From: Kate Johnson <Kate.Johnson@fairwarning.com>
Sent: Thursday, October 24, 2019 4:40 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Shane Whitlatch <Shane.Whitlatch@FairWarning.com>
Subject: NIST Privacy Framework: Preliminary Draft Comments - Feedback from FairWarning LLC

Thank you for the opportunity to provide feedback on this draft privacy framework. Attached please find feedback from FairWarning LLC.

Sincerely,

Kate

Kate Johnson

Senior Healthcare IT and Security Advisor

FairWarning, LLC

(727) 576-6700 x8921

Kate.Johnson@FairWarning.com

www.FairWarning.com

Trust but verify®

Feedback from FairWarning LLC to 'Preliminary Draft of the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk'

October 24, 2019

FairWarning commends NIST for their excellent work on the upcoming publication of this privacy framework. As the world becomes increasingly interconnected, it is imperative that people be protected from the harm of having their most sensitive data compromised.

General feedback on draft framework and its relationship to the current CSF – FairWarning advocates for a tight integration between the privacy and security frameworks. Data protection is, in essence, "a three legged stool" with privacy, cybersecurity and compliance holding integral and interdependent roles. We advocate for a layered approach with cybersecurity providing foundational safeguarding of data and systems, and privacy focused on user identity confidentiality and integrity. From those privacy and security controls, a "mapping out" to the variety of compliance regulations and laws for those controls can then occur.

Below are a few specific feedback points to the draft framework:

1. Protect-P, Develop and implement appropriate data processing safeguards. Identity Management, Authentication, and Access Control – FairWarning recommends this category to be explicitly extended to include auditing (aka accounting). Adding auditing effectively "closes the loop" to ensure the identity management, authentication, and access controls deployed are indeed working as intended. Moreover, having auditing capabilities to see who is accessing data can assist framework users to meet regulations mandating controls over ePHI and personal information dispersion.

2. The CIA (confidentiality – integrity – availability) triad is cited extensively in the framework documentation. That is wisely done as maintaining CIA is integral to both data security and safeguarding user identity and privacy. FairWarning recommends:

    a. In PR.AC-P for there to be entries added specifying the integrity of the user identity be protected (similar to the already present entry of Network integrity protection). If an individual identity and associated personal information are accidentally or maliciously altered, this will lead to privacy risk management problems as noted by NIST that may range from "dignity-type effects such as embarrassment or stigmas to more tangible harms such as discrimination, economic loss, or physical harm."
    b. In PR.DS-P for there to be entries added that specify the need for data access controls. These controls would bolster the CIA triad noted in this category by mitigating user or system account risk to the confidentiality of data (i.e., snooping and identity theft), integrity (unauthorized modification of record), and availability (i.e., introduction of ransomware into a system by a user with excessive privileges).

3. Control- P Data Management – FairWarning recommends for there to be entries added that encourage regular deletion and/or minimization reviews. Data intensive industries such as healthcare and financial services tend to "stockpile" data and retain information (personal and

otherwise) they no longer need or did not need in the first place. Privacy will be enhanced when entities commit to regularly reviewing and fully purging data they hold.

4. In implementing emerging technologies like artificial intelligence, it is imperative that entities be transparent (with themselves and with their customers) on why the technology is being adopted and how it is being used. To that end, FairWarning recommends that entries mandating ongoing transparency reviews be added under Identify – Risk Assessment. Currently, transparency is noted under Communicate-P only.