

2.2 Issues

Return to Existing System

The following issues are associated with the existing Identity workflow:

1. In every activity where Nancy needs to interact with Technology there is a chance of becoming a victim of a [Phishing](#), [Malicious Software \(Malware\)](#) on her electronic devices, or a victim of a [Security Breach](#) or a [Data Breach](#) on any of the servers that store her data.
2. There is a chance of [Physical Security](#) breaches from pickpockets, muggers, or prying eyes.
3. As she is traveling, she needs to be far more cognizant of the situation around here and adopt a more enhance personal [CyberSecurity Culture \(CSC\)](#).
4. Identities used before and after the trip have long lifespans and can expose Nancy to [Identity Theft](#).
5. With the advent of [Multifactor Authentication \(MFA\)](#) that uses [Location Factor](#) and [Time Factor](#) there is an increased risk of not being able to gain access to her on-line resource, especially when those resources require the use of:
 1. [One-Time PIN \(OTP\)](#) that are generally sent to a mobile device
 2. [Smart Cards](#) found on credit cards, debt cards or employer id cards
 3. [Subscriber Identity Module \(SIM\)](#) card installed on her phone

From:
<https://www.omgwiki.org/dido/> - **DIDO Wiki**

Permanent link:
https://www.omgwiki.org/dido/doku.php?id=dido:public:s_cli:05_contents:02prt:identity:02_existing:05_issues&rev=1624583636

Last update: **2021/06/24 21:13**

