Federal Bureau of Investigation
Intelligence
Assessment

Intelligence Assessment

(U) Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity

24 April 2012

UNCLASSIFIED

(U) A Bitcoin logo from https://en.bitcoin.it.

Prepared by

FBI

Directorate of Intelligence

Cyber Intelligence Section
and
Criminal Intelligence Section

(U) Executive Summary

(U//FOUO) Bitcoin—a *decentralized,*[1] *peer-to-peer* (P2P) network-based *virtual currency*—provides a venue for individuals to generate, transfer, launder, and steal illicit funds with some anonymity. Bitcoin offers many of the same challenges associated with other virtual currencies, such as WebMoney, and adds unique complexities for investigators because of its decentralized nature.

(U//FOUO) The FBI assesses with medium confidence[2] that, in the near term, cyber criminals will treat Bitcoin as another payment option alongside more traditional and established virtual currencies which they have little reason to abandon. This assessment is based on fluctuations in the bitcoin exchange rate in 2011 and limited reporting indicating bitcoins are being accepted as payment by some cyber criminals.

(U//FOUO) The FBI assesses with low confidence, based on current user and vendor acceptance, that malicious actors will exploit Bitcoin to launder money. This assessment is based on observed criminal activities, investigations, and prosecutions of individuals exploiting other virtual currencies, such as e-Gold and WebMoney. A lack of current reporting specific to Bitcoin restricts the confidence level.

(U//FOUO) Even though there is no central Bitcoin server to compromise, the FBI assesses with high confidence, based on reliable industry and FBI reporting, that criminals intending to steal bitcoins can target and exploit third-party bitcoin services and an individual's *Bitcoin wallet*. Malicious actors can compromise personal computers and accounts using *malware* and hacking techniques to steal users' bitcoins and use *botnets* to generate bitcoins.

(U//FOUO) Bitcoin will likely continue to attract cyber criminals who view it as a means to move or steal funds as well as a means of making donations to illicit groups. If Bitcoin stabilizes and grows in popularity, it will become an increasingly useful tool for various illegal activities beyond the cyber realm. Since Bitcoin does not have a centralized authority, law enforcement faces difficulties detecting suspicious activity, identifying users, and obtaining transaction records—problems that might attract malicious actors to Bitcoin. Bitcoin might also logically attract money launderers and other criminals who avoid traditional financial systems by using the Internet to conduct global monetary transfers.

(U//FOUO) Although Bitcoin does not have a centralized authority, the FBI assesses with medium confidence that law enforcement can identify, or discover more information about malicious actors if the actors convert their bitcoins into a *fiat currency*. Third-party bitcoin services may require customers to submit valid identification or bank information to complete transactions. Furthermore, any third-party service that qualifies as a *money transmitter* must register as a *money services business* with the Financial Crimes Enforcement Network (FinCEN) and implement an anti-money laundering program.

---

[1] (U) See Appendix A for a glossary of terms. All terms included in the glossary are italicized on their first use.
[2] (U) See Appendix B for a description of confidence levels.

(U) Scope Note

(U//FOUO) The Cyber and Criminal Intelligence Sections, with contributions from the FBI Detroit Division, initiated this intelligence assessment to explore the unique aspects of the P2P virtual currency Bitcoin. This assessment does not attempt to judge the likelihood of Bitcoin's long-term success as an alternate payment method, but explores how bitcoins (or any future virtual currency similar to Bitcoin) are traded and how criminals can use them to conduct illicit activity. This assessment draws primarily on intelligence from January 2011 through April 2012, unless otherwise referenced for historical perspective.

(U//FOUO) This is the FBI's first Criminal and Cyber intelligence assessment related to Bitcoin. In January 2012 the Counterterrorism Division disseminated an intelligence bulletin that explored the potential to conduct illicit financial transactions using Bitcoin. Disseminated FBI intelligence products on other virtual currencies include: *(U) Cyber Criminal Exploitation of Electronic Payment Systems and Virtual Currencies*, dated 23 February 2011and *(U) Cyber Criminal Exploitation of Real-Money Trading*, dated 8 June 2011, both of which discuss cyber criminal misuse of virtual currencies for money laundering. While Bitcoin is a distinct virtual currency, the overarching analytic judgments in this intelligence assessment about the use of virtual currencies by criminal entities are consistent with these previous intelligence products.

(U//FOUO) This assessment will not address malicious actors outside of the *cyber underground*, such as traditional organized crime groups, extremist groups, or child predators. Throughout the paper, the term "Bitcoin," when capitalized, refers to both the open source software used to create the virtual currency and the P2P network formed as a result; "bitcoin" using lower case refers to the virtual currency that is digitally traded between users.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) Source Summary Statement

(U//FOUO) The FBI used open source reporting extensively in this intelligence assessment, both in support of FBI reporting and to provide background information on Bitcoin. FBI sources vary from uncorroborated to highly reliable. FBI case information citing criminal activity is considered highly reliable because it is from FBI employees or FBI sources with direct access to the information.

(U//FOUO) Open source information comes from different online resources describing products or services offered to conduct monetary transactions and are, therefore, considered reliable.

(U//FOUO) The FBI acknowledges that participants in the bitcoin economy have an incentive to emphasize the popularity of Bitcoin. However, Bitcoin users also need reliable information about Bitcoin and the bitcoin exchange rate. For the purposes of this assessment, the FBI assumes that the body of open source information describing Bitcoin is generally indicative of the true state of the Bitcoin economy.

(U//FOUO) No contradictory information was found between FBI and open source reporting. Overall, the FBI considers the body of reporting to be consistent and plausible in the context of the bitcoin environment.

(U) Introduction

(U) Bitcoin[3] is a decentralized, P2P network-based virtual currency that is traded online and exchanged into US dollars or other currencies. Bitcoin, when paired with third-party services, allows users to mine, buy, sell, or accept bitcoins from anywhere in the world. Bitcoin's decentralized feature is unique among virtual currencies. While Bitcoin developers[4,6] maintain Web sites providing guidance to the Bitcoin community, they do not have a centralized database or authority. The P2P network issues bitcoins through the *mining* process and validates all transactions. Since Bitcoin does not have a centralized authority, detecting suspicious activity, identifying users, and obtaining transaction records is problematic for law enforcement.

UNCLASSIFIED

(U) The Bitcoin Economy

- (U) As of 18 April 2012, the third-party bitcoin trading platform Mt. Gox recorded more than $8 million in transactions conducted over the past 30 days through Mt. Gox trading, an average of more than $276,000 per day.[1]
- (U) According to Bitcoin as of April 2012, there were more than 8.8 million bitcoins in circulation.[2] With the average market price in April 2012 between $4 and $5 per bitcoin, the FBI estimates the Bitcoin economy was worth $35 million to $44 million.[3,4]
- (U) From May 2011 Bitcoin values fluctuated with exchange rates on Mt. Gox ranging as high as $30 in June 2011 to a low as $4 in December 2011.[5]

(U) Despite the virtual nature of Bitcoin, users value the currency for many of the same reasons people trust Federal Reserve notes: they believe they can exchange the currency for goods, services, or a national currency at a later date. As such, Bitcoin is currently accepted as a form of payment at hundreds of legitimate retailers including vendors selling clothing, games, music, and some hotels and restaurants.[7] In addition, the unregulated nature of Bitcoin, combined with its other unique features, attracts criminals to this form of payment and transfer method.

(U) *Unique Features Present Distinct Challenges for Detecting and Stopping Illicit Activity*

(U//FOUO) FBI reporting and analysis reveals that cyber criminals use *electronic payment systems* and virtual currencies[5] as a way to launder money and to purchase or sell cyber goods and services in furtherance of their criminal objectives.[8] Bitcoin, like these other virtual currencies, provides opportunities for criminals to transfer, launder, or steal funds. Bitcoin is unique because it is the only decentralized, P2P network-based virtual currency. The way it creates, operates, and distributes bitcoins makes it distinctively susceptible to illicit money transfers, and manipulation through the use of malware and botnets.

---

[3] (U) See Appendix C for a description of how Bitcoin works.
[4] (U) The Bitcoin source code is hosted on Github (https://github.com/bitcoin/bitcoin), a code sharing Web site where developers can work and submit changes. According to bitcoin.org there is a group of six core developers. These developers presumably control which changes are accepted on Github.
[5] (U) For example, WebMoney, Liberty Reserve and Pecunix.

(U//FOUO) All Bitcoin transactions are published online,[9] but the only information that identifies a Bitcoin user is a pseudorandomly[6] generated Bitcoin address, making the transactions somewhat anonymous (see text box). This potential anonymity is distinct from the anonymity provided by other electronic payment systems. For example, WebMoney and Liberty Reserve—which may allow users to register with false information, let suspicious activity go unnoticed, or are located in a country that is not friendly to US law enforcement—still operate as companies with centralized organization capable of instituting programs to ensure compliance with the Bank Secrecy Act (BSA).

(U//FOUO) As a decentralized digital currency system, Bitcoin lacks a centralized entity[10] and is incapable of conducting due diligence (e.g., regulatory guidelines), monitoring and reporting suspicious activity, running an anti-money laundering compliance program, or accepting and processing legal requests like subpoenas.

UNCLASSIFIED

(U) How Anonymous is Bitcoin?

(U) Bitcoin's anonymity depends on the actions of the user. While some news articles have lauded Bitcoin as "untraceable digital currency,"[11] the "About Bitcoin" page on bitcoin.org does not list anonymity as a feature of the currency.[12] All Bitcoin transactions are published online and Internet Protocol (IP) addresses are linked to the public Bitcoin transactions. If a user does not anonymize his or her IP address, an interested party can identify the individual's physical location.[13,14] Additionally, in July 2011 researchers from the University College Dublin, Ireland, demonstrated "the inherent limits of anonymity when using Bitcoin" by conducting passive analysis of various types of public Bitcoin information, such as transaction records and user postings of public-private keys. The researchers suggest that law enforcement agencies or other centralized services (such as *exchangers* or retailers) who have access to less public information (bank account information or shipping addresses) can connect even more real world identifiers to Bitcoin wallets and transaction histories.[15]

(U) What Users Can Do To Increase Anonymity[16, 17, 18, 19]

- (U) Create and use a new Bitcoin address for each incoming payment.
- (U) Route all Bitcoin traffic through an anonymizer.
- (U) Combine the balance of old Bitcoin addresses into a new address to make new payments.
- (U) Use a specialized money laundering service.
- (U) Use a third-party eWallet service to consolidate addresses. Some third-party services offer the option of creating an eWallet that allows users to consolidate many bitcoin address and store and easily access their bitcoins from any device.
- (U) Individuals can create Bitcoin clients to seamlessly increase anonymity (such as allowing user to choose which Bitcoin addresses to make payments from), making it easier for non-technically savvy users to anonymize their Bitcoin transactions.

(U) Bitcoins Used to Purchase Illicit Goods

(U//FOUO) The FBI assesses with medium confidence that, in the near term, cyber criminals will treat Bitcoin as another payment option alongside more traditional and established virtual currencies such as WebMoney, which they have little reason to abandon. This assessment is

[6] (U) Bitcoin addresses are pseudorandom—defined by freedictionary.com as "of, relating to, or being random numbers generated by a definite, nonrandom computational process".

based on fluctuations in the bitcoin exchange rate in 2011 and limited reporting indicating bitcoins are being accepted as payment by some cyber criminals. If the exchange rate for bitcoins stabilizes[7] and Bitcoin becomes more widely accepted by vendors and illicit sellers on the Internet, cyber criminals may increasingly use bitcoins to purchase illegal goods and services and to fund illegal activities.

- (U//FOUO) As of October 2011, a cyber criminal selling a *ZeuS* botnet Trojan advised that he only accepted payments through Bitcoin, Liberty Reserve, or WebMoney, according to a collaborative source with good access, whose information has not been corroborated.[20]

- (U) According to open source reporting as of June 2011, an online marketplace called Silk Road was selling illegal drugs and only accepted payment through Bitcoin. Silk Road allowed parties to communicate anonymously for the purchase and sale of illegal goods, to include the purchase of illegal narcotics, in addition to using Bitcoin. Customers could also leave feedback about their purchase experience in a system similar to other online sellers.[21]

- (U//FOUO) As of June 2011, a member of the online *hacktivist* group LulzSec was using Bitcoin to purchase a botnet, according to an FBI source, some of whose reporting had been corroborated but that had reported for less than one year.[22]

- (U//FOUO) According to open source reporting, as of June 2011 a member of LulzSec claimed the group had received over $18,000 in Bitcoins from fans and supporters.[23] Bitcoin allowed LulzSec to receive donations without revealing the identities of the owners or the recipients. LulzSec provided updates about the donations they received by thanking donors publicly via status updates on the social networking site Twitter.

UNCLASSIFIED

(U) Decentralized Authority Vulnerabilities

- (U) No anti-money laundering software or monitoring capabilities to identify suspicious monetary patterns.
- (U) No identification of account owners or their actual location.
- (U) No historical records of transactions associated with real world identity.
- (U) More difficult to identify the original source of funds compared to other online currencies.
- (U) Law enforcement cannot target one central location or company for investigative purposes or to shut down the system.

(U) Money Laundering

(U//FOUO) The FBI assesses with low confidence that malicious actors will exploit Bitcoin to launder money. The confidence level is based on observed criminal activities, investigations, and prosecutions of individuals laundering money through other virtual currencies, such as e-Gold and WebMoney. A lack of reporting specific to Bitcoin restricts

[7] (U) In 2011 the exchange rate for bitcoins fluctuated from about $1/bitcoin in February to $30/bitcoin on 8 June to about $5/bitcoin in October. (www.bitcoincharts.com)

the confidence level. Since Bitcoin does not have a centralized authority (see text box on page six), law enforcement faces difficulties in detecting suspicious activity, identifying users, and obtaining transaction records—problems that might attract malicious actors to Bitcoin. If Bitcoin becomes more widely accepted among vendors and users, the FBI anticipates seeing increased Bitcoin money laundering activities.

- (U//FOUO) As of June 2011, organized criminal groups were using an online role-playing game to facilitate money laundering by purchasing virtual game currency with the proceeds of criminal activity, according to an FBI sub-source of unknown reliability whose reporting has not been corroborated. The virtual game currency was used to purchase in-game virtual items that were then sold to other players for "clean money."[24]

- (U//FOUO) In August 2010 an FBI source with direct access but of undetermined reliability stated that he used fake names to register for WebMoney, a virtual currency electronic payment system, accounts which he used as part of a money laundering service. The source catered to cyber criminals who earned money from *carding* activities but who were not able to transfer money out of the United States by themselves.[25]

(U//FOUO) The FBI further assesses with medium confidence, based on previously witnessed misuse of other virtual currencies, that malicious actors could increase their anonymity by laundering their bitcoins through third-party Bitcoin services registered outside the US. Some of these services act as exchangers or transmitters (see text box on page eight) that convert virtual currencies to fiat currencies (or other virtual currencies) or transfer bitcoins between members. Offshore services may provide additional anonymity by allowing currency exchange or money transfer without verifying user identification or enforcing any monetary exchange limits.

- (U//FOUO) As of June 2010 unknown subjects created 3,000 online membership accounts using 16,000 bank accounts at a US banking institution, according to a source with direct access and whose information has been corroborated. Using the online accounts, the perpetrators obtained fraudulent funds from victims by receiving payments for nonexistent auction items; these funds were then used to purchase gold from gold farmers. The subjects then sold this gold for *real money*—to others not linked to the malicious actors—using a dedicated third-party service.[26]

- (U//FOUO) As of February 2009, an identified individual operated a Web site offering money laundering services where cyber criminals could view the progress of their transactions, according to a reliable, collaborative source with excellent access. The individual laundered money using WebMoney.[27]

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) Third-Party Bitcoin Services

(U) Bitcoin, like most virtual currencies, requires individuals to use a third-party service to trade bitcoins for fiat currency. Buying, selling, or trading in bitcoins—or converting bitcoins into another currency—must be done using third-party businesses outside the Bitcoin P2P system. The number and diversity of these third-party businesses provide users with options for moving and potentially laundering their money. [28, 29, 30]

(U) Various third-party bitcoin services can, or are used to, facilitate trade between individuals and businesses, buy and sell bitcoins, or convert bitcoins into other currencies.[31] Users who do not want to use an intermediary third-party can also post "buy" and "sell" orders on #bitcoin-otc, a Bitcoin marketplace located on the *freenode Internet relay chat* (IRC) network. [32, 33]

(U) In July 2011 FinCEN revised the definition of "money transmission service" to mean "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds or other value to another location or person by any means." It is likely that the business models of many third-party bitcoin services qualify them as money transmitters, and therefore money services businesses (MSB), under 31 CR Part 1010.100(ff)(5). Third-party bitcoin services that qualify as money transmitters and who wish to operate legitimately must register with FinCEN, implement anti-money laundering programs, retain certain records, and file suspicious activity reports and currency transactions reports as required. Additionally, since any third-party Bitcoin service that falls under the MSB rule would do so as a money transmitter, there is not a transactional threshold (such as 1,000 per day) that must be met for the regulations to apply, unlike dealers in foreign exchange or issuers or sellers of checks or monetary instruments.[34] (Note: In certain states, third-party bitcoin services would also be required to obtain a state license).

(U//FOUO) Law enforcement might have opportunities to discover real user identifying information from some third-party Bitcoin services because users must provide the services with real payment account information to buy, sell, trade, and convert their bitcoins. For example, the Terms of Service for the third-party bitcoin trading platform Mt. Gox states "members agree to provide Mt. Gox with accurate, current and complete information about themselves as promoted by the registration process, and keep such information updated."[35]

(U) Theft of Bitcoins

(U//FOUO) The FBI assesses with high confidence, based on reliable industry and FBI reporting, that criminals intending to steal bitcoins can target and exploit third-party Bitcoin services and an individual's Bitcoin wallet, principally because there is no central Bitcoin server to compromise. Malicious actors can compromise personal computers and accounts using malware and hacking techniques to steal users' bitcoins. Additional techniques involve the creation of botnets to compromise victim computers and servers instructing them to mine bitcoins.

- (U) In mid-June 2011 researchers from a major computer security firm, whose reporting has been reliable in the past, discovered the malware "Infostealer.Coinbit"—the first malware designed to steal bitcoins from compromised users' Bitcoin wallet. The malware is capable of infecting users' computers and transferring their digital Bitcoin wallet to a server in Poland.[36]

- (U) In June 2011 a Bitcoin user posted a message on a Bitcoin forum stating that 25,000 of their bitcoins had been stolen from an unencrypted Bitcoin wallet on their computer.[37, 38, 39] At the June exchange rate of about $20 per bitcoin, the estimated value of the loss was $500,000.

- (U) On 19 June 2011, a compromise involving the third-party bitcoin trading platform Mt. Gox led to an attempt to sell $7 million in bitcoins, driving the trading price to near zero before trading was suspended. [40, 41, 42]

- (U//FOUO) According to a complaint received by the FBI's Internet Crime Complaint Center in April 2011, an individual had 680 bitcoins stolen from his online game site. At the time of this incident the market price was $8 per bitcoin, creating a loss of $5,440.[43]

(U) Theft of Services for the Purpose of Mining Bitcoins

(U//FOUO) FBI and open source reporting indicates that malicious actors can exploit the way bitcoins are generated by compromising victim computers and instructing them to mine bitcoins. Criminals first install malware on a victim's computer, then use these compromised computers to generate bitcoins.

- (U//FOUO) An identified Internet security researcher who has reported reliably in the past identified ZeuS malware that installed software that mined bitcoins. This ZeuS software was spread by links placed on an identified social networking site.[44]

- (U) According to unconfirmed open source reporting from a major periodical whose reporting has proven reliable in the past, a botnet made up of 100,000 infected computers could be used to generate $7,500 worth of bitcoins per day, at late June 2011 exchange rates, by using the computing resources of victim machines.[45]

(U) Since large-scale bitcoin mining requires a large amount of costly processing power and electrical energy, some miners have resorted to "borrowing" processing power from large computing clusters through computer intrusion. In addition to unauthorized access to networks, there have been incidents where unauthorized use of a network had been linked to Bitcoin mining.

- (U//FOUO) FBI reporting from a reliable source indicated that in late May 2011, an unknown actor used several machines on a computing cluster at an identified Midwestern university to manufacture bitcoins.[46] As of 26 May 2011, two IP addresses were used to compromise 22 machines and six computer clusters. On 29 May 2011, two different IP addresses compromised an additional five workstations and two computer clusters. The unknown actor then used the compromised computers to access networks at three other identified universities and tried to gain access to two government facilities.[47]

- (U//FOUO) According to unconfirmed open source reporting, a system administrator for a college near New York City admitted in a May 2011 interview to using the school's computers for Bitcoin mining unbeknownst to the school.[48]

(U) Outlook and Implications

(U//FOUO) Bitcoin will likely continue to attract cyber criminals who view it as a means to transfer, launder, or steal funds as well as a means of making donations to groups participating in illegal activities, such as hactivists. As long as there is a means of converting bitcoins into real money, criminal actors will have an incentive to steal them. Since maintaining anonymity while using Bitcoin requires that users not exchange or transfer their bitcoins using third-party bitcoins services that require real world account information, the use of bitcoins to make donations to disreputable groups (which can be done within the Bitcoin P2P system) will likely remain one of the most popular uses for the virtual currency.

(U//FOUO) If Bitcoin stabilizes and grows in popularity, it will become an increasingly useful tool for various illegal activities beyond the cyber realm. For instance, child pornography and Internet gambling are illegal activities already taking place on the Internet which require simple payment transfers. Bitcoin might logically attract money launderers, human traffickers, terrorists, and other criminals who avoid traditional financial systems by using the Internet to conduct global monetary transfers.

(U//FOUO) Although Bitcoin does not have a centralized authority, the FBI assesses with medium confidence that law enforcement can discover more information about, and in some cases identify, malicious actors, if the actors convert their bitcoins into a fiat currency. Third-party bitcoin services may require customers to submit valid identification or bank information to complete transactions. Furthermore, any third-party service that qualifies as a money transmitter, and therefore a MSB, must register with the FinCEN and implement an anti-money laundering program.[49]

(U) Intelligence Gaps

- (U//FOUO) Who is using Bitcoin to circumvent BSA regulations (e.g., money launderers)?
- (U//FOUO) Which third-party Bitcoin services support illegal activity?
- (U//FOUO) Which criminal, nation state, and terrorist organizations are using Bitcoin to finance their operations?

(U) Intelligence Collection Requirements Addressed in Paper

(U//FOUO) This intelligence assessment will address requirements contained in the following FBI National Standing Collection Requirements topics: Botnets contained in WW-BOT-CYD-SR-0027-11, Money Laundering contained in USA-MLA-CID-SR-0032-10, Cyber Intrusions with a Criminal Nexus contained in WW-CYBR-CYD-SR-0061-10, and Virtual Worlds/Online Games contained in WW-CYBR-CYD-SR-0028-11.

(U) This assessment was prepared by the Domestic Threats Cyber Intelligence Unit, Technology Cyber Intelligence Unit, and the Financial Crimes Intelligence Unit of the FBI. Comments and queries may be addressed to the unit chiefs at 202-651-3051, 202-651-3139 or 202-324-8629, respectively.

(U) Appendix A: Key Terms

(U) **Bitcoin wallet:** A data file that stores bitcoin currency (see appendix C). A user downloads software to a personal computer or may use an online, third-party provider to create a wallet (often called an eWallet) to store bitcoins.

(U) **Botnets:** Any group of two or more computers and/or mobile devices that are controlled and/or updated remotely for an illegal purpose. Botnets can be used to perform denial of service attacks, send spam e-mail, host illegal content, and may aid in most other types of online criminal behavior.

(U) **Carding**: the act of trafficking and/or fraudulent use of stolen credit card account information.

(U) **Decentralized:** No central administration, issuing authority, or database.

(U/FOUO) **Cyber underground**: The extensive network of members engaged in cyber crime activities that have a unique language, an underground economy, a set of expectations about its members' conduct, and a system of social stratification based on knowledge, skill, and activities.

(U) **Electronic payment systems:** Provide a secure means of transferring money among parties to facilitate e-commerce and operate using real money or virtual currency. Electronic payment systems either allow payments to be made between users, vendors, and other merchants, or they only allow payments to be made between users or accounts. There is both a regulated sector and a sector operating outside regulatory systems.

(U) **Exchangers:** Online entities that, for a fee, convert cash, virtual currency, or digital gold currency into the type of currency requested. In general, individuals must use an exchanger to deposit money into an electronic payment system account, unless the electronic payment system has a physical location. Due to this fact, exchangers are a vital part of the money flow for electronic payment systems and virtual currencies.

(U) **Fiat Currency**: Money that has value solely due to government regulation or law. Most modern currencies, such as the US dollar and the Euro are fiat currencies.

(U) **Freenode:** An open source software-focused Internet relay chat network.

(U) **Hacktivists:** Individuals or groups who attack computer systems to draw attention to a particular issue, influence public opinion, or punish perceived entities who oppose their ideological positions.

(U) **Internet Relay Chat (IRC):** A form of real-time Internet synchronous conference, mainly designed for group communication in discussion forums called channels, but also allowing one-to-one communication via private messages.

(U) **Malware or malicious software:** Computer software that facilitates illicit activities, to include data exfiltration, denial of service attacks, fraud, and spam dissemination.

(U) **Mining, Bitcoin (also known as Bitcoin Creation, Bitcoin Generation, and Bitcoin Manufacturing):** The process of allowing the Bitcoin network to use a computer's resources in exchange for the possibility of earning bitcoins. The more computing power a user offers, the more likely they are to receive bitcoins.

(U) **Money services business (MSB)**: Any person doing business in one or more of the following capacities, wholly or in substantial part within the United States: 1.) dealer in a foreign exchange; 2.) check casher; 3.) issuer or seller of traveler's checks or money orders; 4.) issuer, seller, or redeemer of stored value; 5.) money transmitter; 6.) U.S. Postal Service (31 C.F.R. 103.11).[50]

(U) **Money transmitter**: A person that provides money transmission services. The term "money transmission services" means the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, fund, or other value that substitutes for currency to another location or person by any means.[51]

(U) **Peer-to-Peer (P2P):** A type of network in which each workstation has equivalent capabilities and responsibilities. P2P is typically used for the transfer of data from one peer to another and are free programs that can be easily downloaded from the Internet. P2P file-sharing is the primary source for pirated software. Some popular examples include Limewire, Kazaa, and Gnutella.

(U) **Public Key Cryptography (PKI)**: A framework for creating a secure method for exchanging information based on public key cryptography. PKI uses a certificate authority (CA), which issues digital certificates that authenticate the identity of organizations and individuals over a public system such as the Internet.

(U) **Real money:** Coins or paper notes issued and backed by a government and used as a medium of exchange and measure of value.

(U) **Virtual currency:** Something used on the Internet that is in circulation as a medium of exchange but is not backed by a government.

(U) **ZeuS Trojan:** malicious software used by cyber criminals to steal online account credentials.

Appendix B: Confidence Levels

(U) **High confidence** generally indicates that FBI judgments are based on high-quality information from multiple sources or a single highly reliable source, or that the nature of the issue makes it possible to render a solid judgment.

(U) **Medium confidence** generally means that the information is interpreted in various ways, that the FBI has alternating views, or that the information, while credible, is of insufficient reliability to warrant a higher level of confidence.

(U) **Low confidence** generally means that the information is scant, questionable, or very fragmented; that it is difficult to make solid analytic inferences; or that the FBI has significant concerns or problems with the source.

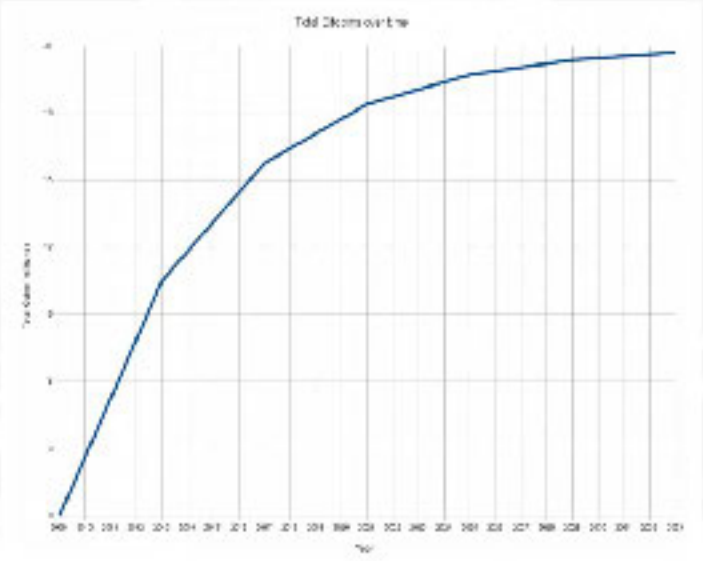
(U) Appendix C: How Does Bitcoin Work?

(U) To use Bitcoin, an individual first downloads and installs the free Bitcoin software (client). The application uses *Public Key Cryptography* (PKI) to automatically generate a Bitcoin address where the user can receive payments. The address is a unique 36 character-long string of numbers and letters and is stored in a user's virtual "wallet" on his or her local file system. Users can create as many Bitcoin addresses as they like to receive payments and can use a new address for every transaction they receive.

(U) To send bitcoins, users input the address they would like to send their bitcoins to and the amount of bitcoins they would like to transfer. The user's computer then digitally signs the transaction and sends the information to the distributed, P2P Bitcoin network. The P2P network verifies that the person sending the bitcoins is the current owner of the bitcoins they are sending, prohibiting a malicious user from spending the same bitcoins twice. Once the transaction has been validated by the Bitcoin network, receivers can spend the bitcoins they have received. This process usually takes a few minutes and is not reversible.

(U) The Bitcoin software program controls the rate of bitcoin creation, but it does not control the market value of a bitcoin; the market value is determined by the supply of bitcoins in circulation and people's desire to hold or trade bitcoins.[52, 53] Unlike most fiat currencies, in which central banks can arbitrarily increase the supply of currency, Bitcoin is designed to eventually contain 21 million bitcoins; no additional coins will be created after that point, preventing inflation.

(U) Bitcoin was created in such a way that the clients "mine" bitcoins at a predetermined rate. This chart illustrates the growth rate from 2009 to 2033, the year the last new bitcoin will be created.



Source: (U) Internet site; Bitcoin Wiki; "Controlled Currency Supply"; https://en.bitcoin.it/wiki/Controlled_Inflation; accessed in 5 March 2012; The source is a community wiki aimed at allowing anyone to freely document information about Bitcoin. Users must create a free account with a valid e-mail address to edit the Bitcoin Wiki.

Distribution

DI/OCA
LEO
SIPRNet
JWICS
NCTC S and TS
LNI
Australian Federal Police (AFP)
Metropolitan Police–Police Central e-Crime Unit (PCeU)
New Zealand Police
Royal Canadian Mounted Police (RCMP)
Serious Organised Crime Agency (SOCA)

(U) Endnotes

[1] (U) Internet site; Bitcoincharts.com; "Mt. Gox (USD/dwolla/SEPA)"; http://bitcoincharts.com/markets/mtgoxUSD.html; accessed on 18 April 2012; the source provides financial and technical data related to the Bitcoin network and uses daily intervals to display information. While this information may contain biases, the FBI assumes the information is generally indicative of the true state of the Bitcoin economy.
[2] (U) Internet site; Bitcoin Block Explorer; "total bc"; http://blockexplorer.com/q/totalbc; accessed on 18 April 2012; The source is a Web site that posts information about Bitcoin transactions based on code developed by a volunteer. While this may contain inaccuracies, the FBI assumes the information is generally indicative of the true state of the Bitcoin economy.
[3] (U) Internet site; Bitcoincharts.com; "Markets"; http://bitcoincharts.com/markets; accessed on 18 April 2012; the source provides financial and technical data related to the Bitcoin network and uses daily intervals to display information. While this information may contain biases, the FBI assumes the information is generally indicative of the true state of the Bitcoin economy.
[4] (U) Internet site; Bitcoincharts.com; "Mt. Gox (USD/dwolla/SEPA)"; http://bitcoincharts.com/charts/mtgoxUSD_trades.html; accessed on 18 April 2012; the source provides financial and technical data related to the Bitcoin network and uses daily intervals to display information. While this information may contain biases, the FBI assumes the information is generally indicative of the true state of the Bitcoin economy.
[5] (U) *op. cit.* endnote 1.
[6] (U) Internet site; Github; "Bitcoin/bitcoin"; https://github.com/bitcoin/bitcoin; accessed on 19 April 2012; the source is a code sharing Web site where developers can work and submit changes.
[7] (U) Internet site; Bitcoin Wiki; "Trade"; https://en.bitcoin.it/wiki/Trade; accessed 18 April 2012; The source is a community wiki aimed at allowing anyone to freely document information about Bitcoin. Users must create a free account with a valid e-mail address to edit the Bitcoin Wiki. While this wiki is edited by the community and may contain biases, the FBI assumes the information accurately reflects businesses which accept bitcoins as payment.
[8] (U) FBI; Intelligence Assessment; *(U) Cyber Criminal Exploitation of Electronic Payment Systems and Virtual Currencies*; 23 February 2011.
[9] (U) Internet site; Bitcoin Block Explorer; http://blockexplorer.com; accessed 18 April 2012; The source is a Web site that posts information about Bitcoin transactions based on code developed by a volunteer. While this may contain inaccuracies, the FBI assumes the information is generally indicative of the true state of the Bitcoin economy.
[10] (U) Internet site; Bitcoin.org; "About Bitcoin"; http://bitcoin.org/about.html; accessed on 9 February 2012; Bitcoin.org is the official Web site of Bitcoin. While this information may contain biases, the FBI assumes the information is generally indicative of the true state of the Bitcoin economy.
[11] (U) Internet site; Adrian Chen; Gawker; "The Underground Website Where You Can Buy Any Drug Imaginable"; 1 June 2011; http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable; accessed on 2 June 2011; The source is an online blog-oriented media site owned by Gawker Media.
[12] (U) *op. cit.* endnote 10.
[13] (U) Internet site; Bitcoin Wiki; "Network"; https://en.bitcoin.it/wiki/Network; accessed on 9 February 2012; the source is a community wiki aimed at allowing anyone to freely document information about Bitcoin. Users must create a free account with a valid e-mail address to edit the Bitcoin Wiki. While this wiki is edited by the community and may contain biases, the FBI assumes the information is generally indicative of the true state of the Bitcoin economy.
[14] (U) Internet Article; Jason Mick; Daily Tech; "Cracking the Bitcoin: Digging Into a $131M USD Virtual Currency"; 12 June 2011; http://www.dailytech.com/Cracking+the+Bitcoin+Digging+Into+a+131M+USD+Virtual+Currency/article21878.htm; accessed on 9 December 2011; The source is an online magazine publishing news, research and discussion on current and upcoming science and information technology issues.
[15] (U) Online Article; Fergal Reid and Martin Harrigan; University College Dublin; "An Analysis of Anonymity in the Bitcoin System"; 22 July 2011; http://arxiv.org/PS_cache/arxiv/pdf/1107/1107.4524v1.pdf; accessed on 20 December 2011; The authors are researchers with the Clique Research Cluster at University College Dublin, Ireland.
[16] (U) Internet site; Bitcoin Wiki; "Anonymity"; https://en.bitcoin.it/wiki/Anonymity; accessed on 9 February 2012; the source is a community wiki aimed at allowing anyone to freely document information about Bitcoin. Users must create a free account with a valid e-mail address to edit the Bitcoin Wiki. While this wiki is edited by the community

and may contain biases, the FBI assumes the information is generally indicative of the true state of the Bitcoin economy.

[17] (U) Internet site; Bitcointalk Forum; "Patching the Bitcoin Client to Make it More Anonymous"; 30 June 2011; https://bitcointalk.org/index.php?topic=24784.msg307661#msg307661; accessed on 9 February 2012; the source is a forum dedicated to Bitcoin discussions. While this information may contain biases, the FBI assumes the information is generally indicative of the true state of the Bitcoin development community.

[18] (U) Internet site; Timothy Lee; Forbes; "How Private are Bitcoin Transactions?"; 14 July 2011; http://www.forbes.com/sites/timothylee/2011/07/14/how-private-are-bitcoin-transactions; accessed on 9 February 2012; the source is an adjunct scholar at the Cato institute with a master's degree in computer science. He is a contributor to Forbes, an Internet media company providing commentary, analysis, tools and real-time reporting to business and investment leaders.

[19] (U) Internet site; Thomas Lowenthal; Active Rhetoric Blog; "Bitcoin: More Covert than it Looks"; 14 July 2011; http://activerhetoric.wordpress.com/2011/07/14/bitcoin-more-covert-than-it-looks; accessed on 9 February 2012; the source is a blog.

[20] (U//FOUO) FBI; IIR; 4 213 0829 12; 12 December 2011; 18 October 2011; "(U//FOUO) Identification of Individual Using Online Moniker 'Cipher' Selling a Zeus Trojan Botnet on an Identified US Web site as of October 2011"; UNCLASSIFIED//FOR OFFICIAL USE ONLY; UNCLASSIFIED//FOR OFFICIAL USE ONLY; A collaborative source with good access, none of whose reporting has been corroborated for less than one year.

[21] (U) *op. cit.* endnote 11.

[22] (U//FOUO) FBI; 17 June 2011; June 2011; FBI Case Information; UNCLASSIFIED//FOR OFFICIAL USE ONLY; UNCLASSIFIED//FOR OFFICIAL USE ONLY; an FBI source, some of whose reporting has been corroborated but that has reported for less than one year.

[23] (U) Internet site; The Next Web; "Lulzsec Claims to Have Received Over $18,000 in Donations"; 24 June 2011; http://thenextweb.com/insider/2011/06/24/lulzsec-claims-to-have-received-over-18000-worth-of-donations/; accessed on 12 October 2011; the source is a technology blog publishing news and views from an international perspective.

[24] (U//FOUO) FBI; 3 June 2011; 27 May 2011; FBI Case Information; UNCLASSIFIED; an FBI sub-source of unknown reliability whose reporting has not been corroborated.

[25] (U//FOUO) FBI; 10 August 2010; 6 August 2009; FBI Case Information; UNCLASSIFIED//FOR OFFICIAL USE ONLY; UNCLASSIFIED//FOR OFFICIAL USE ONLY; An FBI source with first-hand access to the information and whose reliability cannot be determined.

[26] (U//FOUO) FBI; IIR; 4 213 4056 11; 15 August 2011; 9 June 2010; "(U//FOUO) Creation of Bank Accounts by an Internet Bot For Use in a Massively Multiplayer Online Role Playing Game and E-Commerce Payment Site Scheme, June 2010"; UNCLASSIFIED//FOR OFFICIAL USE ONLY; UNCLASSIFIED//FOR OFFICIAL USE ONLY; the source is an FBI agent.

[27] (U//FOUO) FBI; IIR; 4 213 4947 09; 11 August 2009; 18 February 2009; "(U//FOUO) Identification of Money Laundering Web Site Operated by Individual Linked to Internet Fraud Schemes, as of February 2009"; UNCLASSIFIED//FOR OFFICIAL USE ONLY; UNCLASSIFIED//FOR OFFICIAL USE ONLY; A collaborative source with excellent access, much of whose reporting has been corroborated over the past two years. Source spoke in confidence.

[28] (U) Internet site; Bitcoin Wiki; "Selling Bitcoins"; https://en.bitcoin.it/wiki/Selling_bitcoins; accessed on 9 February 2012; the source is a community wiki aimed at allowing anyone to freely document information about Bitcoin. Users must create a free account with a valid e-mail address to edit the Bitcoin Wiki. While this wiki is edited by the community and may contain biases, the FBI assumes the information is generally indicative of the true state of the Bitcoin economy.

[29] (U) Internet site; Bitcoin Wiki; "Buying Bitcoins"; https://en.bitcoin.it/wiki/Buying_bitcoins; accessed on 9 February 2012; the source is a community wiki aimed at allowing anyone to freely document information about Bitcoin. Users must create a free account with a valid e-mail address to edit the Bitcoin Wiki. While this wiki is edited by the community and may contain biases, the FBI assumes the information is generally indicative of the true state of the Bitcoin economy.

[30] (U) Internet site; Bitcoin Wiki; "Secure Trading"; https://en.bitcoin.it/wiki/Secure_Trading; accessed on 9 February 2012; the source is a community wiki aimed at allowing anyone to freely document information about Bitcoin. Users must create a free account with a valid e-mail address to edit the Bitcoin Wiki. While this wiki is edited by the community and may contain biases, the FBI assumes the information is generally indicative of the true state of the Bitcoin economy.

[31] (U) Internet site; Jason Mick; Daily Tech; "Internet Digital Black Friday: First Bitcoin "Depression" Hits"; 10 June 2011; https://www.dailytech.com/Digital+Black+Friday+First+Bitcoin+Depression+Hits/article21877.htm; accessed on 16 June 2011; The source is an online magazine publishing news, research, and discussion on current and upcoming science and information technology issues.
[32] (U) Internet site; Bitcoin-otc; "#bitcoin-otc marketplace"; http://bitcoin-otc.com; accessed on 14 October 2011; The source is an online marketplace for the exchange and sales of bitcoins.
[33] (U) Internet site; Bitcoin Wiki; "Using bitcoin-otc"; http://wiki.bitcoin-otc.com/wiki/Using_bitcoin-otc; accessed on 21 June 2011; the source is a community wiki aimed at allowing anyone to freely document information about Bitcoin. Users must create a free account with a valid e-mail address to edit the Bitcoin Wiki. While this wiki is edited by the community and may contain inaccuracies, the FBI assumes the information is generally indicative of the true state of the Bitcoin community.
[34] (U) Online publication; Federal Register Vol. 76, No. 140; "Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses"; 21 July 2011; http://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf; accessed on 9 March 2012; pages 43585-43597.
[35] (U) Internet site; Mt. Gox; "Terms of Use"; 20 January 2012; https://mtgox.com/terms_of_service"; accessed on 7 March 2012; Mt. Gox is a third-party bitcoin trading platform
[36] (U) Internet site; Kevin Poulsen; Wired; "New Malware Steals Your Bitcoin"; 16 June 2011; http://www.wired.com/threatlevel/2011/06/bitcoin-malware/; accessed 23 June 2011; The source is an online publication that provides news reporting, commentary and reviews on innovation in technology, science, business and culture. Wired.com is part of the Conte Nast Digital Network.
[37] (U) Internet site; Timothy B. Lee; Ars Technica; "A Risky Currency? Alleged $500,000 Bitcoin Heist Raises Questions"; 15 June 2011; http://arstechnica.com/tech-policy/news/2011/06/bitcoin-the-decentralized-virtual-currencyrisky-currency-500000-bitcoin-heist-raises-questions.ars; accessed 2 August 2011; The source is a technology Web site that offers a mix of news, in-depth trend analysis and how-to instruction. Arstechnica.com is part of the Conte Nast Digital Network.
[38] (U//FOUO) FBI; Internet Crime Complaint Center; Complaint Referral Form; 18 June 2011; source is a victim/consumer complaint. The reliability cannot be determined.
[39] (U) Internet Site; Bitcoin Forum, "I just got hacked – any help is welcome! (25,000 BTC stolen)"; 13 June 2011; https://bitcointalk.org/index.php?topic=16457.0; accessed 1 January 2012; The source is a forum where users post messages discussing bitcoins.
[40] (U) Internet site; James Ball; The Guardian; "LulzSec Rogue Suspected of Bitcoin Hack"; 22 Jun 2011; http://www.guardian.co.uk/technology/2011/jun/22/lulzsec-rogue-suspected-of-bitcoin-hack; accessed on 6 July 2011; The source is the online publication of the United Kingdom's Guardian newspaper.
[41] (U) Internet site; Jason Mick; Daily Tech; 19 June 211; http://www.dailytech.com/Inside+the+MegaHack+of+Bitcoin+the+Full+Story/article21942.htm; accessed on 21 June 2011; the source is an online magazine publishing news, research and discussion on current and upcoming science and information technology issues.
[42] (U) Internet site; Sean Ludwig; VentureBeat; "Popular Bitcoin Exchange Mt. Gox Hacked, Prices Drop to Pennies"; 19 June 2011; http://venturebeat.com/2011/06/19/popular-bitcoin-exchange-mt-gox-hacked-prices-drop-to-pennies/; accessed on 21 June 2011; the source is a blog and online news site whose stated mission is to provide news about innovation for forward-thinking executives.
[43] (U//FOUO) FBI; Internet Crime Complaint Center; Complaint Referral Form; 14 May 2011; 23 April 2011; the source is a victim/consumer complaint and the reliability cannot be determined.
[44] (U//FOUO) FBI; 2 Jun 2011; FBI Information; Source is an Internet security researcher who has reported reliably in the past.
[45] (U) *op. cit.* endnote 40.
[46] (U//FOUO) FBI; IIR; 4 213 3647 11; 18 July 2011; 31 May 2011; "(U//FOUO) Compromise of Computer Clusters at Identified US Universities for the Purpose of Manufacturing Virtual Currency, as of May 2011"; UNCLASSIFIED//FOR OFFICIAL USE ONLY; SECRET//NOFORN; a collaborative source with excellent access, much of whose reporting has been corroborated over the past two years.
[47] (U//FOUO) FBI; IIR; 4 213 3754 11; 25 July 2011; May 2011; "(U//FOUO) Update to Compromise of Computer Clusters at Identified US Universities for the Purpose of Manufacturing Virtual Currency, as of May 2011"; UNCLASSIFIED//FOR OFFICIAL USE ONLY; UNCLASSIFIED//FOR OFFICIAL USE ONLY; a collaborative source with excellent access, much of whose reporting has been corroborated over the past two years.

[48] (U) Internet Site; motherboard.tv; "How to Get Rich on Bitcoin, by a System Administrator Who's Secretly Growing Them on His School's Computers"; 27 May 2011; http://www.motherboard.tv/2011/5/27/how-to-get-rich-on-bitcoin-by-a-system-administrator-who-s-secretly-growing-them-on-his-shool-s-computers; accessed on 14 October 2011; the source is a Web site dedicated to the meeting point of science, technology, and culture. It is powered by a community of writers and video producers.
[49] (U) Online publication; Federal Register Vol. 76, No. 140; "Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses"; 21 July 2011; http://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf; accessed on 9 March 2012; page 43596.
[50] (U) Online publication; Federal Register Vol. 76, No. 140; "Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses"; 21 July 2011; http://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf; accessed on 9 March 2012; pages 43585-43597.
[51] (U) Online publication; Federal Register Vol. 76, No. 140; "Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses"; 21 July 2011; http://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf; accessed on 9 March 2012; page 43596.
[52] (U) Internet site; Bitcoin Wiki; "FAQ Page"; http://en.bitcoin.it/wiki/FAQ/; accessed on 20 January 2012; the source is a community wiki aimed at allowing anyone to freely document information about Bitcoin. Users must create a free account with a valid e-mail address to edit the Bitcoin Wiki. While this wiki is edited by the community and may contain biases, the FBI assumes the information is generally indicative of the true state of the Bitcoin economy.
[53] (U) Internet site; Stephen Chapman; ZDNet; "Bitcoin: A Guide to the Future of Currency"; 15 June 2011; http://www.zdnet.com/blog/btl/bitcoin-a-guide-to-the-future-of-currency/50601; accessed on 21 June 2011; the source, available in seven regional editions, is an online resource of technology-related issues featuring blogs, product reviews, software downloads, white papers and research.

Finished Product File Name:

UNCLASSIFIED//FOR OFFICIAL USE ONLY

THE FBI FEDERAL BUREAU OF INVESTIGATION

FBI Customer Satisfaction Survey

Product Title:

Posted Date:

Customer Agency: Select. . . Other:

Customer Role: Select. . .

Customer Responsibilities

Customer's Program: Select. . .

Customer's Region: Select. . .

Relevance to your intelligence needs - Check one

	Strongly Agree	Somewhat Agree	N/A	Somewhat Disagree	Strongly Disagree
This Product increased my knowledge of an issue or topic?	◯	◯	◯	◯	◯
The product helped me decide on a course of action?	◯	◯	◯	◯	◯
This product was timely to my intelligence needs?	◯	◯	◯	◯	◯

How did you use this product in support of your mission?

Integrated into one of my own organization's finished products or intelligence reports

☐ Shared contents with federal partners?
If so, who?

☐ Shared contents with foreign partners?
If so, who?

☐ Shared contents with state, local and tribal partners?
If so, who?

☐ Shared contents with private sector partners?
If so, who?

Additional Comments

Name:

Contact Number or Email:

Submit Feedback

UNCLASSIFIED//FOR OFFICIAL USE ONLY