PILOT IRS- Request for Information (RFI) 2032H8-20-N-00034

Internal Revenue Service (IRS), Criminal Investigation (CI) Cyber Crimes

Cryptocurrency Initiative

1.0 High-Level Summary/Future State

This RFI is associated with a pilot IRS Criminal Investigation Division (CI) program. CI Cyber Crimes is requesting information about systems that will allow developers and testers to conduct investigative research of distributed ledger transactions involving privacy cryptocurrency coins (e.g., Monero (XMR), Zcash (ZEC), Dash (DASH), Grin (GRIN), Komodo (KMD), Verge (XVG), and Horizon (ZEN)); Layer 2 off-chain protocol networks (e.g., Lightning Network (LN), Raiden Network, Celer Network); Side-chains (e.g., Plasma and OmiseGo); and tracing challenges following the integration of the Schnorr Signature algorithm.

The Criminal Investigation Division (CI) is the largest Federal law enforcement agency in the United States Department of the Treasury, consisting of sworn law enforcement officers (Special Agents) and support personnel focused solely on matters related to criminal violations of law. CI is responsible for investigating potential criminal violations of the U.S. tax, money laundering and bank secrecy act laws and related financial crimes. CI is a global leader in cyber criminal investigations involving cryptocurrency and various digital assets. CI has played a leading or pivotal role in the takedown of numerous major Dark Net Marketplaces, virtual currency exchanges and other transnational criminal organizations facilitating stolen identify refund fraud (SIRF), narcotics trafficking, money laundering, terrorist financing, sex trafficking, and child prostitution.

Acquiring applications to allow an investigation to more easily trace privacy coins and other protocols that provide anonymity to illicit actors would allow investigations to be more effective, as well as facilitate a higher level of deterrence by making it harder to conceal criminal activity. It also provides an investigative efficiency that is currently limited.

We are primary interested in: 1) an interactive prototype that provides a GUI for clustering transactions involving a user (similar to tools provided by companies like Chainalysis, CipherTrace, Coinbase, and Elliptic but for the privacy coins and obfuscation technologies); 2) associate user distributed addresses with distributed ledger addresses of users (individuals or entities) suspected or known to be involved in nefarious activities; 3) provide a library of distributed ledger addresses associated with names of users engaged in known or suspected nefarious activities; 4) provide OSINT information/research about identified users, 5) has a mechanism for sharing investigative research between investigators, 6) ability to import/export investigative data in various file formats (e.g., csv and jpg); and 7) an estimate of the cost and return on investment (ROI).

2.0 Background/Current State

Currently, there are few investigative resources for tracing transactions involving privacy cryptocurrency coins, Layer 2 network protocol transactions, side-chain ledger transactions, or transactions on distributed ledgers that are adopting signature algorithms that provide privacy to illicit actors.

The use of privacy coins is becoming more popular for general use, and is also seeing an increase in use by illicit actors. This manifested in April 2020 by a RaaS (Ransomware as a Service) group called Sodinokibi (a former affiliate with the GrandCrab Raas group) stating that future ransom request payments will be in XMR rather than BTC due to transaction privacy concerns (source: BleepingComputer). The CI Cyber Crimes program is working to get in front of this trend through this RFI.

Currently, existing services have only recently announced their addition of investigative services for DASH and ZEC, which demonstrate the investigative support industry's recognition of the worth of committing resources to identify illicit actors using cryptocurrency obfuscation. However, Schnorr

Signature presents a new challenge for investigative support services with no COTS solutions publicly available. The Bitcoin Cash blockchain completed an initial stage integration of Schnorr Signatures in May 2019 through a non-chain split hard fork, and there are plans by the Bitcoin network to integrate Schnorr Signatures into the Bitcoin blockchain. This integration has multiple benefits to users including a reduction in the distributed ledger storage requirements as well as enhanced privacy to protect users, but this also inhibits the effectiveness of certain traditional tracing clustering algorithms.

Regarding Layer 2 protocols, Lightning Labs has developed a monitoring app, Lndmon, for the Bitcoin LN and has released the code on GitHub with no current resources developed for LNs on other distributed ledgers (e.g., Litecoin blockchain), Raiden Network (on the Ethereum platform), etc. The move by Lightning Labs again demonstrates the need to monitor the network. Building off of monitoring code, there is potential to develop solutions for tracking illicit actors on the Layer 2 network. Notable is that the number of nodes on the LN has grown to nearly 10,000 since the initial release in March 2018. Comparing that to the number of full nodes on the Bitcoin mainchain, currently numbered at 10,570 (source: bitnodes.io), demonstrates that the number of users in these networks is significant. Even though Layer 2 protocols have been dismissed by many in the investigative support community, there is clear evidence that this is a growing network.

3.0 Specific Areas of Input Requested/Questions

CI respectfully requests input from industry partners and other parties regarding the following inquiries/topics:

1. Provide summary background on any existing instances of application and solutions in that you have deployed in government or industry that address the tracing/investigative tools developed for privacy coins, Layer 2 protocols, side-chains, and the Schnorr signature algorithm.
2. Are there known infrastructures/interface issues that will make this effort more difficult (i.e., is the innovative solution available in both a cloud and on-premise environment)?
3. Provide recommendations regarding our primary areas of focus and provide recommendations on process improvement.
4. Provide any overarching recommended approaches for technology in this space that we may not be aware of.
5. Provide a Rough Order of Magnitude (ROM) for contract costs to support this initiative with any notations for development, hosting, training, operations, and maintenance.
6. Provide an ROI summary that the CI could reasonably expect to attain with the adoption and implementation of selected technologies in this space.

4.0 Disclaimer

This RFI is issued solely for information and planning purposes. This notice should not be construed as a commitment by the Government for any purpose other than market research. This announcement does not commit the Government to any contractual agreement. The Government is not seeking proposals and will not accept unsolicited proposals. No reimbursement will be made for any costs associated with providing information in response to this announcement or any follow-up information requests.

Respondents will NOT be notified of the results of the analysis. All data received in response to this Sources Sought synopsis that is marked or designated as corporate or proprietary information will be fully protected from release outside the Government. The Government shall not be liable for or suffer any consequential damages for any proprietary information not properly identified. Proprietary information will be safeguarded in accordance with all applicable Government regulations. All documentation shall become the property of the Government and will not be returned.

The deadline for responses to this RFI is 08:00AM EST, July 14, 2020. Responses should be forwarded via email to both the primary and secondary points of contact below. Responses shall not

exceed 5 pages and shall not contain any brochures, advertising or any other type of extraneous, graphic literature or documents that have not been requested and are not relevant or essential in demonstrating the company's ability to provide the required services. Vendors may provide links to relevant websites, as appropriate.

Vendors shall reference **"RFI_Crypto"** in the subject line of their response as well as in the subject line of any other e-mail correspondence referencing this notice.

** THE GOVERNMENT WILL NOT RESPOND TO PHONE CALLS. **

Thank you for your interest.

Contracting Office Address:
IRS, 1111 Constitution Ave. NW
Washington, District of Columbia 20024

Primary Point of Contact:
Marcy Almeida
Marcela.a.almeida@irs.gov
202-317-4087

Secondary Point of Contact:
Cyber Crimes Program Manager
pilotirscicyber@ci.irs.gov