[redacted]

From: Peter Soraparu [redacted]
Date: Tuesday, July 26, 2022 at 4:17:44 PM UTC-4
Subject: Pre-Draft Comments from APF Technologies
To: 800-171comments@list.nist.gov <800-171comments@list.nist.gov>

Hello -

I'm pleased to attach our pre-draft comments on your planned updates to the Controlled Unclassified Information (CUI) series of publications.

If you would like to discuss our comments, we'd be happy to set a time for a meeting or a call with our team. In the meantime, we appreciate the opportunity to submit our comments on the CUI series.

Best regards,

Peter Soraparu
Managing Director, Strategic Communications
APF Technologies
[redacted]
Http://www.apftechnology.com
[redacted]

July 26 2022

Subject: Protecting Controlled Unclassified Information (CUI) (SP 800-171 v3)
Pre-Draft Comments from APF Technologies

As the result of recent advances in technology applications, we strongly suggest enhancing SP 800-171 v3 by adding a new target for access control (AC) and audit: each discrete file that contains CUI.

File level access control is the core principle of NSA's Zero Trust: Data-Centric Security Management, and ensures the safety of data in the event of network breaches or internal misuse. It is now commercially available.

Current file protection relies on access control (AC) of the user, device, application and service, a perimeter based approach that may be penetrated with "regularity" by NSA's reckoning. A device breach would lead to the loss of all data accessible through the device, which could be up to gigabytes or terabytes of data.

Also recognizing the limitations of cloud-based storage, CISA aims to continuously "encrypt all data" on all devices as the optimal mode for the data pillar in its Zero Trust Maturity Model.

File level access control enables many security features that are currently unavailable, and it greatly greatly curtails the loss of data in any circumstances. It could be one of the most significant advancements in cyber defense in years.

1. File level access control enables persistent encryption and seamless end-to end protection: at rest, in use and in transit, on any device at any time

    a. Access Control
        - File exfiltration by bad actors doesn't equal data loss
        - Every access by every user is evaluated in real time using dynamic access policies
        - Device privilege is no longer a factor to determine data access privilege
        - Granular access control uses data classification
        - User access to any file is prevented in real time when a situation warrants it

    b. Audit and accountability:
        - Complete access history logs are maintained for every file by every user
        - Detailed forensic tracing and auditing of a user's file access actions
        - Real time alerts are issued for atypical access patterns
        - AI driven access pattern analysis provides early warning on potential misuse

    c. Data life cycle management is driven by policies

2. Flow control of CUI becomes seamless and is applied to specific users or groups at recipient organizations

    - CUI remains encrypted the entire time
    - CUI owner retains control of access to CUI
    - Recipient organization's access to CUI can be revoked
    - Logs of detailed history by users at recipient organizations provide owners with full visibility
    - Accidental leaks of CUI are prevented if or when the CUI is sent to the wrong organizations

3. Separation of duties

    - Admin privileges or support functions to manage and access the files are no longer factors to determine access to CUI