4.5 National Security Considerations

Return to Common Elements

Overview

Return to Top

> **Note:** See the OMG DIDO-RA Financial Laws, Regulations and Authorities for more on Security.

The following Laws and Regulations governing Privacy, Money Laundering, Terrorism, and Financials apply in the U.S. and need to be part of any DIDO solution concerned with currency, money, financials, or cryptocurrencies. Often these Laws and Regulations are considered obstacles or barriers to innovation, but each law or regulation is developed in response to some situation that occurred in the past. To prevent a “modern” repeat of these situations, the laws and regulations should be upgraded, not ignored or overturned.

Some of these Laws, Regulations, and Authorities have general applicability to DIDOs when the data stored within the DIDO refers to Personal Identifiable Information (PII) and therefore subject to the tenets of privacy. See Right to Privacy..

Some Laws, Regulations, and Authorities are relevant to DIDO when the DIDO is considered a Financial Instrument or a Security. Certain Cryptocurrencies and Initial Coin Offerings (ICOs) may be found to meet the definition of an “investment contract” under the Howey Test from which the U.S. Supreme Court ruling determined that an Investment Contract must:

1. Have an investment of money
2. Enter into a common enterprise
3. Have the expectation of profit
4. Be derived from the efforts of others

Details of National Security Considerations

Return to Top

Table 1 summarizes the number of Laws and Regulations covering National Security Considerations. The total number (i.e., **44**) indicates the complexity of National Security issues that confront the CBDC. The more Laws and Regulations, the more effort to coordinate the CBDC efforts and work with the Legislative and Executive Branches to keep the Laws and Regulations current with CBDC efforts.

Table 1: Summary of the number of laws and regulations covering National Security Considerations.

National Security Consideration	No. of Laws and Regulations
Human Trafficking	14
Drug Trafficking	9
Corruption	10
Money Laundering	11
Total	**44**

National Security Considerations are concerned with: Human Trafficking, Drug Trafficking, Corruption and Money Laundering. These are discussed in more detail in the following subsections:

this namespace doesn't exist: cbdc:private:cbdc_omg:04_doc:15_common:48_natsec

Examples

Return to Top

Table 2: Examples of **security** Desirements identified during the White Paper Analysis conducted by the OMG

Category	Desirements
Benefits	B0005, B0052, B0053
Policies and Considerations	P0005, P0024, P0028
Risks	
Design	D0013, D0016, D0017

Note: B = Benefit, **P** = Policy, **R** = Requirement, **D** = Design.

Discussion of Examples

Return to Top

The “desirements” specified in White Paper and identified by the OMG's White Paper Analysis as **Security Issues** are listed in Table 3.

Table 3: Security references of Desirements in the **White Paper**

Desirement No.	Desirement Text	Comment
B0005	**Protect against criminal activity**	| Criminal Activity is a broad, extensive topic that requires an understanding of the U.S. Laws and Regulations as well as international treaties and agreements. Within the context of the CBDC, criminal activity can be one more of the following: • Human Trafficking • Drug Trafficking • Corruption • Money Laundering
B0052	**Prevent Financial money laundering crimes**	There are already quite a few Laws and Regulations within the U.S. to cover Money Laundering. However, within the context of CBDC, these laws need to be reviewed, updated or amended to reflect Digital Currency and how it might be used in Criminal Activities.

Desirement No.	Desirement Text	Comment
B0053	**Provide resiliency to threats to existing payment services—including:** **1.** **operational disruptions** **2.** **cybersecurity risks**	**1. Operational Disruptions** occur when there is a failure in the infrastructure of the CBDC. This implies a compound Non-Functional Requirement that needs to be levied on the CBDC. The following **Non-Functional** requirements need to be specified for the CBDC: 1. Reliability ◦ Maturity ◦ Availability ◦ Fault Tolerance ◦ Recoverability 2. Maintainability ◦ Modularity ◦ Reusability ◦ Analyzability ◦ Modifiability ◦ Testability 3. Manageability ◦ Types of Manageability Functions ◦ Manageability Costs ◦ System Manageability Issues ◦ Software Manageability Issues **Note:** Although the OMG DIDO-RA provides general definitions for these non-functional requirements, only the Federal Reserve, in conjunction with the CBDC Stakeholders, can define these requirements in terms of the CBDC. This process takes time and there are no shortcuts. It is part of the System Engineering process. **2. Cybersecurity Risks**, as with **Operation Disruptions**, represent a compound non-functional requirement for the CBDC. The following Securability **Non-Functional** requirements need to be specified for the CBDC: • Confidentiality • Data Integrity • Non-repudiation • Authenticity • Accountability Securability is also a layered stack: Figure 1: The layers of Security. The layers of Security: 1. Physical Security 2. Data Security 3. Network Security 4. Platform Security 5. Application Security 6. Culture Security

<table>
<tr><th>Desirement No.</th><th>Desirement Text</th><th>Comment</th></tr>
<tr><td>P0005</td><td>Protect against criminal activity</td><td>See B0005.</td></tr>
<tr><td>P0024</td><td>CBDC would need to comply with the U.S. robust rules</td><td>
<table>
<tr><th>Criminal Activity</th><th>Approx. Number of Laws and Regulations</th></tr>
<tr><td>Human Trafficking</td><td>14</td></tr>
<tr><td>Drug Trafficking</td><td>9</td></tr>
<tr><td>Corruption</td><td>10</td></tr>
<tr><td>Money Laundering</td><td>11</td></tr>
<tr><td>Total</td><td>44</td></tr>
</table>
</td></tr>
<tr><td>P0028</td><td>Require significant international coordination to address issues such as:
1.
common standards
2.
infrastructure,
3.
the types of intermediaries able to access any new infrastructure,
4.
legal frameworks
5.
preventing illicit transactions
6.
the cost and timing of implementation</td><td>1. Common Standards: There are lots of “common standards” that can apply to Blockchains. See within each of these sections for a list of applicable standards:
•
DIDO RA - Technical Standard Bodies
•
DIDO RA - de facto Standards Bodies
Unfortunately, within the “blockchain” world, there is confusion about what constitutes a standard. Often, if something is Open Source, it is considered a standard. However, often these projects lack the rigor needed to be considered a “standard”. Also, see the discussion in the DIDO RA on Talk Openly Develop Openly (TODO) and look at the DIDO RA definition of a Standards Developing Organization (SDO).
2. Infrastructure: The CBDC Infrastructure needs to be considered Mission Critical since any loss of functionality could be considered as a threat to survival. This is why the desirements: B0053, D0015, D0016, D0017 are in the White paper.
3. Types of Intermediaries able to access any new infrastructure:
B0026 specifies bridges between legacy and new payment services and this will require new infrastructure.
D0012 specifies leveraging existing tools already in use by intermediaries
4. Legal Frameworks: There are already legal frameworks in place to handle:
•
National Privacy Considerations
•
National Security Considerations
Although these frameworks were developed without a CBDC, they already “comply with the United States are subject to robust rules” and are continuously being reviewed, updated, and amended based on new information obtained from the field. As part of this process, these frameworks need to add to the existing frameworks rather than created new frameworks.
5. Preventing Illicit Transactions: There are two areas within the existing legal frameworks covering Illicit transactions:
•
Money Laundering
•
Corruption
Although these frameworks were developed without a CBDC, they already “comply with the United States are subject to robust rules” and are continuously being reviewed, updated, and amended based on new information obtained from the field. As part of this process, these frameworks need to add to the existing frameworks rather than created new frameworks.
6. Cost and Timing of Implementation: The CBDC is a complex issue that, once released, could have a life expectancy of many, many years. Only through extensive Systems Analysis, Engineering, Design, and Testing will CBDC have the stability it needs to instill confidence in the public (B0020).</td></tr>
</table>

Desirement No.	Desirement Text	Comment
D0013	**Design should facilitate compliance with a robust set of rules already intended to combat** **1.** **money laundering** **2.** **the financing of terrorism** **3.** **customer due diligence** **4.** **record-keeping** **5.** **reporting requirements**	**1. Money Laundering:** There are roughly **11** Laws and Regulations in the U.S. covering 40_launder that have taken years to create, usually in response to known or discovered Money Laundering schemes that are continuing to evolve. In many ways, it is an *"Arms Race"*. The people with a need to launder money keep developing new ways around existing rules, requiring the government to create new rules. The CBDC must at least start from the same place as the existing systems with as many of the rules in place as possible in order to prevent the entire system from imploding. It also needs to assess the current sets of Laws and Regulations to determine if there are required updates or amendments that need to be made before the CBDC can "go live". **2. Financing of Terrorism:** The main way to finance terrorism is to engage in financial_crimes. There are four main areas of Financial Crimes used to fund terrorism: • Human Trafficking • Drug Trafficking • Corruption • Money Laundering The U.S. and much of the rest of the world have developed extensive systems of Laws and Regulations to combat these crimes and the design of the CBDC should use and leverage these existing systems rather than try to build something new. **3. Customer Due Diligence:** There are two main tools of the Anti-Money Laundering (AML): • Know Your Customer (KYC) • Customer Due Diligence Both of these are well understood and documented in the existing system by Intermediaries. Regardless of the Currency Model used for the CBDC (i.e., Digital Cash Model or Digital Account Model), it should embrace these existing sets of tools and adapt them as need be. **4. Record Keeping:** Under the US Patriot Act, Title III: Anti-money-laundering to prevent terrorism of 2001 Title III facilitates the prevention, detection, and prosecution of international money laundering and the financing of terrorism Second Subtitle attempts to improve communication between law enforcement agencies and financial institutions, as well as expanding **record-keeping** and **reporting requirements**. Also, under the definition of financial_crimes provided by the Federal Reserve, financial institutions must comply with a robust set of rules that are designed to combat Financial Crimes. These rules include Customer Due Diligence, record keeping, and reporting requirements. Therefore, the CBDC should rely on the existing Intermediaries to help provide well documented, tried and true Record Keeping. Blockchain Technology may help alleviate some of the record-keeping responsibilities, but the blocks must include enough information to support **record-keeping** and **reporting requirements**. **5. reporting requirements:** See number 6 above.
D0016	**Design should include offline capabilities to help with operational resilience of the payment system**	See the answer to q18.
D0017	**Design should include digital payments in areas suffering from large disruption, such as natural disasters**	See the answer to q18.

From:
https://www.omgwiki.org/CBDC/ - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:
https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:15_common:48_natsec:start&rev=1651947618

Last update: **2022/05/07 14:20**