Audit of the Federal Bureau of Investigation's Strategy and Efforts to Disrupt Illegal Dark Web Activities

★ ★ ★

AUDIT DIVISION

21-014

DECEMBER 2020

REDACTED FOR PUBLIC RELEASE

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

Executive Summary

Audit of the Federal Bureau of Investigation's Strategy and Efforts to Disrupt Illegal Dark Web Activities

(U) Objective

(U) The Department of Justice (Department) Office of the Inspector General (OIG) conducted this audit to assess the Federal Bureau of Investigation's (FBI) implementation of its dark web strategy.

(U) Results in Brief

(U) The terms "dark web" and "darknet" are often used to refer to a part of the Internet that consists of services and websites that cannot be accessed through standard web browsers; instead, specific software, configurations, or authorization is needed for access. While accessing the dark web is not illegal, dark web sites are often used to engage in illegal activities.

(U) We found that the FBI does not maintain an FBI-wide dark web strategy. Instead, the FBI relies on its operational units to execute individual dark web investigative strategies. We concluded that this decentralized effort could be enhanced by establishing a coordinated FBI-wide dark web approach, that would, among other things, help ensure clarity on investigative responsibilities among operational units, lead to more efficient and cost effective approaches to investigative tool development and acquisition, provide strategic continuity during periods of turnover, and provide baseline data collection guidelines that will enable the FBI to better report its dark web accomplishments.

(U) Additionally, the FBI should complete an FBI-wide cryptocurrency support strategy in concert with its development of an FBI-wide dark web approach. Moreover, the FBI should ensure proper entry of dark web investigative data into the Department's existing investigation deconfliction system.

(U) Recommendations

(U) Our report contains five recommendations to assist the FBI in improving its investigative and planning efforts related to the dark web.

(U) Audit Results

(U) Many users access the dark web for legitimate purposes, including to discuss socially sensitive matters or counter censorship in oppressive areas of the world. However, dark web sites are also used to engage in illegal activities, such as trafficking drugs; firearms and weapons of mass destruction; child sexual abuse material; malware; and other illicit goods and services. According to the Department, the existence of darknet marketplaces is one of the greatest impediments to its efforts to disrupt cybercriminal activities.

(U) FBI responsibility for investigating illegal dark web activities is primarily shared by four operational units: (1) Hi-Tech Organized Crime Unit (Hi-Tech OC Unit), which targets opioids and other drugs trafficked on the dark web; (2) Child Exploitation Operational Unit, which fights the sexual exploitation of children on the dark web; (3) Weapons of Mass Destruction Directorate, Investigative Unit, which targets the purchase and sale of weapons of mass destruction on the dark web; and (4) Major Cyber Crimes Unit, which counters the distribution of illegal hacking tools on the dark web. These investigative units target administrators and moderators of dark web sites engaged in illegal activities, and the technical infrastructure of such sites; money launderers; and vendors, content producers, and customers of illegal goods and services.

(U) *FBI's Dark Web Strategy* – There is no requirement that the FBI develop or maintain a formalized bureau-wide dark web strategy. Instead, we found that FBI operational units were executing individual dark web strategies—some documented, others not—containing varying degrees of comprehensiveness. We found that the Hi-Tech OC Unit, which maintained the most comprehensive strategy, could better ensure that its operations sufficiently target dark web vendors trafficking fentanyl and other opioids in a manner consistent with the priorities articulated by the Deputy Attorney General. Further, the Child Exploitation Operational Unit and Major Cyber Crimes Unit could better track dark web case statistics to enable an accurate and complete assessment of their efforts. In addition, because of the multitude of crimes that occur on darknet marketplaces,

Executive Summary

Audit of the Federal Bureau of Investigation's Strategy and Efforts to Disrupt Illegal Dark Web Activities

some of the operational units' areas of investigative responsibility have become ambiguous. The Hi-Tech OC Unit and Major Cyber Crimes Unit have overlapping strategies to disrupt and dismantle darknet marketplace administrators and infrastructure. We believe their overlapping approaches could result in redundancies, inefficiencies, or investigative assignments that are not properly aligned with skillsets, capabilities, tools, and resources.

(U) We concluded that establishing a coordinated FBI-wide dark web approach could provide significant value, in part, by providing investigative and support units a complete picture of the FBI's capabilities that can be leveraged across mission areas, clarifying investigative responsibilities to reduce potential redundancies or inefficient work, and creating baseline data collection requirements that will enable these units to better demonstrate their dark web accomplishments. An FBI-wide approach can further benefit the operational units as they develop individualized dark web investigative strategies focused on their unique mission areas.

(U) *Tool Development and Acquisition Concerns* – FBI employs a variety of strategies—conventional and technical—to obtain evidence, identify users and infrastructure, and apprehend perpetrators on the dark web. From approximately 2012 through 2017, the FBI's Remote Operations Unit was largely responsible for the development and deployment of technology-based investigative solutions on the dark web. However, over the past 2 years, its dark web role has eroded due to budget decreases and an increased prioritization on tools for national security investigations. This has resulted in the operational units seeking tools useful to dark web investigations independently without a mechanism to share the product of their efforts. We believe this decentralization has also resulted in inefficiencies because operational units reallocated limited investigative resources to tool development. Establishing a coordinated FBI-wide dark web approach could enhance and consolidate investigative tool development and acquisition efforts to address the FBI's needs in a more cost-effective manner.

(U) *Centralization of Dark Web Training Resources* - We found that the FBI maintained a significant amount of dark web-related training resources that could benefit personnel across all divisions and field offices. However, FBI officials were sometimes unaware of the dark web training options available. We concluded that this was due to the decentralization and compartmentalization of the FBI's dark web-related training, and that by establishing a coordinated FBI-wide dark web approach, the FBI can do a better job of centralizing its training materials and communicating its availability and accessibility.

(U) *Dark Web Cryptocurrency Support* – We identified two FBI components that provide operational support, including for dark web investigations, via separate Virtual Currency Teams, jointly funded by the Department's Assets Forfeiture Fund. We found that rising costs and static funding from the Assets Forfeiture Fund resulted in disagreement between these two Virtual Currency Teams on the prioritization of resources and revealed concerns that they are conducting redundant work. FBI also identified similar concerns and is currently evaluating an FBI-wide cryptocurrency support strategy. We believe this should be done in concert with its development of a coordinated FBI-wide dark web approach.

(U) *Deconfliction of Investigative Data –* Deconfliction of investigative data among law enforcement agencies is essential to ensure agent safety, preserve the integrity of ongoing investigations, and to identify targets of common investigative interest. Deconfliction is particularly important in an operating environment like the dark web where anonymity is the norm. The Department requires that all law enforcement components deconflict investigative data and enter the information into the Deconfliction and Information Coordination Endeavor system. Overall, we found that the operational units had entered into this deconfliction system only 47 percent of the data items we tested. This could lead to inefficiencies in investigative efforts or even the misidentification of other government operations as criminal.

(U) AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S STRATEGY AND EFFORTS TO DISRUPT ILLEGAL DARK WEB ACTIVITIES

(U) TABLE OF CONTENTS

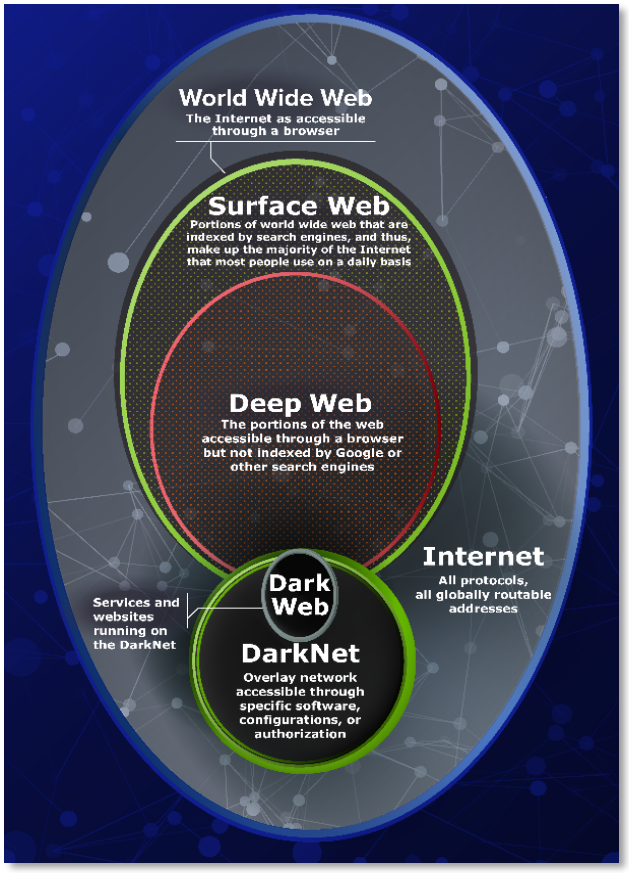
(U) AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S STRATEGY AND EFFORTS TO DISRUPT ILLEGAL DARK WEB ACTIVITIES

(U) INTRODUCTION

(U) The terms "dark web" and "darknet" are often used interchangeably to refer to a part of the Internet that cannot be accessed through standard web browsers and only accessible through specific software, configurations, or authorization.[1] Figure 1 compares the dark web to other parts of the Internet, such as the surface web and deep web. Many users access the dark web for legitimate purposes, including the discussion of socially sensitive matters or to counter censorship in oppressive areas of the world. However, the dark web is also used to engage in illegal activities. Given the difficulty of enforcing the law on this global and largely anonymous platform, investigating illicit dark web activity is both a priority and challenge for the Federal Bureau of Investigation (FBI) and the Department of Justice (Department).

(U) Figure 1

(U) An Anatomy of the Internet



(U) Source: Based on a figure from the Argonne National Laboratory, a Department of Energy Facility.

(U) One of the most commonly used methods to access the dark web is through the "Tor" browser, which is designed to facilitate anonymous communication over the Internet. Tor was originally developed by the U.S. Naval Research Laboratory in the mid-1990s to provide anonymity to U.S. military personnel. Today, the non-profit Tor Project, Inc. maintains and develops the Tor software and is partially funded by the U.S. government.[2] The Tor network is comprised of thousands of volunteer-operated servers throughout the world that allow users to share

[1] (U) Matthew Cronin, *Hunting in the Dark: A Prosecutor's Guide to the Dark Net and Cryptocurrencies*, U.S. Attorneys' Bulletin, Volume 66, No. 4, July 2018, https://www.justice.gov/usao/page/file/1083791/download, 66.

[2] (U) In 2018, the U.S. Department of State and the National Science Foundation contributed funding to the Tor Project, Inc.

information over public networks without compromising privacy.[3] Tor users are able to access websites on the Tor network, referred to as "onion services," or "hidden services" that resemble websites on the surface web but have web addresses that end in ".onion". Both the computer hosting the onion service and user accessing it are theoretically untraceable because their physical location and other identifying information is masked behind layers of routing and encryption.

(U) As noted above, users access the dark web for many legitimate reasons. For example, major press outlets, social media, and other mainstream organizations maintain sites on the dark web. However, the dark web's anonymity and low barriers to entry have attracted scores of criminals that engage in a wide variety of illegal activity in plain sight. Darknet marketplaces (DNM), forums, and other onion services are used to sell or provide fentanyl, heroin, cocaine, and other illegal drugs; firearms and explosives; chemical, biological, radiological, and nuclear materials; child sexual abuse material; malware and other computer hacking tools; fraudulent identification documents; money laundering services; stolen financial information and intellectual property; and other illicit goods and services. Dark web users generally pay for these illicit products and services with cryptocurrencies, such as bitcoin.[4]

(U) According to the Department, Tor and the existence of DNMs is one of the greatest impediments to its efforts at disrupting cybercriminal activities.[5] A related challenge for law enforcement is the resiliency of DNMs and forums. Europol reported that over 100 DNMs offering drugs have operated from 2010 to 2018, usually lasting less than a year before closing due to law enforcement action, scams, hacking, or voluntary exits.[6] For several years now, prominent DNMs have been shuttered by law enforcement for alleged violations of federal laws—including distribution of controlled substances, money laundering, access device fraud, and identity theft—just to be immediately replaced by successor DNMs to which vendors and buyers migrate. Online child exploitation communities provide another example of this persistent problem. According to the FBI, as of May 2019, there were at least 30 child sexual abuse material sites operating openly on the dark web, including 1 site that obtained 150,000 new members within its first 7 weeks of operation. Site memberships grow to this level due to law enforcement difficulties in developing sophisticated techniques to identify both website operators and users who are engaging in criminal activity on a global scale.

---

[3] (U) Tor Project, "Overview," https://2019.www.torproject.org/about/overview.html.en (accessed January 2, 2020).

[4] (U) Kristin Finklea, *Dark Web*, R44101 (Congressional Research Service, March 10, 2017), https://fas.org/sgp/crs/misc/R44101.pdf (accessed September 10, 2018), 12.

[5] (U) U.S. Department of Justice, *Report of the Attorney General's Cyber Digital Task Force*, July 2, 2018, https://www.justice.gov/ag/page/file/1076696/download (accessed September 11, 2018), 123.

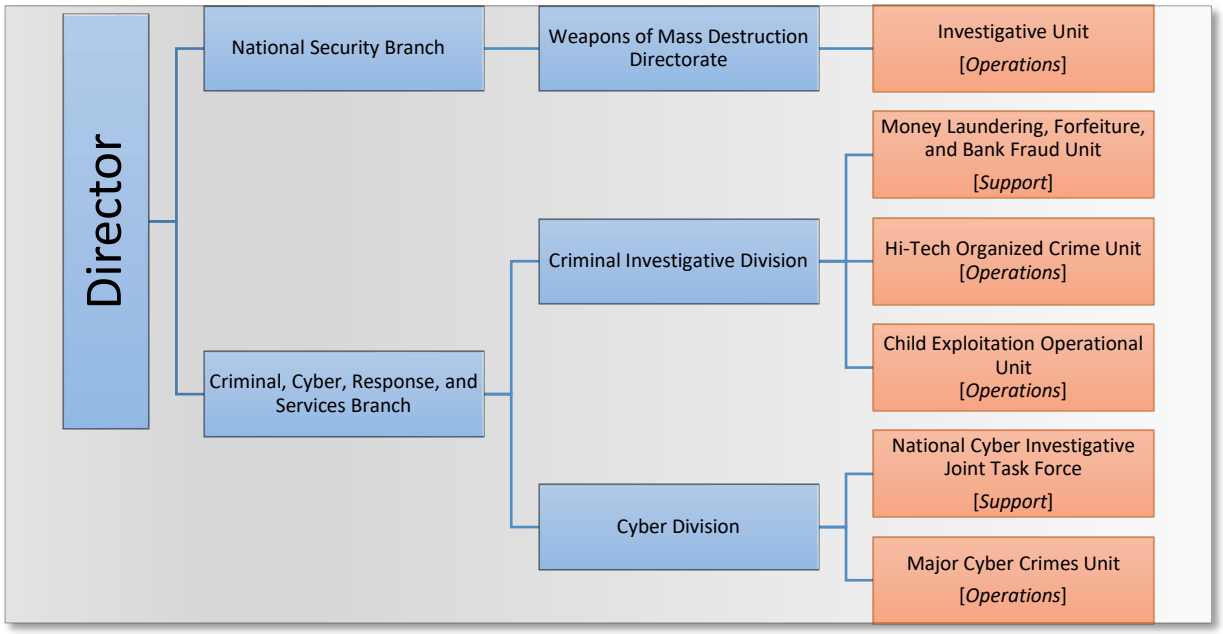
[6] (U) Europol supports law enforcement authorities throughout the European Union in their fight against terrorism, cybercrime, and other serious and organized forms of crime. Europol, *Darknet Markets Ecosystem*, April 2018, http://www.emcdda.europa.eu/publications/posters/2018/darknet-markets-ecosystem_en (website pdf accessed July 19, 2019).

(U) FBI Dark Web Responsibilities

(U) FBI's responsibility for investigating federal criminal activity on the dark web is primarily shared by four operational units and two support units located within the FBI's Criminal Investigative Division, Cyber Division, and Weapons of Mass Destruction Directorate.[7]

(U) Figure 2

(U) FBI Components Responsible for Dark Web Investigations & Support[8]



(U) Source: FBI

(U) FBI dark web investigations target onion service administrators and moderators of sites engaged in illegal activities, and the technical infrastructure of such dark web sites; vendors and content producers of illegal goods and services; money launderers; and customers of illicit goods. Darknets, such as Tor, provide an unprecedented level of anonymity to individuals surfing the dark web, which limits the investigative options available to identify these persons. In an effort to identify those engaged in dark web criminal conduct, the FBI initiates Undercover Operations (UCO), an investigative method that must be conducted in accordance

[7] (U) FBI officials said the Counterterrorism and Counterintelligence Divisions conduct minimal dark web-related work. Therefore, we did not include them in this audit.

[8] (U) Additional detail on each operational and support unit can be found in the Audit Results section.

with Department and FBI policies.[9] Dark web UCOs usually involve a series of related undercover activities over a period of time by an FBI Online Covert Employee (OCE). OCEs are FBI personnel who construct or assume false online personas and then interact with users to gather information on a subject or to build credibility.

(U//~~LES~~) Additionally, the FBI often relies on investigative techniques, such as controlled purchases or deliveries. For instance, FBI OCEs will purchase narcotics from a vendor on the dark web, [redacted] with the end goal being to identify and arrest the vendor. In another example, [redacted] with the end goal being to identify and arrest the customer upon his or her [redacted]

(U) OIG Audit Approach

(U) The objective of this audit was to assess the FBI's implementation of its dark web strategy. Our audit generally covered, but was not limited to, the FBI's activities from October 2014 through April 2019. To accomplish our objective, we reviewed:

- (U) the dark web strategies of the FBI's Hi-Tech Organized Crime Unit (Hi-Tech OC Unit), Child Exploitation Operational Unit (CEOU), Investigative Unit (IU), and Major Cyber Crimes Unit (MCCU) (collectively referred to as the operational units) to determine if they were documented; contained objectives and initiatives supported by performance measures; and had been disseminated throughout the FBI;
- (U) the operational units' investigative efforts, to determine if they aligned with their strategies;
- (U) the operational units' technological tool development and acquisition efforts to determine if they are equipped to identify criminal actors on the dark web;
- (U) FBI's dark web cryptocurrency support and training; and
- (U) FBI's entry of subject monikers and other investigative data into its deconfliction system, in accordance with Department policy.

(U) Appendix 1 contains a more detailed description of our audit objective, scope, and methodology. Appendices 2 and 3 contain a list of acronyms and a glossary of key terms, respectively.

[9] (U) This includes the FBI's Domestic Investigations and Operations Guide, which applies to all investigative and intelligence collection activities conducted by the FBI within the United States, in the U.S. territories, or outside the territories of all countries. The guide aims to ensure that all investigative and intelligence collection activities are conducted within constitutional and statutory parameters and that civil liberties and privacy are protected.

(U) AUDIT RESULTS

(U//~~LES~~) Our audit resulted in a number of findings regarding the FBI's dark web approach. While the FBI does not have a formal FBI-wide dark web strategy, its operational units execute individual dark web strategies—some documented, others not—containing varying degrees of comprehensiveness. We believe the FBI could improve its dark web investigative and strategic planning efforts by establishing a coordinated FBI-wide approach that incorporates dark web needs while recognizing the unique operational requirements of its investigative units that operate on the dark web. In the absence of such an approach, we identified ambiguous dark web investigative responsibilities that have resulted in inefficiencies and redundancies. For example, two critical FBI units were essentially competing by actively developing separate strategies related to targeting DNM administrators and technical infrastructure, with both units believing they were best equipped to handle these responsibilities. FBI officials informed us that the resulting investigative ambiguity remains unresolved, and according to a field office Special Agent, has led to countless deconfliction discussions and investigative inefficiencies. We also found that in the absence of an overarching FBI dark web approach, its investigative tool development and acquisition activities were fragmented. This has led to inefficiencies in the development, acquisition, and utilization of investigative tools. We also identified coordination weaknesses in handling dark web [redacted] Furthermore, an FBI-wide dark web approach could help the FBI provide more agile and relevant dark web training. FBI and OIG also separately identified redundancies between its two Virtual Currency Teams in the areas of training, outreach, and cryptocurrency tracing, which demonstrates the need for the FBI to complete an FBI-wide cryptocurrency support strategy in concert with its development of an FBI-wide dark web approach. Lastly, we identified internal control deficiencies pertaining to the entry of dark web investigative data into a Department-mandated deconfliction system. We elaborate on each of these findings below.

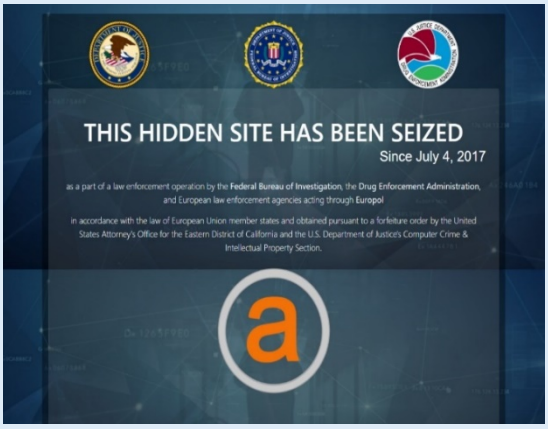
(U) FBI's Dark Web Approach

(U) There is no requirement that the FBI develop or maintain a formalized bureau-wide dark web strategy, and we found that the FBI does not have one. Instead, FBI operational units were executing individual dark web strategies—some documented, others not—with varying degrees of comprehensiveness. Senior FBI officials with whom we spoke had mixed opinions on the value of establishing such a formalized FBI-wide strategy. Some of these officials considered it unnecessary because the dark web is just a medium or platform to commit a crime and represented a small percentage of their unit's operations, or because it did not make sense to have an overarching strategy for multiple divisions with different missions and goals. However, other FBI officials believed that an overarching strategy, or at least centralization of mutual activities, would be beneficial. Department officials outside the FBI, particularly from the Criminal Division, have recognized the need for a government-wide dark web strategy, having created the Department Dark Web Strategic Planning Group in 2017 to "devise, cultivate, and

(U) **AlphaBay Takedown (Operation Bayonet)**

(U) Prior to its shutdown in July 2017, AlphaBay was the largest darknet marketplace on Tor. Users could buy and sell drugs, firearms, malware, identity documents, and other illegal products and services. AlphaBay was reported to have serviced more than 350,000 users and 40,000 vendors.

(U) Operation Bayonet, led by the FBI's Sacramento Field Office, was a joint international operation that dismantled AlphaBay's servers, arrested the site's administrator, and seized $25 million in cryptocurrency and assets. Operation Bayonet funneled departing AlphaBay users into the Hansa darknet marketplace, which had been covertly seized and controlled by the Dutch National Police, enabling the collection of information related to the site's moderators, vendors, and users.



implement comprehensive strategies to investigate, prosecute, and deter serious criminal activity occurring via the Dark Web." The Dark Web Strategic Planning Group aims to develop a nationwide dark web strategy that focuses on key challenges and issues. As of March 2020, the group was still developing a formalized strategy. Members of the group include the FBI; Drug Enforcement Administration (DEA); Criminal Division; Department of Homeland Security, Homeland Security Investigations; U.S. Postal Inspection Service; and Internal Revenue Service, Criminal Investigation Division.

(U//~~LES~~) We found that operational units working on dark web investigations have developed unique areas of specialization. For instance, the WMD Directorate's Investigative Unit (IU) has extensive experience operating [redacted] and is constantly engaged with the international law enforcement community. The CEOU is [redacted] The MCCU has cadres of cyber agents with networking and programming backgrounds and expertise targeting technically sophisticated cyber actors, and taking down dark web infrastructure, such as AlphaBay (see text box); and the Hi-Tech OC Unit, though relatively new to the space, has established the largest FBI investigative presence on the dark web and is emerging as a key player in the areas of training [redacted]

(U) In the absence of an FBI-wide dark web strategy, we assessed the unit-level strategies according to FBI's internal strategic planning standards to understand their approaches and identify commonly shared objectives and initiatives. We then assessed whether the objectives and initiatives were supported

by measures, targets, and milestones, consistent with the FBI's strategic planning standards.[10]

(U) We found that the Hi-Tech OC Unit had developed a written dark web strategy that included objectives and initiatives but lacked performance metrics to establish accountability and gauge success. The other three FBI operational units—CEOU, IU, and MCCU—could broadly convey their dark web investigative and planning approaches but did not maintain comprehensive strategies. As described in greater detail below, we summarized each of the operational units' dark web strategies and compared their concepts.

(U) Hi-Tech OC Unit's Formalized Dark Web Strategy

(U) In March 2017, the FBI created the Hi-Tech OC Unit in response to a determination by the Criminal Investigative Division that it did not have a clear understanding of the extent that criminals were utilizing high-tech tools on the Internet. In January 2018, the Deputy Attorney General directed the FBI and the DEA to develop a strategy to target, identify, and dismantle online opioid vendors, particularly those trafficking synthetic opioids, such as fentanyl.[11] The Hi-Tech OC Unit received a significant funding and personnel enhancement in 2018, and was tasked with managing the Joint Criminal Opioid Darknet Enforcement (J-CODE) initiative to focus on the trafficking of fentanyl and other opioids on the darknet.[12] The Hi-Tech OC Unit aims to disrupt and dismantle transnational organized criminal groups that use the darknet to perpetuate the opioid epidemic by targeting their technical infrastructure, administrative team, vendors, and buyers.

(U) The Hi-Tech OC Unit was the only FBI operational unit required to develop a dark web strategy, as evidenced by the January 2018 Deputy Attorney General directive to target the distribution of fentanyl and other opioids, and by its organizational responsibilities to "develop strategies to undermine confidence in the Darknet" and "create a formalized process to prioritize DNMs, vendors, and administrators…." The Hi-Tech OC Unit created a "Darknet Criminal Enterprise Strategy," or strategy map in January 2018 to articulate its dark web approach, thereby fulfilling these requirements. The fiscal year (FY) 2019 strategy map,

[10] (U) According to the FBI's strategic planning standards: "objectives" are action-oriented and require the FBI to frequently evaluate progress to ensure it is performing those actions correctly; "initiatives" are projects that help accomplish objectives; "measures" are performance indicators that help assess progress against a particular objective; "targets" are the desired level of performance that is defined with clear thresholds; and "milestones" are markers that ensure that initiatives remain on track.

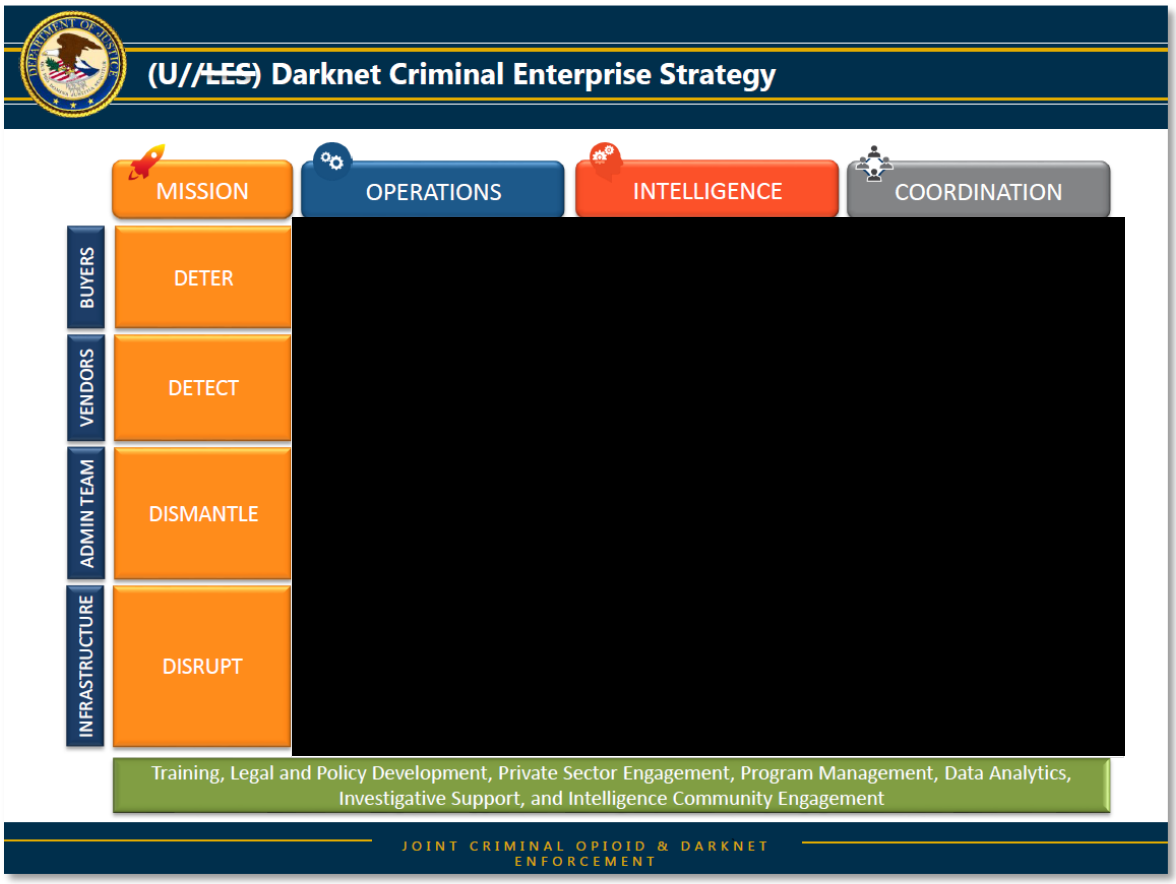
[11] (U) According to the National Institute on Drug Abuse, fentanyl and other synthetic opioids are the most common drugs involved in drug overdose deaths in the United States, and in 2017, 60 percent of opioid-related deaths involved fentanyl compared to 14 percent in 2010.

[12] (U) FBI leads the J-CODE, which was directed to centralize the efforts of domestic partners to more effectively target online opioid vendors. As of January 2020, J-CODE members included the FBI, DEA, Bureau of Alcohol, Tobacco, Firearms and Explosives, and other DOJ components; U.S. Postal Inspection Service; Department of Defense; Defense Intelligence Agency; U.S. Customs and Border Protection; U.S. Department of Homeland Security; and the Financial Crimes Enforcement Network.

pictured below, details the Hi-Tech OC Unit's four dark web mission areas, or objectives, to: (1) deter buyers, (2) detect vendors, (3) dismantle administrative teams, and (4) disrupt infrastructure. Each of these objectives targets a threat, contains initiatives across different organizational perspectives, and includes support features and activities that span all levels of the strategy. The bulleted items shown in Figure 3 are the initiatives necessary to accomplish the objectives.

(U) Figure 3

(U) Hi-Tech OC Unit Strategy Map FY 2019



(U) Source: Hi-Tech OC Unit

(U) The Hi-Tech OC Unit's dark web strategy map provided a complete view of its dark web mission areas, objectives, and initiatives, and had been regularly updated. FBI officials investigating criminal dark web activities outside of the Hi-Tech OC Unit commented that the strategy map could help identify strategic overlap; better attain cohesion across different divisions; help brief senior management; and introduce new employees to the FBI's dark web efforts.

(U//~~LES~~) While the Hi-Tech OC Unit's strategy map was the most comprehensive representation of an FBI unit-level dark web strategy that we encountered during the course of this audit, we identified potential areas of improvement. FBI strategic planning principles state that performance measures are necessary to help inform better decision making and communicate what a unit

is trying to accomplish; define what success looks like; and mark the end of significant or impactful events. However, none of the Hi-Tech OC Unit's strategy map objectives and initiatives were supported by metrics, targets, or milestones. Hi-Tech OC Unit officials stated that they had begun developing internal measures designed to complement their strategy map, including targets for opening investigations into [redacted] the most prolific DNMs or at [redacted] vendors. Further, though the Hi-Tech OC Unit had developed its first strategy map in 2018, it had not distributed the strategy to its squads located in FBI field offices until the OIG inquired about it. The Hi-Tech OC Unit's strategy map is a useful tool for the unit itself as well as the FBI field offices, and we believe that the development of a coordinated FBI-wide dark web approach could further improve the Hi-Tech OC Unit's strategic efforts. As discussed in greater detail below, it could also address a concern the Hi-Tech OC Unit shared with us about overlapping investigative responsibilities. As the Hi-Tech OC Unit undertakes the effort to develop performance measures within the unit, a better understanding of available resources outside of the unit and clarity on its investigative responsibilities should allow for even more targeted and achievable performance measures.

(U) The Hi-Tech OC Unit's UCOs Can Better Focus on the Targeting of Opioid Vendors

(U) To assess whether the Hi-Tech OC Unit's dark web efforts aligned with its dark web strategy, we reviewed and compared Hi-Tech OC Unit statistics and UCOs to the four mission objectives outlined in its strategy map in Figure 3.[13] We found that the Hi-Tech OC Unit had executed operations and established numerous UCOs to address each of the four objectives.

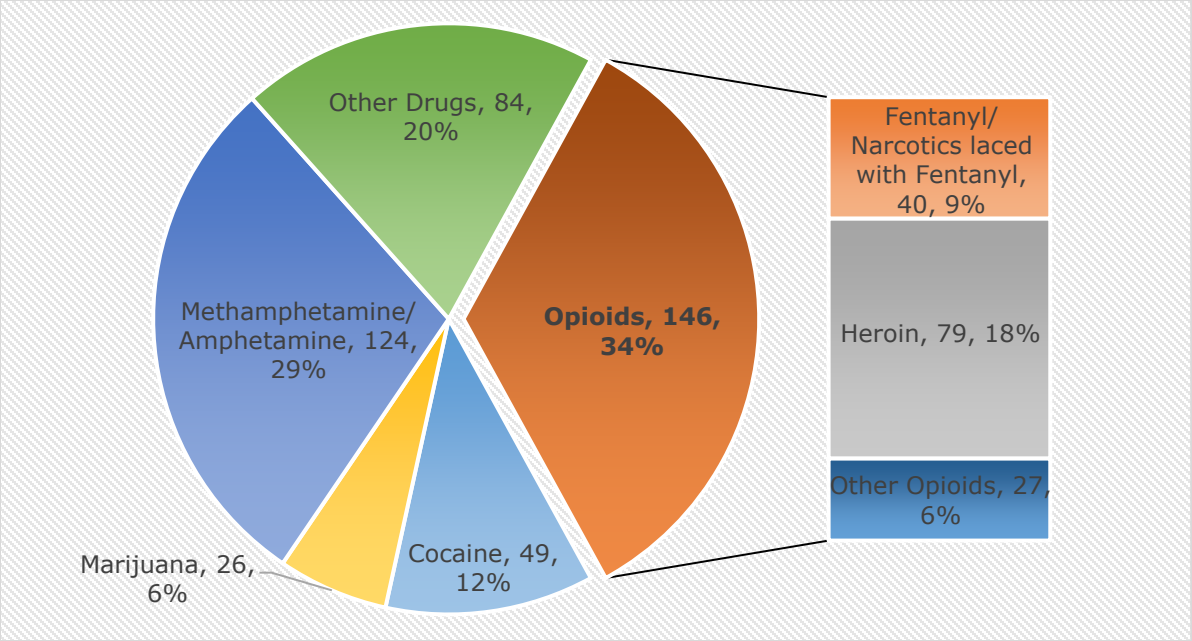
(U) To gauge whether the Hi-Tech OC Unit's efforts aligned with its strategic priority to target fentanyl and other opioid distributors on the dark web, we reviewed the Hi-Tech OC Unit's drug seizure statistics, which includes controlled narcotics purchases and physical seizures from vendors and buyers. As shown in Figure 4, opioids (fentanyl, heroin, and other opioids), which are J-CODE's highest priority, accounted for 34 percent of the Hi-Tech OC Unit's seizures, including fentanyl which accounted for 9 percent.[14]

[13] (U) The OIG's assessment was conducted using an earlier version of the strategy map from 2018. We included the 2019 version in Figure 3 because it is the current iteration and has objectives and initiatives quite similar to the 2018 version.

[14] (U) Hi-Tech OC Unit officials stated that the drug seizure statistics may include buyer seizures but that the vast majority of seizures are from vendors.

(U) Figure 4

(U) Number of Hi-Tech OC Unit Seizures, by Drug Type February 2018 through August 2019[15]



(U) Source: FBI

(U//~~LES~~) A senior Hi-Tech OC Unit official explained that when encountering vendors selling multiple drugs, including fentanyl, the Hi-Tech OC Unit's fentanyl mitigation plan requires agents to [redacted] This is a safety precaution to mitigate the risks associated with [redacted] and may provide some explanation for the low fentanyl seizure percentage.

(U) Table 1 lists the Hi-Tech OC Unit's opioid-related seizure accomplishments across FBI field divisions. According to Hi-Tech OC Unit officials, the top four field divisions were successful for various reasons, including having personnel with the most technical knowledge, being co-located with cyber squads, receiving strong support from field division supervisors, and having outside resources available, such as private sector partnerships.

[15] (U) The Deputy Attorney General mandated the FBI and DEA establish a strategy by February 16, 2018. Figure 4 contains the Hi-Tech OC Unit's 429 seizures from February 17, 2018, through August 28, 2019. "Other Drugs" includes GHB/GBL, LSD, MDMA/Ecstasy, Prescription Drugs-illegally used, and steroids. The difference in this figure's total percent is due to rounding.

(U) Table 1

(U) Hi-Tech OC Unit Opioid Seizures, by Field Division

(U//~~LES~~) Division	(U) Date Established	(U) Months Elapsed (thru Aug. 2019)	(U//~~LES~~) Total Opioid Seizures	(U//~~LES~~) Opioid Seizures per Month
[redacted]	3/15/2019	5	[redacted]	[redacted]
	1/25/2018	19		
	4/17/2018	16		
	4/17/2018	16		
	4/5/2019	4		
	11/13/2018	9		
	5/7/2018	15		
	4/17/2018	16		
	4/17/2018	16		
	10/1/2018	10		
	4/2/2018	16		
	11/13/2018	9		
	10/31/2018	9		
	5/7/2018	15		
	1/24/2019	7		
	1/15/2019	7		
	10/30/2018	9		
	10/16/2018	10		
	10/1/2018	10		
	8/2/2019	0		
	7/18/2019	1		
		TOTAL		**N/A**

(U) Source: FBI

(U//~~LES~~) Conversely, [redacted] field divisions had not recorded any opioid seizures and several others reported few. For those field divisions not reporting any seizures, [redacted] just established their UCOs at the time of our review, and another was operated by a healthcare fraud squad focused on non-opioid narcotics that was set to expire because of a lack of resources and production. Although the Hi-Tech OC Unit can only encourage field divisions on who to target, the Hi-Tech OC Unit provided UCOs the J-CODE funding necessary to operate, and according to Hi-Tech OC Unit officials, established these UCOs with the understanding that large-scale opioid vendors were the priority target. After discussing the opioid seizure results with the Hi-Tech OC Unit, a senior unit official indicated that they needed to track field divisions' opioid-related efforts more closely and provide additional training. Subsequently, the Hi-Tech OC Unit contacted some of the field divisions to reaffirm the J-CODE mission and in September 2019, held a meeting with group supervisors from the above-listed field divisions to discuss the OIG's findings.

(U) In conclusion, we note that the Hi-Tech OC Unit's J-CODE effort primarily targets the principal DNMs that are facilitating the distribution of illicit narcotics, including fentanyl and other opioids. However, Hi-Tech OC Unit seizure statistics indicate that several UCOs are not sufficiently prioritizing the targeting of dark web

illegal opioid vendors—the primary focus of the J-CODE initiative. Accordingly, we recommend that the FBI ensure that the Hi-Tech OC Unit's efforts on the dark web sufficiently target vendors trafficking fentanyl and other opioids in a manner consistent with the priorities articulated by the Deputy Attorney General.

(U) Three Operational Units did not Maintain Formalized Dark Web Strategies

(U) The Child Exploitation Operational Unit (CEOU), Investigative Unit (IU), and Major Cyber Crimes Unit (MCCU) broadly conveyed their dark web approaches but generally did not maintain comprehensive dark web strategies with objectives and initiatives, complete with performance measures, such as metrics, targets, and milestones.

(U) Child Exploitation Operational Unit

(U) CEOU is responsible for investigating criminal violations pertaining to the illegal production, distribution, receipt, and possession of child pornography and targets the sexual exploitation of children on the dark web. FBI first began encountering onion services dedicated to child sexual abuse material (CSAM) in 2007. By 2015, according to an FBI intelligence report, Tor onion services housed a greater volume of CSAM than ever previously observed by the FBI in one online location. In December 2017, another FBI intelligence report concluded that one such onion service was the largest known online population of CSAM offenders, with over 1 million unique registrations.

(U) CEOU did not maintain a formalized, comprehensive dark web strategy. CEOU's then Unit Chief was skeptical of developing a written unit-level dark web strategy, noting that the dark web is just an enabling technology to commit crime. However, when the Hi-Tech OC Unit's strategy map was provided for reference, this official agreed that the CEOU shared common objectives and initiatives with other units in the areas of training, infrastructure exploitation, and coordination. Another senior CEOU official believed that a prospective CEOU version of the strategy could be organized similar to the Hi-Tech OC Unit's, but instead of focusing on DNM buyers and vendors, would target CSAM users and producers.

(U//~~LES~~) CEOU uses a combination of traditional and highly technical tools and techniques on the dark web. Traditional law enforcement tactics included exploiting onion service server configuration errors and mistakes in anonymization use; and conducting open source research. CEOU's counterparts—including the Hi-Tech OC Unit and Investigative Unit—have more traditional techniques at their disposal to identify darknet criminals. For instance, these units used controlled purchases or sales of tangible goods that required shipment through the mail, [redacted] and cryptocurrency

tracing. These options were typically unavailable to the CEOU because the content was digital so there was [redacted], and cryptocurrency tracing was not an option because cryptocurrency was usually not involved; instead, the CSAM was the currency.

(U) With fewer traditional investigative options than its FBI dark web counterparts, the CEOU's investigative approach was primarily driven by advanced technical options available to identify users. This was best demonstrated by Operation Pacifier, which through use of a network investigative technique (NIT) led to the worldwide identification of 8,000 Playpen users. Playpen was a Tor network bulletin board and website involved in the production, advertisement, and distribution of egregious CSAM. Operation Pacifier generated 7,586 leads; 887 arrests, including 55 hands-on-abusers and 26 producers of child pornography; and 351 child recoveries.[16] Operation Pacifier highlighted the difficult and complex investigative choices that law enforcement confronts in this area. FBI assumed control of a child exploitation site to continue to operate under law enforcement control in an effort to identify and arrest significantly more offenders (see text box). In addition, the FBI's use of a NIT to identify thousands of Playpen users throughout the world resulted in complaints by internet privacy and security advocates, and the related prosecutions raised several legal questions. OIG takes no position on any of these issues in this report but includes, in Appendix 1, further information about this high-profile investigation and the issues that followed.

(U) Playpen Takedown (Operation Pacifier)

(U) Playpen had been operating on the Tor network since August 2014 and was involved in the production, advertisement, and distribution of egregious CSAM. According to the FBI, it was the largest of its kind bulletin board and website, with more than 150,000 registered users.

(U) In February 2015, the FBI seized the Playpen web server and arrested a site administrator. However, according to the FBI, seizing the web server did not provide law enforcement the IP address logs necessary to identify and locate other administrators and thousands of Playpen users. Therefore, instead of shutting down the site, the FBI assumed control of Playpen for approximately 2 weeks and obtained a search warrant to deploy a NIT on the server hosting the FBI controlled site, enabling the FBI to identify thousands of Playpen users. According to CEOU officials, as of June 2020, Operation Pacifier stood as the FBI's most successful Tor-based operation ever conducted.

(U) Operation Pacifier and similar previous efforts represented the CEOU's operational approach—to apprehend onion service administrators, seize and operate the web server, and deploy a NIT from the seized server to identify as many CSAM consumers as possible. The rationale was that simply shutting down a dark web site without conducting adequate investigation into its administrators and

[16] (U) The FBI did not have statistics on the number of convictions resulting from Operation Pacifier. Statistics for hands-on-abusers and producers of child pornography are U.S. figures. The rest are worldwide.

consumers was insufficient because they could migrate to another location, resulting in little or no disruption of access to CSAM.

(U//~~LES~~) Replicating Operation Pacifier is contingent upon the availability of NITs, which requires computer exploits that the FBI is increasingly developing for national security purposes but not for criminal investigations, such as on the dark web.[17] In fact, the FBI has not [redacted] and as a result, CEOU-driven case openings, indictments, arrests, and children identifications have significantly declined since that time. From April 2017 through September 2019, the CEOU conducted an international investigation of the top 39 Tor onion services dedicated to the sexual exploitation of children, with a cumulative user-base of nearly 2.4 million users worldwide. During this timeframe, the FBI arrested or supplied information to other law enforcement agencies that led to arrests of 16 individuals, including 7 site administrators. CEOU officials indicated that they were satisfied with these results, even if the 16 arrests were far fewer than the nearly 900 that resulted from the NIT deployed in Operation Pacifier, because they reflected a change in its investigative strategy from focusing on identifying end users to more of an organized crime approach, targeting site administrators and leadership aimed at disrupting and dismantling the most egregious onion services. Table 2 compares the results of Operation Pacifier to the international effort beginning in April 2017.

[17] (U) Computer exploits are software, malware, or commands that can be used to take advantage of vulnerabilities in technology.

(U) Table 2

(U) CEOU Statistical Accomplishments[18]

	(U) Operation Pacifier (Jan. 2015 – May 2017)	(U) Ongoing Operations (April 2017 – Sept. 2019)
Investigative Focus	Identify and target all users of one onion service	Target and disrupt/dismantle onion services and their site administrators
No. of Onion Services Investigated	1	39
Aggregate User-base	150,000	2,373,749
No. of Onion Services Disrupted and/or Dismantled[19]	1	12
No. of Users within Disrupted and/or Dismantled Onion Service(s)	150,000	1,373,499
Cases Opened (U.S. only)	1,128	10
Total Arrests	887	16
Administrators Arrested	3	7
Indictments (U.S. only)	314	3
Children Identified	351	1

(U) Source: FBI

(U) As previously noted, the CEOU shifted in recent years from targeting all CSAM site users and consumers (such as in Operation Pacifier), to targeting site administrators who facilitated the communication and transmission of CSAM content. We find this shift concerning because the FBI and Criminal Division previously determined that simply shutting down a site was not sufficient, as consumers of this illicit content can migrate to other dark web locations, resulting in little or no disruption of access to CSAM. CEOU officials responded that the exponential growth of the threat forced the FBI to reprioritize its efforts and that this strategic shift was based on consultation with its international partners and the Department, and due to: (1) general agreement among the law enforcement community that investigation alone will not address the problem, (2) a lack of law enforcement and prosecutive resources to address mass numbers of individual investigations, and (3) the absence of advanced technical tools to target large numbers of end users.

(U) We note here that our evaluation of the CEOU's operational efforts was initially limited by the CEOU's lack of consistent and readily available case statistics. CEOU tracked its investigative data in separate spreadsheets, databases, and a

[18] (U) CEOU statistics are worldwide, unless otherwise noted.

[19] (U) Disruptions are interrupting or inhibiting a threat actor from engaging in criminal or national security related activity. Dismantlement occurs when the targeted organization's leadership, financial base, and supply network has been destroyed, such that the organization is incapable of operating and/or reconstituting itself.

document containing narrative descriptions of a major operation and several spinoff investigations. CEOU's documents collectively recorded inconsistent data, requiring CEOU personnel to manually normalize the data for comparison over time. By contrast, the Hi-Tech OC Unit and Investigative Unit generated their dark web data by querying Sentinel, the FBI's automated case management system. CEOU could not initially generate a Sentinel report of its dark web casework because such cases did not contain an identifier that enabled the CEOU to distinguish them from its other investigative work.[20] Considering that, as of FY 2019, Tor continues to host the most egregious and voluminous CSAM content the FBI has seen on any platform, we believe that the CEOU needs to better track dark web case statistics to enable an accurate and complete assessment of its operational efforts.

(U) Based on the above, we believe the CEOU would greatly benefit from the establishment of a coordinated FBI-wide dark web approach that considers the overarching needs of the FBI as well as the unique operational needs of units like the CEOU's. An FBI-wide dark web approach could also establish baseline requirements that ensures that units like the CEOU better track their dark web investigative efforts in the Sentinel case management system.

(U) Investigative Unit

(U//~~LES~~) The WMD Directorate's Investigative Unit (IU) is responsible for the oversight of investigations involving domestic and international WMD related matters and targets subjects who use the Internet—predominately the dark web—to illegally acquire, sell, or manufacture WMD. In June 2014, the IU initiated [redacted] to address the use of Internet-based technologies to discuss, refine, and promulgate accurate and actionable information regarding the illegal synthesis and use of WMD.

(U//~~LES~~) IU officials acknowledged that while they did not maintain a concise strategy document similar to the Hi-Tech OC Unit's strategy map to implement their [redacted] they concluded that one was not necessary because their strategy was articulated within their international and domestic engagement plan, as well as the [redacted] standard operating procedures and Application for Undercover Authority. Although we agree that the international and domestic engagement plan was a sound strategic document that included objectives for engaging international partners, we found that the [redacted] standard operating procedures and related Application for Undercover Authority were insufficient to address the remainder of the IU's dark web strategy.

(U//~~LES~~) First, we found that the standard operating procedures were outdated, and focused primarily on the procedures necessary to conduct [redacted] Further, the IU only began analyzing performance against the objectives stated in the Application for Undercover Authority in December 2017—more than 3 years after [redacted] was established. We found that the

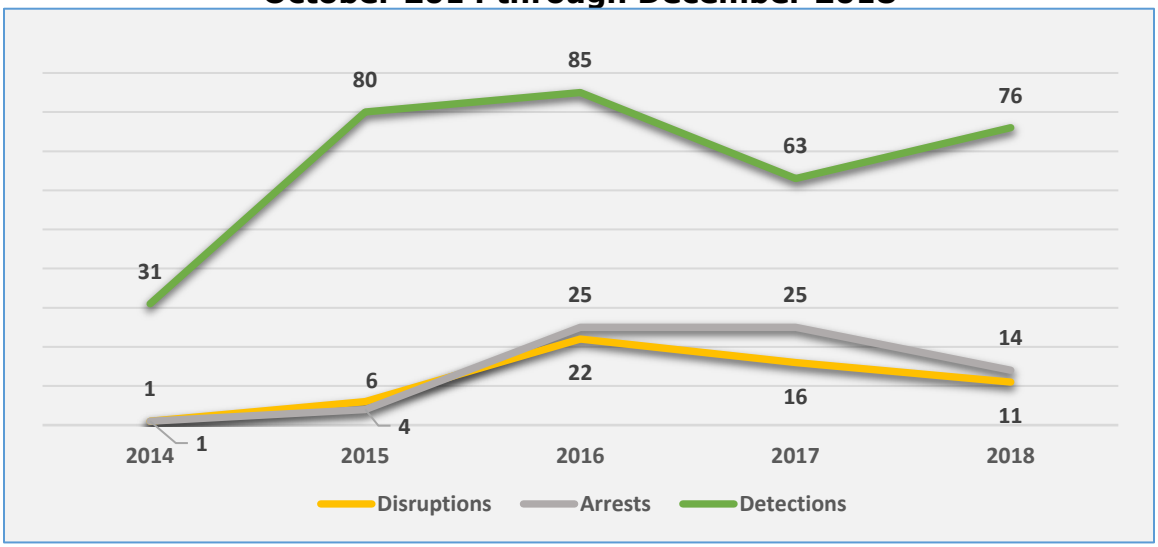
[20] (U) For example, cases tagged with identifiers, such as "encryption" or "anonymizers" could capture dark web investigations, but also numerous non-dark web investigations. In September 2019, the CEOU used Sentinel to provide updated dark web case statistics.

performance analysis consisted of ambiguous, non-measurable narrative descriptions. For example, the [redacted] two most recent performance analyses determined that its objective to [redacted] However, the performance analyses contained vague responses that did not validate this determination. Furthermore, we believe the Application for Undercover Authority is not intended for long-term strategic planning purposes, but to state the current action plan for an undercover operation and to request legal authorities and authorization to initiate or continue the operation.

(U//~~LES~~) As noted in Figure 5 below, the [redacted] began to show a general decline in disruptions and arrests after 2016, which IU officials attributed to challenges, such as keeping pace with subjects' tradecraft; [redacted]

(U) Figure 5

(U//~~LES~~) [redacted] Statistical Accomplishments October 2014 through December 2018



(U) Source: FBI

(U//~~LES~~) We recognize that, in the absence of a formal unit-level strategy, the IU has achieved operational successes through its identification and targeting of subjects using the dark web to illegally acquire, sell, or manufacture WMD. From October 2014 to December 2018, FBI statistics show that the [redacted] detected 335 subjects, arrested 69 individuals, and achieved 56 disruptions. [redacted] engaged more than 29 international partners to detect, disrupt, and arrest buyers and sellers of WMD on the dark web, with [redacted] of arrests occurring outside of the United States. It also produced [redacted] intelligence products, conducted multiple distance learning sessions, and provided operational briefings to foreign partners to foster a better working relationship. However, we believe that even greater success would be possible with a coordinated FBI-wide approach that could consider cross cutting issues experienced by the IU, such as

keeping pace with evolving tradecraft and the latest investigative tools and technologies, [redacted]

(U) Major Cyber Crimes Unit

(U) MCCU's mission is to identify cyber threats to U.S. interests posed by cybercriminal actors, aid field office investigators who are aggressively pursuing the threat, and to ultimately defeat the cyber threat actors. MCCU focuses on numerous violations, targets, and intangible goods on and off the dark web, including botnets, malware, ransomware, banking trojans, business email compromise, Internet fraud, and cyber forums and marketplaces. On the dark web, the MCCU aims to locate administrators, vendors and buyers of illegal hacking tools and dismantle the associated infrastructure.

(U) Like the CEOU and IU, MCCU did not maintain a formalized, comprehensive dark web strategy. MCCU officials initially said this was because its dark web efforts were a small component of its broader cyber strategy. However, these officials acknowledged that the MCCU needed to better define how it measured investigative success on the dark web. MCCU therefore drafted a dark web strategy in February 2019 that contained objectives, initiatives, and performance measures. However, this strategy was never finalized because new senior MCCU officials decided that their predecessors' draft dark web strategy was unnecessary. These officials stated that any strategy developed by the MCCU should address the entire unit and not be specific to technologies, such as Tor.[21]

(U) One preliminary objective of the February 2019 draft MCCU dark web strategy was to identify, dismantle, and seize infrastructure that facilitates cybercriminal activity on the dark web. MCCU planned to accomplish this objective by tracking performance metrics, such as the amount of infrastructure dismantled and seized. Former MCCU senior officials believed such a strategy could help their unit measure its investigative impact on the dark web, justify requests for additional resources and technical capabilities, and coordinate investigative and tool acquisition efforts enterprise-wide. Current MCCU officials remained skeptical of the value of developing a dark web strategy but they acknowledged that it could help improve visibility of the different tools and techniques available throughout the FBI; assist with deconfliction; and be used as a basis to improve investigative consistency between the operational units.

(U) Through our review of operational records and interviews conducted, we found that the MCCU's dark web efforts were generally consistent with its investigative approach. Following the AlphaBay takedown (see text box on page 6), the MCCU established a national dark web initiative to investigate, disrupt, and dismantle illicit dark web marketplaces and forums. MCCU also established several undercover operations to investigate onion services marketing illegal cyber-specific

[21] (U) As of September 2019, the MCCU had not developed a strategy for the unit's overall cybercriminal investigative efforts.

goods; and to collect intelligence, identify emerging schemes, and gather evidence in support of criminal investigations.

(U) However, our evaluation of the MCCU's operational efforts was limited by its lack of statistics. Specifically, the MCCU could not generate a report in Sentinel of its dark web casework because those cases did not contain an identifier that enabled the MCCU to distinguish them from its other investigative work. Without those statistics, the MCCU could not comprehensively and consistently evaluate its dark web accomplishments over time. For example, the MCCU could not provide reliable data pertaining to the number of disruptions and dismantlements of DNMs, forums, money laundering services, and other illegal onion services for all investigations related to the dark web. MCCU lacked data on its enforcement efforts against hackers and dark web merchants of stolen accounts and financial information.

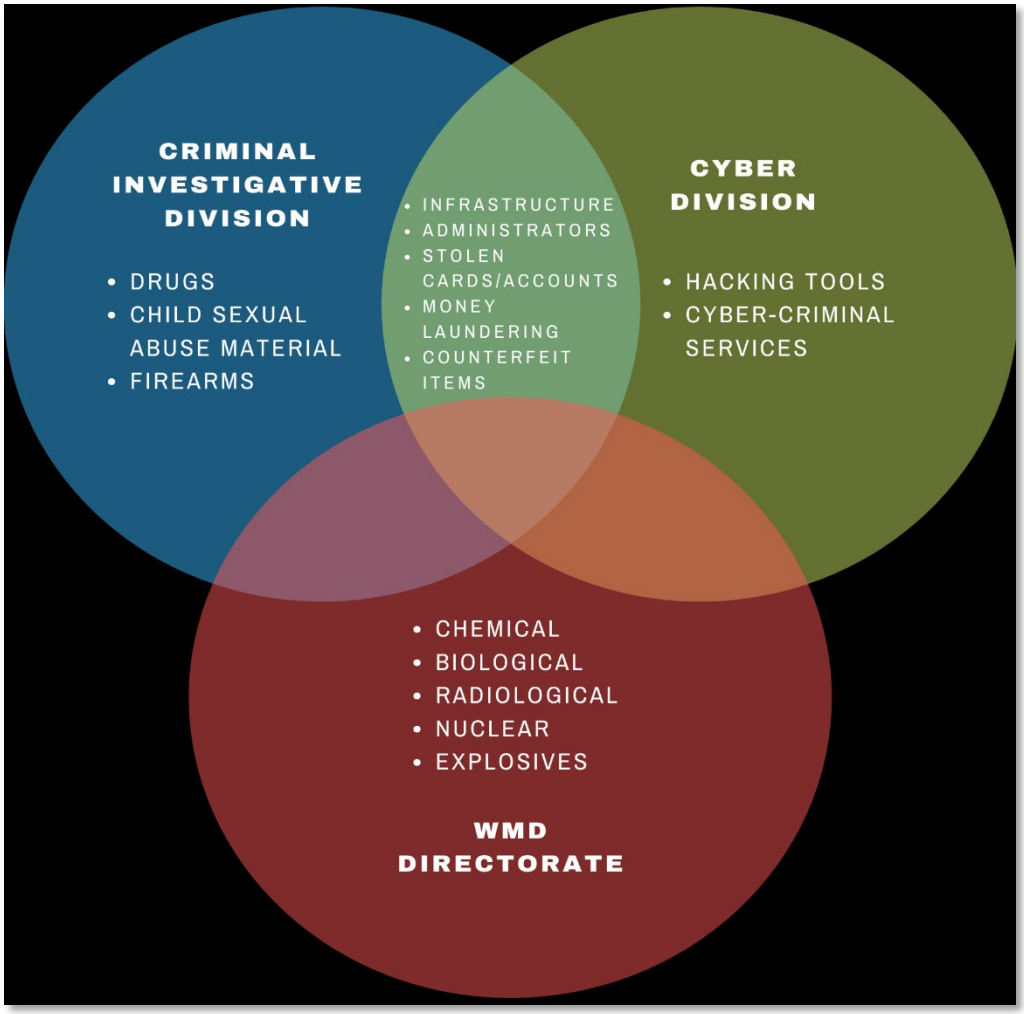
(U) Considering that the dark web is one of the MCCU's top cybercriminal threats and—according to the Department's Cyber Digital Task Force—"one of the greatest impediments to the Department's efforts," we believe that the MCCU needs to better track dark web case statistics to enable an accurate and complete assessment of its operational efforts in this area. Furthermore, one of the impediments to the MCCU's abovementioned effort to draft a dark web strategy was that they did not have the data necessary to assess their strategic progress. As we noted above when discussing the CEOU, the creation of a coordinated FBI-wide dark web approach could help FBI units establish baseline requirements that ensure that they adequately track their dark web investigative efforts in the Sentinel case management system.

(U) Ambiguous Investigative Responsibilities

(U) FBI's investigative responsibilities on the dark web, from a threat perspective, are generally divided among divisions and units in a manner that aligns with each component's mission and objectives. For instance, the IU targets the purchase and sale of chemical, biological, radiological, nuclear, and explosive materials on the dark web; and the MCCU and Hi-Tech OC Unit target vendors of illegal hacking tools and narcotics, respectively. However, investigative responsibilities appear ambiguous when targeting centralized DNM administrators and technical infrastructure, stolen cards/accounts, money laundering, and counterfeit items.

(U) Figure 6

(U) Investigative Responsibility, by Threat



(U) Source: FBI and OIG

(U//~~LES~~) Before the Hi-Tech OC Unit was created, the FBI Cyber Division (CyD) was responsible for targeting DNM administrators and infrastructure.[22] At the field level, the FBI's Sacramento field office Cyber Squad led the investigation that shuttered AlphaBay and arrested its administrator. Another FBI field office Cyber Squad investigated the administrator and technical infrastructure of [redacted]

(U) However, the March 2017 establishment of the Hi-Tech OC Unit and its emphasis on targeting drug trafficking on the dark web (particularly fentanyl and other opioids) created questions about which unit is best situated and has the organizational mandate to target DNM administrators and technical infrastructure.

[22] (U//~~LES~~) As of August 2018, CyD was targeting some of the major DNMs, [redacted] Wall Street, [redacted]

Both the Hi-Tech OC Unit and MCCU were essentially competing by developing strategies that emphasized the disruption and dismantlement of DNM administrators and infrastructure. Early in our audit, both believed their units and field office squads were best situated to target them.[23] A field office Special Agent explained that the lack of clarity regarding investigative responsibilities between the units had led to countless deconfliction discussions as well as inefficiencies in investigations in order to deliberate on which unit is the lead investigator versus providing support. This Special Agent expressed the need for the FBI to establish a policy that assigns responsibilities over dark web investigations. FBI unit-level officials agreed, stating that the establishment of a framework to resolve investigative overlap and ambiguity could enhance coordination and better facilitate the assignment of targeting responsibilities throughout the field.

(U) Department officials familiar with FBI dark web investigations also observed the lack of clarity about investigative responsibilities, noting that the border between the CID and CyD is ill-defined and hard to solve because the dark web falls right on the dividing line. Senior FBI Executives acknowledged that there was an overlap of responsibilities but were hesitant to "draw hard lines" for investigative responsibilities since the environment changes quickly and would limit the FBI's flexibility. The Hi-Tech OC Unit anticipated this challenge, stating in its establishing document that one of its responsibilities was to "coordinate with Cyber Division, as well as other sections within [CID], to *develop joint strategies and to define clear investigative and program management lanes*." (OIG's emphasis in italics). CyD determined in a FY 2019 strategy document that to address cybercriminal activity, it would need to develop and implement a strategy to integrate cyber resources with CID resources to develop and share skillsets across different programs. Though our fieldwork has determined that the Hi-Tech OC Unit and MCCU coordinate frequently and amicably, this ambiguity remains unresolved and, according to an FBI official, as of May 2019 had reached an impasse at the unit level. In June 2019, the MCCU rotated its dark web program management and the new Program Managers explained that the MCCU no longer intended to target administrators and infrastructure on drug predominant DNMs, seeming to alleviate the issue. While the current program management had shifted the MCCU's focus, a future rotation of program management may have differing ideas when it comes to investigative priorities.

(U) According to FBI officials, similar ambiguities exist in other dark web-related violations, such as money laundering, stolen cards/accounts, and counterfeit items. Money laundering, for instance, falls within the organizational scope of the Hi-Tech OC Unit, MCCU, and the Money Laundering, Forfeiture, and Bank Fraud Unit (MLFBU). The Hi-Tech OC Unit's establishing document stated that it was responsible for targeting transnational criminal enterprises engaged in money

[23] (U//~~LES~~) Hi-Tech OC Unit officials believed that since major DNMs predominantly traffic narcotics and are hierarchical criminal enterprises, the Hi-Tech OC Unit should be the lead investigator focused on DNM administrators and infrastructure. Conversely, MCCU officials believed they best equipped to handle these responsibilities because they have cadres of cyber agents throughout the field, have expertise targeting technically sophisticated cyber actors, [redacted]

laundering through sophisticated and technical means. MCCU had a "money-laundering-cyber" case classification and worked several cases against online currency exchangers because cybercriminals use these services as a cash-out mechanism for cyber illicit proceeds. However, the FBI's anti-money laundering effort is housed in the MLFBU, especially for third-party facilitators that have no connection to a particular crime but function as service providers that set up shell accounts, bank accounts, and cryptocurrency wallets to move money for criminals. MLFBU officials said that third party facilitators are their main threat and that investigating them requires significant knowledge of banking and financial systems. These officials were concerned that such cases being investigated outside of its purview were being directed to personnel without the requisite knowledge or skillset.

(U//~~LES~~) Another example of ambiguous responsibility was the FBI's investigation of firearms (e.g., handguns and rifles) on the dark web. Based on our interviews with FBI staff, the Hi-Tech OC Unit has unofficial responsibility for investigating firearms trafficking on the dark web. Our review of the Hi-Tech OC Unit's then [redacted] identified [redacted] predicated subject advertising firearms, and an FBI official informed us that the [redacted] Through our work, we found that IU investigative subjects have frequently demonstrated an interest in purchasing firearms. [redacted] Currently, if the IU encounters a subject whose sole intent is to acquire or sell firearms, it refers that subject to a law enforcement partner. IU officials had little familiarity with the Hi-Tech OC Unit's capabilities investigating firearms on the dark web. In May 2019, the OIG brought to the FBI's attention our concern that it had not sufficiently assessed the availability of firearms on the dark web and whether its investigative coverage was commensurate with the threat. In August 2019, the Hi-Tech OC Unit was considering the addition of a Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) analyst to its J-CODE team to target firearm sales on the dark web. If the Hi-Tech OC Unit decides to add the targeting of firearms vendors to its dark web strategy, coordination with ATF and the IU may be necessary.

(U) We believe that the aforementioned lack of clarity across different investigative areas could result in redundant and inefficient work, or investigative assignments not aligned with FBI personnel skillsets, capabilities, tools, and resources. Further, units like the Hi-Tech OC Unit may have overlapping investigative priorities with other DOJ components, such as ATF, or external organizations, such as the Department of Homeland Security (DHS). We believe this further demonstrates the need for an FBI-wide approach to the FBI's investigative efforts on the dark web.

(U) Summary of the Benefits of Developing a Coordinated FBI-wide Dark Web Approach

(U) As we discussed in the previous sections, we found that the four operational units are executing individual investigative strategies on the dark web—some documented, others not—with varying degrees of comprehensiveness.

Although we recognize the importance of the operational units' establishment of dark web strategies that are unique to their operational needs, we believe the development of a coordinated FBI-wide approach can help the operational units better implement their own strategies, while leveraging resources available beyond just the unit-level. For example, an FBI-wide dark web approach should:

- (U) provide investigative and support units a complete picture of the FBI's capabilities that can be leveraged across mission areas;
- (U) limit the compartmentalization of information and help the FBI streamline, consolidate, and share each unit's unique dark web knowledge and expertise, best practices, and resources related to common areas of interest;
- (U) help relevant FBI operational units strengthen and develop more targeted unit-level strategies that are unique to their individual program areas, better gauge success and accountability at the unit-level and better contribute to the overall Department effort to counter bad actors on the dark web;
- (U) clearly define investigative responsibilities on the dark web, such as more effectively addressing overlapping dark web objectives related to infrastructure exploitation and targeting administrators, thereby enabling the FBI to better manage its limited resources and avoid duplicative efforts;
- (U) ensure strategic continuity at every level, across program areas, especially when potentially disruptive leadership and other personnel changes can occur suddenly and with relative frequency;
- (U) provide baseline data collection guidelines to track operational units' dark web investigative efforts and better inform FBI senior management and external stakeholders, such as the Department, of their accomplishments; and
- (U) introduce new employees to the FBI's dark web efforts; and provide useful information and training opportunities to the field offices to assist in their prioritization and planning purposes.

(U) Therefore, we recommend that the FBI develop a coordinated FBI-wide dark web approach that assesses enterprise-level needs, while considering the unique needs of its operational and support units. At a minimum, this strategy should address ambiguous or overlapping investigative responsibilities, and provide baseline data collection guidelines to track operational units' efforts that position the FBI to provide useful and accurate information to internal and external stakeholders. Throughout the remainder of this report, we identify additional recommendations that we believe should be integral components of a newly developed FBI-wide dark web approach.

(U) Tool Development and Acquisition Concerns

(U//~~LES~~) FBI employs a variety of strategies—both conventional and technical—to find and obtain evidence, identify users and infrastructure, and apprehend perpetrators on the dark web. Though law enforcement tools and

methods (e.g., use of OCEs and confidential human sources, partnering with other law enforcement agencies, open source intelligence, and the issuance of subpoenas to third parties) are important to dark web investigators, the need to develop and acquire new technologies is paramount to allow law enforcement to identify criminals and illicit sites operating on the dark web. Some investigative tools trace cryptocurrency transactions while other tools [redacted] As expressed by the co-chair of the Department's Dark Web Strategic Planning Group, the constant need to develop and acquire new technologies is one of the biggest challenges to conducting investigations of criminal activities on the dark web.

(U) Operational Technology Division's Diminishing Role Developing Tools Useful to Dark Web Investigations

(U//~~LES~~) The Operational Technology Division (OTD) is responsible for the development and deployment of technology-based solutions for law enforcement operations. The Remote Operations Unit (ROU) within OTD's [redacted] provides computer network exploitation capabilities and online investigative techniques [redacted] ROU is [redacted] and from approximately 2012 through 2017 was largely responsible for addressing FBI requests for tools useful to dark web investigations, having supported [redacted] such requests during this timeframe, including a first of its kind takeover of a Tor site and deployment of a network investigative technique (NIT) in 2012.[24] ROU's former Unit Chief explained that the ROU worked with FBI divisions on several operations to identify Tor users, with each effort becoming increasingly sophisticated.

(U//~~LES~~) ROU was instrumental in helping develop the NIT that enabled the CEOU to successfully identify thousands of users on Playpen (see text box on page 13). Development of the NIT used for Operation Pacifier began in late 2014 and, according to ROU officials, required a significant commitment of the ROU's time and resources. The effort cost approximately [redacted] prepare and conduct the operation, which included [redacted]

(U//~~LES~~) While the ROU has had critical involvement developing tools useful to dark web investigations, since 2017 the ROU's role as an FBI source for such tools has eroded. Throughout 2018 and 2019, the ROU only processed [redacted] total requests for dark web support. ROU's former Unit Chief said this was due to several factors, including:

1. (U//~~LES~~) [redacted] (such as the NIT in Operation Pacifier), and [redacted]

[24] (U//~~LES~~) [redacted] A NIT enables investigators to uncover identifying information of target devices and users.

2. (U) resource prioritization to support the FBI's highest mission priorities, which are national security-related; and
3. (U//~~LES~~) ROU's budget declining 18 percent from FY 2015 to FY 2018, resulting in fewer funds available for [redacted][25]

(U//~~LES~~) ROU's diminished dark web role left a void in the FBI's enterprise-level investigative tool development efforts at a time when the FBI's investigative presence on the dark web and need for sophisticated tools was growing. Specifically, after the FBI dismantled AlphaBay in 2017, the MCCU increased its operational footprint by [redacted][26] By September 2018, [redacted] Establishing the Hi-Tech OC Unit in March 2017 increased investigative efforts against the trading of illicit goods and services on the dark web as well as recent increased efforts to disrupt and dismantle DNMs facilitating the distribution of fentanyl and other opioids. CEOU continues to investigate Tor hidden services, which as of FY 2019, hosts the most egregious and voluminous CSAM of any online platform.

(U//~~LES~~) Despite the growing need for sophisticated tools, FBI operational units have continued to request ROU assistance developing tools for use on the dark web, with limited success. The widespread perception among FBI officials we interviewed was that the OTD no longer fulfilled their requests for computer network exploitation on criminal investigations, including on the dark web, and that the OTD's role has shifted to providing consulting and advisory services. While FBI officials were cognizant of the OTD's resource and prioritization changes and recognized that sophisticated tools cannot be readily available, they were nonetheless dissatisfied with the recent lack of support. Department officials familiar with this matter said that the most significant problem they currently face is the lack of tools available for criminal, non-national security investigations. They noted that the FBI chose to prioritize national security cases over criminal cases, and there are reasons to do so, but they noted that it came at a cost. According to an FBI official, [redacted] Operation Pacifier in [redacted]

(U//~~LES~~) In May 2018, the FBI assessed that [redacted] the number of such offenders would continue to increase. In 2019, [redacted] CEOU consulted the ROU [redacted] but the ROU was unable to provide assistance. ROU officials said they had not received sufficient technical detail from the CEOU to develop a solution, and even if such technical detail

[25] (U//~~LES~~) Though the ROU's budget decreased 18 percent from FY 2015 to FY 2018, its budget increased 35 percent from FY 2018 to FY 2019. [redacted] such as on the dark web.

[26] (U) For additional information on the takedown of AlphaBay, see page 6.

existed, they did not have the resources to fulfill the request.[27] The CEOU official stated that [redacted]

(U) Decentralized Tool Development and Acquisition

(U//~~LES~~) ROU's prior role as the source for developing investigative tools for use on the dark web provided an FBI-wide centralization, enabling the ROU to collect and consolidate the investigative tool needs of multiple FBI divisions, and then decide the best manner to satisfy the various operational unit requirements. With the ROU unable to fulfill dark web and Tor-related requests, the operational units and field office squads assumed the tool development and implementation responsibilities. Such decentralization can be beneficial, especially throughout field offices and resident agencies, to drive innovation and develop technological solutions. For example, the OTD [redacted] In [redacted], one of the FBI's field offices [redacted] According to FBI officials, this field office [redacted] and was able to [redacted]

(U//~~LES~~) ROU's former Unit Chief explained that FBI divisions seek similar toolsets that aim to: [redacted] This official expressed concern that the increasingly decentralized tool development had led to operational units proceeding independently instead of through a concerted effort, in part, because there is no longer a central authority. According to several FBI and Department officials responsible for dark web investigations and prosecutions, the lack of coordination in the area of tool development and acquisition are "pervasive" and "huge" problems. This lack of coordination has led to operational units individually requesting to develop tools similar to each other that would be more beneficial through a concerted effort.

(U//~~LES~~) One example of deficiencies with FBI-wide coordination is the effort to obtain [redacted] In 2018, the four operational units we discuss in this report were either developing, acquiring, or in the process of developing or acquiring their own [redacted] These units spent a minimum of [redacted] during 2018 and 2019. Some officials were skeptical of the FBI developing [redacted] may have different attributes and features, and that there can be

[27] (U//~~LES~~) OTD officials said it is unknown if [redacted] have been made available or would have worked effectively.

value in multiple efforts to identify the best solution among several options, but the operational units' tool development and acquisition efforts appeared duplicative, uncoordinated, or even unbeknownst to each other.

(U//~~LES~~) Additionally, the assumption of investigative tool development and implementation responsibilities can be costly, labor-intensive, and result in reallocating limited resources that could otherwise be used for dark web investigative work. In June 2018, [redacted] created the [redacted] to help compensate for the void left by the OTD's absence. [redacted] was responsible for a wide variety of technical projects [redacted] investigations, including [redacted] on the dark web. As of June 2020, [redacted] was authorized to hire [redacted][28] [redacted] of these annual costs and [redacted] positions would be devoted to dark web investigations. The former Assistant Section Chief of the [redacted] said that [redacted] enables [redacted] to more [redacted]

(U//~~LES~~) The FBI's difficulties addressing the development of investigative tools for use on the dark web were part of a broader FBI challenge to provide FBI-wide support [redacted] in a wide variety of non-dark web criminal mission areas, including [redacted] In response to concerns from FBI subject matter experts [redacted] had become a priority gap, the FBI's Digital Transformation Office (DTO) began a project in 2018 to understand the current state of the FBI's [redacted] capabilities. DTO's project included the ROU and three of the four operational units discussed in this report—the Hi-Tech OC Unit, CEOU, and IU. DTO reached conclusions similar to the OIG's, including that operational divisions needed additional [redacted] to be successful, [redacted] resulting in inefficient, costly, and potentially redundant tool procurement. As of August 2019, the DTO's review was ongoing and though it issued recommendations to FBI executive management, no official decisions or actions had been taken.

(U//~~LES~~) We have similar concerns with one of DTO's findings that the FBI is not proactive enough in the area of research and outreach aimed at identifying

[28] (U//~~LES~~) As of June 2020, [redacted] positions had not been filled. The cost estimates were from July 2019.

[redacted] tools for use on the dark web.[29] In addition to [redacted] are leading the efforts to improve in this area, having established contracts with third parties to [redacted] requested additional funding in FY 2020 to "conduct more proactive outreach," and acquired the assistance of several field office [redacted] and [redacted]

(U) While some coordination occurs among FBI units, we believe it could be greatly enhanced with a strategy for developing and acquiring tools useful to dark web investigations that would be part of the FBI-wide dark web approach we recommend above. At a minimum, we believe this portion of the FBI-wide approach should: (1) catalog the FBI's investigative tool needs, particularly ones that benefit all operational units; (2) estimate the cost and resources necessary to address the identified technical requirements; and (3) enable operational units to distribute tool development responsibilities—including research and outreach—in a more coordinated and cost-effective manner.

(U//~~LES~~) Furthermore, we believe there are longer-term opportunities for more coordinated investigative tool development throughout the Department. For instance, the DEA's FY 2020 congressional budget submission contains an approximately $1 million request for tool research and development for use in dark web/cyber-related cases. DEA further states that it "lacks techniques that would provide access to encrypted dark web servers and supporting infrastructure." Different federal agencies have unique areas of dark web expertise. For instance, [redacted] DEA also requested $2 million to consolidate its cryptocurrency-related efforts while the FBI is also in the process of doing the same. The often-borderless nature of crime on the dark web means that Department-wide coordination is integral to ensure limited funds are used as efficiently as possible.[30]

(U) As a result, we recommend that the FBI includes in its FBI-wide dark web approach, a process to enhance and consolidate investigative tool development and acquisition efforts in a manner that addresses the FBI's and potentially the Department's dark web needs in a more cost-effective manner.

[29] (U//~~LES~~) One of the DTO's findings was about the need for [redacted] DTO recommended the FBI be more forward-looking by diversifying its toolsets amidst the constantly changing technological landscape.

[30] (U) In addition, the Attorney General's Cyber Digital Task Force's July 2018 report states that the Department should work with partners to develop new technological tools that will enable law enforcement to identify the true location of dark web sites engaged in criminal activity.

(U) Improved Coordination of the Use of Existing Investigative Tools

(U//~~LES~~) Through our audit work, we identified [redacted] investigative tools useful to dark web investigations in operation or in development [redacted] These tools were developed internally by FBI personnel, acquired through contractors, [redacted] or leveraged through other agencies. The OIG's effort to compile a comprehensive list of the FBI's tools useful to dark web investigations was challenging because the FBI did not have a central authority or location to manage [redacted]

(U//~~LES~~) It is important that operational units be constantly aware of one another's technological capabilities to ensure that tools be deployed for maximum impact during their limited window of opportunity, as tools can quickly become ineffective or obsolete. We encountered instances where senior FBI officials responsible for dark web investigations were [redacted] According to an FBI Computer Scientist, [redacted] During this 2-year period between [redacted] we were told that the FBI was [redacted] Despite the [redacted] IU's Unit Chief was [redacted] FBI officials indicated that this was not problematic [redacted] However, our review of the IU's investigative records shows that [redacted] Thus, the IU could benefit from [redacted]

(U//~~LES~~) Additionally, Hi-Tech OC Unit [redacted] several [redacted][31] We selected four [redacted] and determined that, as of April 2019, two had not been [redacted] However, as explained previously, the [redacted] and the FBI's [redacted] Hi-Tech OC Unit officials responded that [redacted] and the Hi-Tech OC Unit intends to [redacted] going forward.

(U//~~LES~~) CyD officials also noted that the FBI was slow to raise awareness of [redacted]

[31] (U//~~LES~~) [redacted]

[redacted] This [redacted] may be the result of the aforementioned absence of a central authority assigned with ensuring that all stakeholders are aware of the available tools. An FBI official also noted that, when [redacted] Therefore, the FBI needs to better ensure that operational units share available tools to prevent delays or missed opportunities.

(U) IU and Hi-Tech OC Unit officials agreed that centralizing the FBI's tools useful to dark web investigations would be beneficial. Doing so could help identify the common requirements shared amongst the operational units and potentially reduce unnecessary expenses. We recommend that the FBI includes in its FBI-wide dark web approach a process to centralize the FBI's tools useful to dark web investigations to allow visibility to and access by other FBI components.

(U//~~LES~~) Enhanced Process to More Efficiently Use [redacted]

(U//~~LES~~) As previously described, [redacted] and the FBI's [redacted] are responsible for [redacted] for operational units investigating [redacted] The associated process requires the FBI obtain [redacted]

(U//~~LES~~) [redacted] officials explained that [redacted] Dark web-related [redacted] During the course of our audit, CyD and CID officials shared concerns that the process to [redacted] One CID official responsible for administering [redacted] noted that if the [redacted]

(U//~~LES~~) [redacted] Unit Chief said the OIG was the first to bring the CID's and CyD's [redacted] and believed the process's timeliness could be improved. [redacted] necessary to obtain [redacted] The process [redacted] if the FBI [redacted]

[redacted] If these conditions do not exist, [redacted] completion can vary significantly. [redacted] may occur if [redacted] also explained that [redacted] Given the [redacted] of the CID and CyD, [redacted] officials did offer suggestions to improve the process, including: (1) contacting [redacted]—such as when [redacted] to provide [redacted] conduct background research on [redacted]

(U//~~LES~~) [redacted] We recommend that the FBI ensure that the CyD and CID coordinate with OTD to develop formal procedures for handling dark web [redacted]

(U) Centralization of Dark Web Training Resources

(U) Training is critical in a complex and evolving online environment, such as the dark web, which is characterized by rapidly changing technologies and a sophisticated user community that constantly adapts to law enforcement actions. FBI personnel must be knowledgeable about topics, such as Tor and other anonymity networks, onion services, encryption, cryptocurrencies, and investigative tools and techniques useful to dark web investigations. OCEs are integral to dark web investigations, as they identify potential threats, interact with buyers and sellers, complete cryptocurrency transactions, and collect evidence. Several FBI personnel said that on-the-job training was most crucial to successfully conducting dark web investigations. Others sought more general cross-programmatic dark web training, saying that the FBI's 1-week OCE certification course was insufficient to prepare OCEs to operate on the dark web.[32] These varying responses as well as the range of case circumstances reflect the differing degree of OCE training and knowledge necessary to successfully operate on the dark web.

(U) Although we did not identify any concerns with the content of the FBI's dark web-related training material that we reviewed, we found that the FBI maintained a significant amount of general dark web-related training resources only at the unit level. For example, centralized training repositories, such as the FBI's

[32] (U) To become certified as an OCE, the FBI required personnel attend a 1-week course that discussed topics, such as digital communications, evidence collection, and operating covertly. The only topic related to the dark web was a 1-hour cryptocurrency course.

Virtual Academy contained almost no dark web-related training.[33] This left many FBI personnel unaware of available in-house training related to topics, such as cryptocurrency tracing, evidence handling and seizure procedures, and conducting controlled purchases. These types of training resources are relevant across several FBI programs; however, because of the difficulty in locating them at the unit level, we found that some FBI personnel sought such training outside of the FBI. In addition, we found redundancies in some of the FBI's internally developed training, such as for cryptocurrency, because several different FBI units developed, administered, and maintained their own dark web trainings.

(U) FBI can improve its training efforts by developing a central repository for all of the FBI's internally developed dark web training. We believe this will improve the visibility and availability of key training for all FBI personnel combatting crime on the dark web. Therefore, we recommend that the FBI include in its FBI-wide dark web approach, a process to centralize and eliminate outdated or redundant dark web training opportunities and inform FBI personnel of the availability of the training across all applicable FBI divisions.

(U) Dark Web Cryptocurrency Support

(U) Cryptocurrency, particularly bitcoin, is the preferred method of payment for illicit transactions on the dark web because of its perceived anonymity. The use of cryptocurrencies for criminal transactions presents ongoing challenges to U.S. law enforcement agencies and their international partners. We were told that the FBI has investigations in almost every field office where subjects have used cryptocurrency, including in terrorism, money laundering, drug trafficking, cyber intrusion, and essentially all other violations that are capital driven. Due to the increasing challenge that cryptocurrencies present, the FBI's CID and CyD combined their efforts to address the FBI's Virtual Currency Initiative (VCI), which is comprised of subject matter experts that provide cryptocurrency expertise to FBI investigations in the field offices.

(U) According to the FBI, investigations involving the illicit use of cryptocurrency have increased from 15 cases in 2015 to over 350 cases in 2019, and resulted in the seizure of over $100 million in cryptocurrency, with such work rapidly increasing across numerous federal violations throughout multiple divisions and nearly every FBI field office. The majority of the FBI's cryptocurrency-related efforts are handled by the CID's MLFBU and CyD's NCIJTF through separate Virtual Currency Teams (VCT) that began around 2015 when they both separately sought funding from the Department's Assets Forfeiture Fund (AFF). Though the VCTs generally operated independent of each other, the FBI established the VCI to consolidate their AFF budget requests, share the AFF funds, and to track their collective efforts, which include providing cryptocurrency tracing, forfeiture assistance and training. VCI efforts have increased substantially over the past several years. In FY 2016, the VCI seized $478,000 in assets, opened 38

[33] (U) Virtual Academy is a web-based portal by which all training endeavors affiliated with the FBI are disseminated, tracked, and maintained. We searched Virtual Academy for the terms darknet, dark web, dark, hidden, onion, Tor, cryptocurrency, currency, bitcoin, blockchain.

cryptocurrency-related cases, and trained 1,400 personnel. By comparison, in FY 2018 the VCI seized nearly $58 million, opened 92 cryptocurrency-related cases, and trained about 5,900 personnel. See Table 3 for additional information on the FBI's VCTs.

(U) Table 3

(U) FBI's Virtual Currency Teams

	(U) CID MLFBU[34]	(U) CyD NCIJTF
MISSION	To address the cross-programmatic threat posed by the illicit use of cryptocurrencies.	To assist the FBI, other federal, state, and local law enforcement, and the intelligence community with identifying cryptocurrency investigative leads and actionable intelligence.
TEAM COMPOSITION	FBI and contract staff	FBI, other government agencies, and contract staff
PRIMARY CUSTOMERS	FBI field offices	FBI and other government agencies
RESPONSIBILITIES		
CRYPTOCURRENCY TRACING	✓	✓
INTELLIGENCE DISSEMINATION	✓	✓
TRAINING/OUTREACH	✓	✓
SEIZURE AND FORFEITURE	✓	✓
INTERAGENCY COLLABORATION	✗	✓

(U) Source: FBI

(U) VCI does not have dedicated funding, instead relying on the AFF to fund the bulk of its expenses. Over the past 4 years, AFF funding has remained static while the VCI costs have increased annually, particularly the licensing costs for analytical tools. For example, the cost of the FBI's premier tracing tool increased over 700 percent from approximately $150,000 to $1,200,000 from 2016 to 2019. In FY 2019, the VCI requested $4.2 million for analytical tools, training, outreach, personnel, and other expenses, but received $1.5 million in AFF funding. CID and CyD were able to cover some of the funding shortfall, but the increasingly scarce VCI resources have resulted in disagreement between the VCTs on the appropriate prioritization of AFF resources. Particularly, MLFBU officials were concerned that the increasingly limited VCI resources would erode its ability to acquire additional licenses for analytical tracing tools, which numerous officials described as integral, and questioned the NCIJTF's use of contractors, which it considered redundant and unnecessary given that the FBI has its own staff with such knowledge. NCIJTF officials were concerned that, if the cost of tools continued to increase or if AFF funds were no longer available, it may no longer afford the contract staff necessary to meet its VCT's mission, particularly in its investigative support, liaison and outreach to FBI headquarters divisions, field offices, and agencies external to the

[34] (U) MLFBU's VCT includes officials from the FBI's Transnational Organized Crime Intelligence Unit; and Money Laundering Intelligence Unit.

FBI. The dwindling resources also shed light on FBI concerns that it had no comprehensive strategy for addressing the cryptocurrency threat in the future and that the VCTs are conducting redundant work, particularly in the areas of training, outreach and cryptocurrency tracing. For instance, the VCTs both provided separate introductory cryptocurrency training, with different curriculums, to various FBI and non-FBI entities. We believe these efforts could be more efficiently coordinated and streamlined. MLFBU and NCIJTF officials concluded that redundancies existed because the FBI had no clearly delineated guidelines related to which divisions and units perform which function, resulting in duplicative efforts; confusion among field offices, prosecutors, industry, and academia; and a strain on the VCI's limited funding.

(U) In 2019, FBI executive management—recognizing these growing issues—assigned the VCTs to develop an FBI-wide cryptocurrency support strategy that leverages and centralizes the FBI's expertise and resources. At the time of this audit report, only NCIJTF had developed and disseminated a document on how it envisioned the future state of FBI cryptocurrency efforts. NCIJTF proposed several solutions but preferred the consolidation and centralization of the FBI's cryptocurrency resources and functions, including those of the VCTs, into a single unit.

(U) Because the FBI is still awaiting similar reports from other FBI divisions, we recommend that the FBI develop timelines to obtain feedback from remaining FBI divisions and complete its development of the FBI-wide cryptocurrency support strategy.

(U) Deconfliction of Investigative Data

(U) FBI units operating on the dark web are frequently at risk of unknowingly crossing into the investigation of another government agency or even another FBI unit. Therefore, timely deconfliction of investigative data among law enforcement agencies is essential to ensure agent safety, preserve the integrity of ongoing investigations, and share information to identify targets of common investigative interest. In May 2014, the Department issued a memorandum requiring all Department law enforcement components to enter investigative data into deconfliction systems, including the Deconfliction and Information Coordination Endeavor (DICE). DICE provides real-time connectivity to deconfliction information and once a common link has been identified, appropriate personnel are notified and provided contact information to share, coordinate, and avoid conflicting equities. Investigative data subject to DICE deconfliction include social network identifiers, online monikers, addresses, phone numbers, dates of birth, email addresses, IP addresses, bitcoin wallet addresses, and financial account numbers.

(U) During our review of the FBI's dark web UCOs, we identified investigative data, such as subject monikers, OCE monikers, and shipping addresses that were being investigated by different FBI field offices and non-DOJ components. For example, one subject moniker was being targeted by multiple FBI field offices, the DEA, U.S. Postal Inspection Service, and DHS. To assess whether operational units responsible for dark web investigations were complying with Department and FBI

deconfliction requirements, we judgmentally sampled 95 investigative data items for entry into DICE. We determined that only approximately 47 percent of these items were properly entered (see below).

(U) Table 4

(U) Deconfliction Testing Results

(U) Operational Unit	(U) Sampled Investigative Data Items	(U) Investigative Data Items Properly Entered into DICE	(U) % Investigative Items Properly Entered into DICE
IU	9	8	89%
Hi-Tech OC Unit	52	31	60%
MCCU	19	6	32%
CEOU	10	0	0%
Other[35]	5	0	0%
Total	**95**	**45**	**47%**

(U) Source: OIG and the FBI

(U) The Hi-Tech OC Unit, MCCU, and CEOU provided the following explanations why they had not fully complied with Department or FBI deconfliction requirements.

- A Hi-Tech OC Unit official stated they were not sure why field office personnel were not entering covert shipping addresses into DICE. The Hi-Tech OC Unit issued an electronic communication in April 2019 reminding their offices with UCOs that they must follow the Department memorandum and enter covert mailboxes and darknet vendors into DICE.
- An MCCU official stated they create so many monikers that it can be difficult to enter all of them into DICE. The official also mentioned that some field offices were not aware of DICE.
- A CEOU official stated they do not enter investigative data into DICE because they are the only DOJ component in this respective space and that they regularly deconflict with other U.S. law enforcement agencies.

(U) Not entering information into DICE could lead to inefficiencies in investigative efforts or even an incident where a failure to deconflict results in agents being misidentified as criminals. To address the deconfliction issues identified in our report, we recommend that the FBI either supplement its FBI-wide deconfliction policy with, or separately develop, a formal oversight process to

[35] (U) "Other" refers to the FBI's Economic Crimes Unit, which does not have a significant investigative presence on the dark web, but had one UCO involving dark web investigative data. We performed DICE testing on this investigative data.

ensure that investigative data encountered on the dark web is properly entered into the DICE deconfliction system.[36]

(U) CONCLUSION AND RECOMMENDATIONS

(U) Our audit determined that the FBI does not maintain a formalized FBI-wide dark web strategy. Instead, FBI operational units are executing individual dark web strategies—some documented, others not—containing varying degrees of comprehensiveness. Of the operational units reviewed, the Hi-Tech OC Unit's dark web strategy provided the most comprehensive view of its dark web mission and objectives. CEOU, IU, and MCCU broadly conveyed their dark web approach, but generally did not maintain formalized strategies. Although each of these units could point to significant successes on the dark web, we believe that the establishment of a coordinated FBI-wide dark web approach could better ensure clarity on investigative responsibilities among the various units, enable more efficient and cost effective investigative tool development and acquisition, highlight relevant and current training opportunities, offer strategic continuity, and provide baseline data collection guidelines that enable the FBI to better report its overall dark web successes. Such an FBI-wide approach will also guide the operational units as they consider unit-level strategies and determine how to best measure their performance in this area.

(U//~~LES~~) We also identified coordination weaknesses in handling dark web [redacted] and found redundancies between two VCTs in the areas of training, outreach, and cryptocurrency tracing, which demonstrates the need for the FBI to consider an FBI-wide cryptocurrency support strategy as part of this overall effort. We also determined that operational units had not been consistently entering investigative data into the Department-mandated deconfliction system. As a result, we provide five recommendations to assist the FBI in improving its current approach to address criminal activity conducted on the dark web.

(U) We recommend that the FBI:

1. (U) Ensure that the Hi-Tech OC Unit's efforts on the dark web sufficiently target vendors trafficking fentanyl and other opioids in a manner consistent with the priorities articulated by the Deputy Attorney General.

[36] (U) The "FBI-wide deconfliction policy" refers to a recommendation from a joint report of the Inspectors General for DOJ and DHS on agency cooperation on the Southwest border. The report included a DOJ OIG recommended that the FBI develop, implement, and share an FBI-wide deconfliction policy. FBI concurred with the recommendation and the FBI efforts to implement it are ongoing. Department of Justice OIG and Department of Homeland Security Office of Inspector General, *A Joint Review of Law Enforcement Cooperation on the Southwest Border between the Federal Bureau of Investigation and Homeland Security Investigations*, Evaluation and Inspections Report 19-03, Special Reviews and Evaluations OIG Report 19-57 (July 2019), https://oig.justice.gov/reports/2019/e1903.pdf, 30.

2. (U) Develop a coordinated FBI-wide dark web approach that assesses enterprise-level needs, while considering the unique needs of its investigative and support units. At a minimum, this approach should address:

    a. (U) ambiguous or overlapping investigative responsibilities;

    b. (U) baseline data collection guidelines to track operational units' dark web investigative efforts that position the FBI to provide useful and accurate information to internal and external stakeholders;

    c. (U) processes to enhance and consolidate investigative tool development and acquisition efforts in a manner that addresses the FBI's and potentially Department's dark web needs in a more cost-effective manner, and to centralize the FBI's tools useful to dark web investigations to allow visibility to and access by other FBI components; and

    d. (U) a process to centralize and eliminate outdated or redundant dark web training offerings and inform FBI personnel of the availability of dark web training across all applicable FBI divisions.

3. (U//~~LES~~) Ensure that the CyD and CID coordinate with OTD to develop formal procedures for handling dark web [redacted]

4. (U) Develop timelines to obtain feedback from remaining FBI divisions and complete its development of the FBI-wide cryptocurrency support strategy.

5. (U) Supplement its FBI-wide deconfliction policy with, or separately develop, a formal oversight process to ensure that investigative data encountered on the dark web is properly entered into the DICE deconfliction system.

(U) APPENDIX 1

(U) OBJECTIVE, SCOPE, AND METHODOLOGY

(U) Objective

(U) Our audit objective was to assess the FBI's implementation of its dark web strategy.

(U) Scope and Methodology

(U) Our audit generally covered, but was not limited to, the FBI's activities from October 2014 through April 2019. Our primary references were FBI strategic planning standards, the FBI's Domestic Investigations and Operations Guide, and the Department's Memorandum for the Mandatory Use of Deconfliction Systems. To accomplish our objective, we reviewed the Investigative Unit's (IU), Hi-Tech Organized Crime Unit's (Hi-Tech OC Unit), Child Exploitation Operational Unit's (CEOU), and Major Cyber Crimes Unit's (MCCU)—collectively referred to as the operational units—strategies to determine if the FBI's overarching dark web strategy was documented; contained objectives and initiatives supported by performance measures, such as metrics, targets, and milestones; and disseminated throughout headquarters and the field. To develop an understanding of unit strategies, we also interviewed personnel responsible for dark web-related activities from FBI field offices and FBI headquarters.

(U) To determine if the operational units' investigative efforts aligned with the unit-level dark web strategy, we evaluated investigative case data and metrics to measure the FBI's efforts and impact on the dark web. We also reviewed each unit's Application for Undercover Authority for the Undercover Operations (UCO) used to support the dark web efforts.

(U) We assessed the operational units' technological tool development and acquisition efforts to determine if they were equipped to identify criminal actors on the dark web. This included identifying the universe of tools available for dark web investigations through reviewing contract documentation, interviewing personnel, and examining the Application for Undercover Authority.

(U) We evaluated the resources available for dark web investigations related to the FBI's cryptocurrency-related support and training. We interviewed FBI officials from the two support units that assist with investigations involving cryptocurrency, to gain an understanding of the resources available. Additionally, we learned about the dark web and cryptocurrency-related trainings available to FBI personnel through interviews and by reviewing training materials developed by the operational and support units.

(U) We conducted site work at FBI headquarters in Washington, D.C.; the FBI field office in Sacramento, California; and FBI facilities in Chantilly, Virginia; Quantico, Virginia; and Linthicum, Maryland. We selected these sites to examine the FBI's dark web operational efforts. In total, we interviewed over 40 FBI

officials, including Assistant Section Chiefs, Unit Chiefs, Supervisory Special Agents, Special Agents, Staff Operations Specialists, Intelligence Analysts, and Computer Scientists.

(U) Statement on Compliance with Generally Accepted Government Auditing Standards

(U) We conducted this performance audit in accordance with generally accepted government auditing standards. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

(U) Internal Controls

(U) In this audit we performed testing, as appropriate, of internal controls significant within the context of our audit objective. A deficiency in internal control design exists when a necessary control is missing or is not properly designed so that even if the control operates as designed, the control objective would not be met. A deficiency in implementation exists when a control is properly designed but not implemented correctly in the internal control system. A deficiency in operating effectiveness exists when a properly designed control does not operate as designed or the person performing the control does not have the necessary competence or authority to perform the control effectively.[37]

(U) As noted in the Audit Results section of this report, we identified a deficiency in the FBI's internal controls that are significant within the context of the audit objectives and based upon the audit work performed that we believe may adversely affect the FBI's ability to achieve its dark web objectives. Specifically, we found issues when deconflicting investigative data through the use of the Deconfliction and Information Coordination Endeavor (DICE) system. This weakness in internal controls could lead to inefficiencies in investigative efforts or even an incident where a failure to deconflict results in agents being misidentified as criminals.

(U) Compliance with Laws and Regulations

(U) In this audit we also tested, as appropriate given our audit objective and scope, selected transactions, records, procedures, and practices, to obtain reasonable assurance that the FBI's management complied with federal laws and regulations for which non-compliance, in our judgment, could have a material effect

[37] (U) Our evaluation of the FBI's internal controls was not made for the purpose of providing assurance on its internal control structure as a whole. FBI management is responsible for the establishment and maintenance of internal controls. Because we are not expressing an opinion on the FBI's internal control structure as a whole, this statement is intended solely for the information and use of the FBI. This restriction is not intended to limit the distribution of this report, which is a matter of public record. However, because this report contains sensitive information that must be appropriately controlled, a redacted copy of this report with sensitive information removed will be made available publicly.

on the results of our audit. Our audit included examining, on a test basis, the FBI's compliance with the following laws and regulations that could have a material effect on the FBI's operations:

- (U) Attorney General's Guideline for Domestic FBI Operations (Guidelines are issued under the authority of the Attorney General as provided in 28 U.S.C. sections 509, 510, 533, and 534, and Executive Order 12333); and
- (U) Domestic Investigations and Operations Guide (Derived from the authority of the Attorney General as provided in 28 U.S.C. sections 509, 510, 533, and 534).

(U) This testing included interviewing auditee personnel, evaluating investigative case data, assessing the operational units' technological tool development, and reviewing training and support records. However, nothing came to our attention that caused us to believe that the FBI was not in compliance with the aforementioned laws and regulations.

(U) Sample-based Testing

(U) To accomplish our audit objective, we performed sample-based testing on the DICE deconfliction system. A judgmental sampling design was applied to capture whether the FBI was entering subject monikers and other investigative data into DICE in accordance with Department policy. For this we selected a judgmental sample of subject monikers from 7 of the 24 (29 percent) operational units' UCOs, based on the timing and number of dark web UCOs conducted by each operational unit, and reviewed DICE records to ensure the subject monikers were entered properly. This non-statistical sample design did not allow projection of the test results to the universe from which the samples were selected.

(U) Computer-Processed Data

(U) During our audit, we obtained information from the Sentinel and DICE systems. We did not test the reliability of those systems as a whole, therefore any findings identified involving information from those systems were verified with documentation from other sources.

(U) Operation Pacifier – Legal Issues

(U) In 2015, the FBI seized a child sexual abuse material (CSAM) site on the Tor network called "Playpen" and, instead of shutting it down, continued to run it from a government site in the Eastern District of Virginia for about 2 weeks. The FBI and Criminal Division determined that simply shutting down the site was not sufficient, as users would migrate to a different website. They decided that every effort should be taken to identify as many users as possible. During the approximately 2-week site seizure, the FBI deployed a network investigative technique (NIT) that gathered identifying information from Playpen users' computers. The single NIT warrant, executed in Virginia, implicated more than 100

defendants across the U.S.[38] This FBI effort, called Operation Pacifier, generated controversy because of the ethical and moral implications of the U.S. government allowing a child exploitation site to continue to operate under law enforcement control. The FBI's use of a NIT to identify thousands of Playpen users throughout the world also resulted in complaints by internet privacy and security advocates.

(U) The prosecutions resulting from Operation Pacifier raised constitutional and legal questions, and generated discovery disputes. In general, defendants sought to suppress evidence and have the charges dismissed by arguing that: (1) the FBI's operation of the Playpen website constituted "outrageous" government conduct that violated due process; (2) the NIT warrant violated the Fourth Amendment; and (3) the NIT warrant was unlawful because the issuing magistrate judge had no authority to issue a warrant to search personal property, such as home computers, located outside the magistrate's federal judicial district. Some of the challenges raised by individual defendants were supported by amicus briefs filed by civil liberties and advocacy organizations.

(U) The due process argument has been uniformly rejected by circuit courts of appeals.[39] Many courts found that the initial warrant violated Federal Rule of Criminal Procedure 41, which, at the time, did not authorize magistrate judges to issue warrants outside of their judicial district.[40] Despite this violation, every Federal Circuit to address the issue has determined that evidence obtained from this NIT should not be suppressed because of the "good faith" exception to the Fourth Amendment's exclusionary rule.[41] Under this exception, evidence obtained by law enforcement officials who had an objectively reasonable, good faith belief that they were acting pursuant to legal authority is admissible even if the search warrant is later found to be defective.[42]

(U) In addition, numerous defendants argued that the government must disclose the programming code for the NIT that was deployed on their personal computers. Many courts denied such motions on the grounds that the entire code was not material to the defense.[43] However, in one instance, when the district

---

[38] (U) *United States* v. *Horton*, 863 F.3d 1041 (8th Cir. 2017), *cert. denied*, 138 S. Ct. 1440 (2018).

[39] (U) *United States* v. *Wagner*, 951 F.3d 1232, 1253 (10th Cir. 2020) ("Every circuit to consider the issue has held the FBI's operation of Playpen was not outrageous government conduct.") (collecting cases).

[40] (U) Rule 41 was subsequently "amended to authorize magistrate judges to issue warrants to search computers and seize or copy electronically stored information located outside the magistrate judge's district if the district where the computer or information is located has been concealed through technological means." *United States* v. *Werdene*, 883 F.3d 204, 207 (3d Cir.), *cert. denied*, 139 S. Ct. 260 (2018) (citing Fed. R. Crim. P. 41(b)(6)).

[41] (U) *United States* v. *Grisanti*, 943 F.3d 1044, 1049 (7th Cir. 2019) ("[W]e held that the good-faith exception applies to agents who relied on this very warrant. Ten other circuits have agreed with that conclusion.") (collecting cases).

[42] (U) *United States* v. *Leon*, 468 U.S. 897, 920-921 (1984).

[43] (U) *E.g., United States* v. *Harney*, No. 16-38-DLB-CJS, 2018 WL 1145957, at *9 (E.D. Ky. Mar. 1, 2018), *aff'd*, 934 F.3d 502 (6th Cir. 2019) (collecting cases).

court ordered disclosure of the complete code, the Department moved to dismiss the pending charges to avoid disclosure of the sensitive investigative technique.[44] As of early 2020, many Operation Pacifier-related cases remain in litigation.

(U) The OIG included this detail on Operation Pacifier in this report because of its significance to the FBI's dark web investigative efforts and strategy. The OIG takes no position on whether the FBI's investigative techniques were proper or whether the Department's legal arguments in past or pending litigation related to Operation Pacifier have merit.

[44] (U) *United States* v. *Michaud*, No. 3:15-cr-05351-RJB, 2016 WL 337263 (W.D. Wash, January 28, 2016).

(U) APPENDIX 2

(U) ACRONYMS

(U) AFF	(U) Assets Forfeiture Fund
(U) ATF	(U) Bureau of Alcohol, Tobacco, Firearms and Explosives
(U) CEOU	(U) Child Exploitation Operational Unit
(U) CID	(U) Criminal Investigative Division
(U) CSAM	(U) Child Sexual Abuse Material
(U) CyD	(U) Cyber Division
(U) DEA	(U) Drug Enforcement Administration
(U) DHS	(U) Department of Homeland Security
(U) DICE	(U) Deconfliction and Information Coordination Endeavor
(U) DNM	(U) Darknet Marketplace
(U) DTO	(U) Digital Transformation Office
(U) FBI	(U) Federal Bureau of Investigation
(U) Hi-Tech OC Unit	(U) Hi-Tech Organized Crime Unit
(U) IU	(U) Investigative Unit
(U) J-CODE	(U) Joint Criminal Opioid Darknet Enforcement
(U) MCCU	(U) Major Cyber Crimes Unit
(U) MLFBU	(U) Money Laundering, Forfeiture, and Bank Fraud Unit
(U) NCIJTF	(U) National Cyber Investigative Joint Task Force
(U) NIT	(U) Network Investigative Technique
(U) OCE	(U) Online Covert Employee
(U) OIG	(U) Office of the Inspector General
(U) OTD	(U) Operational Technology Division
(U) ROU	(U) Remote Operations Unit
(~~U//LES~~)	(~~U//LES~~) [redacted]
(U) Tor	(U) The Onion Router
(U) UCO	(U) Undercover Operation
(U) VCI	(U) Virtual Currency Initiative
(U) VCT	(U) Virtual Currency Team
(U) WMD	(U) Weapons of Mass Destruction
(U) WMD Directorate	(U) Weapons of Mass Destruction Directorate

(U) APPENDIX 3

(U) GLOSSARY

Administrator	The individual responsible for creating, maintaining, and operating a darknet marketplace and keeping its content and design backed up and fully functional. Often the individual with access to the site's servers and databases, and control over the site's cryptocurrency wallets.
Application for Undercover Authority	Form titled "Application for Undercover Authority," must be used to obtain approvals for all undercover operations.
Assets Forfeiture Fund (AFF)	A U.S. Treasury fund for collecting the proceeds of forfeitures pursuant to any law enforced or administered by the Department. The Attorney General is authorized to use the AFF to finance expenses associated with the execution of asset forfeiture functions and, with specific limitations, certain general investigative costs.
AlphaBay	A defunct darknet marketplace that operated on the Tor network where users could buy and sell drugs, firearms, malware, identity documents, and other illegal products and services. Shut down by law enforcement in July 2017.
Cryptocurrency	A decentralized digital currency that uses encryption techniques to both regulate and generate new units of currency and verify the transfer of funds.
Dark Web & Darknet	A part of the Internet that consists of services and websites that cannot be accessed through standard web browsers and are only accessible through specific software, configurations, or authorization.
Darknet Marketplace (DNM)	Commerce website on a darknet, such as Tor, that primarily functions to sell a variety of illicit goods via individual postings.
Moderator	Individuals that review and moderate disputes, such as between a darknet marketplace's vendors and buyers.
Network Investigative Technique (NIT)	Computer code that when deployed to a person's computer, causes that computer to send to the government its actual IP address and other related information.
Onion Service	Services (such as a website) that are only accessible through the Tor network. Often referred to as a "hidden service."
Online Covert Employee (OCE)	A trained and certified employee of the FBI or a sworn law enforcement officer of a federal, state, or local law enforcement agency, working under the direction and control of the FBI, whose identity as an employee of the FBI or another law enforcement agency is concealed from subjects or persons of investigative interest.
Operation Pacifier	An FBI operation focused on "Playpen," a Tor network bulletin board and website involved in the production, advertisement, and distribution of egregious child sexual abuse material. In February 2015, the FBI seized and operated the site for approximately 2 weeks, resulting in the identification and arrests of hundreds of users worldwide.
Technical Infrastructure	Refers to the collection of servers, databases, and applications used to host and operate onion services.

Tor Network	Open network operated by volunteers to enable anonymity on the Internet. Works by routing traffic through multiple nodes and employing asymmetric cryptography to limit any node's knowledge or influence. The nonprofit Tor Project Inc. is responsible for maintaining Tor.

(U) APPENDIX 4

(U) FEDERAL BUREAU OF INVESTIGATION RESPONSE TO THE DRAFT REPORT

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

July 24, 2020

The Honorable Michael E. Horowitz
Inspector General
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Dear Mr. Horowitz:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your office's report entitled, *Audit of the Federal Bureau of Investigation's Strategy and Efforts to Disrupt Illegal Dark Web Activities.*

We are glad that your team has found that FBI operational units were executing individual dark web strategies containing varying degrees of comprehensiveness. We agree it is important to work towards a more coordinated FBI wide dark web approach. In that regard, we concur with your five recommendations for the FBI.

Should you have any questions, feel free to contact me. We greatly appreciate the professionalism of your audit staff throughout this matter.

Sincerely,

Terry Wade
Executive Assistant Director
Criminal, Cyber, Response and Services Branch

Enclosure

UNCLASSIFIED

FBI'S STRATEGY AND EFFORTS TO DISRUPT ILLEGAL DARK WEB ACTIVITIES

OIG Recommendation 1: (U) Ensure that the Hi-Tech OC Unit's efforts on the dark web sufficiently target vendors trafficking fentanyl and other opioids in a manner consistent with the priorities articulated by the Deputy Attorney General

FBI Response to Draft Report Recommendation 1: (U) Criminal Investigative Division (CID) Hi-Tech Organized Crime Unit (HTOCU) concurs with the recommendation. HTOCU's mission though JCODE focuses on combating the illicit distribution and sale of opioids conducted through online platforms. In addition to appropriately defining the nature of rapidly evolving events, successfully executing this mission, and prioritizing safety in the field, HTOCU implemented and follows a fentanyl mitigation strategy in partnership with the United States Postal Inspection Service. HTOCU surged resources to provide guidance and education regarding this strategy to field office personnel in order to underscore the importance and education regarding this strategy to field office personnel in order to underscore the importance of safety while successfully mitigating the opioid threat. In addition to opioids, vendors on Darknet market traffic use various types of drugs that include methamphetamine, cocaine, hallucinogens and other potentially deadly, illicit drugs. Methamphetamine carries harsher punishments in court and has a more familiar objective which can be the reason some field offices prioritize this in seizures. HTOCU continues to work with Department of Justice (DOJ) officials to address this priority, an example is shown through the establishment of the counter-methamphetamine working group by the Attorney General in March 2020. The FBI will continue to ensure efforts on the Darknet target vendors trafficking opioids and synthetics such as fentanyl in a manner consistent with priorities articulated by the DOJ.

OIG Recommendation 2: (U) Develop an FBI-wide dark web strategy that assesses enterprise-level needs, while considering the unique needs of its investigative and support units. At a minimum, this strategy should address

a. ambiguous or overlapping investigative responsibilities.

b. baseline data collection guidelines to track operational units' dark web investigative efforts that position the FBI to provide useful and accurate information to internal and external stakeholders.

c. processes to enhance and consolidate investigative tool development and acquisition efforts in a manner that addresses the FBI's and potentially Department's needs in a more cost-effective manner, and to centralize the FBI's tools useful to dark web investigations to allow visibility to and access by other FBI components; and

d. a process to centralize and eliminate outdated or redundant dark web training offerings and inform FBI personnel of the availability of dark web training across all applicable FBI divisions

UNCLASSIFIED

UNCLASSIFIED

FBI Response to Draft Report Recommendation 2 (U) We concur with the OIG's recommendation to develop an FBI wide dark web strategy that assess enterprise level needs. While considering the unique needs of its investigative and support units.

(U) Weapons of Mass Destruction Directorate (WMDD): WMDD concurs with this recommendation. WMDD will continue to work closely with other FBI divisions invested in dark web matters in order to ensure a coordinated approach toward common goals, tool development/use and to share best practices across the enterprise.

(U) Operation Technology Division (OTD): OTD concurs with this recommendation and will coordinate with others to close out the recommendation.

(U) Cyber Division (CYD): CYD concurs with the recommendation to develop on FBI-wide dark web approach that allows for each operational division to execute individualized investigative strategies against their respective threats. To accomplish this, CYD will document its dark web responsibilities and coordinate with CID and WMD to ensure minimal overlap in responsibilities with their documented dark web responsibilities. In addition, CYD will implement baseline data collection guidelines for Cyber investigations into Dark Net Marketplaces, contribute to FBI consolidation of tools and contribute to FBI efforts to centralize dark web training offerings.

(U) CID: CID concurs with the recommendation in particular pertaining to sub recommendation A and that cross-programmatic investigation, collaboration and sharing of intelligence should not be discouraged. Pertaining to sub recommendation B, we will utilize our case management system to support enhancement towards addressing this sub-recommendation. For sub recommendation C, we believe OTD would be useful in assisting with publishing tool availability across the enterprise. Pertaining to sub recommendation D, Training Division should be utilized.

OIG Recommendation 3 :(U//~~LES~~) Ensure that CyD and CID coordinate with OTD to develop formal procedures for handling Dark Web [redacted]

FBI Response to Draft Report Recommendation 3: (U)

(U) CID: Child Exploitation Unit (CEOU) concurs with this recommendation.

(U) CYD: CYD concurs with the recommendation and will provide input to fulfill Cyber's operational requirements related to this recommendation.

(U) OTD: OTD concurs with this recommendation and will coordinate with others to close out the recommendation.

UNCLASSIFIED

UNCLASSIFIED

OIG Recommendation 4: (U) Develop timelines to obtain feedback from remaining FBI divisions and complete its development of the FBI-wide cryptocurrency support strategy.

FBI Response to Draft Report Recommendation 4: (U) CYD and CID concurs with the OIG's recommendation to develop timelines to obtain feedback regarding the overall virtual currency approach. CYD and CID is engaged on finalizing this approach and will document timelines accordingly

OIG Recommendation 5: (U) Supplement its FBI-wide deconfliction policy with, or separately develop, a formal oversight process to ensure that investigative data encountered on the dark web is properly entered into the DICE deconfliction system

FBI Response to Draft Report Recommendation 5: (U) We concur with the OIG's recommendation and will supplement our wide deconfliction policy with, or separately develop a formal oversight process to ensure investigative data encountered on the dark web is properly entered into DICE deconfliction system.

(U) WMDD: WMDD concurs with the recommendation and will continue to use DICE as its primary deconfliction tool. WMDD will make every effort to ensure all relevant selectors are entered into DICE in a timely manner. Due to the large number of cases with international reach, WMDD will also continue to deconflict within the appropriate channels to avoid redundancy with our foreign law enforcement partners.

(U) CYD: CYD concurs with the recommendation to ensure that investigative data encountered on the dark web is entered into the DICE deconfliction system. CYD will implement oversight procedures through its Major Cyber Crimes Unit, which has program oversight for Cyber Criminal Cases. CYD's policy team will engage with DOJ policy counterparts to determine whether a Cyber-specific deconfliction policy that supersedes the 2014 DOJ Memorandum referenced in the report would better serve the Department's interest in deconflicting Cyber investigations.

(U) CID: CID concurs with this recommendation, however, CEOU does not feel that DICE is an effective tool for deconfliction in the child exploitation workspace. While mandated by Deputy Attorney General (DAG) James M. Cole's Memorandum of May 1, 2014 use of DICE does not provide deconfliction with agencies outside the Department of Justice (DOJ) such as Homeland Security Investigations (HSI) or any of the FBI's foreign law enforcement partners. Use of DICE fails to provide deconfliction for the numerous DOJ funded Internet Crimes against

UNCLASSIFIED

UNCLASSIFIED

Children (ICAC) Task Forces that facilitate state and local law enforcement action to combat child exploitation. Other alternatives for deconfliction should be explored.

(U) HTOCU utilizes DICE in coordination with DOJ and Department of Homeland Security as well as enters all relevant data into the DICE system as it relates to illicit drug investigations. Program Managers and Headquarters personnel work closely with their DICE deconfliction counterparts at Special Operations Division and are consistent communicating their requirement to utilize DICE as the official interagency deconfliction tool.

UNCLASSIFIED

(U) APPENDIX 5

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

(U) The OIG provided a draft of this audit report to the Federal Bureau of Investigation (FBI) for review and official comment. The FBI response is incorporated in Appendix 4. In response to our audit report, the FBI concurred with our recommendations and discussed the actions the FBI will implement in response to our findings. As a result, the status of the audit is resolved. The following provides the OIG's analysis of the responses and summary of actions necessary to close the report.

(U) Recommendations for the FBI:

1. **(U) Ensure that the Hi-Tech OC Unit's efforts on the dark web sufficiently target vendors trafficking fentanyl and other opioids in a manner consistent with the priorities articulated by the Deputy Attorney General.**

   (U) Resolved. FBI concurred with our recommendation. The Hi-Tech Organized Crime Unit (Hi-Tech OC Unit) stated that it will continue to target dark web vendors trafficking opioids and synthetics such as fentanyl in a manner consistent with priorities articulated by the Deputy Attorney General. The Hi-Tech OC Unit also noted that some field offices prioritize methamphetamine seizures because it carries a harsher court-imposed punishment, and that methamphetamine will continue to be a priority, given the Attorney General's establishment of a counter-methamphetamine working group in March 2020.

   (U) This recommendation can be closed when we receive evidence that Hi-Tech OC Unit's undercover operations throughout the various FBI field divisions are sufficiently targeting fentanyl and other opioids in a manner consistent with the priorities articulated by the Deputy Attorney General.

2. **(U) Develop a coordinated FBI-wide dark web approach that assesses enterprise-level needs, while considering the unique needs of its investigative and support units. At a minimum, this approach should address:**

   a. **(U) ambiguous or overlapping investigative responsibilities;**

   b. **(U) baseline data collection guidelines to track operational units' dark web investigative efforts that position the FBI to provide useful and accurate information to internal and external stakeholders;**

c. (U) processes to enhance and consolidate investigative tool development and acquisition efforts in a manner that addresses the FBI's and potentially Department's dark web needs in a more cost-effective manner, and to centralize the FBI's tools useful to dark web investigations to allow visibility to and access by other FBI components; and

d. (U) a process to centralize and eliminate outdated or redundant dark web training offerings and inform FBI personnel of the availability of dark web training across all applicable FBI divisions.

(U) Resolved. FBI concurred with our recommendation. The Weapons of Mass Destruction Directorate (WMDD) stated that it will continue to work closely with other FBI divisions invested in dark web matters to ensure a coordinated approach toward common goals, tool development/use, and to share best practices across the enterprise. Cyber Division (CyD) stated that it will document its dark web responsibilities and coordinate with the Criminal Investigative Division (CID) and WMDD to ensure minimal overlap; implement baseline data collection guidelines for Cyber investigations into darknet marketplaces; and contribute to the consolidation and centralization of investigative tools and training, respectively. CID stated that the Operational Technology Division (OTD) would be useful in assisting with publishing tool availability across the enterprise, and Training Division should be utilized to centralize and eliminate outdated or redundant dark web training offerings and inform FBI personnel of the availability of dark web trainings across all applicable FBI divisions.

(U) This recommendation can be closed when we receive evidence that the FBI has developed a coordinated dark web approach that adequately addresses sub-recommendations 2a through 2d.

3. (U//~~LES~~) Ensure that the CyD and CID coordinate with OTD to develop formal procedures for handling dark web [redacted]

(U) Resolved. FBI concurred with our recommendation. CyD and OTD stated that they would coordinate to address this matter.

(U//~~LES~~) This recommendation can be closed when we receive evidence that CyD and CID have coordinated with OTD to develop formal procedures for handling dark web-related [redacted]

4. (U) Develop timelines to obtain feedback from remaining FBI divisions and complete its development of the FBI-wide cryptocurrency support strategy.

(U) Resolved. FBI concurred with our recommendation. CyD stated that it has already engaged with CID on finalizing its cryptocurrency support strategy approach and will document timelines accordingly.

(U) This recommendation can be closed when we receive evidence that the FBI developed timelines to obtain feedback from remaining FBI divisions and ultimately completed development of an FBI-wide cryptocurrency support strategy.

5. (U) Supplement its FBI-wide deconfliction policy with, or separately develop, a formal oversight process to ensure that investigative data encountered on the dark web is properly entered into the DICE deconfliction system.

(U) Resolved. FBI concurred with our recommendation.

(U) WMDD stated that it will make every effort to ensure all relevant selectors are entered into DICE in a timely manner. CyD stated that it will implement oversight procedures through its Major Cyber Crimes Unit, which has program oversight for Cyber Criminal Cases. CyD also said it plans to determine whether a Cyber-specific deconfliction policy, that would better serve the Department's interest in deconflicting cyber investigations, supersedes the DOJ's 2014 Memorandum referenced in the report. The Hi-Tech OC Unit stated that program managers and headquarters personnel work closely with their DICE deconfliction counterparts and are consistently communicating the requirement to utilize DICE as the official interagency deconfliction tool.

(U) CID's Child Exploitation Operational Unit (CEOU) does not believe the Deconfliction and Information Coordination Endeavor (DICE) system is an effective tool for deconfliction in the child exploitation workspace. CEOU stated that DICE fails to provide deconfliction for the numerous DOJ-funded Internet Crimes against Children task forces that facilitate state and local law enforcement action to combat child exploitation. CEOU suggested that other alternatives for deconfliction be explored. CEOU also stated that DICE does not provide deconfliction with agencies outside the Department, such as Homeland Security Investigations (HSI) or any of the FBI's foreign law enforcement partners.

(U) We do not dispute CEOU's claim that DICE is not available to its foreign law enforcement partners. However, DICE is in fact used outside the DOJ, and HSI is subject to a Department of Homeland Security deconfliction policy—which is nearly identical to the DOJ's 2014 memorandum—that requires all DHS law enforcement components use DICE to deconflict

investigative data and targets.[45] If DICE is an ineffective tool for CEOU in its operating environment, it may be beneficial for the FBI to consult the Department of Justice for additional guidance. However, the policy makes clear that all DOJ law enforcement components, to include CEOU, must use DICE for investigative data and target deconfliction.

(U) This recommendation can be closed when we receive evidence that the FBI supplemented its FBI-wide deconfliction policy with, or separately developed, a formal oversight process to ensure that investigative data encountered on the dark web is properly entered into the DICE deconfliction system.

[45] (U) U.S. Department of Justice (DOJ) Office of the Inspector General (OIG), *A Joint Review of Law Enforcement Cooperation on the Southwest Border between the Federal Bureau of Investigation and Homeland Security Investigations*, Evaluation and Inspections Report 19-03, Special Reviews and Evaluations OIG Report 19-57 (July 2019), https://oig.justice.gov/reports/2019/e1903.pdf (accessed September 2020), 5-6.