GDIT

Date: July 16, 2021 RIN 3064-ZA25

FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)

REQUEST FOR INFORMATION AND COMMENT ON DIGITAL ASSETS (RIN 3064-ZA25)

Submitted Electronically to:

Federal Deposit Insurance Corporation

Comments@fdic.gov

Submitted by:

General Dynamics Information Technology, Inc.

POC Name: Frederick Stith, Contracts Lead

Address: 3150 Fairview Park Drive, Suite 100

Falls Church, VA 22042-4504

Phone: (667) 786-7843

Email: Frederick.stith@gdit.com

www.gdit.com

DISCLOSURE STATEMENT

This RFI includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this RFI. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to the restriction are contained in sheets with the following legend: "Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this RFI Response"

GDIT Introduction

General Dynamics Information Technology, Inc. (GDIT) is a Federal System Integrator (FSI) and global leader, providing full-lifecycle Information Technology (IT) services that include leading solutions and technologies leveraging the emerging digital asset ecosystem, such as being custodians, reserve holders, issuers, and exchange or redemption agents; performing node functions; and holding digital asset issuers' money deposits. GDIT understands the challenges with regards to the utilization of Digital Assets by financial institutions in their provision of services to customers and for other business or operational purposes, such as those involving closed and open payment systems, other token-based systems for banking activities other than payments (e.g., lending), and acting as nodes in networks (e.g., distributed ledgers).

Our interest in responding to this RFI is to illustrate industry expertise in Cryptocurrency and provide trusted partnership in FDIC's pursuit for future people, process and tools related to this fast growing and emerging segment. Aside from this RFI submission, we are actively writing an industry white paper on the application development, system integration aspect of modernizing existing Government off-the-shelf (GOTS) and Commercial off-the-shelf (COTS) with the Web3 (Decentralized Web) Free and Open Source (FOSS) development, which much of the cryptocurrency world builds and operates within. System integration with legacy financial, reporting, taxation and telemetry will be a pivotal undertaking over the next few years as the financial infrastructure and governments begin to operate as a participant in these spaces as well as provide a framework to interact and exchange data.

GDIT looks forward to our continued support as a trusted advisor and leading industry expert to facilitate financial institutions' use of Digital Assets in a safe and sound manner and in compliance with applicable laws and regulations, including those related to consumer protection.

GDIT Response

Question #1: ***In addition to the broad categories of digital assets and related activities described above, are there any additional or alternative categories or subcategories that IDIs are engaged in or exploring?***

There are many emergent trends that may have effect on Insured Depository Institutions (IDIs) scope, however, GDIT believes Non-Fungible Tokens (NFT's) will have a tight integration with institutional wallets by necessity, as most of these assets are directly tied to a user's private key. If customers move their funds to custodial based services, say within a bank, then there is a high chance they will want to inherit the protections, security, and terms of service with their banking provider, including FDIC coverage. These assets (NFTs) could also be held under these institutional wallets as the existing architecture does not prevent those assets going to any address within an Ethereum wallet, as an example.

The NFT Market place is growing exponentially and is challenging the very fundamental understanding of transfer of wealth. Where typical secondary Store of Value mediums, such as Art is a physical representation, NFT marketplace is tied directly to the cryptocurrency wallet. Soon, cryptocurrency wallets being used by nearly all participants, will have wallets that also track specific cryptographic assets, NFTs that have an established price discovery and price. Respectful to the IDI mission and scope, these wallets will have 'value' complementary values associated to these assets.

Question #1: ***In addition to the broad categories of digital assets and related activities described above, are there any additional or alternative categories or subcategories that IDIs are engaged in or exploring?***

How this will integrate into the banking infrastructure, accounting and taxation will be pivotal when looking at the IDI's range of coverage:

From an architecture and design standpoint, most of the existing development and software specification related to cryptocurrencies is open source. Over the last 18 months, extensive development around ABCI (Application Blockchain Interfaces), the Web3 equivalent of an API have matured significantly. Many open-source specs now exist to import chain data, meta and state data have prewritten scripts and integration test already created. A banks decision to create their own hardware wallet infrastructure (cryptographic 2FA with Hardware layer ECA) or inherit a baseline from known good states will be at a bank-to-bank decision. Integration of other services such as 2nd layer transaction state, such as Polygon/Matic (SideChains) or Lighting Network (Bitcoin) will also play into the architecture decision making. Each of these are their own 'network', with the one caveat that the typical ICA (Interconnection Agreements) is completely permissionless, speeding up the time dependency significantly. This will allow a bank, accounting department or taxation departments to quickly gain access to important Know-Your-Customer/Anti-Money Laundering (KYC/AML) user referenced data to their on-chain activity through custom built interfaces, without the need to coordinate like typical data services.

Question #7: ***How are IDIs integrating these new technologies into their existing cybersecurity functions?***

Cryptocurrency specific Application Development and Legacy Fintech Application Rationalization are critical components to the integrated DevSecOps/Cybersecurity execution for IDIs. There are many cryptocurrencies, with interesting technical problems such as coin splits (network splits) resulting in new potential value, smart contracts that have potential no recourse withdraws, along with extensive cyber targeting of financial institutions that hold cryptocurrency accounts. The cybersecurity aspects need to be viewed from lessons learned from existing industry exchange participants. The unique architecture around multi-signature cryptography is to ensure there is no one single point of failure. These ideas are regularly implemented within the Department of Defense (DoD), to ensure there are multiple checks in place before execution of any major decision. When IDI's are integrating cryptocurrency nodes within their infrastructure, the associated application, reporting and business systems that have direct interaction with the cryptocurrency wallets should follow the leanest approach possible, as to expose potential errors/bugs into the accounts process. Where a centralized banking institution can create an accrual for a ledger mistake, if the same mistake is completed on cryptocurrency, or done as a malicious act, the consequences are immediate and may result in a full loss of the account. Conversely, from a cybersecurity footprint perspective, each single account is independently secured by a separate private key, from an architecture aspect, risk of access, the loss of funds from an entire range of accounts is significantly harder; unless funds are pooled into a single hot wallet or multi-factor signatures/process is not required to invoke cold wallets.