Audit of the Department of Justice's Efforts to Protect Federal Bureau of Prisons Facilities Against Threats Posed by Unmanned Aircraft Systems

★ ★ ★

AUDIT DIVISION

20-104

SEPTEMBER 2020

REDACTED FOR PUBLIC RELEASE

The full version of this report contains information that the Department considered to be law enforcement sensitive and therefore could not be publicly released. To create this public version of the report, the Office of the Inspector General redacted (blacked out) portions of the full report.

Executive Summary

Audit of the Department of Justice's Efforts to Protect Federal Bureau of Prisons Facilities Against Threats Posed by Unmanned Aircraft Systems

Objectives

The Department of Justice (DOJ) Office of the Inspector General (OIG) completed an audit of DOJ's efforts to protect Federal Bureau of Prisons (BOP) facilities against threats posed by unmanned aircraft systems (UAS), commonly referred to as drones. The objectives of this audit were to: (1) determine the extent to which the BOP can detect and track attempts to deliver contraband to BOP facilities via drones, and (2) assess the Department's current policies and efforts to protect BOP facilities against security threats posed by drones. The audit covers March 2015, when the first BOP facility recorded a drone incident, through March 2020.

Results in Brief

We found that the BOP faces significant and growing challenges to protect its facilities from drone threats. Drones have been used to deliver contraband to inmates, but could also be used to surveil institutions, facilitate escape attempts, or transport explosives. The BOP's incident data shows that the number of reported drone incidents increased by over 50 percent from 2018 to 2019. While the BOP recorded 57 drone incidents in 2019, these figures likely underreport the full extent of the current threat for a number of reasons. The BOP has taken steps to address this threat by coordinating with the Federal Aviation Administration on flight restrictions and DOJ to clarify authority to deploy drone mitigation technology. However, the BOP is still identifying technology solutions and developing policies to deploy such measures. Continued coordination between the BOP, DOJ, and outside agencies will be necessary to effectively protect BOP facilities from security threats posed by drones.

Recommendations

Our report contains seven recommendations to improve the BOP's tracking of drone incidents and promote efforts to protect its facilities against drone threats. The BOP and DOJ agreed with these recommendations and on April 13, 2020, the Attorney General finalized guidelines on how DOJ components will be authorized to counter drone threats.

Audit Results

The BOP has identified drones as one of the major security threats facing the federal prison system. Drones may be used not only to deliver traditional contraband to inmates, but also to surveil institutions, facilitate escape attempts, or transport dangerous weapons such as firearms or explosives.

Improved Drone Incident Tracking is Needed – In 2018, the BOP began to formally track drone incidents at its federal facilities, and the data reflects a growth in reported incidents from 23 in 2018 to 57 in 2019. However, we believe this number likely underreports the number of drone incidents due to challenges the BOP faces in [redacted] tracking information about such incidents. We found the BOP could improve its tracking by clarifying its reporting policy for federal facilities, as well as taking steps to comprehensively track drone incidents at its contract facilities. Improved tracking will allow the BOP to better determine the extent of the threat and identify areas of highest risk.

Improving Drone Response Guidance – Recent flight restrictions and certain legal authorities gained from 2018 to 2019 will help DOJ combat the drone threat at BOP facilities. However, delays in finalizing DOJ-level guidance on implementing authorities to counter drones has hampered the BOP's ability to propose and receive approval for deploying counter-drone measures. Additionally, we found the BOP does not have protocols or staff training regarding how to safely approach and secure downed drones.

Identifying and Obtaining Protective Solutions – DOJ faces several challenges in its ongoing evaluation of solutions suitable to secure BOP facilities from drone threats. These include identifying appropriate technologies, verifying that they deliver on promised capabilities, and assessing the cost and benefits of these purchases. Given the limited resources available to the BOP and the rapid evolution of technology, continued collaboration both within DOJ and among other federal agencies will be essential to addressing these challenges and protecting BOP facilities from drone threats.

AUDIT OF THE DEPARTMENT OF JUSTICE'S EFFORTS TO PROTECT FEDERAL BUREAU OF PRISONS FACILITIES AGAINST THREATS POSED BY UNMANNED AIRCRAFT SYSTEMS

TABLE OF CONTENTS

AUDIT OF THE DEPARTMENT OF JUSTICE'S EFFORTS TO PROTECT FEDERAL BUREAU OF PRISONS FACILITIES AGAINST THREATS POSED BY UNMANNED AIRCRAFT SYSTEMS

INTRODUCTION

The Federal Bureau of Prisons (BOP) has identified unmanned aircraft systems (UAS), commonly referred to as drones, as one of the major security threats facing the federal prison system and BOP leadership has identified the use of drones to drop contraband into prisons as an ongoing problem that continues to evolve.[1] The Department of Justice (DOJ or Department) Office of the Inspector General (OIG), in our most recent Top Management and Performance Challenges report, listed the BOP's ability to manage a safe, secure, and humane prison system as one of the top challenges facing the Department and the BOP, and specifically identified the smuggling of contraband into prisons using drones as contributing to this challenge.[2]

Drones have emerged as a relatively new tool to introduce types of dangerous contraband, including cell phones, drugs, and tobacco products, that have persisted as common security concerns to BOP facilities. In recent years, federal, state, and local correctional facilities have encountered numerous attempts to smuggle contraband into prisons via drones, which can carry significant amounts of dangerous contraband. Indeed, BOP data on drone incidents, which the BOP only began formally tracking at federal facilities in 2018 (and as we describe below likely underreports the number of incidents), shows an increase from 23 drone incidents in 2018 to 57 incidents in 2019, an over 50 percent increase in one year. Moreover, OIG investigations reflect the potential seriousness of these drone incidents. For example, in one OIG investigation, a drone (pictured in Figure 1 below) was recovered at a BOP facility with a package containing 20 cell phones, 23 vials of injectable drugs, dozens of syringes, and multiple packages of tobacco, among other contraband items.

[1] Kathleen Hawk Sawyer, Director, Federal Bureau of Prisons, before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee on the Judiciary, U.S. House of Representatives, concerning "Oversight of the Federal Bureau of Prisons and Implementation of the First Step Act of 2018" (October 17, 2019), https://docs.house.gov/meetings/JU/JU08/20191017/110089/HHRG-116-JU08-Wstate-SawyerK-20191017.pdf (accessed January 9, 2020).

[2] U.S. Department of Justice (DOJ) Office of the Inspector General (OIG), *Top Management and Performance Challenges Facing the Department of Justice – 2019* (October 2019), https://www.oversight.gov/sites/default/files/oig-reports/2019.pdf (accessed February 5, 2020), 1-2.

Figure 1

Drone Recovered at BOP Facility

Source: BOP

Beyond the introduction of common contraband items, BOP personnel have expressed concerns about other threats posed by evolving drone technology. Drones could be used to surveil BOP facilities, collecting information on the facility layout and the movement of staff and inmates that could be used to facilitate prison incursions, track or harm BOP personnel, or initiate prisoner escapes.[3] BOP personnel we spoke with also expressed their concern that drones could deliver even more dangerous contraband—such as handguns or other weapons—to inmate-accessible areas, and thus pose grave and immediate harm to staff and inmates. Several DOJ officials cited the possibility of individuals using a drone offensively by arming it with firearms or explosives and targeting persons on the ground. As drone technology evolves, BOP officials told us that future devices may even have payload capabilities that could allow for the lifting of an adult out of a prison. Given trends in both the industry and observed incidents involving drones at prisons, the threat posed by drones to BOP facilities will likely increase as drone technology continues to advance.

OIG Audit Approach

The objectives of our audit were to: (1) determine the extent to which the BOP can detect and track attempts to deliver contraband to BOP facilities via drones, and (2) assess the Department's current policies and efforts to protect BOP facilities against security threats posed by drones. The scope of our audit covered

[3] One state correctional system we spoke with recorded a swarm of 15 drones over 1 of its facilities, which an official believed was an effort to identify the facility's tactical response to drone incursions, as well as cause interference with the facility's security systems.

the period of March 2015, when the BOP recorded its first drone incident at a federal facility, through March 2020, the conclusion of our fieldwork.

To accomplish our objectives, we analyzed drone incident data available to the BOP for both federally-owned and operated facilities, as well as privately contracted prisons. We also reviewed available DOJ and BOP policies and procedures that would be relevant to tracking and responding to drone incidents at prisons. In addition, we interviewed officials throughout the BOP who are involved in the BOP's efforts to address security threats, including those posed by drones. We spoke with BOP officials who worked in a wide variety of positions, including officials in headquarters and regional office roles, wardens, special investigative personnel, and correctional officers responsible for facility security. Because efforts to protect federal prisons from drones have not been isolated to the BOP, we also interviewed officials across the Department of Justice who have been involved in DOJ-wide counter-drone efforts, including officials from the Office of the Deputy Attorney General (ODAG), Executive Office of U.S. Attorneys (EOUSA), Federal Bureau of Investigation (FBI), Office of Legal Policy (OLP), National Security Division (NSD), and Office of Justice Programs' National Institute of Justice (NIJ). In addition, we spoke with officials from the Department of Transportation's Federal Aviation Administration (FAA), which implements regulations governing use of the national airspace.

We also conducted several site visits to the two BOP federal facilities that had reported the most drone incidents in order to obtain an on-the-ground perspective from facility personnel of the threat posed by drones. During one of these visits, we attended a site survey of counter-drone detection technology. Additionally, to ensure we captured non-federal law enforcement perspectives on drone countermeasures, we spoke with officials from three large state correctional systems.

AUDIT RESULTS

The BOP has Improved how it Tracks Drone Incidents but Needs to Take Further Action to Mitigate Evolving Drone Threats

Drones have emerged as a new security threat for the BOP, and the BOP has made progress towards quantifying the extent of the threat posed to its facilities. However, this audit identified a number of challenges pertaining to the BOP's ability to ascertain the full extent of this threat, due in part to the BOP's ability to [redacted] and inconsistency in what the BOP defines as a reportable drone incident at the facility level. Without [redacted] and consistent tracking of drone incidents, the BOP will continue to lack a complete understanding of the threat posed by drones to its facilities.

Available Drone Incident Data

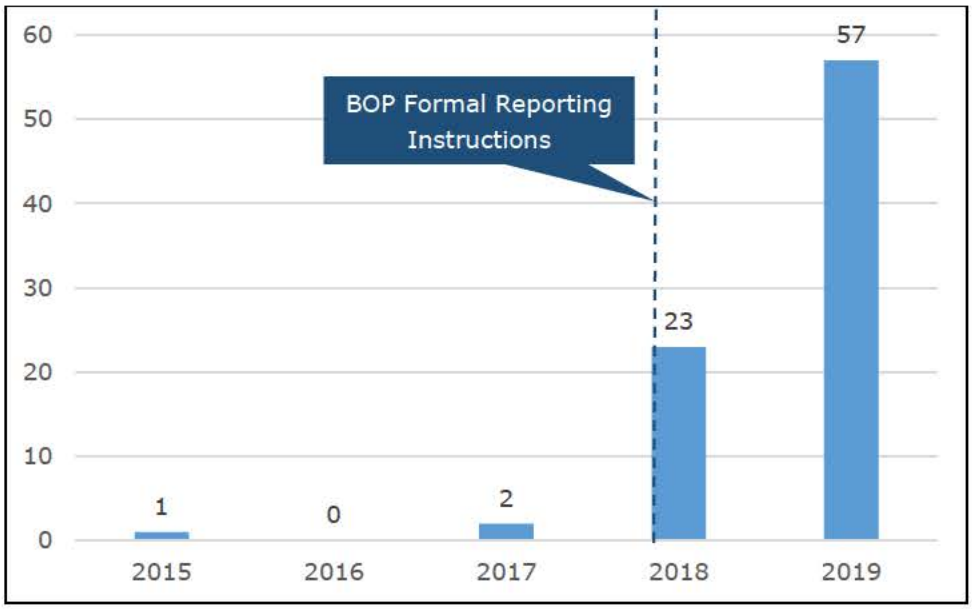
The BOP reported its first facility drone incident in 2015 at a federal correctional institution (FCI) in Victorville, California. Following OIG's June 2016 Review of the BOP's Contraband Interdiction Efforts, BOP officials determined they needed to track incidents involving drones at their facilities.[4] While a handful of drone incidents were reported via the BOP's TruIntel incident report process prior to 2018, in January 2018, the BOP implemented a policy specifically requiring its 122 federal facilities to begin tracking drone sightings and recoveries via its existing TruIntel incident report process. The BOP instructed staff to categorize drone incursions in this database under existing incident type options (e.g., "Introduction of Contraband") and include the word "drone" in the synopsis portion of the report, in order to facilitate a keyword search of incidents involving drones.

Based on our review of drone incident data the BOP provided from its incident database, there were 83 reported incidents involving drones at facilities owned and operated by the BOP between March 2015 and December 2019. As shown in Figure 2, there was a marked increase in reported drone incidents at BOP facilities following the BOP's 2018 implementation of reporting requirements, with 23 reported incidents in 2018, compared with 3 incidents for the previous 3 years combined. Even after the BOP implemented this new reporting requirement, the reported incident figures still rose significantly, with 57 incidents reported through the end of 2019.

[4] U.S. Department of Justice (DOJ) Office of the Inspector General (OIG), *Review of the Federal Bureau of Prisons' Contraband Interdiction Efforts*, Evaluations and Inspections Report 16-05 (June 2016), https://oig.justice.gov/reports/2016/e1605.pdf (accessed December 5, 2019).

Figure 2

Number of Reported Drone Incidents at BOP Federal Facilities, March 2015—December 2019



Note: The BOP's TruIntel incident data reported 85 total incidents involving drones from March 2015 to December 2019; however, as 2 of these incidents did not explicitly involve drone flights into the facility, we removed them for the purposes of this analysis.

Source: OIG analysis of BOP TruIntel data

Two BOP facilities represented the largest share of recorded drone incidents among BOP-owned and operated institutions. As of December 2019, one facility had reported 12 drone incidents and the second facility had reported 11 incidents since 2015. Site visits and interviews with correctional staff revealed that certain geographic features of these facilities make them particularly vulnerable to drone incursions.

Our analysis also included 14 prison facilities operated by private contractors between March 2015 and December 2019.[5] We reviewed the reporting requirements for the BOP's private contractors and requested drone incident numbers from the BOP for these 14 contract facilities. The BOP's standard Statement of Work for these contractors requires contract facilities to report all criminal activity to the BOP and the appropriate law enforcement agency. In addition, this Statement of Work requires contractors to report to the BOP any serious incident occurring at a contract facility, and a senior official from the BOP's Privatization Management Branch told us that a drone incident would qualify as a serious incident. However, the BOP's contract facilities do not follow the same TruIntel drone reporting process as BOP-owned and operated facilities. Instead,

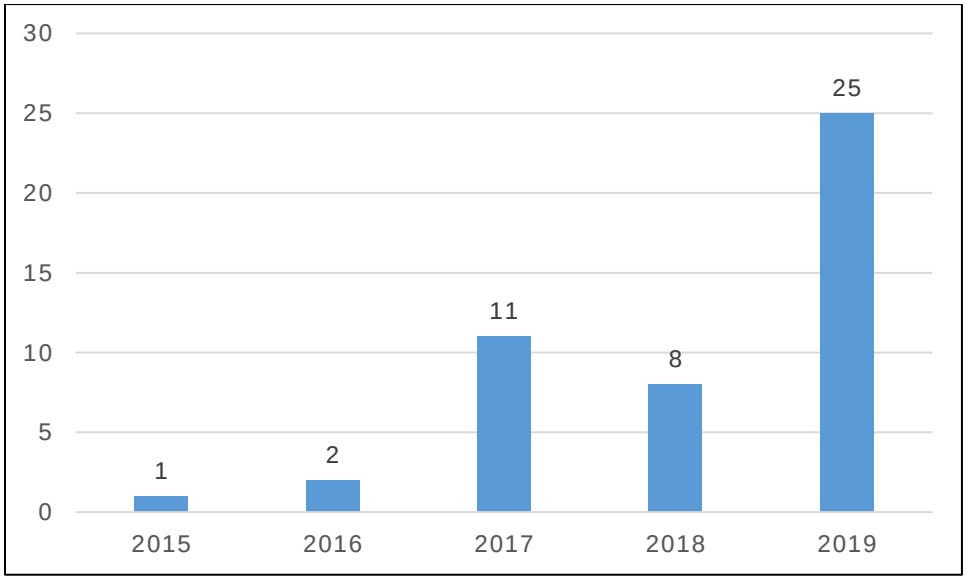
[5] Not all 14 contract facilities were active during this entire period. Between March 2015 and December 2019, the BOP ended contracts with two facilities, started a new contract with another facility, and activated a previously inactive facility.

the BOP requires contractors to report serious incidents immediately via telephone to the BOP staff member serving as the Contracting Officer's Representative, who in turn notifies the Privatization Management Branch at BOP headquarters. Though BOP contract facilities are also required to fill out a hard-copy Report of Incident Form for all incident types listed on the form, the form does not specify drone incidents. A senior BOP official explained that, historically, contract facilities have verbally notified the Contracting Officer's Representative of any incidents involving drones.

We reviewed the available drone incident data provided by the BOP for its contracted facilities and found that these facilities recorded 47 incidents involving drones between March 2015 and December 2019. Similar to BOP-owned and operated facilities, the contract facilities had an increase in reported drone incidents from 2015 to 2019, as shown in Figure 3.

Figure 3

Number of Reported Drone Incidents at BOP Contract Facilities, March 2015—December 2019



Note: The BOP did not have data available for one facility with a contract that ended in 2017 and reported it had limited data available for another facility with a contract that ended in 2019.

Source: OIG analysis of contractor data collected by the BOP for the OIG

The number of recorded incidents varied significantly among the contract facilities. One contract facility recorded 24 drone incidents since 2015, while the rest of the BOP's contract facilities each recorded between 1 and 4 drone incidents. Although the BOP described the location and layout of this facility as typical for the BOP's contract facilities, the BOP did not posit an explanation for why this facility had recorded the majority of the BOP's contract facility drone incidents, or more broadly, why the BOP's contract facilities on average appeared to have recorded more drone incidents than BOP-owned and operated facilities over the same

period—47 incidents at 14 contract facilities compared to 83 incidents at 122 federal institutions.

Limitations of Drone Incident Data

Although BOP data demonstrates a clear upward trend of drone incidents since 2015, we identified several challenges affecting the BOP's ability to track these incidents that limits the data's reliability. We also identified various factors suggesting that the total number of drone incursions at BOP facilities is likely higher than the data indicates.

As described in more detail in Table 1 below, we identified the following challenges that limit the BOP's ability to ascertain the actual number of drone incursions and the extent of the threat such incursions pose to its facilities: (1) limited ability to [redacted], (2) potentially inconsistent reporting by staff of detected incidents, (3) ambiguity in guidance on the threshold for making a report, (4) limited availability of information in instances when a drone is sighted but not recovered, and (5) tracking process flaws.

Table 1

Challenges for the BOP's Tracking of Drone Incidents

1.	[redacted]	[redacted]
2.	**Inconsistent Reporting**	**The BOP's incident data only reflects what staff report** • BOP officials cautioned that the data only includes drones that facility personnel [redacted] recorded—and in the case of the BOP's contracted facilities, also passed on to the BOP. • [redacted]
3.	**Reporting Thresholds**	**There are inconsistencies in the reporting threshold for incidents** • We learned of many instances [redacted] • Some facilities require [redacted], while others do not: Officials estimated that 10 to 20 such instances at a single BOP facility *were not* reported as drone incidents. Conversely, BOP contract facilities recorded several such instances that *were* included as drone incident reports to the BOP.
4.	**Limited Incident Data**	**There is often limited descriptive information available for incidents** • It is difficult for staff to ascertain [redacted], actions taken ([redacted]), and what was seen or heard by staff. • Most of the BOP's recorded incidents involve observations of drones in flight. [redacted]
5.	**Tracking Process Flaws**	**Methods for tracking incidents created the potential for inaccuracies** • The BOP's method of tracking drone incidents using [redacted] resulted in the inclusion of several incidents that were not always relevant, and risked omitting other relevant drone incidents because they did not contain [redacted]. • For contract facilities, the BOP does not regularly maintain cumulative reporting of drone incidents in any central location, so records have to be pulled from each contract facility.

Source: OIG Analysis

Drone incident data is dependent on not only the actual number of drone incursions, but also other variables including the facility's ability to [redacted] and the level of engagement among staff in following reporting procedures. A major limitation for the BOP is that its facilities [redacted]. Thus, drone incident data depends on [redacted] Further, while the BOP's policy states that staff should report all incidents "involving the sighting, interdiction, or recovery of drones," we received differing

accounts of whether staff must obtain visual confirmation of the drone itself to merit a formal incident report. BOP officials described multiple scenarios that could indicate a drone incursion without [redacted] of the drone, [redacted] Based on interviews with BOP officials and discussions with corrections professionals working for state systems around the country, we believe the actual number of drone incidents is likely higher than the reported figures. This figure is likely continuing to increase due to the growing awareness and availability of drone technology, attractive cost-benefit ratios of the price of a drone relative to the value of the payload inside a prison, and enhanced BOP efforts to interdict the introduction of contraband via other, more traditional methods.

With more consistent tracking of drone incidents, we believe the BOP could better ascertain the extent of the threat posed to its facilities, as well as identify potential trends that could help the BOP target its resources to the highest risk areas. When the BOP is able to recover a drone, its forensic laboratory may be able to obtain details to inform an investigatio [redacted].[6] Since drone recoveries have been [redacted], the BOP must leverage any information it is able to gather from other instances when a drone is detected but not recovered.

With respect to the BOP's contracted facilities, we found that the BOP has limited access to drone incident information for some of its contract facilities. For example, the BOP reported that drone incident data was either limited or not available for two facilities with contracts that ended during our scope. Further, a BOP official told us that the BOP does not maintain cumulative records of drone incidents that have occurred at its contract facilities. Thus, to obtain information necessary to this audit the BOP had to request drone incident data from each contractor, which had to be obtained from incident data maintained at each facility. We found that the data provided did not consistently contain descriptive information that the BOP could use to identify trends or risk areas.

We note that the BOP has taken some steps to improve its tracking of drone incidents occurring at its facilities, such as adding drone-specific designations in its database with options to select [redacted] or [redacted] under incident type. According to BOP policy, BOP facilities are still required to include the keyword "drone" in the incident report description, though it did not appear that the BOP provides guidance on what other information specific to drone incidents would be useful for facilities to include. The additional pre-populated options, which the BOP added to its database in September 2019, should allow for more accurate reporting of drone incident numbers for BOP-owned and operated facilities.

[6] The BOP works with the FBI or other federal or local law enforcement agencies to investigate drone incidents.

However, we recommend that the BOP further enhance its reporting and tracking of drone incidents by clarifying for its facilities what constitutes a drone incident and what information its personnel should record.

Furthermore, as of February 2020, the BOP noted that it was updating its incident report form for contract facilities to include options to select drone-specific incident types, similar to the options added to the TruIntel incident reporting process for federal facilities. A senior BOP official also stated that, in December 2019, the BOP's Privatization Management Branch filled a previously vacant intelligence analyst position, and that this individual will be responsible for collecting the contract facility incident report forms and monitoring reported drone incidents. We believe that these updates should improve the BOP's ability to track drone incidents at its contract facilities, and we recommend that the BOP collect, track, and assess data on drone incidents at its contracted facilities, in order to better determine the extent of drone threats to contracted facilities and identify any trends relevant to management of its own federal facilities.

The BOP and DOJ Need to Continue to Refine Drone Response Guidance and Evaluate Effective Drone Countermeasures

Over the past several years, the BOP has worked closely with DOJ officials engaged on protecting facilities against drone threats, though there remain challenges that the BOP faces in combatting this threat. DOJ and the BOP have made some advancements in deterring drone incursions, for example through coordination with the Federal Aviation Administration (FAA) on airspace restrictions over BOP facilities. However, the BOP's ability to implement other drone countermeasures, [redacted] has been restricted by actual and perceived limitations in its legal authorities, which is part of the reason why BOP facilities have [redacted] While recent legislation has clarified DOJ authorities to take action to protect BOP facilities, as of March 2020, neither DOJ nor the BOP had finalized guidance on how to implement these authorities, which we believe necessary in order to make continued progress in combatting the threat posed by drones.[7]

DOJ first established a DOJ Unmanned Aircraft Systems (UAS) Working Group around 2015 to coordinate efforts related to both DOJ's affirmative use of drones for law enforcement, as well as its use of countermeasures to mitigate

[7] Following receiving a draft of this report, on April 13, 2020, the Attorney General finalized and released *Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems* (see https://www.justice.gov/ag/page/file/1268401/download, accessed June 3, 2020). This document outlines how the BOP and other DOJ components will seek approval to deploy counter-drone technologies to protect certain facilities or assets.

threats posed by drones.[8] The DOJ UAS Working Group has evolved over time. As of March 2020, the group was chaired by the Office of Legal Policy (OLP), under the direction of the Deputy Attorney General, and composed of representatives from more than a dozen DOJ components. Made up of a relatively small but active group of DOJ personnel, DOJ's working group members communicate regularly on the issue of drones as they relate to DOJ operations. This group has focused its efforts on examining the legal and practical considerations of DOJ components' use of drone-related technology, and has also undertaken several specific efforts to help mitigate threats posed by drones. For example, the Counter-UAS Operational Test and Evaluation Committee, led by the National Institute of Justice (NIJ) under the auspices of the DOJ UAS Working Group, is aggregating research to assist DOJ components in identifying effective counter-drone technology. Additionally, Executive Office of U.S. Attorneys (EOUSA) personnel are pursuing efforts to promote the education and training of federal prosecutors regarding options to hold accountable those who engage in the misuse of drones, which DOJ officials believe will lead to an increase in the number of federal prosecutions for misuse of drones.[9] The UAS Working Group also advised Congress in developing legislation related to clarifying DOJ authorities to counter drones.

We believe any further advancements in DOJ's ability to protect BOP facilities from drones will rely on continued communication and coordination between DOJ components and other invested federal entities, such as the FAA and the Department of Homeland Security (DHS). Yet, clear guidance and effective coordination will only constitute part of any solution to the drone threat. The rapid and continuing evolution of the technology, for both the capabilities of drones themselves and countermeasures to inhibit them, will continue to present ongoing challenges to DOJ as it tries to identify and obtain reliable solutions that are not cost-prohibitive.

Evolving Legal Authorities

Under federal law, drones are considered aircraft. The FAA, which has authority over operations of aircraft in the national airspace, promulgates rules for use of drones. Using its authority under 14 C.F.R. §99.7, the FAA may restrict airspace in the interest of national security at the request of a federal security or intelligence agency. Over the past several years, BOP officials have coordinated with the FAA to secure temporary flight restrictions (TFR) to prohibit drone flights over its facilities. The BOP's original goal was to obtain TFRs covering all of its federal facilities. While the BOP initially reported experiencing delays in securing

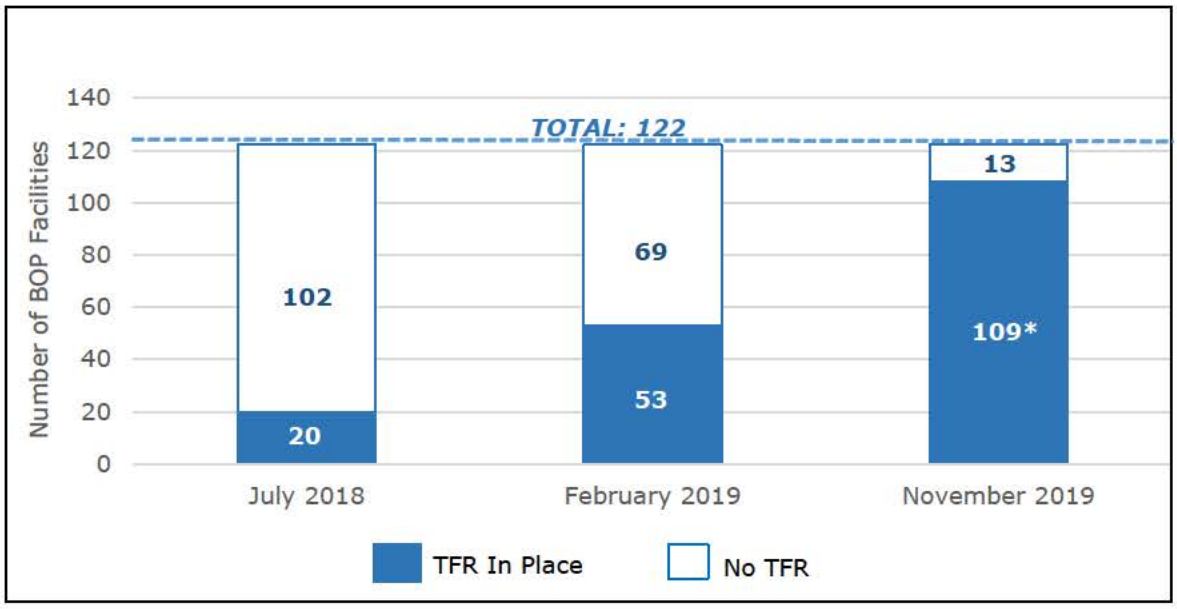
[8] This group grew out of prior OIG recommendations that ODAG convene a working group that, among other activities, could identify and address drone policy concerns that are shared across components or require coordination among components and other federal agencies. See DOJ OIG, *Interim Report on the Department of Justice's Use and Support of Unmanned Aircraft Systems*, Audit Report 13-37 (September 2013), https://oig.justice.gov/reports/2013/a1337.pdf (accessed December 5, 2019), 17.

[9] Recent federal prosecutions for misuse of drones have applied statutes related to failure to register a drone and violation of a temporary flight restriction. DOJ officials stated that EOUSA's criminal enforcement efforts are important to deterring drone smuggling.

requested flight restrictions, in July 2018 the FAA approved flight restrictions up to 400 feet over 20 high-security BOP penitentiaries. The FAA approved these TFRs on the basis that BOP facilities house individuals who pose a threat to national security. Since then, the BOP has continued to pursue expanding TFR coverage across all of its facilities. In February 2019, the FAA approved flight restrictions for 33 additional BOP facilities, including high-rise jails, medical referral centers, and medium security facilities that adjoin high security facilities. The FAA granted a BOP request for restricted airspace over an additional 55 BOP correctional facilities in November 2019. Including one additional TFR that the FAA had granted to another agency, a total of 109 of the BOP's 122 federal facilities were covered by TFR as of March 2020, and it is the BOP's goal to eventually obtain FAA approval for TFR coverage over all 122 facilities. Figure 4 shows the progression of TFR coverage for the BOP's facilities.

Figure 4

Progression of Temporary Flight Restrictions Granted by the FAA for BOP Federal Facilities



*Note: This graph represents each phase of FAA approvals to the BOP. The November 2019 total of 109 facilities covered by TFR includes one of the BOP's facilities that was separately covered by a TFR granted to another agency.

Source: BOP public website

Concurrent to efforts to obtain FAA flight restrictions, DOJ and the BOP have sought to clarify the legal authorities to mitigate drones that pose a threat to DOJ facilities. Prior to October 2018, several laws could be understood to pose potential

obstacles to a DOJ component's ability to take action against malicious drones.[10] For example, interference with a drone in flight, as with any aircraft, could implicate the Aircraft Sabotage Act—potentially opening DOJ personnel up to criminal or civil liability. Thus, while DOJ components may have had some authority to counter drones under certain circumstances, the BOP ultimately followed a more restrictive legal interpretation of its authorities. A June 2017 BOP memorandum addressed to all wardens stated that [redacted]

In 2016, the National Security Council directed the OLP to lead an interagency working group to identify the major legal issues concerning the ability of federal agencies to respond to threats posed by drones, and develop a legislative solution that would better define counter-drone authorities for federal agencies. Following the passage of legislation in 2017 that granted the U.S. Department of Defense authority to counter drones, the working group focused its efforts on drafting legislation to acquire similar authority for federal law enforcement agencies. Several key members of the group, including those from the Office of the Deputy Attorney General (ODAG), National Security Division (NSD), and the BOP's Office of Security Technology, cited the threat posed by drones introducing dangerous contraband into BOP facilities as a tangible risk and an example as to why DOJ needed drone mitigation authority.

The *Preventing Emerging Threats Act of 2018* (the Act), 6 U.S.C. § 124n, passed in October 2018, assists DOJ and DHS in preventing emerging threats posed by drones. The legislation states that the Attorney General may authorize personnel to take such actions *"necessary to mitigate a credible threat"* as defined by the Attorney General, in consultation with the Secretary of Transportation, "*that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset.*" 6 U.S.C. § 124n(a). The statute lists the countermeasures the Attorney General may authorize with respect to unlawful drones, which include:

- detect, identify, monitor, and track unmanned aircraft without prior consent;
- disrupt control of the unmanned aircraft, including by disabling, intercepting, or interfering with communications used to control the aircraft;
- seize the unmanned aircraft; and
- use reasonable force, if necessary, to disable, damage, or destroy the unmanned aircraft. 6 U.S.C. § 124n(b)(1).

[10] These include the Wiretap Act (18 U.S.C. Chapter 119), Pen-Trap Act (18 U.S.C. Chapter 206), Aircraft Sabotage Act (18 U.S.C. § 32), Computer Fraud and Abuse Act (18 U.S.C. § 1030), Interference with the Operation of a Satellite (18 U.S.C. § 1367), and Aircraft Piracy Act (49 U.S.C. § 46502), all of which are cited at the beginning of the Preventing Emerging Threats Act of 2018, which is discussed in more detail below.

Limitations of Recently Obtained Authorities

While the FAA TFRs carry civil or criminal (misdemeanor) penalties for drone operators who violate the restrictions, some BOP officials noted that these penalties are not strong enough to present an effective deterrent for individuals attempting to smuggle contraband into facilities via drones. However, these restrictions can potentially assist the BOP by limiting traffic from non-malicious drone operators who should be aware of the restrictions near BOP facilities. Additionally, if a TFR is already in place, it may be easier for a component to obtain approval for other counter-drone measures.

The Act limits the application of counter-drone measures for BOP facilities in several key ways. First, the text of the Act appears not to extend authorities to non-DOJ personnel or facilities, raising significant questions about the scope of authority for private contractors that own or operate facilities housing BOP inmates. The Act defines "personnel" whom the Attorney General may authorize to take drone countermeasures as limited to "officers and employees of [...] the Department of Justice." 6 U.S.C. § 124n(k)(6). Further, the "covered facilities or assets" referenced in the statute are defined as including Department missions pertaining to the "protection of penal, detention, and correctional facilities and operations conducted by the Federal Bureau of Prisons" and the "protection of the buildings and grounds leased, owned, or operated by or for the Department of Justice," provided they are located in the United States and determined to be high-risk and a potential target through a risk-based assessment. 6 U.S.C. § 124n(k)(3)(C)(ii)(II) and (III). These statutory provisions appear to raise questions about whether facilities that are not DOJ-owned, leased, or otherwise administered by DOJ employees (and not contractors) fall within the statutory definition of a covered facility or asset.

If contract facilities are not within the definition of a "covered facility," then they risk being in an "observe and report" posture that potentially limits their ability to deploy certain counter-drone technology while adhering to the law, leaving them unable to take more active measures to combat drones. [redacted] We recommend that DOJ continue to explore, with the input of the BOP, solutions regarding how contract facilities can better address the security vulnerabilities posed by drones. As part of this ongoing effort, the BOP should consider making appropriate contractual amendments and DOJ should research potential legislative adjustments.

A second way in which the Act limits the application of counter-drone measures is that the statute requires special authorizations before DOJ may deploy drone interdiction technology. Under the statute, the Attorney General must undertake a "risk-based assessment" to determine if a facility or asset is high-risk

and a potential target for unlawful drone activity. 6 U.S.C. § 124n(k)(3)(A). This risk-based assessment must analyze several factors, including:

1. the potential impact of drone countermeasures on the national airspace system (NAS);
2. options for mitigating any identified impact on the NAS from drone countermeasures;
3. the ability to provide reasonable notice to aircraft operators;
4. the setting and character of the covered facility or asset; and
5. the potential consequences to national security, public safety, or law enforcement if the threat posed by the drone is not mitigated. 6 U.S.C. § 124n(k)(8).

Thus, the statute requires DOJ to assess numerous factors to determine whether its facilities—such as its federal prisons—are covered under the Act as high-risk and a potential target for unlawful drone activity.[11]

In addition, even if senior DOJ officials deem a specific BOP prison a "covered facility or asset" under the Act, DOJ components must also obtain approval from the Attorney General and coordinate with the FAA regarding the protective measures proposed for deployment. DOJ components must specify and obtain approval for the scope of operation, type of technology to be used, and nature of the deployment in each instance. The required coordination and approval of specific operational plans at this level of detail between two federal agencies, though necessary to ensure the safety of the national airspace, is another hurdle faced by DOJ in exercising its recently obtained authorities to prevent emerging threats posed by drones. The BOP is actively cooperating, in concert with DOJ, with the FAA through a joint working group to develop and use efficient processes to provide this needed coordination.

Need for Clarification of Authorities and Procedures

While the Act formalized DOJ's ability to protect BOP facilities from drones, as of March 2020, DOJ had yet to establish final guidance for its components on how to implement the authorities under the Act. The BOP had therefore not implemented internal policies and procedures related to protecting its facilities from threats posed by drones.

DOJ Guidance

ODAG and NSD officials told us throughout the course of the audit that they were working on final Attorney General (AG) Guidance to serve as a roadmap for components seeking approval to deploy protective measures at covered facilities or assets, as authorized by the statute. However, as of March 2020, the AG Guidance

[11] See the following section, *Need for Clarification of Authorities and Procedures,* for a discussion of how the DOJ prepared its requests to invoke drone mitigation technology authorities, which required an assessment of risk.

remained in draft. As such, DOJ components including the BOP did not have formal, standing guidance on the extent of their relevant authorities under the Act, nor did they have clear instructions on the appropriate mechanism of approvals for proposed protective measures.

Without this formal guidance or an established procedure, DOJ components had to rely on ad hoc requests and provisional instructions. As of March 2020, we identified only a handful of instances when DOJ pursued approval to deploy drone mitigation technology. In the absence of finalized AG Guidance, the requesting DOJ component in each case had to rely on interim guidance it developed in partnership with NSD specifically for each circumstance. We believe the absence of official guidance in this matter hindered the ability of DOJ components such as the BOP to discern the parameters of their authority and identify instances where it would be appropriate to request approval of drone counter-measures. Therefore, we recommend that DOJ finalize guidance for its components on how to implement the authorities under the Act.[12]

Another unresolved issue related to the protection of prisons under the Act is the process that DOJ components will use to obtain approval of requests for countermeasures. Looking forward, one issue we believe such guidance will need to address is whether the BOP will submit separate requests to obtain approval for counter-drone measures at each of its 122 federal institutions, or whether it may group such requests together.[13] FAA officials we spoke with suggested that DOJ components may ultimately be able to group similar requests for approval together if they involve the same technology and consistent features, such as the nature and environment of deployment. With OLP assistance, the BOP anticipates refining the form and content of countermeasure requests regarding its facilities and assets over time and with experience.

We believe that the DOJ should seek opportunities to streamline the request process to facilitate more efficient approvals for deployment of protective measures at BOP facilities. Therefore, we recommend that DOJ continue to work with the BOP on identifying opportunities to maximize the efficiency of BOP requests to deploy protective measures at BOP facilities, while still meeting all purposes of the AG Guidance and the requirements of the statute on which it is based. Such efforts should involve communication from DOJ on how details in the request inform the approval considerations, and how BOP requests that are similar in nature could be grouped together or replicated in a way to streamline the approval process.

---

[12] As previously stated, following DOJ's receipt of a draft of this report for formal comment, DOJ issued guidance on April 13, 2020 outlining the process by which components will seek approval for use of counter-drone technologies to protect certain facilities or assets. We therefore issued this report with this recommendation closed. See Appendix 3 for the status of report recommendations.

[13] We reviewed a document package in which a DOJ component requested and received approval to invoke drone mitigation technology authorities under the Act. This request received numerous approvals, including from the component head, the Office of the Deputy Attorney General, and the Attorney General. A DOJ official stated that other requests have followed a similar format, though some approval authorities had been delegated to other officials since the time of the first request.

BOP Policy and Procedures

BOP officials told us that they were waiting for the final AG Guidance before establishing any BOP policies or procedures specifically related to the deployment of counter-drone measures because they did not want to proceed on a course of action that might later be contradicted by DOJ instructions. Once DOJ finalizes the AG Guidance, BOP officials said they planned to incorporate it into component-level policies and procedures. Until then, [redacted]

One area in which the BOP has taken initiative without relying on DOJ guidance relates to facility searches—a function that does not implicate any of the statutes DOJ officials originally believed could pose obstacles to DOJ's ability to take action against drones, or the more recent 2018 Act. We learned that the BOP directed all federal facilities to develop their own search procedures specific to the event of a drone sighting. In response to the significant threats posed by drones, at least two facilities had already implemented special search procedures prior to the BOP-wide instructions on this topic. [redacted]

However, beyond the guidance relating to searches, officials from the BOP's Correctional Programs Division, Northeast Regional Office, and facilities we visited confirmed that [redacted] When a drone is no longer in flight and on the ground, DOJ officials we spoke with did not interpret the aforementioned legal questions to limit the BOP's handling of a drone recovery. Several BOP officials at facilities we visited echoed this view, telling us that for recoveries of drones that have crashed or landed, the institutions follow the BOP's standard operating procedures for introduction of contraband and handling of evidence.[14]

Several individuals stated that [redacted] In our discussions with outside agencies, FAA officials described drone recovery safety protocols at the Los Alamos National Laboratory that treated downed drones similar to improvised explosive devices, and officials at a military base adjoining a BOP facility suggested that ordnance disposal teams were best suited to retrieve downed

[14] 18 U.S.C. § 1791 (Providing or possessing contraband in prison).

drones, which could potentially carry explosives or other weapons. However, we did not learn of any standard BOP protocol for these situations. We did learn of one instance when a [redacted], though we were told this individual acted out of instinct and was not specifically trained to do so.

The draft AG Guidance we reviewed during the audit acknowledged the safety concern posed to DOJ personnel recovering drones and calls for DOJ components to include in their policies instructions about how to approach downed drones safely. However, BOP officials reported that they were waiting on final AG Guidance before implementing BOP-specific policies and procedures—including policies and procedures about how to recover and secure downed drones safely. In light of the fact that BOP staff already encounter downed drones that may pose a risk to safety, and given the BOP's view that its standard procedures for contraband govern the handling of downed drones, we believe the BOP should not wait to promulgate guidance for its facilities about how to approach and secure downed drones. Therefore, to protect personnel responding to drone incidents, we recommend that the BOP identify best practices and provide training for relevant staff on how to safely approach and secure recovered drones.

Exploration and Evaluation of Appropriate and Effective Technology

While DOJ and the BOP are in the early stages of researching and evaluating a multitude of technologies and solutions offering both affirmative use and counter-drone capabilities, we have identified four main challenges facing DOJ in its evaluation of suitable technology solutions for protecting the BOP. These are identifying and verifying technology that delivers on promised capabilities, balancing security priorities that compete for limited resources, assessing the cost and benefits of these purchases, and making federal procurements that keep pace with the rapid evolution of technology.

Many vendors of counter-drone technologies offer unproven capabilities or results that may only be achievable in a controlled environment. [redacted] Nevertheless, both DOJ and BOP personnel are respectively researching solutions and also gathering information from other customers on what solutions may be effective in protecting BOP facilities from drone threats. The BOP's Office of Security Technology (OST), which is responsible for using technology to address threats to the BOP's physical security, is the office within the BOP that is most directly engaged on the exploration and evaluation of technology purported to detect and mitigate malicious drones. OST officials have attended demonstrations of counter-drone technologies from various vendors and are assessing the capabilities of specific systems.

In fall 2019, OST submitted to the Office of Management and Budget an FY 2021 budget request for $10.25 million to procure "20 fixed detection and mitigation systems (CUAS) to protect high-security installations," and "1 mobile

(CUAS) system to use in 4-5 high-risk prison transfers."[15] As of February 2020, the President's FY 2021 budget request included $5.2 million to allow the BOP to purchase 10 fixed and 1 mobile detection and mitigation counter-drone systems—half of what the BOP originally requested. According to a senior OST official, the BOP had available year-end funding that it would use for testing and evaluation of new counter-drone technologies. In December 2019, the BOP issued a Request for Information for participation of counter-drone systems in a formal BOP test and evaluation program, the goal of which is for OST to identify solutions or systems it believes will be effective in combatting drones. While OST is currently focused on procuring technology solutions for the BOP's highest priority facilities, an official from the BOP's Privatization Management Branch stated that any contract facilities that wish to deploy counter-drone technology may submit a proposal to the BOP. However, the contractor would not only need to pay for the proposed solution, but also obtain BOP concurrence on any deployment of technology at a contract facility—which may hinge on the nature of the proposed countermeasures, given that the Act contains specific restrictions in this area that appear to limit the legal authority for contractors to deploy drone mitigation technology.

Despite agreeing that drones pose a major security threat, BOP officials have cautioned that the issue of drones has to be taken in context with the other security threats the BOP faces and the finite resources available to combat all of these threats. For example, OST, which will ultimately be responsible for implementing counter-drone technology, is staffed with a small number of Full-time Equivalent (FTE) employees. Similarly, the BOP's forensics lab, already responsible for running forensics on confiscated cell phones, is staffed with a small number of FTE employees who are also responsible for running forensics on recovered drones and other electronic devices. The BOP reported that this lab received for examination over 3,000 devices in 2019 alon [redacted][16] The FY 2021 budget for the BOP does not fund any additional positions for counter-drone efforts in either OST or the forensics lab. We are concerned that this may limit the BOP's ability to promptly respond to future drone threats.

Additionally, the prices of even the most rudimentary countermeasures for drones can easily become cost prohibitive. For example, officials from two large state correctional systems stated that cost has been the primary barrier to their implementation of counter-drone measures, with one reporting that even non-technology options such as netting over the prison yard could cost millions of dollars for one large prison. An official from a third state correctional system stated that, while they had identified a reasonably priced and effective drone detection system, due to funding limits they had procured only one mobile system that officials transport among the state's prison facilities.

[15] In its budget request, the BOP specifically stated that the request was responsive to this OIG audit.

[16] Previous OIG work has found that this group has struggled to keep pace with the volume of other, non-drone devices awaiting examination. DOJ OIG, *Contraband Interdiction Efforts*, 40.

We note that we identified one BOP facility at the forefront of efforts to explore and implement counter-drone technology. [redacted] A private vendor of a technology designed to detect the location of both the drone and the operator has conducted a site survey [redacted], which the BOP attended. [redacted] officials expressed interest in layering mitigation and detection technologies [redacted] which, depending on the placement of the technology, could encompass the [redacted] BOP facility. This would make this prison the first BOP facility to be covered by counter-drone technology. However, any use of counter-drone equipment [redacted] to the benefit of the BOP would still require necessary coordination to ensure lawful operations under the relevant statutes governing federal counter-drone operations.

As DOJ and the BOP continue to evaluate various counter-drone technologies and solutions, we believe the newly-formed Counter-UAS Operational Test and Evaluation Committee (COTEC), led by NIJ under the auspices of the DOJ UAS Working Group, can play a helpful role. The COTEC was first convened in June 2019 and plans to help DOJ components navigate the hundreds of available counter-drone technologies and vendors by conducting research, aggregating information on DOJ-wide acquisitions, and leveraging expertise from DOJ and other federal agencies. Though the COTEC will not directly test technology, officials explained that the group will lead information-sharing efforts across DOJ components. These efforts are intended to maximize efficiencies when it comes to testing and evaluating technology, by preventing duplicative testing and helping to avoid the procurement of ineffective technology. DOJ officials stated that, ideally, this work would lead to the use of systems that are interoperable across components. However, officials cautioned that the benefits of the COTEC can only be achieved if components share with the group their particular use cases and the results of any testing and evaluation efforts, so that the COTEC can help to identify appropriate technology solutions.

We believe that information sharing between DOJ components and outside agencies on counter-drone technologies will be essential to the BOP's ability to effectively identify, evaluate, and implement technology solutions—especially considering the funding the BOP has available to test, evaluate, and procure technology options. DOJ officials involved in the COTEC recognize that counter-drone systems could quickly become obsolete as drone technology continues to evolve. Therefore, DOJ components would benefit from the Department's expertise and information-sharing on options that would best suit this evolving area while adhering to federal procurement rules.

Additionally, we found that DOJ's counter-drone efforts are heavily dependent upon a few key individuals in each component who have worked together on this issue for a number of years. Information sharing will not only help to ensure that components inform each other of promising technology, but will also help ensure that institutional knowledge of this issue is spread across individuals and components. We recommend that the DOJ continue to support the COTEC, by

encouraging its components to share information with the group related to the testing, evaluation, and procurement of counter-drone technology. This will benefit the BOP as it pursues technology options to help protect its prison facilities from threats posed by drones.

CONCLUSION AND RECOMMENDATIONS

Drones pose a serious threat to the safety and security of the BOP's institutions, inmates, and staff. BOP staff cited concerns over use of drones to introduce dangerous contraband into secure prison environments, as well as fears that drones could be used to surveil institutions, facilitate escape attempts, or enable attacks. The BOP's drone incident data demonstrates that the threat posed by drones to BOP facilities is increasing, though we found that the BOP can take steps to improve its tracking of incidents in order to better ascertain the extent of the threat.

While the BOP and the Department have made significant efforts to address the threat posed by drones, we found that the BOP continues to face barriers to protect its facilities. Although BOP and DOJ officials have worked closely on clarifying the BOP's legal authority to deploy counter-drone technology, the Department's finalization of guidance for components on implementing this authority has experienced some delays. The BOP will also need to develop internal policies and procedures in line with this guidance, including safety procedures for staff handling of recovered drones. Until the Department and the BOP more formally define how the request and approval process will work for implementing drone countermeasures, the BOP will remain limited in how it can proceed with steps to protect its facilities. In addition, the BOP's ability to protect its facilities from drone threats is constrained by resource and technological limitations: though the BOP's Office of Security Technology has worked to secure funding for testing, evaluation, and procurement of counter-drone systems, the BOP still faces challenges in identifying and verifying solutions that are reliable, cost-effective, and able to keep pace with rapidly advancing drone technology. Until approval processes are finalized and the BOP is able to identify effective solutions, the BOP will continue to face challenges to address threats posed by drones.

Individuals from various DOJ components and across the federal government have a range of expertise that is relevant to addressing the threat posed by drones to DOJ facilities, including prisons. The sharing of counter-drone ideas and efforts—both across the Department and among outside agencies—will be helpful as the BOP attempts to identify, evaluate, and implement counter-drone solutions, given the variety of stakeholders, complexity of the legal authorities, and intricacy of technical considerations related to drones. The DOJ has taken preliminary steps to engage in this cooperation, and we expect the future success of DOJ efforts to protect BOP facilities from drones will require the Department's continued commitment to this type of sustained collaboration.

We recommend that the BOP:

1. Further enhance its reporting and tracking of drone incidents by clarifying for its facilities what constitutes a drone incident and what information its personnel should record.

2. Collect, track, and assess data on drone incidents at its contracted facilities, in order to better determine the extent of drone threats to contracted facilities and identify any trends relevant to management of its own federal facilities.

3. Identify best practices and provide training for relevant staff on how to safely approach and secure recovered drones.

We recommend that DOJ, through the Office of the Deputy Attorney General:

4. Continue to explore, with the input of the BOP, solutions regarding how contract facilities can better address the security vulnerabilities posed by drones.

5. Finalize guidance for its components on how to implement the authorities under the Act.[17]

6. Continue to work with the BOP on identifying opportunities to maximize the efficiency of BOP requests to deploy protective measures at BOP facilities, while still meeting all purposes of the AG Guidance and the requirements of the statute on which it is based.

7. Continue to support the COTEC, by encouraging its components to share information with the group related to the testing, evaluation, and procurement of counter-drone technology.

[17] DOJ issued guidance on April 13, 2020 outlining the process by which components will seek approval for use of counter-drone technologies to protect certain facilities or assets. As discussed in Appendix 3, we therefore issue this report with this recommendation closed.

APPENDIX 1

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The objectives of the audit were to: (1) determine the extent to which the BOP can detect and track attempts to deliver contraband to BOP facilities via drones, and (2) assess the Department's current policies and efforts to protect BOP facilities against security threats posed by drones.

Scope and Methodology

The scope of our audit covers the period of March 2015, when the BOP recorded its first drone incident at a federal facility, through March 2020, the conclusion of our fieldwork. To achieve our audit objectives, we analyzed drone incident data provided by the BOP for both its federally-owned and operated facilities as well as its contracted facilities from March 2015 through December 2019. We identified laws and regulations relevant to DOJ's authority to counter drones. We reviewed component-level policies and procedures related to the BOP's response to and tracking of drone incidents, and interviewed BOP officials involved in these efforts. We also interviewed officials from the Office of the Deputy Attorney General (ODAG), Executive Office of U.S. Attorneys (EOUSA), Federal Bureau of Investigation (FBI), Office of Legal Policy (OLP), National Security Division (NSD), Office of Justice Programs' National Institute of Justice (NIJ) and Federal Aviation Administration (FAA) regarding efforts to address threats posed by drones to DOJ facilities.

In addition to our interviews, we conducted site visits to two BOP federal facilities that had reported the most drone incidents—[redacted]—in order to obtain an on-the-ground perspective from facility personnel of the threat posed by drones. During one of these visits, we attended a site survey of counter-drone detection technology [redacted] Additionally, to ensure we captured non-federal law enforcement perspectives on drone countermeasures, we spoke with officials from three large state correctional systems.

Statement on Compliance with Generally Accepted Government Auditing Standards

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Compliance with Laws and Regulations

Given our audit objectives and scope, we identified the laws and regulations relevant to this audit. The *Preventing Emerging Threats Act of 2018*, 6 U.S.C. § 124n, governs DOJ's authority to take protective measures to counter threats posed by drones. We analyzed the language of this statute to determine what actions DOJ is authorized to take to counter drones, the requirements DOJ must meet before deploying protective measures, and the facilities to which protective measures may be applied. Additionally, we identified the following laws and regulations related to the BOP's ability to protect its facilities from threats posed by drones:

- 18 U.S.C. § 1791
- 14 C.F.R. § 99.7

Though we did not specifically test the BOP's compliance with these laws and regulations, nothing came to our attention that caused us to believe that the BOP was not in compliance with the aforementioned laws and regulations.

Computer-Processed Data

During our audit, we obtained information from the BOP's TruIntel system. TruIntel is a database containing incident reports from BOP facilities, which we queried for incidents involving drones. While we did not test the reliability of the TruIntel system as a whole, we reviewed the drone incident data pulled from TruIntel as part of this audit. We identified some limitations of the data, which we outline in our report. We therefore supplemented our analysis of this data with testimony from our interviews with BOP officials. We did not rely on this data to support our audit findings or conclusions.

APPENDIX 2

THE DEPARTMENT OF JUSTICE AND FEDERAL BUREAU OF PRISONS JOINT RESPONSE TO THE DRAFT AUDIT REPORT

U.S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General — *Washington, D.C. 20530*

April 20, 2020

The Honorable Michael E. Horowitz
Inspector General
U.S. Department of Justice
Washington, D.C.

Dear Mr. Horowitz:

The Department of Justice appreciates the opportunity to respond to the draft report, "Audit of the Department of Justice's Efforts to Protect Federal Bureau of Prisons Facilities Against Threats Posed by Unmanned Aircraft Systems." We recognize the Office of Inspector General spent considerable effort to produce this report, and we have appended our formal response to this letter.

Sincerely yours,

G. Bradley Weinsheimer

Bradley Weinsheimer
Associate Deputy Attorney General

Thomas R. Kane

Thomas R. Kane
Deputy Director
Federal Bureau of Prisons

CC:
Office of Legal Policy
National Security Division

Enclosure

Department of Justice and Federal Bureau of Prisons Joint Response to the Office of the Inspector General Report, "Audit of the Department of Justice's Efforts to Protect Federal Bureau of Prisons Facilities Against Threats Posed by Unmanned Aircraft Systems" (April 2020)

The Department of Justice ("Department") appreciates the work of the Office of the Inspector General ("OIG") in its report, "Audit of the Department of Justice's Efforts to Protect Federal Bureau of Prisons Facilities Against Threats Posed by Unmanned Aircraft Systems" ("OIG Report"). Efforts to protect Federal Bureau of Prison facilities from the threat posed by unmanned aircraft systems ("UAS" or "drones") by implementing the authorities of the Preventing Emerging Threats Act of 2018 ("the Act"), codified in relevant part at 6 U.S.C. § 124n, have been underway since 2018. As certain of the recommendations from the OIG Report are directed to, or otherwise involve, the Office of the Deputy Attorney General ("ODAG"), and whereas the balance of the recommendations are directed at the Federal Bureau of Prisons (the "BOP"), this response to OIG is submitted jointly by ODAG and the BOP. The Department has organized this coordinated response in three sections. In the first section, we address the first three recommendations, which are directed at the BOP; the BOP agrees with all three recommendations and, as explained in greater detail below, has already taken steps to implement some of them or to otherwise address the underlying issue in the recommendation. In the second section, we address one recommendation to ODAG for which the responsive action is now complete. Finally, in the third section, we address the remaining three recommendations to ODAG, with which we also agree, and explain how ODAG has and will continue to work with the BOP on the underlying issues going forward.

I. Three Recommendations Directed at BOP

The BOP agrees with OIG's first three recommendations: 1) that the BOP further enhance its reporting and tracking of drone incidents by clarifying for its facilities what constitutes a drone incident and what information its personnel should record; 2) that the BOP collect, track, and assess data on drone incidents at its contracted facilities in order to better determine the extent of drone threats to contract facilities and identify any trends relevant to management of its own federal facilities; and 3) that the BOP identify best practices and provide training for relevant staff on how to safely approach and secure recovered drones.

The BOP has already taken concrete measures to address all three recommendations. With respect to the first recommendation (that the BOP clarify what constitutes a drone incident and what information personnel must record), on October 7, 2019, the BOP updated its Report of Incident form ("BOP Form 583") to include the categories, "Drone Sighting" and "Drone Recovered," as reportable incidents. The OIG Report acknowledges this change. *See* OIG Report at 9-10. The guidance provided to federal correctional institutions instructs that when a UAS (drone) is observed or recovered by a BOP institution, then a BOP Form 583 must be completed. BOP Form 583 requires information such as where the drone was sighted, whether inmates or other staff were involved, whether force was used, and a narrative of the incident. Files may be attached to BOP Form 583, such as photographs or video of a sighted or recovered

drone. The BOP automated reports system collects the reports on drone incidents and can be reviewed for historical data.

With respect to the second recommendation (that the BOP collect, track, and assess data on drone incidents at its contracted facilities to better determine the extent of drone threats to contracted facilities and identify any trends relevant to management of its own federal facilities), the OIG Report notes that the BOP is updating its incident report form for contract facilities, similar to updates to reporting for its own facilities, to include options to include drone-specific incidents. *See* OIG Report at 10. In addition to that measure already taken, BOP's Privatization Management Branch is working with other branches within the BOP to assess the requirements and determine if the BOP's TRULINC system can be modified to allow for reporting of incidents at private contract facilities. Further, the Privatization Management Branch is enhancing the contractor's monthly reporting of statistical data to include drone sightings and recoveries. This data will then be discussed during the monthly performance meeting with the contractor to determine courses of action to detect and deter future drone incidents. These measures will allow the BOP to better track UAS incidents and develop consistent reporting at both federal and contracted facilities.

With respect to the third recommendation (that the BOP identify best practices and provide training for relevant staff on how to safely approach and secure recovered drones), the BOP has drafted an agency policy concerning how to safely approach and secure recovered drones based on best practices. Once the policy is approved and disseminated, training for relevant staff will be developed and deployed.

II. Completed Recommendation Directed at ODAG

Recommendation 5 is that the Department "[f]inalize guidance for its components on how to implement the authorities under the Act." *See* OIG Report at 22. On April 13, 2020, the Attorney General signed and issued the guidance, "Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems" ("C-UAS Guidance"). Thus, the Department asks that the OIG close Recommendation 5.

III. Remaining Three Recommendations Directed at ODAG

In this section, we provide responses to the remaining recommendations contained in the OIG Report, all of which are directed at ODAG. Recommendation 4 is that ODAG, with the BOP, continue to explore solutions regarding how contract facilities can better address security vulnerabilities posed by drones. ODAG will support the BOP's actions discussed above in response to Recommendation 2, namely by assisting the BOP in assessing drone incident data collected as a result of the update to the incident report form for contract facilities and any additional data obtained from monthly performance meetings with the contractor. Further, ODAG will monitor the determination of whether BOP's TRULINC system can be used at private contract facilities. After obtaining additional data, ODAG can assist BOP in developing courses of action to detect and deter future drone incidents. The OIG report accurately describes two shortfalls in 6 USC § 124n concerning non-Department personnel or facilities. *See* OIG Report, pp 13-14. The Attorney General has no authority under the Act to authorize non-

Department personnel to take drone countermeasures and may not designate a facility or asset as a "covered facility or asset" at which C-UAS actions may be taken under the statute when that facility or asset is not owned, leased, or otherwise administered by the Department. ODAG will continue to explore these two issues in the Department's semi-annual briefings to and notifications with the appropriate congressional committees required by 6 USC § 124n(g). Accordingly, ODAG agrees with this recommendation and believes it should be closed.

Recommendation 6 is that ODAG "[c]ontinue to work with the BOP on identifying opportunities to maximize the efficiency of BOP requests to deploy protective measures at BOP facilities, while still meeting all purposes of the AG Guidance and the requirements of the statute on which it is based." The C-UAS Guidance tasks the Department's Office of Legal Policy ("OLP"), "in consultation with the Department's UAS [Working Group] and any appropriate subgroups to the extent appropriate and helpful," with the responsibility of "[c]oordinating, prioritizing, and de-conflicting component requests to designate covered facilities or assets or to authorize protective measures, and making recommendations concerning such requests." *See* C-UAS Guidance at 10. Under the direction of ODAG, OLP chairs the Department's UAS Working Group, which will assist the BOP in maximizing their requests and fully coordinate deployment of protective measures at BOP facilities with the Federal Aviation Administration. Accordingly, ODAG agrees with this recommendation and believes it should be closed.

Finally, Recommendation 7 is to "[c]ontinue to support the COTEC, by encouraging its components to share information with the group related to the testing, evaluation, and procurement of counter-drone technology." *See* OIG Report at 22. The OIG has summarized the Department's intent for the Counter-UAS Operational Test and Evaluation Committee ("COTEC"). In March 2020, ODAG approved two new co-chairs to lead the COTEC, including the C-UAS Section Chief for the Drug Enforcement Administration and the Chief, Office of Security Technology at the BOP, who serves as the C-UAS program lead. Through selection and approval of these two new co-chairs to lead the COTEC, ODAG has ensured that the components coordinate and share information with one another on all testing, evaluation, and procurement of C-UAS technology. Additionally, the C-UAS Guidance charges OLP with the tasks of "[f]acilitating and coordinating procurement and training," and "[i]dentifying recommended technologies and equipment for use by authorized Department components." *See* C-UAS Guidance at 10. Accordingly, ODAG agrees with this recommendation and believes it also should be closed.

APPENDIX 3

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

The OIG provided a draft of this audit report to the Department of Justice's (DOJ or Department) Federal Bureau of Prisons (BOP) and Office of the Deputy Attorney General (ODAG). We incorporated the BOP and ODAG's joint response in Appendix 2 of this final report. In response to our audit report, the BOP and ODAG concurred with our recommendations and discussed the actions they will implement in response to our findings. As a result, the status of the audit report is resolved. The following provides the OIG analysis of the response and summary of the actions necessary to close the report.

Recommendations for the BOP:

1. **Further enhance its reporting and tracking of drone incidents by clarifying for its facilities what constitutes a drone incident and what information its personnel should record.**

   Resolved. The BOP agreed with our recommendation. The BOP stated in its response that the BOP, as noted in our report, updated its Report of Incident form to include categories for tracking drone sightings and recoveries. Additionally, the BOP stated that guidance provided to BOP facilities instructs the facilities to record instances when a drone is observed or recovered, and that the BOP's Report of Incident form requires facilities to record certain information.

   This recommendation can be closed when we receive evidence that the BOP has provided additional guidance to its facilities that: (1) clarifies the BOP's policy to record all drone sightings and recoveries in a Form 583 Report of Incident, and (2) explains what information, specific to drone incidents, would be useful for facilities to record when documenting a drone sighting or recovery. We believe that additional clarification in these two areas is necessary to ensure that all pertinent information related to drone incidents at BOP facilities is recorded and provided to BOP headquarters, in order to assist the BOP in better identifying the extent of the threat.

2. **Collect, track, and assess data on drone incidents at its contracted facilities, in order to better determine the extent of drone threats to contracted facilities and identify any trends relevant to management of its own federal facilities.**

   Resolved. The BOP agreed with our recommendation. The BOP stated in its response that the BOP is updating its incident report form for contract facilities to include categories to track drone-specific incidents. Additionally, the BOP stated that its Privatization Management Branch is assessing

whether drone incidents at contract facilities could be reported through the BOP's incident tracking database. The BOP also stated that the Privatization Management Branch is enhancing contract facilities' monthly reporting of statistical data, to include drone sightings and recoveries, which will be assessed during performance meetings to determine courses of action to detect and deter future drone incidents.

This recommendation can be closed when we receive evidence that the BOP: (1) has updated its incident report form for contract facilities to include categories for tracking incidents involving drones, and (2) is regularly collecting and assessing drone incident data from its contract facilities.

3. Identify best practices and provide training for relevant staff on how to safely approach and secure recovered drones.

Resolved. The BOP agreed with our recommendation. The BOP stated in its response that it has drafted an agency policy on how to safely approach and secure downed drones based on best practices, which will be disseminated to staff once approved. The BOP further stated it would develop and deploy training for relevant staff.

This recommendation can be closed when we receive evidence that the BOP: (1) has approved and disseminated a policy to staff on how to safely approach and secure downed drones, and (2) has provided training on this policy to relevant staff.

Recommendations for DOJ, through ODAG:

4. Continue to explore, with the input of the BOP, solutions regarding how contract facilities can better address the security vulnerabilities posed by drones.

Resolved. ODAG agreed with our recommendation. ODAG stated in its response that it will assist the BOP in assessing drone incident data for contract facilities, as well as monitor the determination of whether the BOP's incident tracking database can be used by contract facilities. After obtaining additional data, ODAG stated it can assist the BOP in developing courses of action to detect and deter future drone incidents. Further, ODAG acknowledged the shortfalls of the Preventing Emerging Threats Act concerning non-Department personnel or facilities. ODAG stated it will continue to explore these limitations in the Department's semi-annual briefings to appropriate congressional committees. ODAG requested closure of this recommendation.

This recommendation can be closed when we receive evidence that the BOP has worked with DOJ to assess contract facility drone incident data and determined whether contract facilities can use the BOP's incident tracking database.

5. Finalize guidance for its components on how to implement the authorities under the Act.

Closed. ODAG agreed with our recommendation. In its response, ODAG stated that the Department issued guidance entitled "Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems" on April 13, 2020. ODAG requested closure of this recommendation.

The OIG reviewed the Department's guidance issued April 13, 2020, which outlines the process by which components will seek approval for use of counter-drone technologies to protect certain facilities or assets. This recommendation is closed.

6. Continue to work with the BOP on identifying opportunities to maximize the efficiency of BOP requests to deploy protective measures at BOP facilities, while still meeting all purposes of the AG Guidance and the requirements of the statute on which it is based.

Resolved. ODAG agreed with our recommendation. ODAG stated in its response that the finalized Attorney General Guidance tasks the Office of Legal Policy (OLP), in consultation with the DOJ Unmanned Aircraft Systems (UAS) Working Group, with coordinating, prioritizing, and deconflicting component requests to deploy protective measures. ODAG further stated that OLP will assist the BOP in maximizing its requests to deploy protective measures and coordinating with the Federal Aviation Administration. ODAG requested closure of this recommendation.

This recommendation can be closed when we receive evidence that the BOP has coordinated with the OLP, in consultation with the DOJ UAS Working Group, to prioritize and deconflict requests to deploy protective measures at its facilities.

7. Continue to support the COTEC, by encouraging its components to share information with the group related to the testing, evaluation, and procurement of counter-drone technology.

Closed. ODAG agreed with our recommendation. ODAG stated in its response that, in March 2020, it approved new leadership for the Counter-UAS Operational Test and Evaluation Committee (COTEC), to include counter-drone subject matter experts from the BOP and the Drug Enforcement Administration. ODAG stated that this leadership, along with continued facilitation by the OLP, will ensure that DOJ components coordinate and share information on testing, evaluation, and procurement of counter-drone technology. ODAG requested closure of this recommendation.

Based on the Department's stated efforts to support the COTEC and encourage information-sharing between DOJ components, this recommendation is closed.