Federal Register Notice 88 FR 7999, Federal Register: Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan, March 3rd, 2023

Request for Information on the 2023 Federal Cybersecurity Research and Development Strategic Plan

Jennifer O'Connor

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

From: JENNIFER O'CONNOR [redacted]
Sent: Friday, March 3, 2023 1:46 PM
To: cybersecurity <cybersecurity@nitrd.gov>
Subject: Re: RFI Response: Federal Cybersecurity R&D Strategic Plan

Ironically, an article appeared in my feed this morning on an interesting privacy policy. If it was needed but inappropriate seems like there are cyber training gaps. Plus the US is far behind international privacy laws. Why put law enforcement in that position. Raise the bar fairly.

https://fcw.com/digital-government/2023/03/watchdog-secret-service-ice-failed-follow-federal-statutes-using-cell-phone-tracking-devices/383568/

On Thu, Mar 2, 2023 at 10:42 PM JENNIFER O'CONNOR [redacted] wrote:
Dear Mr. Vagoun,

Under item 1, there is an urgent need to train state and local law enforcement with regard to cyber and general privacy and security. The DC metro area is especially ripe for social engineering which when combined with dated cyber knowledge and skill sets means retirees and uninitiated are targets unaware of how easy it seems to be to gain control of a person's private information. Personal experience has found that local law enforcement does not have the resources to look for patterns of emerging threats to individuals, families and companies because reporting and review is on an incident by incident basis with evidence based physical threat driving risk assessment and thus victim outcomes.   Privacy violations are overwhelming and the current best source of info for retired non-cyber individuals is AARP magazine. It is the Wild West with regard to an individuals control of their data and what used to be difficult to do in terms of spoofing, etc can be Friday night chat for teenagers.

Open AI is going to make the problem worse rapidly as spoofing of legitimate official communications is automatible.

Best practices could immediately be updated and disseminated to level the proverbial playing field and aid citizens in forming 'verified communities' in real life as a check and balance on social media based identity. Further attention to the relationship of privacy loss, dignified help learning new cyber skills and mental health could actually make a difference in community building and turn the tide in identity and accompanying financial fraud.

Sincerely,
Jennifer O'Connor, PhD