of sentenced jail inmates meet the criteria for drug dependence or abuse (Bronson et al., 2017). In California, for example, one-quarter of the state's prison population was drug tested and nearly 23 percent tested positive (Associated Press, 2014). Therefore, it is not surprising that inmates spend significant time and effort to obtain drugs.

The group noted that drugs can undermine institutional security in a variety of ways. For example, STGs often control the drug trade inside institutions and use violence to protect their interests and/or to collect unpaid debts. Staff can be manipulated into bringing drugs into a facility and, once compromised, can be forced to participate in other nefarious activities. The presence of drugs also can hinder rehabilitative efforts, particularly for those inmates who are sincere in their desire to overcome addiction. Some drugs can cause dangerous behaviors that affect security, particularly in the case of synthetic marijuana (e.g., K2 and Spice). Several news reports have described inmates exhibiting acute psychotic reactions to these drugs, and symptoms include aggression or assaultive behavior (Schoenly, 2015). Finally, overdose deaths are on the rise, according to the Bureau of Justice Statistics (Noonan, 2016a; Noonan, 2016b). There is also evidence that many more deaths are associated with these drugs than are reported in the official statistics (Kennedy, 2018). Although all types of drugs may be introduced into a correctional institution, the group identified synthetic cannabinoids (e.g., K2 and Spice) and opioids (e.g., buprenorphine/Suboxone and fentanyl) as the most troublesome at the moment. These drugs can be highly potent, and users require smaller quantities. The relatively small quantities trafficked make detection difficult.

Drugs may be introduced into an institution in a variety of ways, including being transported by inmates, visitors, staff, or contractors; hidden in incoming mail and packages; and, in some cases, deposited over secure perimeters. One main pathway for drugs to enter an institution is through the mailroom. Conspirators will mail drugs in various forms to inmates in hopes that they will go undetected and reach the intended recipient. For example, suboxone strips, an often-abused prescription medication designed to treat opioid addiction, may be hidden under postage stamps or concealed by drawings. Letters may be soaked with liquefied drugs to be divided and consumed once they reach the cell block. The group noted that, although most institutions employ a variety of techniques to deter and detect this activity, more capability is needed.

Although all types of drugs may be introduced into a correctional institution, the group identified synthetic cannabinoids (e.g., K2 and Spice) and opioids (e.g., buprenorphine/Suboxone and fentanyl) as the most troublesome at the moment.

Cost-effective technologies that can quickly identify particular substances in or on mail would be helpful, but the group also recognized that it may be futile in some cases to try to detect exact drugs (e.g., synthetic or homemade cannabinoids) because the formulations are constantly changing. Rather, it might be more useful to develop a solution that could detect anomalies (i.e., anything other than paper and ink). If feasible, policies could be developed to prohibit any mail that is determined to contain any other material or substance.

Drug-infused mail can pose serious health risks to staff, especially those responsible for sifting through the large volumes of mail arriving at institutions each day. Exposure to fentanyl, a synthetic opioid many times more potent than heroin, is a particular concern, because small amounts of the drug can be lethal when inhaled or absorbed through the skin (U.S. Drug Enforcement Administration, undated). Although there have been no known fatalities, several cases of hospitalizations because of adverse reactions have been reported (White, 2017; Darby, 2018). To combat this threat, many institutions are taking measures to protect mailroom staff, including the use of gloves and negative air pressure exhaust systems. Furthermore, supplies of Naloxone are made available in case staff members are exposed to an opioid. The group argued that best practices for mailroom safety should be developed and promulgated.

Ultimately, the solution may include banning all physical, non-legal mail from entering a correctional facility, a policy

Table 3. Needs Identified Related to Drugs

Tier	Problem or Opportunity	Associated Need
1	Drugs arriving by mail is a consistent problem.	• Develop technology that can identify whether there is more than just paper (and ink) in a piece of correspondence. • Conduct research on best practices for personal protective equipment for staff handling the mail. • Identify the costs and benefits of digitization systems that can handle the range of offender correspondence (which might include electronic delivery of legal documents). • Develop technology that can identify specific drugs infused in offender correspondence.
	Drugs transported by visitors and staff are hard to detect.	• Conduct research to identify best practices with regard to searching staff and visitors. • Conduct research on the risks and benefits of using body scanners on staff and visitors.

that the Pennsylvania Department of Corrections recently implemented (Melamed, 2018). This agency has contracted with an outside vendor to receive inmate mail, convert it to digital form, and transmit it to the institution, where it will be printed and distributed to the inmates. The group called for research to analyze the costs and benefits of fully digitized inmate correspondence systems.

Drugs are also introduced into institutions by inmate visitors and compromised staff. Searching visitors for drugs is generally considered a more sensitive matter than searching inmates, and policy across agencies varies considerably in terms of what types of searches are permissible. Depending on the agency and the circumstances, visitors may be subject to a variety of different searches (e.g., metal detector, pat down, personal item search, consensual strip search). Similarly, staff may transport drugs on their way into work (echoing the importance of institutional leaders and organizational culture in reducing a broad range of threats). Correctional staff have historically received the benefit of the doubt and often were permitted to walk into the facility without search. That has slowly changed as levels of contraband have increased, and many institutions now permit various levels of screening; some require staff to carry their lunches and other personal items in clear containers to make it more difficult to smuggle contraband. The group noted that best practices are needed to help agencies mitigate this threat. The use of full-body scanners on staff and visitors requires particular attention, according to the group. These scanners emit low doses of radiation to detect drugs and other contraband hidden under clothing or in body cavities. Because of radiation exposure and privacy concerns, the group called for research to assess the risks and benefits of using this technology on staff and visitors.

Cell Phones

Contraband cell phones have been described as the most pressing concern by many correctional administrators. These devices pose a significant threat to institutional security and to public safety in general. For example, inmates have used cell phones to plan the murder of witnesses in the community, facilitate escapes, arrange attacks on corrections staff, and coordinate in-facility disturbances. Inmates have terrorized victims and operated ongoing criminal enterprises ranging from drug smuggling to elaborate wire fraud and money-laundering schemes. This problem has been well understood by the corrections sector for decades, but it has become so widespread in the past few years that the head of the Federal Communications Commission (FCC) stated that, "In the hands of an inmate, a cell phone is a weapon" (Wiltz, 2016).

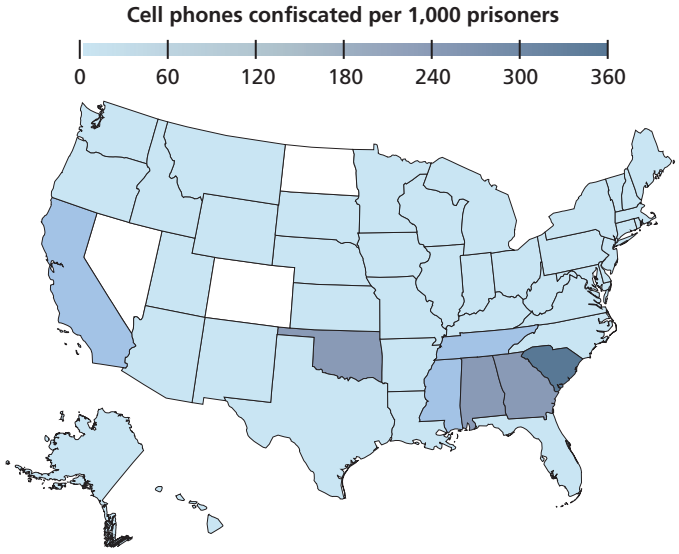
Although there is agreement that contraband cell phones represent a serious and growing threat, national statistics on prevalence are not gathered by any official source. By conservative estimates, many tens of thousands of contraband cell phones are confiscated each year. That total, however, may represent only a fraction of the total number of cell phones in circulation within the U.S. corrections system. Some states struggle more than others—see Figure 2 for an example of the amount of confiscated cell phones by state. For example, prisons in South Carolina confiscate one cell phone for every three inmates, and, in Oklahoma, the ratio is one for every six

inmates (Riley, 2017). The workshop participants argued that a national entity (e.g., federal government, Association of State Correctional Administrators [ASCA], American Correctional Association, American Jail Association) should be designated to gather and report data on the number of confiscated cell phones, which would help quantify the scope of the problem and establish trends.

Correctional institutions use a variety of strategies to combat contraband cell phones. One approach is to locate the physical devices, either in the facility itself or as they are being smuggled into the facility. Institutions commonly use intensive searches (sometimes using canines), metal detectors (including those optimized to detect components in cell phones), and full-body scanners designed to detect material under clothing or within body cavities. Other technology can detect cellular signals and provide the general location of phones in use. More-advanced solutions, known as *managed access systems*, can block unauthorized cell phones from completing a call, but do nothing to locate the device. Each of these approaches has advantages and disadvantages, but none is a silver bullet, which is why institutions typically employ a combination of approaches incorporating a mix of technologies, policies, and practices. To help agencies develop strategies to mitigate the threats posed by contraband cell phones, the group called for research into the effectiveness, costs, and benefits of each approach.

Some correctional administrators view jamming cellular signals (i.e., the transmission of interference to make it impossible for phones in facilities to connect with the cellular network) as the ultimate solution, but there are legal and technical hurdles. FCC regulations prohibit the use of jamming by state and local agencies. Furthermore, jamming is considered indiscriminate and imprecise; therefore, there are concerns that efforts to defeat contraband cell phones will inadvertently interfere with public safety communications and/or bleed over and disrupt authorized communications in the community surrounding a correctional facility using the approach. Such federal agencies as the Federal Bureau of Prisons (BOP) can obtain waivers to conduct jamming operations, and the BOP, in conjunction with the National Telecommunications and Information Administration, has tested variations of this approach in a prison environment on two occasions (U.S. Department of Justice, 2018). In the most recent tests, a technique known as "micro-jamming" showed promise in its ability to disrupt wireless signals inside a prison cell while allowing transmissions at distances of 20 and 100 feet outside the same cell. Although this technique is promising from a technical perspective, the cost of this approach is currently prohibitive for most correctional systems. The group acknowledged the value of these tests, however, and argued that state and local agencies should be able to evaluate existing and emerging technology solutions (currently legal or not) for viability. To accomplish

Figure 2. Where Cell Phones in Prisons Are Confiscated, 2017



SOURCES: Adapted from Riley, 2017; NBC News research; state corrections agencies; and the U.S. Bureau of Labor Statistics.

Table 4. Needs Identified Related to Cell Phones

Tier	Problem or Opportunity	Associated Need
1	Contraband cell phones are being used to coordinate criminal activity.	• Assemble a research and testing group in which state and local entities can test current device mitigating technologies using their specific use cases. • Identify the costs, risks, and benefits of existing technologies and policies for detecting, locating, and blocking contraband devices (including layered defense).
	An unknown number of contraband cell phones are being used to coordinate criminal activity.	• Conduct research to quantify the size of the problem (partner with the ASCA or other appropriate organization).

this, the group called for the development of a research, testing, and evaluation center empowered with the authority or blanket permission required to evaluate potential solutions as they emerge.

Weapons

The presence of weapons in a correctional institution presents a significant threat to both inmates and staff. Weapons may be manufactured by inmates using materials available inside the institution, such as pieces of plexiglass or aluminum from building materials, which can be sharpened and weaponized. Weapons also may be smuggled into the institution. Many weapons are composed of ferrous metals (e.g., iron and steel), and staff typically employ handheld or walk-through detectors to locate this contraband on inmates or incoming visitors. Non-ferrous or non-metallic weapons, such as ceramic knives, and improvised weapons, such as sharpened toothbrushes or other plastic items, are much more difficult to detect. Although full-body scanners are able to detect these threats, they are expensive and lack portability. The group argued for research to identify the feasibility of more cost-effective, hand-held technology to detect these threats.

Contraband Delivery via Drones

Unmanned aircraft systems, also known as drones, are an emerging threat to institutional security. The Federal Aviation Administration reports that more than 1 million drones are registered in the United States (U.S. Department of Transportation, 2018). The devices are relatively inexpensive, powerful, and easy to operate, which makes them a convenient vehicle for carrying contraband over facility perimeters. Drones have been used by conspirators to execute coordinated deliveries of cell phones, drugs, tobacco, pornography, and other items over secure perimeters for inmate retrieval (Craig, Russo, and Shaffer, 2016). Sometimes the package does not reach the intended target: A drone dropping tobacco and marijuana in an Ohio prison yard caused a disturbance as inmates fought for the package (Ferrigno, 2015). More-extreme examples of contraband payloads include loaded handguns and items that can be used to facilitate escape attempts, such as hacksaw blades and hair dye (Harvey, 2018). In one case, authorities believe that a drone delivered a pair of wire cutters that were used in a successful escape (Kinnard, 2017).

To counter this threat, correctional institutions are exploring drone detection and mitigation options (Craig, Russo, and Shaffer, 2016). Passive detection technologies include radio frequency detection systems, acoustic detection systems, video surveillance systems, thermal imaging and infrared devices, and seismic sensor systems that monitor the environment and use software analytics to track the location of the drone relative to the position of the deployed sensors. Active detection technologies (e.g., radar) emit energy and detect any reflection that indicates that a drone is operating in a controlled area. These technologies are relatively expensive, and their effectiveness is unknown. Once a drone is detected, however, response or mitigation options are limited. For example, current federal regulations prohibit interference with a drone's radio frequency signals or attempts to capture or "shoot down" a drone before it enters the secure perimeter. As a result, when drones are sighted, authorities must physically respond in some way to try to prevent the payload from reaching the inmate population. Independent research is needed to develop and identify the most cost-effective approaches to detecting and/or defeating drones, including options that are currently prohibited by law.

Although the participants recognized drones as an emerging threat, they also noted that there is a lack of national data quantifying the scope of the problem. Some states are beginning to gather and report these data. For example, 138 drone sightings were reported at Georgia Department of Corrections prisons in the past year, with 67 in one prison alone (Travis, 2018). As in the case of the contraband cell phone issue, the group suggested that comprehensive, national statistics on drone activity are needed because they would help identify trends and be useful to galvanize support for deterrence, detection, and mitigation strategies.

Table 5. Needs Identified Related to Weapons

Tier	Problem or Opportunity	Associated Need
1	Non-ferrous metal contraband (e.g., plastics, ceramics, aluminum) is extremely hard to detect.	• Conduct research into technologies that could cost-effectively detect these materials in a correctional environment.

Table 6. Needs Identified Related to Contraband Delivery via Drones

Tier	Problem or Opportunity	Associated Need
2	Unmanned aerial systems are being used to transport contraband.	• Conduct research to identify interdiction options (pursue obtaining legal permissions in advance as necessary).
3	Unmanned aerial systems are being used to transport contraband.	• Conduct research to quantify the size of the problem (suggest partnering with ASCA or other appropriate organization and looking for factors that might influence significant differences, such as pay, hiring practices, etc.).

INFORMATION TECHNOLOGY AND CYBER THREATS

Today's correctional institutions leverage a variety of information technology (IT) systems, many of which are provided and/or maintained by outside vendors. These systems include communications platforms (e.g., inmate telephone and email, video visitation, telemedicine, staff radios), security platforms (e.g., surveillance cameras, access control points, perimeter intrusion detection, cell doors), health and safety platforms (e.g., fire alarms, HVAC), and inmate management platforms (e.g., access to computers or tablets for entertainment, education, job skills, and reentry planning). Furthermore, institutions maintain or have access to large data sets that include case records and other information about staff and inmates. These systems often are poorly planned, coordinated, or secured, which may expose the institution to cyber threats. For example, without adequate firewall protection, the addition of third-party remote maintenance services with security flaws may create a back door into more-sensitive systems.

Several documented incidents have illustrated the vulnerabilities of institutional IT systems. Ohio inmates assigned to a program to recycle computers were able to build two computers out of parts. These computers were used to access the prison's IT network to create passes to move freely around the institution, access other inmate's records to apply for credit cards, and research tax refund fraud (Crespo, 2017). A Michigan man used a phishing scheme to hack into a county computer system and was able to change an inmate's release date (Moran, 2018). Inmates in the United Kingdom have accessed unprotected Wi-Fi hotspots to view pornography on their contraband cell phones (Parker, 2017). Furthermore, researchers have identified that control of institutional security systems, such as cell doors, may be vulnerable to malicious malware attacks (Newman, Rad, and Strauchs, 2011). The following sections highlight the group's major recommendations with respect to cyber threats to institutional security. The full list of needs can be found in Table 7.

Increasing the Awareness of Cyber Risks

Although correctional institutions are using more IT, they are generally failing to adequately manage cybersecurity risks to their systems, assets, and data, according to the participants in our workshop. The field would benefit from the development and dissemination of best practices and lessons learned based on the unique requirements of correctional institutions. Particular emphasis should be placed on integrating multiple IP-based systems into operations while protecting the institution's network and sensitive information.

The group noted that institution leadership (e.g., wardens and security chiefs) tends to focus more on physical security than on cybersecurity. This is due in part to the backgrounds of these staff, who typically come up through the ranks, beginning as correctional officers. Although such a path results in staff who are very well versed in correctional operations and physical security systems, they may lack awareness of and appreciation for the impact that cyber threats can have on an institution. Education and training are required, not to

Although correctional institutions are using more IT, they are generally failing to adequately manage cybersecurity risks to their systems, assets, and data, according to the participants in our workshop.

Table 7. Needs Identified Related to Information Technology

Tier	Problem or Opportunity	Associated Need
1	Correctional institutions are increasingly integrating automation and IT systems for daily management of cells, release date calculation, etc. There is some evidence that this increased use is introducing new vulnerabilities.	• Develop best practices specifically tailored to the unique vulnerabilities of (and unique data managed by) correctional agencies.
	Wireless internet access systems in the vicinity of institutions often can be used for communication and can be hard to detect.	• Develop guidance for monitoring the threat.
	Newer devices that are being installed to manage infrastructure (HVAC, steam plants, water systems, etc.) are often designed with connectivity that introduces vulnerabilities (i.e., the internet of things).	• Conduct research to determine best practices for how to manage these devices.
2	To facilitate reintegration and for other legitimate purposes, inmates need access to certain services on the internet (job skills, employment, etc.).	• Conduct research to determine best practices to manage the risks.
	Institutional leaders (e.g., chiefs of security, wardens) are often not up to date on institutional threats that arise in the cyber realm.	• Develop best practices and suggest standards for continuing education.
3	It is often unclear which offenders should be denied access to institutional electronic devices.	• Develop best practices for identifying offenders who should be restricted from accessing computers in an institution.
	Institution staff sometimes take risks by allowing offenders to access institutional computer systems to perform work (on behalf of staff). This may increase vulnerability on other parts of the system.	• Develop best practices for governing inmate access to IT systems.
	It is difficult to hire IT security specialists that are needed to secure the IT infrastructures at institutions.	• Conduct research into incentives that facilitate hiring and retention of IT personnel (e.g., develop capacity in-house).
	External parties often require network access to perform required services (e.g., offender management, HVAC, entertainment systems, education systems). This introduces new vulnerabilities.	• Develop a guide with best practices that considers contracting, background checks, and network configurations.

make these staff information security experts but to help them recognize that cyber threats are just as critical and potentially dangerous as physical threats. Furthermore, greater appreciation for these risks will likely help reinforce adherence to IT security policy emanating from the chief information officer or county-level IT administrators.

Need for Specialized Staff Skills

Ideally, institution leadership can rely on IT security staff to help manage these threats, but the participants noted that institutions often struggle to recruit these professionals. Not only is there a cybersecurity workforce shortage (National Institute of Standards and Technology, 2018), but qualified individuals generally can earn more money in the private sector, and the work environment may be more pleasant than in a correctional facility. To overcome this obstacle, the group called for research into actionable incentives that would attract IT security professionals to the corrections sector and, once hired, make it possible to retain them for longer periods.

Managing Inmate Access to Technology

Today's society is highly dependent on technology, which presents a significant dilemma for correctional administrators. Because 95 percent of all state inmates will be released at some point (Hughes and Wilson, 2003), it is important to prepare these individuals for reentry. Inmates need access to modern computers and applications to improve their job skills and marketability upon release. Inmates also require access to certain internet content (e.g., benefit applications, educational programs, employment applications). On the other hand, administrators recognize that access to technology and the internet poses security threats that cannot be ignored. Although many

inmates view these programs as a privilege and an opportunity for self-improvement, there are others who will seek to manipulate the system. Best practices and guidance are needed to help institutions provide inmates with access to technology to improve reentry outcomes while mitigating the inevitable risks to institutional security. Part of this assessment, according to the workshop group, should be an evaluation of an inmate's suitability for access and the restrictions, if any, that should be in place. This aspect has been underexplored but will become increasingly important as the inmate population grows more tech-savvy and more technology is introduced into the institutional setting.

Improving Policies and Procedures

As is often the case for organizations in general, users—including correctional institution staff, third-party contractors, and inmates—are typically the weakest link with respect to cybersecurity. Phishing attacks can compromise security. One state auditor conducted a fake attack and found that almost one-fifth of the 5,000 employees not only clicked on the link but entered their user ID and password (Eggert, 2018). Once armed with user credentials, a hacker can access a multitude of systems. Indeed, the Michigan hack referenced earlier was facilitated by a phishing scheme. Institutions need guidance and training on the importance of cybersecurity, including reinforcement of existing policy against allowing inmates unauthorized access to institution computers and systems, securing their login credentials, and requiring frequent password updates. Furthermore, agencies need best practices with respect to third-party vendors, many of whom require network access to perform services. Protocols should be implemented to properly vet these contractors in order to minimize threats posed by a bad actor.

SECURITY THREAT GROUPS AND CRIMINAL ACTIVITY

STGs represent a significant and growing threat to institutions and public safety. STGs are primarily made up of gangs or criminal organizations that operate inside institutions, but many also have significant reach into the community (Atherton and Phillips, 2007). Although proportions of STG members vary greatly by agency, an estimated 13 percent of the inmate population—more than 280,000 individuals—are STG members (Winterdyk and Ruddell, 2010; Kaeble and Cowhig, 2018). STG activity is linked to higher rates of violence, including homicide and control of black markets (e.g., drugs and cell phones), and can undermine rehabilitative programming. Furthermore, STGs may attempt to wield their power within the institution and in the community to manipulate or intimidate correctional staff (Winterdyk and Ruddell, 2010).

Although much STG activity may be considered part of the daily institutional routine (e.g., providing protection to vulnerable inmates for a fee), a recent incident illustrates the importance of criminal enterprises to STGs and their willingness to resort to violence to protect their interests. A disturbance at the Lee Correctional Institution in South Carolina was prompted by a gang-related dispute over control of the contraband cell phone market. This riot is considered the deadliest in 25 years: Seven inmates were murdered and 17 others were wounded (Simpson, 2018). The following section highlights the workshop participants' major recommendations with respect to STGs. The full list of needs can be found in Table 8.

Institutions use a variety of strategies to manage, contain, or disrupt STGs. For example, members may be segregated in restrictive housing to isolate leadership from the rank and file or may be transferred or displaced to another institution within a correctional system. In some cases, leaders (or "shot-callers") may be transferred to another state via established Interstate Compact Agreements. For those STG members that remain in the general population, some agencies seek to keep rival

Best practices and guidance are needed to help institutions provide inmates with access to technology to improve reentry outcomes while mitigating the inevitable risks to institutional security.

Table 8. Needs Identified Related to STGs and Criminal Activity

Tier	Problem or Opportunity	Associated Need
1	STGs are a persistent source of criminal activity both inside and outside of institutions.	• Develop best practices for managing STG populations (above and beyond concentration, dispersion, and isolation approaches).
	There are large volumes of inmate communications that go unanalyzed (e.g., recorded phone conversations, video conferencing, emails, letters). This information can be used to detect potential criminal activity.	• Assess the costs and efficacy of existing systems that can be used to identify and highlight problematic patterns.
2	Agencies are collecting STG intelligence and data (sometimes at a statewide level) but are not readily sharing that information with other agencies.	• Promote the existence and benefits of the Corrections Intelligence Initiative.
	STGs are a persistent source of criminal activity both inside and outside of institutions.	• Conduct research on the benefits and risks of housing offenders from different STGs together or separately (e.g., collect the evidence and publish findings and statistics).
3	STG-specialized skill staff attrition negatively affects the institution's knowledge base and effectiveness.	• Conduct research into the impact of incentives for officers who maintain STG specialization and expertise.
	STGs are a persistent threat to criminal activity both inside and outside of institutions.	• Increase awareness of the benefits and risks of using interstate transfers as a defense against STG violence.
	Movement and association patterns can be indicative of criminal activity (or potential criminal activity) within an institution.	• Conduct research into video analytics that could be used to identify problematic patterns.
	There are large volumes of offender communications that go unanalyzed (e.g., recorded phone conversations, video conferencing, emails, letters). This information can be used to detect potential criminal activity.	• Identify the benefits and risks of employing local hackathon groups to develop low-cost solutions.
	Some risk assessment tools (e.g., problem classification or prediction) are out of date. They were often designed with different assumptions in mind (institution structure, practices, etc.).	• Conduct research into the processes and best practices for validating risk assessment tools (to include timelines for revalidation).

groups apart or, conversely, attempt to balance membership in housing units so as to limit the power of any single group. Other strategies focus on treatment-based approaches designed to change behavior. These strategies typically take the form of gang renunciation or disassociation programs and may incorporate anger management and other cognitive-based interventions designed to improve decisionmaking skills and identify alternatives to violence.

Existing research on the effectiveness of these strategies is limited, and the results of the research that is available are mixed. Indeed, no single strategy has been proven effective; results seem to vary depending on jurisdiction and characteristics of the STG (Winterdyk and Ruddell, 2010). The workshop group argued that more research is required in order to identify which interventions are achieving the desired outcomes and, to the extent possible, the reasons for success so that they can be broadly adopted.

Many institutions designate a staff member to serve as an STG intelligence coordinator, which is a critical position, according to the workshop group. This individual is typically responsible for coordinating efforts to identify and validate inmates as gang members at intake and throughout incarceration. This staff member also monitors STG activity trends, processing intelligence information from various systems (e.g., searches, mail, phone, visitation, inmate accounts); identifies early warning signs; and helps develop proactive intervention strategies. STG coordinators must keep abreast of activity inside their institutions, and they often interface with federal, state, and local law enforcement. These staff members develop a specialized skill set and expertise over time, becoming "gang experts." The group recognized the importance of maintaining continuity in this position, but it also noted obstacles. For example, in many agencies, there is no opportunity for advancement: In order to be promoted, STG coordinators must

transfer to another role. The group called for exploration of how incentives (e.g., creating a career ladder within this specialization) can be designed to keep key staff in place.

Technology also can be leveraged to better identify and disrupt criminal behavior, according to the participants. For example, inmate movement patterns can identify potential associations indicating an individual's involvement with an STG. Movement patterns among groups may indicate burgeoning alliances or impending battles between such groups. Finally, patterns of interactions between individual inmates may provide insight as to which inmates are dealing in contraband. Research is needed to determine whether automated video analytics, biometrics, or other technologies can be an effective method of detecting criminal activity.

Better tools are needed to improve the process of screening inmate communications. Resource constraints make it impractical for institutions to thoroughly analyze the volumes of telephone conversations, emails, texts, letters, and other forms of communication that go into and out of institutions every day. Automated analytical tools are needed to quickly identify items of interest or concern. Ideally, these tools would be able to translate and analyze foreign words, whether written or spoken.

Finally, correctional staff gather a wealth of information, but deficiencies exist in sharing intelligence with other correctional institutions and law enforcement agencies across the country. This represents a missed opportunity because many STGs have a national presence and criminal or other disruptive activities may be coordinated by inmates in different parts of the country. Agencies should leverage existing platforms for information-sharing, such as the National Joint Task Force's Corrections Intelligence Initiative, the Regional Information Sharing Systems, and the Federal Bureau of Investigation's National Data Exchange System. However, the group noted that there may be a lack of awareness of these resources. Better promotion of the existence and benefits of these initiatives is required so that agencies can fully leverage them.

Resource constraints make it impractical for institutions to thoroughly analyze the volumes of telephone conversations, emails, texts, letters, and other forms of communication that go into and out of institutions every day.

EMERGENCY PREPAREDNESS

Beyond the daily threats that confront correctional institutions are emergency situations that may arise with little—if any—notice. Natural disasters, such as hurricanes, tornados, earthquakes, wildfires, and flooding, may require mass evacuations. Even fairly routine situations, such as an extended blizzard, may prevent staff from getting to work to relieve their coworkers.

During emergencies large and small, institutions must maintain their responsibility to inmate, staff, and overall public safety. It is therefore critical that continuity of operations plans (COOPs) are in place and staff are prepared to carry them out. The group noted that although most, if not all, institutions have COOPs, best practices are needed because there is much that can be learned from organizations that have developed particularly effective plans and/or have executed them in extreme conditions and have the benefit of real-world experience.

Table 9. Needs Identified Related to Emergency Preparedness

Tier	Problem or Opportunity	Associated Need
2	Institutions are unaware of particularly effective COOPs and practices that other agencies and institutions may have figured out.	• Conduct research into and identify best practices for developing institutional COOPs.

CONCLUSION

Correctional institutions have enormous and complex responsibilities. They are charged with protecting the public from dangerous individuals, but, at the same time, they must prepare those under correctional control for successful, law-abiding lives in the community after release. Correctional institutions face significant security threats that may compromise both of these objectives. The 20 high-priority (Tier 1) needs identified during the workshop define the following agenda for action by research, technology, and institutional actors in order to make progress in addressing threats to institutional correctional security at all levels:

- **The importance of a quality workforce:** Humans often are the weakest link in any security program, and many correctional institutions struggle to recruit and retain a high-quality workforce. High vacancy and turnover rates contribute to understaffing and an increase in the number of inexperienced officers. Furthermore, compromised staff are a major problem with respect to contraband introduction. Inadequate staffing in terms of numbers and/or quality is a direct threat to institutional security. Innovative strategies are needed to attract recruits, and processes are required to screen out individuals who may be prone to misconduct or compromise. Supervisors are key to improving officer engagement and job satisfaction, which can support retention efforts.
- **Strategies for stopping contraband:** Drugs, cell phones, and non-metallic weapons were identified as the types of contraband that pose the greatest threats to institutional security. The group argued for better technology options for detection and exploration of best practices to search staff and visitors. Furthermore, the viability of fully electronic mail systems should be explored to reduce the influx of drugs and protect staff and inmates from harm. Finally, national data are needed on the extent of the cell phone and drone problem in correctional facilities, and more flexibility is needed at the state and local levels to test all available options to detect and defeat these emerging threats.
- **STGs and inmate criminal activity:** STGs continue to plague correctional institutions. Research is needed to identify best practices to manage this difficult population. Technologies to efficiently analyze inmate communications and identify associations based on inmate movement patterns would help control criminal activity. Furthermore, institutions need to do a better job of sharing information on STGs with counterparts across the country, as well as with law enforcement agencies.
- **Cyber threats:** The correctional institution of today faces security threats that were likely not anticipated only a few decades ago. Many institutions have incorporated numerous IT and other automated systems to support operations; however, few have the resources or foresight to focus on the associated cyber threats. Institutions need greater awareness of these threats, as well as greater information security specialist capacity. Furthermore, because it is becoming more important to allow inmates access to technology to prepare them for reentry, it is critical that institutions understand best practices for managing inherent risks.

Some threats to institutional security (e.g., violence, escape attempts, contraband) are as old as the institutions themselves. Other threats (e.g., computer hacks, synthetic drugs, cell phones, drones) have evolved with societal and technological changes. Many of these threats present risks not only to the institution but also to public safety as a whole. Unfortunately, resource and staffing challenges limit the ability of correctional institutions to adapt to such shifts in threats and to adjust security and staffing strategies over time. Furthermore, a perpetual lack of empirical data hampers efforts to effectively develop interventions to address threats. Addressing the research needs and developing the tools and resources—as prioritized by the workshop participants—is one route to providing correctional institutions the support needed to confront security threats going forward.

APPENDIX. TECHNICAL METHODS

This appendix presents additional detail on the panel process, needs identification, and prioritization carried out to develop the research agenda presented in the main report.

Pre-Workshop Activities

University of Denver and RAND researchers recruited the panel members by extending invitations to knowledgeable individuals identified through existing professional and social networks (e.g., LinkedIn) and by reviewing literature published on the topic. At the time of the invitation, panelists were provided with a brief description of the workshop's focus areas. To prepare for the workshop, panelists were provided with read-

ahead materials and were given an opportunity to identify the issues and topics that they felt would be important to discuss during the workshop. The read-ahead document and results of the pre-panel questionnaire are discussed in the main report. The workshop agenda is presented in Table A.1.

Prioritization of Needs

During the workshop, the moderators led the participants through a discussion of each of the themes that were identified prior to the workshop. While conducting this review, participants suggested areas worthy of additional research or investment. Workshop participants also considered whether there were areas that were not included in the existing list and suggested new ones.

To develop and prioritize a list of technology and policy areas that are likely to benefit from research and development investment and implementation by corrections agencies, we followed a process that has been used in previous research (see, for example, Jackson et al. [2016] and references therein). The panelists discussed and refined issues and problems in each category and also identified potential needs (e.g., solutions) that could address each issue or problem. In addition to needs that represented defined solutions to problems, in some cases needs were actions needed to capitalize on opportunities—e.g., new technologies or possible changes in practice that could improve performance or efficiency in the sector.

At the end of the discussion of each theme, the panelists were given an opportunity to review and revise the list of problems and opportunities and their corresponding needs. These were each displayed in the front of the room using Microsoft PowerPoint slides.

Once the panel agreed on the wording of each slide, we asked panelists to anonymously vote using a handheld "clicker" (specifically, the ResponseCard RF LCD from Turning Technologies). Each panelist was asked to individually score each issue and its associated need using a 1–9 scale for the following dimensions: (1) importance, and (2) probability of success. For each dimension, participants were instructed that 1 was a "low" score and 9 was a "high" score:

- Participants were told to score the importance/payoff dimension with a 1 if the need/solution would have little or no impact on the problem and with a 9 if the need/solution would reduce the impact of the problem by 20–30 percent

Table A.1. Workshop Agenda

Day 1	
8:30	Welcome, Overview, and Introductions
9:00	Identify Emerging Threats: Challenges and Solutions—Theme 1
10:00	Rank, Discuss, Re-Rank Needs—Theme 1
10:30	Break
10:45	Identify Emerging Threats: Challenges and Solutions—Theme 2
11:45	Rank, Discuss, Re-Rank Needs—Theme 2
12:15	Lunch
1:30	Identify Emerging Threats: Challenges and Solutions—Theme 3
2:30	Rank, Discuss, Re-Rank Needs—Theme 3
3:00	Break
3:15	Identify Emerging Threats: Challenges and Solutions—Theme 4
4:15	Rank, Discuss, Re-Rank Needs—Theme 4
5:00	Adjourn

Day 2	
8:30	Identify Emerging Threats: Challenges and Solutions—Theme 5
9:30	Rank, Discuss, Re-Rank Needs—Theme 5
10:00	Break
10:15	Identify Emerging Threats: Challenges and Solutions—Theme 6
11:15	Rank, Discuss, Re-Rank Needs—Theme 6
11:45	Lunch
1:00	Discuss/Adjust Overall Rankings
2:15	Meeting Wrap-Up/Administrative Issues
3:00	Adjourn

(or more). Anchoring the performance scale with percentage improvements in performance is intended to help make rating values more comparable from participant to participant.
- For the probability of success dimension, panelists were instructed to treat the 1–9 scale like a percentage chance of success from 10 percent to 90 percent. Probability of success was intended to include not only technical concerns (e.g., would the need itself be hard to meet?) but also the effect of factors that might lead corrections agencies to not adopt the new technology, policy, or practice even if it were developed (e.g., cost, staffing concerns, societal concerns).

After the panelists voted on a particular slide (i.e., either on the importance or probability of success for a need), we presented them with a histogram-style summary of their responses directly on the PowerPoint slide being displayed at the front of the room. If there was a significant disagreement among the panel (the degree of disagreement was determined by the moderators' visual inspection of the histogram), the panelists were asked to verbally discuss or advocate for their views at one end of the spectrum or the other (i.e., participants who voted high making an argument to persuade those who voted low, or vice versa). If a second-round discussion occurred, the panelists were given an opportunity to adjust their vote by voting a second time on the same question. This second round vote was optional, and any vote cast by a panelist would replace the vote they provided during the first round. This process was repeated for each question and dimension at the end of each topical section. An example of the importance and probability of success slides are shown in Figure A.1 and Figure A.2, respectively.

Once the panelists had completed the voting process for all topical sections, we summarized their votes into a single prioritized list. We rank-ordered the list by calculating an expected value using the method outlined in Jackson et al. (2016). For each question, the final (round 2) importance and likelihood of success votes were multiplied to produce an expected value (EV) for the need. We then calculated the median of that product as the group's rating of the need.

The resulting EV scores were then clustered using a hierarchical clustering algorithm. The algorithm we used was the "ward.D" spherical algorithm from the "stats" library in the R statistical package, version 3.4.4. We chose this algorithm to minimize within-cluster variance when determining the breaks between tiers. The choice of three tiers is arbitrary but was done in part to remain consistent across the set of technology workshops we have conducted for NIJ. Also, the choice of three tiers represents a manageable system for policymakers. Specifically, the top tier is made up of the priorities that should be the primary focus for practitioners, researchers, and policymakers. The middle tier should be examined closely by the same groups, and the final tier is probably not worth much attention at present, although changes in circumstances or environment that shift the perceived value or likelihood of success could change that assessment in the future.

Because the panelists initially rated the needs of one topical group at a time, we provided the participants an opportunity at the end of the workshop to review and weigh in on the entire tiered list of all the identified needs. The intent of this step was to let the panel members see the needs in the context of the other tiered needs and allow them to consider whether there were needs that appeared too high or low relative to the others. To collect this assessment, we had a modified "third Delphi round" (similar to that employed in Hollywood et al., 2016): The entire tiered list was printed onto a paper form and distributed to the panelists, and we asked them to examine the overall tiering and ranking of each of the problems/opportunities and their corresponding needs. We then gave them the opportunity to provide a single vote for each need that they felt should be higher or lower on the list. An example of this form is provided in Table A.2.

After the workshop concluded, we tallied the panelists' round 3 responses and applied those votes to produce a final prioritized and tiered list. To adjust the EVs using the up and down votes from the third round of prioritization, we assigned a value to each vote based on the range in EV scores between the lowest-rated Tier 3 need and the highest-rated Tier 1 need. Specifically, if every panel member voted "up" on the item at the bottom (or conversely voted down on the item at the top), then the collective effect of those votes would be to adjust the EV of the item at the bottom of the list of priorities to equal the EV of the item at the top (or vice versa). To implement this change, the full range of EVs was divided by the total number of panelists to determine the "EV point value" for a single vote.

To prevent the (somewhat rare) situation in which small numbers of votes would have an unintended outsized impact (e.g., where the EV range for a tier is particularly "thin" or where a tier consisted of several items that are all tied for EV score), we also required that at least 25 percent of the workshop participants voted on that item before the need's EV would be adjusted. This constraint is intended to reflect the goal of the Delphi process to produce a group consensus rating, and the

threshold was defined to identify cases in which a significant percentage of the group believed the tier assigned to the need was incorrect. For this workshop, there were 17 participants, so for any Round 3 votes to have an effect on a need's EV, at least four of the attendees would have had to have voted on the item in Round 3. For needs with at least four votes, their EV was then adjusted based on the net votes they received (i.e., if a Tier 2 need received two up votes and two down votes, the up and down votes would cancel each other out even though it had met the 25-percent threshold for the votes to be considered).

After applying the up and down vote points to the Round 2 EVs, we then compared the modified EV scores to the tier boundary EVs. As with prior work (e.g., Jackson et al. [2016]), we set a higher bar for an item 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:

- A need could *increase or decrease by one tier* if the modified EV was higher than the lowest EV score in the tier above (or lower than the highest EV in the tier below). That is, as long as its increase or decrease was enough to get above the highest need in its original tier or below the lowest need in the tier, then the need would be moved from the lower to the higher tier (or vice versa).
- However, *to increase or decrease by two tiers* (which was only possible for needs that started in Tiers 1 or 3), the score had to increase or decrease by an amount that fully placed the need into the range two tiers away. This means that—for cases in which clusters of needs EVs had some separation between them—just getting into the score range between two tiers was not enough to move two full tiers.

As a result of the third round of voting, 24 needs did not change their position, two needs fell one tier, and 13 needs rose one tier. Two needs changed by two tiers (one down and one up).[3] The output from this process became the final ranking as the panel's prioritized results.

Figure A.3 shows the distribution of needs by the EV score before and after the Round 3 voting process. The height of the bar indicates the number of needs that had that score, and the color of the bar indicates the tier that the need was ultimately assigned to by the clustering algorithm and the Round 3 voting process.

Figure A.1. Example Slide for Importance

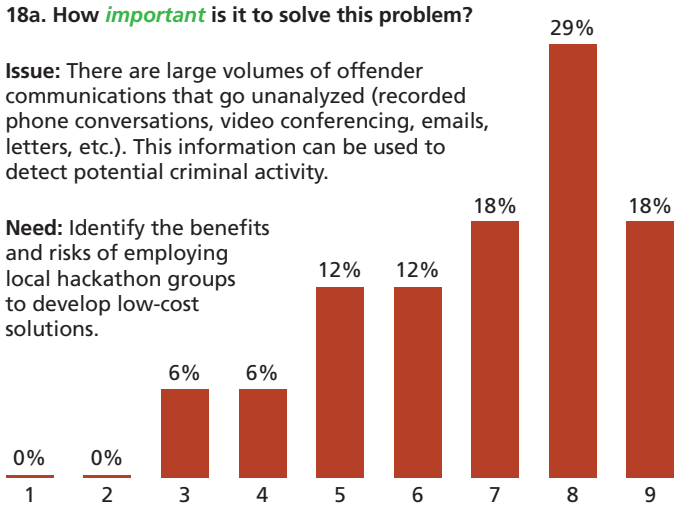


Figure A.2. Example Slide for Probability of Success

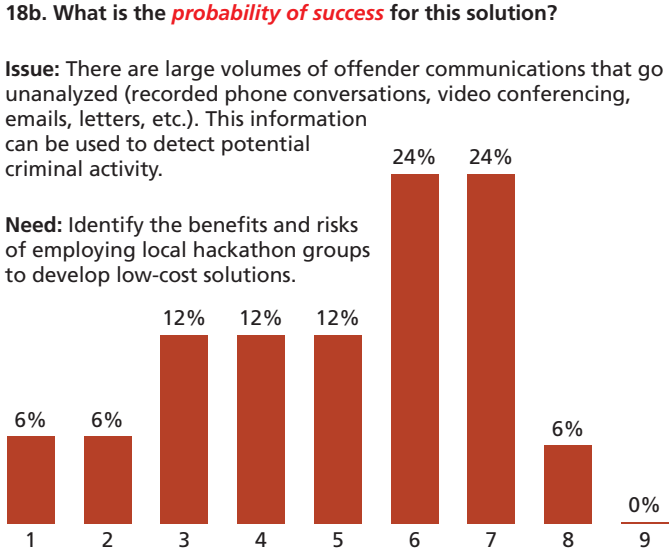
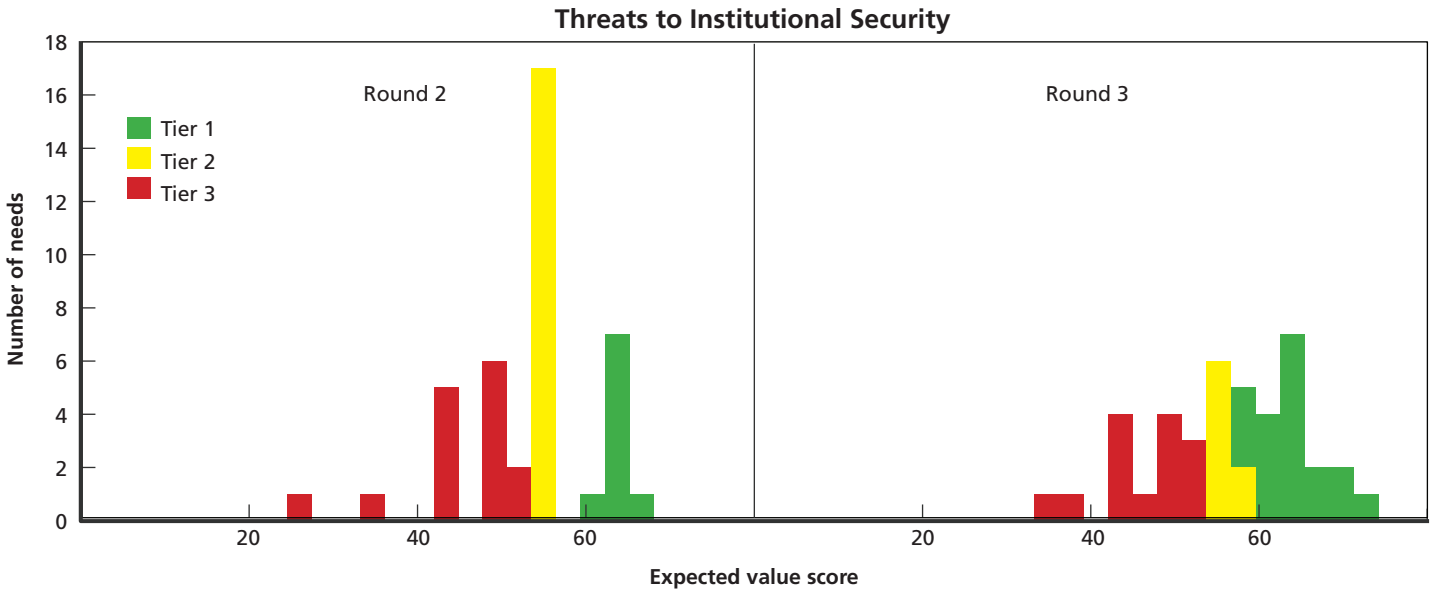


Table A.2. Example Portion of the Delphi Round 3 Voting Form

Question	Tier	Vote Up	Vote Down
Tier 1			
Issue: Some factors may make certain staff more vulnerable to STGs or other negative influences than others, which make them more susceptible to compromise. **Need:** Develop a risk assessment (i.e., suitability test) instrument to inform hiring and management decisions.	1		
Issue: Correctional institutions are increasingly integrating automation and IT systems for daily management of cells, release date calculation, etc. There is some evidence that these systems are introducing new vulnerabilities. **Need:** Develop best practices specifically tailored to the unique vulnerabilities of (and unique data managed by) correctional agencies.	1		
Tier 2			
Issue: Unmanned aerial systems are being used to transport contraband. **Need:** Conduct research to identify interdiction options (pursue obtaining legal permissions in advance as necessary).	2		
Issue: Training may be inadequate to prepare staff to avoid/manage inmate attempts to manipulate or otherwise compromise their positions. **Need:** Conduct research and assessment to ensure that the educational model and trainers are up to date with the latest approaches (best practices for duration, location, delivery, etc.).	2		
Tier 3			
Issue: STGs are a persistent threat to criminal activity both inside and outside of institutions. **Need:** Increase awareness of the benefits and risks of using interstate transfers as a defense against STG violence.	3		
Issue: It is difficult to hire IT security specialists that are needed to secure the IT infrastructures at institutions. **Need:** Conduct research into incentives that facilitate hiring and retention of IT personnel (e.g., develop capacity in-house).	3		

NOTE: Shaded cells indicate that up or down votes were not possible (e.g., Tier 1 is the top tier, so it was impossible to upvote items in that tier).

Figure A.3. Distribution of the Clustered Needs Following Rounds 2 and 3



Notes

[1] Greater detail on the prioritization process is included in the Technical Appendix.

[2] The output from the workshop actually produced one additional need, for a total of 41 prioritized needs. However, two of the needs relating to STGs were extremely similar, and both fell into the same tier after prioritization. For simplicity, they were combined in postanalysis to produce the final set of 40 needs.

[3] The need that moved up by two tiers in Round 3 was conducting research to quantify the scale of the problem of contraband cell phones being used to coordinate criminal activity. The need that dropped two tiers focused on the development of best practices to address risk from external parties having access to correctional agency IT networks for service provision and maintenance.

References

Associated Press, "California Prisons Find 1 in 4 Inmates Used Drugs," April 7, 2014. As of August 22, 2016: http://losangeles.cbslocal.com/2014/04/07/california-prisons-find-1-in-4-inmates-used-drugs/

———, "Decades of Neglect Underpins $1.65 Billion Prisons Request," *Fortune*, November 27, 2016. As of March 4, 2019: http://fortune.com/2016/11/27/oklahoma-prison-maintainence/

Association of State Correctional Administrators, "Current Issues in Corrections Survey," 2017a.

———, "Survey on Correctional Officer Salary, Vacancy and Turnover," 2017b.

Atherton, Eugene E., and Richard L. Phillips, *Guidelines for the Development of a Security Program*, 3rd ed., Alexandria, Va.: American Correctional Association, 2007.

Bronson, Jennifer, Jessica Stroop, Stephanie Zimmer, and Marcus Berzofsky, *Drug Use, Dependence, and Abuse Among State Prisoners and Jail Inmates, 2007–2009*, Bureau of Justice Statistics, June 2017.

Cheeseman, Kelly A., Bitna Kim, Eric G. Lambert, and Nancy L. Hogan, "Correctional Officer Perceptions of Inmates and Overall Job Satisfaction," *Journal of Crime and Justice*, Vol. 34, No. 2, July 2011.

Craig, Todd R., Joe Russo, and John S. Shaffer, "Eyes in the Skies: The Latest Threat to Correctional Institution Security," *Corrections Today*, November/December 2016.

Crespo, Gisela, "Investigation Found Ohio Inmates Built and Hid Computers in Prison," CNN, April 12, 2017. As of July 6, 2018: https://www.cnn.com/2017/04/12/us/ohio-jail-computers-trnd/index.html

Darby, Chris, "Allen County Sheriff Working to Protect Jail After Hazmat Incidents," Wane.com, June 7, 2018. As of July 6, 2018: https://www.wane.com/news/local-news/allen-county-sheriff-working-to-protect-jail-after-hazmat-incidents/1222689294

DeLisi, Matt, "Criminal Careers Behind Bars," *Behavioral Sciences and the Law*, Vol. 21, No. 5, September/October 2003, pp. 653–669.

Eggert, David, "1 in 3 Michigan Workers Tested Opened Fake 'Phishing' Email," Phys.org, March 16, 2018. As of July 6, 2018: https://phys.org/news/2018-03-michigan-workers-fake-phishing-email.html#jCp

Ferrigno, Lorenzo, "Ohio Prison Yard Free-for-All After Drone Drops Drugs," CNN, August 5, 2015. As of July 7, 2018: https://www.cnn.com/2015/08/04/us/prison-yard-drone-drugs-ohio/index.html

Gokavi, Mark, "Suspect in Jail Fentanyl OD Death Sentenced in 2 Federal Drug Cases," Dayton Daily News, August 28, 2018. As of November 28, 2018: https://www.daytondailynews.com/news/crime--law/suspect-jail-fentanyl-death-sentenced-federal-drug-cases/Ng7JJjlqFZnCwJljHzIFCJ/

Grommon, Eric, Jeremy Carter, and Charles Sheer, "Quantifying the Size of the Contraband Cell Phone Problem: Insights from a Large Rural State Penitentiary," *The Prison Journal*, Vol. 98, No. 5, 2018, pp. 630–648.

Harvey, Kyle, "Hair Dye Kits, Heroin and Hacksaw Blades Among Items Delivered to Prisons via Drones," *Eyewitness News*, April 20, 2018. As of July 7, 2018: https://bakersfieldnow.com/news/investigations/state-prisons-fight-growing-number-of-drones-delivering-contraband

Hennigan, W. J., "Experts Say Drones Pose a National Security Threat—and We Aren't Ready," *Time*, May 31, 2018. As of March 4, 2019: http://time.com/5295586/drones-threat/

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*, Santa Monica, Calif.: RAND Corporation, RR-1462-NIJ, 2016. As of May 10, 2018: http://www.rand.org/pubs/research_reports/RR1462.html

Hughes, Timothy, and Doris James Wilson, "Reentry Trends in the United States," Bureau of Justice Statistics, August 2003. As of May 10, 2019: https://www.bjs.gov/content/reentry/reentry.cfm

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*, Santa Monica, Calif.: RAND Corporation, RR-1255-NIJ, 2016. As of May 10, 2019: http://www.rand.org/pubs/research_reports/RR1255.html

Johnson, Kevin, "Exclusive: As Federal Prisons Run Low on Guards, Nurses and Cooks Are Filling In," *USA Today*, February 13, 2018. As of July 6, 2018: https://www.usatoday.com/story/news/politics/2018/02/13/ill-equipped-and-inexperienced-hundreds-civilian-staffers-assigned-guard-duties-federal-prison-secur/316616002/

Kaeble, Danielle, and Mary Cowhig, *Correctional Populations in the United States, 2016*, Bureau of Justice Statistics, April 2018. As of May 10, 2019: https://www.bjs.gov/content/pub/pdf/cpus16.pdf

Kennedy, Emma, "Drugs in Panhandle Prisons: 75% of Non-Natural or Suicide Prison Deaths Involved Spice," *Pensacola News Journal*, June 16, 2018. As of July 6, 2018: https://www.pnj.com/story/news/crime/2018/06/16/drugs-panhandle-prisons-75-non-natural-suicide-prison-deaths-involved-spice/703041002/

Kinnard, Meg, "SC Officials: Illegal Cellphone, Drone Aided Inmate's Escape," *Washington Post*, July 8, 2017. As of July 7, 2018: https://www.washingtonpost.com/amphtml/national/escaped-inmate-may-have-used-wire-cutters-delivered-by-drone/2017/07/07/10c6e3fc-638d-11e7-80a2-8c226031ac3f_story.html&freshcontent=1

Lyman, Brian, "Alabama Corrections Officers' Ranks Drop 20 Percent," *Montgomery Advertiser*, January 7, 2017. As of December 5, 2017: http://www.montgomeryadvertiser.com/story/news/politics/southunionstreet/2017/01/08/alabama-corrections-officers-ranks-drop-20-percent/95762920/

Matz, Adam K., James B. Wells, Kevin I. Minor, and Earl Angel, "Predictors of Turnover Intention Among Staff in Juvenile Correctional Facilities: The Relevance of Job Satisfaction and Organizational Commitment," *Youth Violence and Juvenile Justice*, Vol. 11, No. 2, April 1, 2013.

McShane, Marilyn D., and Franklin P. Williams, eds., *Encyclopedia of American Prisons*, New York: Garland Publishing, 1996.

Melamed, Samantha, "Pa. Prison Books and Mail Policies Draw Protests, Petitions, and Possible Legal Challenges," *Philadelphia Inquirer*, September 13, 2018. As of November 28, 2018: http://www2.philly.com/philly/news/books-through-bars-pennsylvania-prisons-k2-security-john-wetzel-20180913.html

Moran, Darcie, "Man Gets 7 Years in Federal Prison for Hack that Cost Washtenaw $235k," MLive.com, April 26, 2018. As of July 6, 2018: https://www.mlive.com/news/ann-arbor/index.ssf/2018/04/man_gets_7_years_in_federal_pr.html

National Institute of Standards and Technology, "Report: U.S. Needs Immediate and Sustained Improvements in Its Cybersecurity Workforce," webpage, May 30, 2018. As of July 6, 2018: https://www.nist.gov/news-events/news/2018/05/report-us-needs-immediate-and-sustained-improvements-its-cybersecurity

Newman, Teague, Tiffany Rad, and John Strauchs, "SCADA and PLC Vulnerabilities in Correctional Facilities," white paper, July 30, 2011. As of July 6, 2018: https://www.wired.com/images_blogs/threatlevel/2011/07/PLC-White-Paper_Newman_Rad_Strauchs_July22_2011.pdf

Noonan, Margaret E., *Mortality in Local Jails, 2000–2014—Statistical Tables*, Washington, D.C.: Bureau of Justice Statistics, NCJ 250169, December 2016a.

———, *Mortality in State Prisons, 2000–2014—Statistical Tables*, Washington, D.C.: Bureau of Justice Statistics, NCJ 250150, December 2016b.

Ovalle, David, "Two Inmates Indicted for Murder in Fentanyl Overdose Death in Miami-Dade Jail," *Miami Herald*, November 8, 2018. As of November 28, 2018: https://www.miamiherald.com/news/local/crime/article221280565.html

Parker, Andrew, "Inmates Busted Using WiFi from Nearby Homes to Watch Porn," *New York Post*, July 30, 2017. As of July 6, 2018: https://nypost.com/2017/07/30/inmates-busted-using-wifi-from-nearby-homes-to-watch-porn/

Prudente, Tim, "Indictment Alleges Jessup Prison Guard Moonlighted as Crips Gang Chief," *Baltimore Sun*, November 30, 2017. As of July 13, 2018: http://www.baltimoresun.com/news/maryland/crime/bs-md-prison-gang-indictments-20171130-story.html

RAND Corporation, "Delphi Method," webpage, undated. As of May 10, 2019: https://www.rand.org/topics/delphi-method.html

Riley, Matt, "Southern Prisons Have a Cellphone Smuggling Problem," *NBC News*, September 30, 2017. As of July 7, 2018: https://www.nbcnews.com/news/corrections/southern-prisons-have-smuggled-cellphone-problem-n790251

Russo, Joe, Dulani Woods, George B. Drake, and Brian A. Jackson, *Building a High-Quality Correctional Workforce: Identifying Challenges and Needs*, Santa Monica, Calif.: RAND Corporation, RR-2386-NIJ, 2018. As of May 10, 2019: https://www.rand.org/pubs/research_reports/RR2386.html

Schoenly, Lorry, "Synthetic Marijuana: A Very Real Contraband Hazard," *CorrectionsOne*, August 25, 2015. As of July 6, 2018: https://www.correctionsone.com/corrections/articles/8720953-Synthetic-marijuana-A-very-real-contraband-hazard/

Simpson, Ian, "Deadly South Carolina Prison Riot Exposes Staffing Shortage," Reuters, April 19, 2018. As of July 14, 2018: https://www.reuters.com/article/us-south-carolina-prison-guards/deadly-south-carolina-prison-riot-exposes-staffing-shortage-idUSKBN1HQ1A5

Tolbert, Michelle, and Jordan Hudson, *Educational Technology in Corrections 2015*, Washington, D.C.: U.S. Department of Education, Office of Career, Technical, and Adult Education, 2015. As of May 10, 2019: https://www2.ed.gov/about/offices/list/ovae/pi/AdultEd/policybriefedtech.pdf

Travis, Randy, "Fox 5 I-Team Tests Prison Drone Warning System," Fox 5, May 23, 2018. As of July 7, 2018: http://www.fox5atlanta.com/news/i-team/fox-5-i-team-tests-prison-drone-warning-system

U.S. Department of Justice, "Prison Test Shows Micro-Jamming May Counter Criminal Threat of Contraband Cell Phones," press release 18-794, June 15, 2018. As of July 7, 2018: https://www.justice.gov/opa/pr/prison-test-shows-micro-jamming-may-counter-criminal-threat-contraband-cell-phones

———, Office of the Inspector General, Review of the Federal Bureau of Prisons' Contraband Interdiction Efforts , June, 2016. As of July 1, 2019: https://oig.justice.gov/reports/2016/e1605.pdf

U.S. Department of Transportation, "FAA Drone Registry Tops One Million," press release, January 10, 2018. As of July 7, 2018: https://www.transportation.gov/briefing-room/faa-drone-registry-tops-one-million

U.S. Drug Enforcement Administration, "Fentanyl," webpage, undated. As of July 6, 2018: https://www.dea.gov/factsheets/fentanyl

Wagner, Peter, and Wendy Sawyer, "Mass Incarceration: The Whole Pie 2018," Prison Policy Initiative, press release, March 14, 2018. As of July 6, 2018: https://www.prisonpolicy.org/reports/pie2018.html

White, Patrick, "Series of Fentanyl Exposures Puts Canadian Prison Staff on High Alert," *The Globe and Mail*, August 9, 2017. As of July 6, 2018: https://www.theglobeandmail.com/news/national/series-of-fentanyl-exposures-in-three-week-span-puts-canadian-prison-staff-on-high-alert/article35918236/

Wiltz, Teresa, "States Bedeviled by Contraband Cellphones in Prisons," Pew Stateline blog, June 7, 2016. As of July 7, 2018: http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2016/06/07/states-bedeviled-by-contraband-cellphones-in-prisons

———, "Should Social Media Be Banned in Prison?" Pew Stateline blog, January 13, 2017. As of March 4, 2019: https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2017/01/13/should-social-media-be-banned-in-prison

Winterdyk, John, and Rick Ruddell, "Managing Prison Gangs: Results from a Survey of U.S. Prison Systems," *Journal of Criminal Justice*, Vol. 38, No. 4, July 2010, pp. 730–736.

Worley, Robert Michael, and Vidisha Barua Worley, "Games Guards Play: A Self-Report Study of Institutional Deviance Within the Texas Department of Criminal Justice," *Criminal Justice Studies*, Vol. 26, No. 1, March 2013, pp. 115–132.

Acknowledgments

The authors would like to acknowledge the participation and assistance of the members of the Emerging Threats to Correctional Institution Security expert workshop listed in the body of the report. This effort would not have been possible without their generous willingness to spend their time participating in the effort. The authors would also like to acknowledge the contributions of Steve Schuetz, Jack Harne, and Marie Garcia of the National Institute of Justice. The authors also acknowledge the valuable contributions of the peer reviewers of the report, Meagan Cahill and Lori Uscher-Pines of RAND and Mark Foxall of the University of Nebraska-Omaha, and the anonymous reviewers from the U.S. Department of Justice.

The RAND 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 the National Institute of Justice. 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 both the New York City Departments of Correction and Probation. He has an M.S. in criminal justice.

Dulani Woods is a data science practitioner adept at data acquisition, transformation, visualization, and analysis. His primary areas of research have included homeland security and justice policy. He has a master's degree in agricultural economics (applied economics).

John S. Shaffer is an independent correctional consultant and subcontractor to the University of Denver. He served 31 years with the Pennsylvania Department of Corrections before retiring from his position as the Executive Deputy Secretary. His recent research topics include correctional health care services and technology evaluations. He holds a Ph.D. in public administration.

Brian A. Jackson is a senior physical scientist at the RAND Corporation. 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 has a Ph.D. in bioinorganic chemistry.

About This Report

On behalf of the U.S. Department of Justice, National Institute of Justice (NIJ), the RAND Corporation, in partnership with the Police Executive Research Forum (PERF), 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 initiative is a component of the National Law Enforcement and Corrections Technology Center (NLECTC) System and is intended to support innovation within the criminal justice enterprise. For more information about the NLECTC Priority Criminal Justice Needs Initiative, see www.rand.org/well-being/justice-policy/projects/priority-criminal-justice-needs

This report is one product of that effort. It presents the results of an expert workshop focused on identifying and prioritizing ways to address institutional security concerns in the corrections sector. This report and the results it presents should be of interest to planners from corrections agencies, research and operational criminal justice agencies at the federal level, private-sector technology providers, and policymakers active in the criminal justice field.

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

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

This publication was made possible by Award Number 2013-MU-CX-K003, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice.

Limited Print and Electronic Distribution Rights

www.rand.org

RAND CORPORATION

The RAND Corporation 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-2933-NIJ