Public Comments for ICR 202311-1670-001

Author Full Name : Moti Gindi **Received Date :** 12/17/2023 10:21 AM

Comments Received :

Section III, clause 1

We suggest to expand clause 1 e) to cover the end to end control and governance processes for sensitive data, beyond encryption, as following (suggested changes marked in ***):

e) *** Maintaining a real time inventory of sensitive data - such as PII, PCI, PHI, credentials, API keys - available in source code and across all environments ***; Encrypting sensitive data, such as credentials - to the extent practicable and based on risk;

Rationale:
Encryption is one of the possible controls on sensitive data. But as hinted also in the suggested text, it may not always be feasible. We believe that maintaining an inventory of all sensitive data, even when not encrypted, is key for implementing realistic compensating controls for PO.5.2 and PS.3.1 in the SSDF Practices and Tasks (eg key rotation, validation, secure storage).